جامعة الجيلالي اليابس. سيدي بلعباس

كلية الحقوق والعلوم السياسية

قسم الحقوق.

التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)

رسالة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية(القانون الخاص).

من إعداد:

بوحزمة نصيرة

تحت إشراف:

أ.د. معوان مصطفى

أعضاء لجنة المناقشة:

أ. د/ **بوسندة عباس**	أستاذ التعليم العالي	جامعة سيدي بلعباس	رئيساً
أ. د/ **معوان مصطفى**	أستاذ التعليم العالي	جامعة سيدي بلعباس	مشرفاً ومقرراً
د/ **بلباي إكرام**	أستاذة محاضرة"أ"	جامعة مستغانم	عضواً مناقشا
د/**بوربابة صورية**	أستاذة محاضرة"أ"	جامعة بشار	عضواً مناقشا

السنة الجامعية (2021-2022)

قال الله تعالى

﴿ وَلَقَدْ آتَيْنَا دَاوُودَ وَسُلَيْمَانَ عِلْمًا ۖ وَقَالَا الْحَمْدُ لِلَّهِ الَّذِي فَضَّلَنَا عَلَىٰ كَثِيرٍ مِّنْ عِبَادِهِ الْمُؤْمِنِينَ﴾

سورة النمل، الآية 15.

إهـــــداء

العائلة أولاً، ثمّ الأقربون قلبا.. ثمّ أصدقاء المواقف،

أهدي ثمرة نجاحي

إلى والداي المغفور لهما إن شاء الله من علماني أن الحب ليس له عمر وان العطاء ليس له حدود، إلى البنيان المرصوص إخوتي و أخواتي، إلى زوجي العزيز، إلى أبنائي قرة عيني، إلى صديقاتي وأصدقائي و كل من أحب.

شكر و عرفان

عن أبي هريرة رضي الله عنه أنّ النبي صلى الله عليه و سلم قال: "لا يشكر الله من لا يشكر الناس" فالحمد لله الذي أعطانا الصبر لإتمام هذا العمل العلمي المتواضع، وعليه أتوجه بجزيل الشكر و الامتنان إلى الأستاذ أ.د. معوان مصطفى لقبوله الإشراف على هذه الأطروحة والذي لم يبخل عليا بإرشاداته القيمة و توجيهاته لإثراء هذا العمل .

كما أشكر اللجنة الموقرة لقبولهم مناقشة هذه الأطروحة .

و لا أنسى بالشكر كل من قدم لي يد العون من قريب أو من بعيد في إنجاز هذا العمل.

قائمة المختصرات

أولا: باللغة العربية

ج.ر.ج.ج : الجريدة الرسمية للجمهورية الجزائرية.

ص: الصفحة.

ق.ت.ج: قانون تجاري جزائري.

ق.ع.ج.: قانون العقوبات الجزائري.

ق.ع.م: قانون العقوبات المصري.

ق.ع.ي: قانون العقوبات اليمني.

ق.ع.ف: قانون العقوبات الفرنسي.

ق.إ.ج.ج: قانون الإجراءات الجزائية الجزائري.

ق.إ.ج.م: قانون الإجراءات الجنائية المصري.

ق.إ.ج.ب: قانون الإجراءات الجنائية البحريني.

ق.إ.ج.ي: قانون الإجراءات الجزائية اليمني.

ق.إ.ج.ف: قانون الإجراءات الجنائية الفرنسي.

ثانيا: باللغة الأجنبية

Art : Articles.

E dit : Edition.

PUF : Presses universitaires de France.

L.G.D.j : la librairie general de droit et de jurisprudence.

N° : Numéro.

Op.cit : Ouvrage Précédent cité.

P : page.

C.P.F : Code pénal français.

C.P.P.F : Code procédure pénale français.

مقدمة

أضحت الثورة العلمية في مجال المعلومات و الاتصال حجر الزاوية في حياة الأفراد والدول حيث تعتمد جميع القطاعات في وقتنا الحالي بشكل أساسي على استخدام الأنظمة المعلوماتية، نظرا لما تتميز به من دقة وسرعة في تجميع المعلومات وتخزينها ومعالجتها ومن ثم نقلها وتبادلها، وعلى الرغم من المزايا الهائلة التي تقدمها هذه الأخيرة إلا أنه قد صاحبتها انعكاسات سلبية، حيث أن هناك أصحاب النفوس الضعيفة من يستغل التقنية الحديثة في مآرب غير مشروعة ما أدى إلى ظهور إجرام جديد يرتكب في فضاء إلكتروني يسمى الجريمة الإلكترونية، والتي تختلف في شكلها ومضمونها ووسائلها عن الجريمة بشكلها التقليدي، ويستمد هذا النوع المستحدث من الإجرام نشاطه من الإمكانات الهائلة للحاسب الآلي والبرامج، وتطور شبكة الإنترنت، والتطور الثقافي والعلمي في التعامل مع التكنولوجيا الحديثة بمختلف أنواعها. وتتعاظم المخاطر الناتجة عن الجرائم الإلكترونية لقدرتها الفائقة على التطور والانتشار وتخطيها للحدود الجغرافية، مستغلة في ذلك ما أتاحته شبكة الإنترنت من انفتاح معلوماتى على العالم بأسره .

وتزايدت مخاطر هذه الجريمة على المستوى الدولي والإقليمي والمحلى بسبب وجود قصور في التعامل مع هذه الجرائم ومواجهتها، وترجع أسباب القصور في التعامل مع الجرائم الإلكترونية إلى المعوقات التي يواجهها المحقق الجنائي، المنوط به كافة الإجراءات الأمنية والقانونية في التعامل مع هذه الجرائم، بدءاً من تلقى البلاغات حتى الضبط ومثول المتهم أمام العدالة لمحاكمته محاكمة عادلة ،لذا أصبح من الضروري إدراك رجال التحقيق القائمين على مكافحة الجرائم المعلوماتية للمفاهيم والأساليب القانونية لمكافحة هذه الجرائم، ومتابعة التغييرات التي طرأت على الجريمة عقب الدخول في عصر المعلوماتية، وما أضافته المعلوماتية من أبعاد جديدة في المجال الإجرامي.

كما أن التحقيق الجنائي هو عملية مكملة للقوانين الموضوعية والإجرائية، فمن وجهة قانون العقوبات والقوانين المكملة له، يساهم ويرشدنا إلى الطرق التي يمكننا بها استكمال وإثبات الأركان الواجب توافرها في كل جريمة تقع، ويساعدنا على الوصول إلى معرفة الوقائع التي تحدد وصفها القانوني، ويبين الوسائل التي تكشف بها الظروف المحيطة بكل جريمة ويكون من شأنها تشديد أو تخفيف العقوبة، ومن وجهة قانون الإجراءات الجزائية فإن عملية التحقيق الجنائي تثبت لنا كيفية القيام بإجراءات التحقيق في خطواتها المتعددة، و بشكل عام يعتمد على ذكاء المحقق وفطنته وقوة ملاحظته

وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق والبحث فيها ومتابعتها، والبحث في الأدلة والتنقيب عنها وصولا إلى إظهار الحقيقة.

لذا يجب دراسة ومتابعة رجال الشرطة للسلوك الإجرامي المعلوماتي، والتطور الذى لحق به إلى أن نال من حريات الأشخاص وهدد بياناتهم والمعلومات الخاصة بهم، ووضع حياتهم كاملة تحت التهديد والابتزاز والتشهير...إلخ. فمواجهة صور الجرائم المعلوماتية، تتطلب استنفار كافة الجهود، سواء داخل جهاز التحقيق، أو من خلال تعميق مفهوم التعاون المشترك الدولي والإقليمي والمحلي والمجتمعي والفردي، تحت المظلة الحكومية لتوفير الأمن والحماية اللازمة للمعلوماتية، وسد القصور التشريعى ودعم دور التعاون الدولي من خلال المنظمات والكيانات الدولية لمسايرة التقدم التكنولوجى على مستوى العالم أجمع.

ونظرا لحداثة هذا النوع من الجرائم كان من الصعب إدراجها من النصوص الجنائية التقليدية، فعملت النظم القانونية على إصدار تشريعات كفيلة بقمع هذا النوع من الجرائم، فكما صيغت نصوص جنائية موضوعية يمكن تطبيقها على هذا النوع المستحدث من الجرائم كذلك الشأن بخصوص النصوص الجنائية الإجرائية، حيث تم استحداث نصوص تتناسب وعملية البحث أمام سلطات باختلاف مستوياتها ومهامها، خاصة وأن أهم إشكال يعترض رجال التحقيق في الجريمة الالكترونية عندما تكون عابرة للحدود، كما عملت النظم القانونية على كيفية من الاستفادة من الكفاءات العلمية والتقنية في مجال التحقيق باعتماد نظام التدريب والتكوين لأن الحاجة كانت ملحة في مجال التحقيق في الجريمة الإلكترونية إلى إعداد مهارات فنية وعلمية و قانونية وإدارية، كما تم إنشاء هياكل مختصة بالجريمة الالكترونية مختصة، وتم انتقاء ذوي المواهب والقدرات التقنية للعمل فيها.

فعلى الرغم من التشابه الكبير بين التحقيق في الجريمة الإلكترونية وباقي الجرائم، حيث يعتمد بشأنها إجراءات تتشابه في عمومها، إلا أن الطابع الخاص بالجريمة الإلكترونية استدعى تطوير أساليب التحقيق الجنائي وإجراءاته بصورة تتلاءم مع خصائص الجريمة الالكترونية، بحيث تمكن المحقق من كشفها والتعرف على مرتكبيها.

فدوليا وضعت أول اتفاقية حول الإجرام المستحدث وهي اتفاقية بودابست[1]، والتي تضمنت مختلف أشكال الإجرام الإلكتروني، إضافة إلى الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] لسنة 2003[3].

كما تمكنت العديد من التشريعات من إرساء قواعد إجرائية تتوافق وطبيعة الجريمة الإلكترونية لمكافحتها، ذلك أن الجرائم التي تم الكشف عنها من طرف رجال التحقيق أقل بكثير من تلك التي لم يكتشف عنها الستار، ومرد ذلك يتمحور في معوقات إثبات هذا النوع من الجرائم والمتعلق أساسا بطبيعة الجريمة، لاختفاء آثارها وغياب الدليل المرئي فيها والذي يتطلب اكتشافه مهارة فائقة إلى جانب سهولة محو وتدمير الادلة التي تخلفها الجريمة الإلكترونية، إضافة إلى معوقات تتعلق بجهات التحقيق والمتعلقة أساسا بشخص المحقق من جهة، وبأساليب التحقيق من جهة أخرى، حاول من ضمنها المشرع الجزائري تعزيز المنظومة التشريعية الجزائية في مجال مكافحة الجريمة الإلكترونية، فإلى جانب تعديل قانون الإجراءات الإجراءات الجزائية[4]، ومن خلال القانون رقم 04/09، المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[5]، وتعديل قانون العقوبات في سنة 2015، أضاف مرسوما رئاسيا هو المرسوم الرئاسي رقم 20-05، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية[6]، لتشمل المنظومة مجلسا وطنيا لأمن الأنظمة المعلوماتية إلى جانب وكالة لأمن الأنظمة المعلوماتية، تتمحور جملة مهامهم في أمن الأنظمة المعلوماتية عموما ومواجهة الجريمة الإلكترونية

---

[1]- إتفاقية بودابست(الاتفاقية الأوروبية المتعلقة بالجرائم المعلوماتية) بتاريخ 2001/11/08، والتي وضعت للمصادقة في 2001/11/23.

[2]- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010.

[3]- صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 13 ذي القعدة عام 1435 الموافق 8 سبتمبر 2014، الجريدة الرسمية العدد 57، ص 4.

[4]- القانون رقم 06-22، المؤرخ في 20 ديسمبر 2006، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية العدد 84، المؤرخة في 24 ديسمبر 2006.

[5]- القانون رقم 09-04، المؤرخ في 14 شعبان عام 1430 هـ الموافق ل 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها والذي دخل حيز التنفيذ بموجب الجريدة الرسمية العدد 47، الصادرة بتاريخ 16 أوت 2009.

[6]- المرسوم الرئاسي رقم 20-05، المؤرخ في 20 جانفي 2020، المتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية، الجريدة الرسمية العدد 04، المؤرخة في 26 جانفي 2020، ص 5.

خصوصا، كإجراء تحقيق رقمي من طرف الوكالة في حالة وقوع هجمات إلكترونية على مؤسسات الدولة.

كما عزز المشرع الجزائري في سنة 2020 منظومة تشريعية جزائية في نفس الإطار وهو مكافحة الجريمة الإلكترونية بتعديل جديد لقانون العقوبات بموجب القانون 20-06، وأضاف إلى رصيده القانوني الهام، القانون رقم 20-05، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، حيث أنه جرم هذا السلوك إذا ارتكب باستعمال تكنولوجيا الإعلام والاتصال، من خلال المادة 31 منه الفقرة الأخيرة، إلى جانب الفصل السادس من القانون الذي خصصه للتعاون القضائي الدولي لمكافحة هذا النوع من الجرائم، ليثبت المشرع بذلك القضاء على كل السلوكات الجريحة الإلكترونية محاولا مكافحتها بشتى الطرق القانونية.

ومادام أن الجريمة الإلكترونية عابرة للحدود، الأمر الذي يجعل نتائجها والقضاء عليها من الأمور صعبة منال، وقد فرض البعد الدولي للجريمة الالكترونية على المجتمع الدولي كذلك البحث عن وسائل أكثر ملائمة لطبيعتها، وتضييق الثغرات القانونية التي برع مرتكبوها في استغلالها للتهرب من العقاب و لنشر نشاطهم في مناطق مختلفة.

فنظرا لصعوبة الوضعية التي يكون فيها رجال التحقيق في الجريمة الالكترونية خاصة عنما تتعدى الإقليم الوطني، تظهر أهمية هذا الموضوع إضافة إلى صعوبة إثبات هذا النوع من الجرائم لسرعة ودقة تنفيذها وإمكانية محو آثارها.

لذلك تعالت الأصوات لضرورة مكافحة الجريمة الإلكترونية، وتعددت السبل من بينها إنشاء جهات بحث وتحري مختصة تمتلك من الكفاءة التقنية والفنية ما يمكنها من التصدي لحداثة هذا النوع من الإجرام، حيث أنه يرتكب في فضاء إلكتروني يصعب البحث والتحري فيه إضافة إلى اعتبار الجريمة الالكترونية من الجرائم المعقدة على أساس أن نسرح الجريمة فيها لا حدود فيه.

وهو ما أشارت إليه اتفاقية بودابست للإجرام المعلوماتي، حيث نادت بضرورة إنشاء مثل هذه الأجهزة على المستوى الوطني وسن الإجراءات التشريعية اللازمة لذلك، حيث جاء في نص المادة 14 منها: "...يجب على كل طرف أن يتبنى من الإجراءات التشريعية أو اي إجراءات أخرى يرى أنها

ضرورية من أجل إنشاء السلطات ووضع الإجراءات المنصوص عليها في هذا القسم بغرض التقنيات أو الإجراءات الجنائية الخاصة...".

ورغم ذلك فأغلب الدول تمنح سلطة التحقيق في الجريمة الإلكترونية للقضاء العادي في شقه الجزائي، إلا أن القضاة فيه ليسوا مختصين في المجال تقني المعلوماتي ورغم أن القانون يتيح لهم الاستعانة بالخبرة إلا أنه لو أن من قام بالتحقيق من يملك الكفاءة التقنية لكان تحقيق العدالة من خلاله أحسن من الخبرة، لذلك اتجهت العديد من التشريعات المقارنة إلى إنشاء ضبطية مختصة بالجريمة الإلكترونية تختلف عن الضبطية العادية، ففي الولايات المتحدة الأمريكية أنشأت العديد من الوحدات المتخصصة في البحث والتحري عن الجريمة الإلكترونية ومن بينها المكتب المركز لمكافحة الجريمة المرتبطة بتكنولوجيا المعلومات والاتصالات، كذلك وحدة جرائم الإنترنت، أما في فرنسا فقام المشرع الفرنسي بموجب المرسوم 40/2000 بإنشاء المكتب المركزي لمكافحة الإجرام المتعلق بتكنولوجيا الإعلام والاتصال، والمتواجد على مستوى المديرية المركزية للشرطة القضائية، بينما في الجزائر فتم إنشاء جهات مختصة بالجريمة الإلكترونية على مستوى جهاز الشرطة والدرك، كما تم إنشاء هيئة وطنية مختصة بمكافحة جرائم تكنولوجيا الإعلام والاتصال.

ولأنه ما من دولة يمكنها التصدي للجريمة الإلكترونية وحدها كان لابد من التعاون والتنسيق مع غيرها، فكان من الضروري تعزيز التعاون الدولي في مجال تكوين رجال العدالة وتدريب الكوادر البشرية، حيث أن الدول تنادي صراحة بالتعاون بينها في مجال تبادل الخبرات وتدريب الكوادر.

من هنا تظهر أهمية دراسة موضوع التحقيق الجنائي في الجريمة الإلكترونية، باعتباره موضوع جدير بالاهتمام والرعاية ويتطلب التحيين في كل مرة خاصة مع تنامي وتزايد الوعي والإدراك الدولي بخطورة هذه الجريمة، التي أضحت تشكل صعوبة بالغة لأجهزة إنفاذ القانون، وخاصة أنظمة العدالة الجزائية في مجال المكافحة المقررة لها.

كما أن دراسة هذا الموضوع تكتسي أهمية بالغة نتيجة تزايد معدلات الجريمة المعلوماتية، بما يمثله ذلك من تهديد للأمن العام يعود بالسلب على الأنظمة الاقتصادية والاجتماعية للدول، وبالنظر إلى الطبيعة الخاصة لتلك الجرائم والمتمثلة في صعوبة إثباتها أو صعوبة التوصل إلى مرتكبيها بأدوات البحث الجنائي التقليدية، الأمر الذي استوجب على سلطات الضبط القضائي مسايرة هذه الأنماط من

الجرائم من خلال الاستعانة بالتقنيات العلمية الحديثة خلال مرحلة جمع الاستدلالات، مما يستدعي البحث المتعمق في المسائل الإجرائية والعملية المتصلة بتحقيق وإثبات جرائم المعلومات، لذا فإن هذه الدراسة تنصب على سبر غور المسائل القانونية والفنية ذات الصلة بسلطة مأمور الضبط القضائي في مواجهة الجريمة الإلكترونية.

ولرجال التحقيق تاريخ طويل في العمل الوطني، وهو ما تحرص عليه في إطار التمسك بقيم النزاهة والصدق والأمانة في مكافحة الظلم والفساد، وذلك من خلال عقيدة راسخة في نفوس جميع رجال التحقيق دفاعاً عن الحق، ومواجهة الخارجين على القانون بالحسم دون المساس بكرامتهم الإنسانية، ومن هنا تأتي أهمية دور جهاز التحقيق في حماية المجتمع من أخطار الجرائم المعلوماتية.

وتتجلى أهمية الدراسة أيضا في إشكالية الاختصاص القضائي لجهات التحقيق الجنائي من ناحيتين الأولى هي أن القاعدة العامة المطبقة في أغلب الدول فيما يتعلق بالاختصاص القضائي هي مبدأ الإقليمية، بمعنى أن القانون الجنائي يطبق على الجرائم التي تقع في تراب الدولة بغض النظر عن جنسية فاعلها أو مرتكبها، ومع هذا فإن تطور الإجرام وتوسعه إلى دول العالم تطلب وجود اتفاقيات دولية لتسليم المجرمين، غير أن غالبية الدول لا تسلم رعاياها وفقا لمبدأ السيادة من جهة، ومن جهة اخرى للتعارض مع مبدأ أساسي في القانون وهو عدم جواز محاكمة شخص عن فعل واحد أكثر من مرة، والثانية إضافة هي أن الجريمة الإلكترونية ترتكب في فضاء إلكتروني فهي غالبا ما تكون عابرة للحدود تثير إشكالية تنازع الاختصاص الدولي والإقليمي.

وتبدو أهمية البحث في أنه يخدم أسلوبا عمليا وقانونيا يبين كيفية التحقيق في الجرائم الإلكترونية التي تتم عبر أجهزة الكمبيوتر.

كما وتتضح الأهمية العملية للدراسة أن التحقيق في الجرائم الإلكترونية من أهم الإجراءات التي تتخذ في الدعوى، من ثم فإن المحقق يجب أن يتبصر لبعض الأمور وأن ينتبه لها أثناء التحقيق، من خلال التأكيد على ضرورة اكتسابه لمهارات فنية وتقنية مختلفة مع ضرورة الاستعانة بخبراء استشاريين في مجال جرائم الإلكترونية، حيث أنه لابد من توافر الخبرة والمهارات التقنية لكشف الأدلة الناتجة عن هذه الجرائم، وأيضا إلى لفت انتباه المعنيين والمسؤولين عن الأجهزة والتنظيمات والمؤسسات العلمية للمساهمة في مكافحتها والحد منها والتحذير من مخاطرها.

وعلى هذا الأساس سنحاول البحث عن معيار يتلاءم وطبيعة الجريمة الإلكترونية يسمح بمتابعة وملاحقة مرتكبي الجريمة الإلكترونية دون المساس بحقوق وحريات الأفراد التي تقرها المواثيق الدولية، ووجوب احترام مبدأ الشرعية لضمان عدم إفلات الجناة من المتابعة الجزائية، وتوقيع العقوبة المناسبة عليهم.

من هنا جاء اختياري هذا الموضوع بالدراسة في ضوء بعدين ذاتي وموضوعي، الأسباب الذاتية، ترجع خاصة في ظل زيادة الاهتمام الوطني و الدولي بالجرائم الإلكترونية و اعتبارها من الأحداث اليومية الواقعة في العديد من المناطق داخل الدول، مما يجعل الشعور بأهمية و ضرورة البحث في هذا الموضوع و الطموح العلمي الذي يدفع باتجاه تقصي الجديد في ميدان القانون الجنائي الإجرائي، والرغبة في المساهمة ولو بشكل محدود في إثراء النقاش القانوني في مثل هذه المواضيع، وهذا قد يرجع إلى وجود خلل في النظام الإجرائي السائد في الدول، وهو ما حملني لدراسة هذا الموضوع.

أما الأسباب الموضوعية فتمحورت حول الحداثة القانونية و التشريعية للإجراءات الخاصة في التحقيق الجنائي المعلوماتي، مما يدفع نحو البحث في مدى انسجام النصوص القانونية لهذه المنظومة مع المستجدات الراهنة في مجال المعاملات الإلكترونية، فضلا عن وسائل الحماية الإجرائية المعتمدة من قبل المشرع لمواجهة الجرائم الإلكترونية.

وتهدف الدراسة إلى تلمس طبيعة الجريمة الإلكترونية التي لا تبدوا في كثير من الحالات غامضة ومعقدة فحسب، بل تمثل تحديا هائلا يستدعي سرعة التأهب نحو نقلة علمية وتقنية ذاتية تحققها بالذات مجالات الضبط القضائي والقضاء والنيابة، وأيضا تحديد مفهوم هذه الجرائم وأنماطها وخصائصها، التي باتت تشكل أهم جرائم هذا العصر وأعقدها، خاصة في المجالات الأمنية لحماية المواقع الإلكترونية والبيانات الشخصية، ومنع الاعتداء على الأموال الإلكترونية وحماية التوقيع الإلكتروني، وحماية المستهلك الإلكتروني، وبل والاقتصاد الوطني وغيرها، ومن هنا فإن تطبيق البرامج التدريبية والأخذ بالتجارب الناجحة للتعامل مع الأدلة الجنائية ومواكبة مستجداتها هو المعول عليه للارتقاء بالتحقيق وكافة الإجراءات الإجرائية المطلوبة في هذه الجرائم، و تحقيق التوازن الفكري الإلكتروني للمحقق والباحث في الجرائم الإلكترونية وشبكات التقنية الإلكترونية الرقمية المعلوماتية الاجتماعية للحصول على الدليل الإلكتروني.

زيادة على ذلك، تهدف هذه الدراسة في محاولة الوصول إلى استراتيجية متكاملة على المستوى التشريعي والتقني والأمني لمكافحة الجرائم الإلكترونية، ببيان الأصول الإجرائية والعملية لإجراءات الاستدلال في البيئة الرقمية، وأساليب التحقيق الحديثة، ومعرفة كيفية استخلاص أدلة الإثبات التقنية في هذا النوع من الإجرام، إضافة إلى تفعيل التعاون القضائي الدولي للحد منها و ضبطها، وذلك في حدود اختصاصهم التي حددها لهم القانون الموضوعي والإجرائي والتعليمات التي تقررت في هذا الشأن إن وجدت.

لقد كان لهذا الموضوع دراسات سابقة تمثلت في دراسة وطنية أهمها مايلي: التحقيق الجنائي في الجرائم الإلكترونية لبراهيمي جمال وهو بحث مقدم لنيل شهادة الدكتوراه في العلوم، تخصص قانون، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو،2018/06/27.

كل ذلك يجعلنا نتساءل عن: **مدى فعالية الإجراءات القانونية التي تمكن أجهزة التحقيق في الكشف ومتابعة مرتكبي الجرائم الإلكترونية لمكافحتها في ظل متطلبات الشرعية الإجرائية، وهل المشرع الجزائري واكب التطورات الحاصلة في التشريعات المقارنة المتعلقة بالخصوصية التقنية للجرائم المتصلة بتكنولوجيا المعلوماتية ؟**

ورغم الأهمية الكبيرة التي يحضى بها الموضوع، قد واجهتنا بعض الصعوبات والعقبات من ناحية فإن بحث التحقيق الجنائي في الجريمة الإلكترونية يستلزم الوقوف على الأساليب الحديثة والمهارات المتقدمة في تحقيق الجريمة الإلكترونية، وهو ما يتسم بالدقة ويستلزم قدرا من التخصص، من جهة أخرى قلة الأحكام القضائية ذات العلاقة بالموضوع، فالقضايا التي تناولها القضاء و العقوبات التي أصدرت في حق الجانحين (الإلكترونيين) لم نستطع الحصول على نسخ منها من طرف موظفي المحكمة أو المجلس القضائي بحجة سرية العمل، وعدم المساس بشخصية المتهمين، بالإضافة إلى غياب الإحصائيات الدقيقة والمتخصصة في هذا المجال، إلا ما تم نشره للعامة من طرف الأجهزة المختصة .

قصد دراسة موضوع التحقيق الجنائي في الجريمة الإلكترونية، تم الاعتماد بالشكل الأولي على المنهج الوصفي تحليلي، وذلك بتسليط الضوء على النصوص القانونية الموضوعية والإجرائية التي تسري على هذه الجريمة وتحليلها، والوقوف على مدى فعاليتها في هذا الميدان، وكذا بيان أوجه النقص أو القصور في مجال هذا النوع من الإجرام، وكذلك التطرق إلى النصوص القانونية الواردة

في أهم الاتفاقيات المتعلقة بهذه الجريمة والأنشطة المرتكبة في إطارها، ومدى تقيد الدول بتكريسها في تشريعاتها الداخلية، والمصادقة عليها.

على كل حال فإن التحقيق الجنائي في الجرائم الإلكترونية هو غاية في حد ذاته فضلا عن أنها عملية مستمرة ومتطورة من أجل الحد منها، وبحثا عن أن أدلة الجريمة نفيا أو إثباتا.

وهذا كله إلى جانب المنهج المقارن، بغية الوصول إلى تحقيق الأهداف والغايات المتوخاة من هذه الدراسة، وذلك من خلال تسليط الضوء بمقارنة التحقيق الجنائي في الجرائم الإلكترونية، في بعض القوانين العربية والأجنبية، وبيان معالجتها للمشكلة في القوانين التقليدية والإلكترونية، ومدى اعتراف القضاء بذلك في الإثبات من جهة ومقارنة التشريعات الحديثة للتحقيق الجنائي في هذا النوع من الإجرام.

وتتوسع المقارنة بين القوانين الغربية كالقانون الفرنسي، والقوانين العربية كالقانون الأردني، إمارتي، اليمني والمصري مع التركيز على القانون الجزائري، وأهم الاتفاقيات الدولية كالاتفاقية الأوروبية بودابست سنة 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

و للإجابة عن هذه الإشكالية المطروحة وفق للمنهج المعتمد استلزم الأمر منا مناقشة الموضوع وفق خطة ثنائية في بابين:

الباب الأول: الأحكام الموضوعية للتحقيق الجنائي في الجرائم الإلكترونية

الباب الثاني: الأحكام الإجرائية للتحقيق الجنائي في الجرائم الإلكترونية

الباب الأول

الأحكام الموضوعية للتحقيق الجنائي في الجرائم الإلكترونية

إن التطور التكنولوجي في مجالات الحياة المختلفة أدى إلى دخول الإنسانية عصراً جديداً لم تألفه من قبل، بحيث انعكست نتائج استخدام تكنولوجيا المعلومات على المجتمعات الحديثة وأثرت تأثيرا كبيراً في سلوكات الإنسان.

غير أن هذا التطور نشأت ونمت عنه أنواع جديدة من الجرائم أطلق عليها بالجرائم الإلكترونية، هذه الأخيرة التي ما كانت لتبصر النور لولا ظهور الآلة التي اتفق على تسميتها بجهاز الكمبيوتر.

فالجرائم الإلكترونية تنوعت واتخذت مظاهر مختلفة بحيث أصبحت اليوم تطرح إشكالات خطيرة سواءاً على الصعيد الاقتصادي أو القانوني، مما يستدعي مراجعة شاملة للأحكام والنصوص القانونية، هذه المراجعة تظهر أن القوانين التقليدية قاصرة على تغطية هذه الجرائم، لأن تطبيق هذه القوانين يفترض وقوع الجرم على أموال مادية، في حين هذه الجرائم تقع على أموال معنوية لا تغطيها هذه القوانين.

ونشير في هذا المقام إلى أن هذه الجرائم الإلكترونية تتنوع وتتضاعف يوماً بعد يوم، كما أنها تتميز بخصائص وصفات لا تتوفر في الجرائم التقليدية من حيث أسلوبها وطريقة ارتكابها، ويختلف مرتكبوها عادةً عن المجرمين التقليديين لأنهم في الغالب أشخاص على مستوى عالٍ من العلم والمعرفة.

وقد ظهرت بظهور هذه الجرائم العديد من المشكلات منها ما يتعلق بالتحقيق، حيث أصبح المحققين يواجهون صعوبات عند ممارسة وظائفهم في إثبات هذه الجرائم الإلكترونية، من حيث التلاعب في الأدلة الإلكترونية وإخفائها، إلى جانب مدى حجيتها في الإثبات، ومن تم صعوبة تحديد فاعل الجريمة، وهو ما يتطلب مجهوداً إضافياً وتعاونا من الجهات ذات العلاقة لإثبات هذا النوع من الجرائم.

وقصد الإحاطة بالأحكام الموضوعية للتحقيق الجنائي في الجرائم الإلكترونية، تعين تقسيم هذا الباب إلى فصلين: الفصل الأول (ماهية الجريمة الإلكترونية موضوع التحقيق)، والفصل الثاني(ماهية التحقيق الجنائي في الجرائم الإلكترونية).

الفصل الأول: ماهية الجريمة الإلكترونية موضوع التحقيق

قبل الخوض في تفاصيل موضوع التحقيق الجنائي في الجرائم الإلكترونية، إرتأينا بأنه من الضروري أن نتعرف أولا في هذا الفصل من دراستنا على الجرائم الإلكترونية، بحيث نكون على قدر من المعرفة عنها باعتبارها صنفا مستحدثا من الجرائم التي تتحدى القواعد التقليدية للتجريم والعقاب طبقا لمبدأ شرعية الجرائم والعقوبات من جهة، و بإعتبارها موضوع التحقيق من جهة أخرى.

فالجريمة الإلكترونية هي جريمة ناتجة عن استخدام المعلوماتية المتمثلة في استخدام الكمبيوتر والانترنت في أعمال وأنشطة إجرامية ،عادة ما ترتكب بهدف أن تحقق عوائد مالية ضخمة جراء أعمال غير شرعية يعاد ضخها في الاقتصاد الدولي عبر شبكة الإنترنت باستخدام النقود الإلكترونية أو بطاقات السحب التي تحمل أرقاما سرية بالشراء عبر الإنترنت أو تداول الأسهم وممارسة الأنشطة التجارية عبر هذه الشبكة.[1]

مما يصعب حصرها وتعدادها نظرا لازديادها وتنوع أساليبها كلما ازداد العالم في استخدام شبكة الانترنت وازداد التعمق فيها، فهذه الجرائم تكلف الدول المتطورة كأمريكا المليارات من الدولارات سنويا، أي ما يعادل ميزانيات أغلب دول العالم الثالث تقريبا، بسبب عمليات القرصنة الإلكترونية من نسخ برامج أو أفلام أو بسبب هجمات تعطيل المواقع، ويمكن القول ببساطة أن الإنترنت ساحة إجرام مثالية تتحدى الأجهزة الأمنية والقضائية بثغرات قانونية ضخمة.[2]

ففي إطار التصدي للسلوكيات الإجرامية المستحدثة والمتمثلة في الجريمة الإلكترونية والتي تفطنت لها جل التشريعات العربية والغربية[3] واستحدث بها نصوصا، وحرص مجلس أوروبا على

---

[1]– عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترت (الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، 2007، ص 15.

[2]– عماد مجدي عبد الملك، جرائم الكمبيوتر والأنترنت، دار المطبوعات الجامعية، الإسكندرية، 2011، ص 27–28.

[3]– تعد دولة السويد الدولة الأولى التي سنت قانونا يتعلق بجرائم الكمبيوتر والأنترنت، حيث أصدرت قانون البيانات السويدي لعام 1973 الذي عالج قضايا النصب عن طريق الحاسب الآلي مثلا، وتبعت الولايات المتحدة الأمريكية السويد حيث شرعت قانونا خاصا بحماية أنظمة الحاسب الآلي (1976–1985)، وفي هذا الخصوص أيضا كان للسودان قانون مكافحة تقنية المعلومات سنة 2006، أيضا الإمارات العربية المتحدة من خلال القانون الاتحادي رقم 12 لسنة 2006. أنظر في هذا الصدد: شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005، ص110. أنظر أيضا: عزيزة رابحي، الأسرار المعلوماتية

التصدي للاستخدام غير المشروع للحاسبات وشبكات المعلومات، تجلى ذلك في اتفاقية بودابست الموقعة في 23 نوفمبر 2001 المتعلقة بالجرائم المعلوماتية، إيمانا من الدول الأعضاء في هذا المجلس والدول الأخرى الموقعة على هذه الإتفاقية بالتغيرات العميقة التي حدثت بسبب الرقمية والتقارب والعولمة المستمرة للشبكات المعلوماتية.[1]

وأمام ظهور هذا النوع من الجرائم والتي هي عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي أو الهواتف الذكية الموصولة بشبكة الأنترنت بطريقة مباشرة أو غير مباشرة لتنفيذ الفعل الإجرامي، أصبحت هذه الجرائم في الوقت الحالي تهدد أمن وسلامة الأفراد أوالمؤسسات أو حتى الحكومات، ما يقتضي التعرف على

ماهية هذا النوع من الإجرام باعتباره شكل جديد للجريمة المنظمة تنشأ في بيئة إفتراضية (المبحث الأول) ، و أساليب ارتكابها و دوافعها(المبحث الثاني).

المبحث الأول: مفهوم الجريمة الإلكترونية

نتج عن التطور التكنولوجي في مجال الحاسوب[2] والأنظمة المعلوماتية وأنظمة الاتصالات بما ذلك شبكة الإنترنت[3] مزايا في شتى مجالات الحياة المختلفة [1]، إلا أن ذلك التطور وتلك التقنية لم تسلم من الهجوم عليها فظهرت أنواع جديدة من الجرائم سميت بالجرائم الإلكترونية.

وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017-2018، ص 96. وأنظر أيضا: مليكة عطوي، الجريمة المعلوماتية، حوليات جامعة الجزائر، العدد 21، جوان 2012، ص 18-19.

[1]- عزيزة رابحي، المرجع نفسه، ص 96.

[2]- يعرف الحاسب لغة: بأن مصدره الفعل أو نحوه وعلم الحاسب هو علم الأعداد وهي من عدد والتدبير الدقيق، وتعني كلمة الحاسب بالإنجليزية Computer وقد تعددت الترجمات العربية لهذه الكلمة فأطلق عليها حاسوب، كما أطلق عليها العقل الإلكتروني، ثم أخيرا أطلق عليها الحاسب، وكلمة Computer يقابلها في اللغة الفرنسية Ordinateur أي ناظمة آلية، وقد صدر معجم الحاسبات عن مجمع اللغة العربية سنة 1987 بدون إضافة كلمة إلكترونية أو آلية إلى كلمة الحاسبات. أنظر: أحمد خليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2000، ص 25.

[3]- تعرف الإنترنت بأنها الشبكة الدولية للمعلومات والتي اصطلح على تسميتها بالإنترنيت وهي عبارة عن شبكة من أجهزة الحاسوب متصلة ببعضها البعض عن طريق مزود الخدمة والخادم " السيرفر" في جميع الدول، فالحاسوب الذي لم يرتبط بمزود الخدمة لا يمكن أن يتصل بالشبكة الدولية للمعلومات، ولا يستفيد من خدمات الإنترنيت، كما أن الجرائم

فالبحث في الجريمة الإلكترونية شأنه في ذلك شأن أي بحث في فرع من فروع المعرفة، لابد من بيان مفهومه من خلال تعريف سماته الأساسية لكي يتم رسم الصورة العامة لهذا البناء المعرفي، لذا يقتضي تقسيم هذا المبحث إلى ثلاث مطالب، يتناول الأول تعريف الجريمة الإلكترونية، أما الثاني فيهتم بخصائص الجريمة الإلكترونية وأطرافها، أما الثالث فنخصصه لمحل الجريمة الإلكترونية.

المطلب الأول: تعريف الجريمة الإلكترونية

إن ظاهرة الجريمة الإلكترونية بالرغم من اختلاف تسميتها و دلالتها يبقى تعريفها عموما في نطاق القانون الجنائي العام بأنها سلوك الفرد عملا كان أو امتناعا يواجهه المجتمع بتطبيق عقوبة جزائية، وذلك بسبب الاضطرابات التي يحدثه في النظام الاجتماعي[2]، وهو التعريف الذي يستند على عناصر الجريمة إلى جانب بيانه لأثرها (السلوك، والسلوك غير المشروع وفق القانون، الإرادة الجنائية وأثرها العقوبة أو التعبير الذي يفرضه القانون) وهي الأوصاف التي تتميز بين الجريمة عموما، وبين الأفعال المستهجنة في نطاق الأخلاق أو الجرائم المدنية أو التأديبية.

أما فيما يخص الجريمة الإلكترونية فلا يوجد تعريف مجمع عليه وذلك لغياب تعريف قانوني لها عند جل التشريعات[3]، إلا أن الفقه الجنائي قد بذل من أجل ذلك عدة محاولات لتعريف هذه الجريمة،

الإلكترونية لا تتم إلا عن طريق هذه الشبكة. أنظر: خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، دار الثقافة، عمان، 2011، ص 50-51.

[1]- ظهرت سمات عدة في مجال تكنولوجيا المعلومات سواءا على الفرد أو المؤسسة أو الدولة، فعلى سبيل المثال، التليفون التقليدي الذي كان يقتصر دوره على تبادل الصوت البشري، قد أصبح الآن يتبادل كميات هائلة من البيانات التي يمكن أن تحتوي على أصوات ونصوص وأنغام موسيقية وأفلام وصور، وهذا التبادل لم يعد يحدث فقط بين البشر، ولكنه أصبح يحدث أيضا بين البشر وأجهزة الحاسب، كذلك يكفي أن يتم إدخال البيانات إلى شبكة معينة من خلال عنوان المرسل إليه حتى تصبح متوافرة لأي شخص يريد الدخول إليها، كما أن الاستخدام العام للبريد الإلكتروني ووصول الجمهور لمواقع الويب عبر الأنترنت من أمثلة هذا التطور. أنظر: هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003، ص 30-31.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي، الطبعة الثالثة، دار هـــومة، 2006، ص 03.

[3]- إن الخلاف حول تعريف الجريمة الإلكترونية جعل بعض الدول تفضل عدم وضع تعريف لها تحسبا للتطور العلمي والتقني المستمر، ولعدم حصر قاعدة التجريم في نطاق أفعال معينة قد تتغير أو تتبدل في المستقبل، واكتفت في قوانين متعاقبة بتجريم أفعالها بعد أن تصنفها تبعا لأهدافها، في حين هناك مشرعين في دول أخرى أتو على تعريف صريح لها كالمشرع الجزائري من خلال المادة 1/2 من القانون 04/09، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة

لكنه لم يتفق على إيراد تسمية موحدة لها، فبينما استعمل البعض اسم الجرائم الإلكترونية، أطلق البعض الآخر اسم جرائم الحاسب الآلي والأنترنت أو الجرائم المتصلة بالكمبيوتر وجرائم تكنولوجيا المعلومات، في حين هناك من فضل تسمية جرائم المعلوماتية، وهناك من وجد في تسمية جرائم إساءة استخدام تكنولوجيا المعلومات والإتصال أكثر دلالة ومواكبة للتطور الذي يشهده عالم الإعلام والإتصال، وهذا المسمى استخدم في مشروع القانون العربي النموذجي الموحد الصادر عن جامعة الدول العربية سنة 2004، والذي اعتمده مجلس وزراء العدل العرب في الدورة التاسعة عشر بالقرار رقم 495-19 بتاريخ 2003/10/08.[1]

وتسمية الجريمة الإلكترونية راجع إلى كون التقنية الإلكترونية والحاسب الآلي أحد عناصرها، كما أن الفعل الإجرامي يستخدم التقنية الإلكترونية الرقمية من حاسب آلي إلى رقمي أو إحدى شبكات المعلومات كوسيلة تنفيذ الغرض من الجريمة.[2]

وعليه من يتصدى لتعريف الجريمة الإلكترونية يتناول تعريفها بالاستناد إلى وسيلة ارتكابها (الفرع الأول)، أو بالاستناد إلى موضوعها(الفرع الثاني)، أو على أساس المعرفة الفنية باستخدام الحاسوب(الفرع الثالث)، وقد يستند البعض الآخر على أكثر من معيار لتعريف هذه الجريمة (الفرع الرابع).

الفرع الأول: تعريف الجريمة الإلكترونية بالاستناد إلى وسيلة ارتكابها

يستند أنصار هذا الاتجاه في تعريفه للجريمة الإلكترونية على وسيلة ارتكابها، فيشترطون وجوبها بواسطة الكمبيوتر، لذلك عرفها الفقيه **تايديمان Tiédemen** بأنها: " كل أشكال السلوك غير

بتكنولوجيا الإعلام والإتصال، المؤرخ في 14 شعبان 1430 هـ الموافق ل05 أوت 2009 والذي دخل حيز النفاذ بموجب الجريدة الرسمية العدد 47، الصادرة بتاريخ 16 أوت 2009.

[1]- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنيت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007، ص35. وأنظر أيضا: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2008، ص112.

[2]- مصطفى محمد موسى، المرجع نفسه، ص 113.

المشروع (أو الضار بالمجتمع) الذي يرتكب باستخدام الحاسب الآلي[1]"، أو هي " كل جريمة تتم في محيط الحاسبات الآلية"[2].

كما عرفها **توم فوريستر** في مؤلفه عن قصة تقنية المعلومات تعريفا يكاد يكون مطابقا للتعريف السابق بقوله " أنها فعل إجرامي يتم باستخدام الحاسوب كأداة رئيسية".[3]

وعرفت أيضا بأنها " الجرائم التي قد وقع في مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسوب، وبعبارة أخرى هي تلك الجرائم التي يكون دور الحاسوب فيها إيجابيا أكثر منه سلبيا".[4]

كما جاء في تعريف آخر" أنها الفعل الإجرامي الذي يستخدم في اقترافه الحاسب الآلي كأداة رئيسية".[5]

وقد ميز الفقهاء بين مظهرين للسلوك الإجرامي في الجرائم الإلكترونية، حيث يكون استخدام الحاسب الآلي إما من أجل ارتكاب جريمة أخرى بغرض الحصول على مكسب مادي، أو أن يكون الغرض من الإعتداء هو إلحاق الضرر بالمجني عليه[6].

ولقد اعتمد نظام مكافحة جرائم المعلوماتية السعودي لسنة 2007 هذا الاتجاه إذ عرفها "أي فعل يرتكب متضمن استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام[7].

غير أنه يؤخذ على هذه التعريفات التي أوردها أنصار هذا الاتجاه ، بأنه لا ينبغي تجريم السلوك بناءا على الوسيلة ، فقد اعتمد هؤلاء معيارا فيه توسع كبير لنطاق الجريمة الالكترونية، مثل سرقة الحاسب الآلي أو أحد مكوناته المادية تبقى جرائم تقليدية ، أو الجرائم التي يستعمل فيها الحاسب لطباعة مستند ما أو تزوير محرر تبقى كذلك جرائم تقليدية لا تدخل ضمن نطاق الجرائم الإلكترونية هذا من جهة .

---

[1]- TIEDEMAN (klaus), Frande et autre délits d'affaires commis à t'aide d'ordinateur électroniques,rev, Dr, Pén, crime and the lawcrim n 7, Bruxelles, 1984, P 61.

[2]- Roden(Adrian), computer crime and the law , CLT .1991. VOL 15, P. 399.

3- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2004، ص15.

4 - TATTY (Richard) and hard castle (Antony) , computer- Related Crime in informations technology and the law, Macmilla publishers, UK, 1986 ,P 26.

5- هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص13.

6 - Ball (Leslie D) computer Crime in the information technology revolution, combridge 1985, P 543.

7- المادة الأولى الفقرة الثامنة من نظام مكافحة جرائم المعلوماتية السعودي ،2007 .

من جهة أخرى تعريف الجريمة الإلكترونية يقوم في الأساس على العمل الرئيسي المكون لها وليس فقط على الوسائل المستخدمة فيها، لأنه لا يمكن أن يطلق على جريمة ما أنها جرائم الحاسب الآلي لمجرد أن الحاسب قد استخدم في ارتكابها [1].

كما أن الوسيلة لم تكن موضوع اعتبار لدى المشرع الجزائي عند التجريم، فالوسائل أغلبها متساوية، والتكوين القانوني للجريمة وتوافر أركانها مجتمعة هو موضوع الاعتبار عند انطباق نص التجريم [2].

الفرع الثاني : تعريف الجريمة الإلكترونية بالاستناد إلى موضوعها

يستند أصحاب هذا الاتجاه في تعريفهم للجريمة الإلكترونية إلى وجوب أن يكون الكمبيوتر هو محل الجريمة، فيجب أن يتم الاعتداء على الحاسب الآلي أو على نظامه ، حيث يضيق أنصار هذا الاتجاه من نطاق الجرائم الإلكترونية ويحصرونها في الحالات التي تكون الحاسب محلا للجريمة، كأن يتم سرقة أو تقليد أو إتلاف أو تعطيل برنامج الحاسوب أو إفشاء محتوياته أو حذف أو تغيير أو تزوير أو نسخ المعلومات المعالجة ويمثل هذا الاتجاه الفقيه **روزنبلات** Rosenblat الذي عرف الجريمة الإلكترونية بأنها "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تحول عن طريقه"[3].

وعرفت هذه الجريمة أيضا بأنها "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو نقلها ".[4]

1- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنيت في القانون العربي النموذجي، المرجع السابق ، ص 25. أنظر أيضا :

Michel, D Rostoker and Robert H ; Rimes, computer jurisprudence, leyelresponses to the information revolution, ocona publication, mc,1986, P 333.

2- محمود أحمد عبابنة، المرجع السابق ، ص 18.

3- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011، ص 20.

4- وضع هذا التعريف مجموعة من خبراء منظمة التعاون الاقتصادي والتنمية في اجتماعها في باريس سنة 1983 ضمن حلقة الإجرام المرتبط بتقنية المعلومات.

في حين أشارت الدكتورة هدى قشقوش إلى أن جرائم الحاسب الآلي هي: " مجموعة الجرائم التي تتصل بالمعلوماتية ،حيث حصرت هذه الجرائم في الاعتداء على الأموال المعلوماتية "، التي هي عبارة عن الأدوات المكونة للحاسب الآلي وبرامجه ومعداته ، حيث أننا نكون بصدد جرائم معلوماتية [1]حينما تكون المكونات غير المادية للنظام من بيانات وبرامج مخزنة في ذاكرة الحاسب أو المنقولة عبر شبكة الاتصال، قد تعرضت لاعتداء بسرقة أو التزوير أو ادعاء ملكيتها أو تقليدها أو إتلافها أو تعطيلها .

غير أن هناك من يرى بأن هذا المعيار المعتمد عليه لتعريف الجريمة الإلكترونية أدى إلى إيراد تعريفات عامة ومطلقة ، لا تحدد الأفعال المتصلة بجرائم الكمبيوتر بصورة دقيقة ، ذلك لأن الأخذ به يؤدي إلى اعتبار بعض الأفعال من جرائم الكمبيوتر، مع أنها ليست كذلك في حقيقة الأمر، كإتلاف البيانات قبل معالجتها [2]، بالإضافة إلى عدم وجود اتفاق حتى الساعة على الأفعال المعنوية تحت وصف جرائم الكمبيوتر، كما أن هذه التعريفات لا تستند في الحقيقة إلى موضوع الجريمة بالمعنى القانوني، الذي هو محل الاعتداء فركزت على أنماط السلوك الإجرامي وأبرزتها متصلة بالموضوع لا الموضوع ذاته .

الفرع الثالث : تعريف الجريمة الإلكترونية بالاستناد إلى المعرفة الفنية باستخدام الحاسوب

هنالك اتجاه فقهي آخر لا يهتم بالوسيلة أو موضوع الجريمة الإلكترونية، و إنما يعرفها بوصفها مرتبطة بالمعرفة الفنية أو التقنية باستخدام الحاسب الآلي بمعنى آخر إن أنصار هذا الاتجاه يستندون إلى معيار شخصي يستوجب أن يكون الفاعل ملما بتقنية المعلومات واستخدام الحاسب الآلي من بينهم **ديفيد تومبو David thompson** الذي عرف هذا النوع من الجرائم بقوله أنها: " أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسب. "[3]

1- يـطلق كذلك على الجريمة الإلكترونية بالجريمة المعلوماتية في كل من القانون الفرنسي والسعودي وهو ما سار عليه فقهاء القانون المصري.

2- محمود أحمد عبابنة، المرجع السابق، ص 18.

3 -Thompson (David), currrent trends in computer control crime, computer quarterly, vol 9 N 1, 1991, P 2.

أيضا الفقيه **ستين سكيولبيرج Stien Schiolobero** الذي عرفها بأنها: " أي فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه والتحقيق فيه وملاحقته قضائيا. "[1]

كما عرفت الجريمة الإلكترونية بالقول أنها: " واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب."[2]

ويؤخذ على هذا الاتجاه أنه يضيّق على نحو كبير من نطاق الجريمة الإلكترونية لأنه وبحسب رأي المنتقدين له يحصر الجريمة في نطاق معرفة فنية كبيرة لمرتكبها وهذا يمكن وقوعه في حالات ما وليس في جميع الحالات إذ يرتكب الجاني[3] الجريمة الإلكترونية دون الحاجة إلى قدر كبير من المعرفة والخبرة الفنية[4]، كعملية إتلاف البيانات المخزنة مثلا فتعتبر من الأفعال غير المشروعة لا تتطلب مهارة وقدر من العلم والمعرفة لارتكابها .

كما يلاحظ أن هذه الجرائم وفي كثير من الأحيان ترتكب من قبل مجموعات تتوزع أدوارهم بين التخطيط والتنفيذ والتحضير والمساهمة ، وقد لا تتوفر في بعضهم المعرفة بتقنية المعلومات والتي يطرح بشأنها التساؤل التالي : ماهي معايير تحديد المعرفة التقنية للقول بارتكاب الجريمة ؟ خاصة وأن الحياة المعاصرة ومساعي المتعاملين الناشطين في الميدان تسعى من أجل نشر منتجاتها وتحقيق الأرباح إلى تبسيط وسائل المعالجة وتبادل المعطيات ، وتحويل الجهاز المعقد إلى جهاز بسيط يمكن كل من يجهل علوم الكمبيوتر استخدام ، فلا تشترط إذن المعرفة بتقنية المعلومات ليتمكن شخص بسيط من إرسال مئات بل آلاف الرسائل الإلكترونية دفعة واحدة إلى أحد المواقع لتعطيل عملها، يرتكبها كذلك شخص معنوي[5]، مما يدفع إلى التساؤل عن مدى مسؤولية الشخص المعنوي عن الجرائم

1- محمود أحمد عبابنة، المرجع السابق ، ص16.

2- سامي جلال فقي حسين، المرجع السابق، ص 21.

3- يتجه الباحثون إلى الإقرار بأن أفضل تصنيف لمجرمي التقنية هو التصنيف القائم على أساس أغراض الاعتداء ويعد من أفضل التصنيفات لمجرمي التقنية الذي أورده David Icove Vonstouch , Paul Sergret Wiliam، تصنيف مجرمي المعلوماتية إلى ثلاث طوائف: المخترقون ، المحترفون والحادقون. أنظر في هذا الصدد: نسرين عبد الحميد نبيه ، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف. الإسكندرية، 2008، ص40.

4- سامي جلال فقي حسين، المرجع السابق، ص 22.

5- الأشخاص المعنوية هي عبارة عن مجموعة من الأموال والأشخاص التي ترمي لتحقيق غرض معين فيمنحها القانون الشخصية القانونية بالقدر اللازم لتحقيق هذا الغرض. أنظر: صمودي سليم، المسؤولية الجزائية للشخص

التي ترتكب في البيئة الإلكترونية ؟ في هذا الصدد يمكن القول أن تقرير مبدأ المسؤولية الجزائية للشخص المعنوي[1] في نطاق الجرائم الإلكترونية هو ما نص عليه المشرع الجزائري في المادة 394 مكرر 04 ق. ع. ج والتي تنص على ما يلي : "يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل كمرات الحد الأقصى للغرامة المقررة للشخص الطبيعي".

إلى جانب المشرع الجزائري نجد أن المشرع الفرنسي يقرر بدوره مسؤولية الشخص المعنوي في مجال المعالجة الآلية للمعطيات، وذلك بموجب المادة 323-6 ق.ع. ف، والتي تنص على ما يلي: "يمكن أن يحكم على الأشخاص المعنوية بالمسؤولية الجزائية وفقا للشروط المحددة في المادة 121-2 ....".

وعليه يمكن القول بأن المشرع الجزائري وفقا لما سبق أقر المسؤولية الجزائية للشخص المعنوي ، وقد عنون الباب المخصص لها ب "**العقوبات المطبقة على الأشخاص المعنوية** " ، وقد عددت المادة 18 مكرر ق.ع.ج مجموعة من العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح كما يلي :

1- الغرامة التي تساوي مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة .

2- واحدة أو أكثر من العقوبات التكميلية الآتية :

- حل الشخص المعنوي .
- غلق المسؤولية أو فرع من فروعها لمدة لا تتجاوز 5 سنوات .
- الإقصاء من الصفقات العمومية لمدة لا تتجاوز خمس سنوات .
- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة لا تتجاوز 5 سنوات .

المعنوي، دار الهدى الجزائر، 2006، ص 06 . وانظر أيضا :عجة الجيلالي، مدخل للعلوم القانونية ، الجزء الثاني، برقي للنشر، بدون سنة النشر، ص 187.

1- استثنى المشرع الجزائري الأشخاص المعنوية العامة من الخضوع للمسؤولية الجزائية بنص المادة 51 مكرر ق.ع.ج.

- مصادرة الشيء الذي استعمل في ارتكاب الجريمة أو نتج عنها .
- نشر وتعليق حكم الإدانة .
- الوضع تحت التصرف لمدة لا تتجاوز 5 سنوات ، وتنصب الحراسة على ممارسة النشاط الذي أدى إلى جريمة أو الذي ارتكبت الجريمة بمناسبته .

ومما تجدر الإشارة إليه في هذا المقام أن هذه العقوبات ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية فحسب ، بل توقع على كل الجرائم التي يرتكبها الشخص المعنوي وإن كانت الغرامة وفق المادة 394 مكرر 04 هي ذات حد واحد ، حيث أوجبت الأخذ بالحد الأقصى لهذه العقوبة وهو 5 مرات فيما يتعلق بالجرائم الإلكترونية.

أما فيما يخص المشرع الفرنسي ، فتشمل العقوبات المقررة للشخص المعنوي طبقا لنص المادة 323 –6 ق.ع .ف فيما يلي :

1– الغرامة البالغة خمس أضعاف ما يفرض على الشخص الطبيعي بموجب القانون الذي يعاقب على الجريمة المادة 131 – 38 ق.ع. ف .

2– إذا نص القانون على جناية أو جنحة يسأل عنها الشخص المعنوي فإنه يمكن أن يعاقب بعقوبة أو أكثر من العقوبات الواردة في المادة 131 – 39 ق.ع.ف ومنها :

- المنع من مزاولة نشاط أو عدة أنشطة مهنية أو اجتماعية بشكل مباشر أو غير مباشر، نهائيا أو لمدة 5 سنوات أو أكثر .
- الإغلاق بصفة نهائية أو لمدة 5 سنوات أو أكثر المحلات أو واحدة أو أكثر من مؤسسات المشروع التي استخدمت في ارتكاب الوقائع الإجرامية .
- الإقصاء من الصفقات العمومية بصفة نهائية أو لمدة تتجاوز خمس سنوات .
- الوضع 5 سنوات أو أكثر تحت الحراسة القضائية .
- مصادرة الأشياء التي استخدمت أو كان من شأنها أن تستخدم في ارتكاب الجريمة .
- نشر أو تعليق حكم الإدانة .

3– المنع المحدد في المادة (131 – 39) فقرة (2) بالنسبة لنشاط المهني الذي وقعت الجريمة بمناسبته .

وهذه العقوبات في القانونين الجزائري والفرنسي ليست خاصة بجرائم الاعتداء على نظم المعالجة الآلية كما سبق القول، وإنما يمكن أن توقع على كل الجرائم التي يرتكبها الشخص المعنوي .

الفرع الرابع: التعريف المستند إلى معايير مختلفة ومتنوعة

لقد اختلف هذا الاتجاه في المعايير المتبناة لتعريف الجريمة الإلكترونية بعيدا عن المعايير السابقة منها التعريف الذي أورده الجزاء البلجيكيون في معرض الإجابة عن الاستبيان الذي أجرته منظمة التعاون الاقتصادي والتنمية حول الغش المعلوماتي[1]، في اجتماع عقد بباريس عام 1982 حيث تم تعريف الجريمة الإلكترونية:

" كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية"[2].

في حين يذهب الفقيه الفرنسي **ماسي Massé** إلى أن المقصود بالجريمة الإلكترونية "الاعتقادات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[3] وعلى نفس المنوال جاء تعريف الخبير الأمريكي **دون باركر Doneparker**، حيث قال بأنها "فعل إجرامي أيا كانت صلته بتقنية المعلومات فيه يتكبد المجني عليه نتيجة له خسارة ويحقق الفاعل ربحا بصفة عمدية"[4].

ويرى الأستاذ باكر كذلك أن الجريمة الإلكترونية الخالصة تنطوي على ست خطوات أساسية، يتم تنفيذها آلياً بواسطة برامج او عدّة برامج ، دون تدخل العنصر البشري ويمكن تحديد هذه الخطوات في مايلي[5]:

1- يعرف بعض الفقه الغش المعلوماتي بأنه " مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة العقاب" أنظر في هذا الصدد: ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة والوراقة الوطنية، مراكش، 2011، ص 10.

2- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2006 ، ص 42.

3-Masse (Michel) infactioncontre pordre financier, rev , sc , crim, janvier1985 N1 , p 107.

4-Parker (Done B), Fighting computer crime « A new fram work for protecting information , john wiley and son , 1998,p 112.

5 - محمد عبد الله أبو بكر سلامة ، جرائم الكمبيوتر والأنترنيت ، المكتب العربي الحديث، الإسكندرية، 2007، ص 14-15.

1. البحث عن نظام الحاسب الآلي الذي يحتوي على المعلومات أو البرامج المستهدفة.
2. الوصول إلى نقاط الضعف في النظّام الذي يحتوي على هذه المعلومات أو البرامج.
3. الاستفادة من هذه النقاط للدخول إلى النظام ثم التحكم فيه.
4. تنفيذ السلوك الإجرامي الذي تم التخطيط له وتحديده مسبقا.
5. تحويل هذا السلوك إلى ربح غير مشروع يحصل عليه الجاني، أو إلى خسارة تلحق بالمجني عليه.
6. إخفاء جميع الأدلة تجنبا لكشف الفاعل وسلوكه الإجرامي.

كما عرفت الجريمة الإلكترونية بأنها " عمل أو امتناع يأتيه الإنسان إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، التي يحميها قانون العقوبات ويفرض له عقابا"[1].

وهذا التعريف يمتاز بالسمات التالية :

1- يحتوي على كل صور الإعتداء الإيجابية أو السلبية التي تقع إضرارا بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصّة به، باعتبارها من المصالح والقيم المتطورة التي تمتد مظلة قانون العقوبات لحمايتها.

2- يتضمن الأثر الجنائي المترتب على العمل أو الامتناع غير المشروعين، ويمثل في الجزاء الجنائي بكافة صوره وأنواعه، وهو أشكال التعبير عن معنى الالتزام في القاعدة القانونية[2].

3- أنه يحافظ على الشريعة الجنائية وتعني أنّه لا جريمة ولا عقوبة إلاّ بنص إذ لا يمكن أن يوجه أي اتهام ضد الشخص لارتكابه فعلا معيّنا مالم يكن منصوص على تحريم هذا الفعل في القانون [3].

---

1 – هلالي عبد اللاه أحمد ، التزام الشاهد بالإعلام، المرجع السابق، ص14.

2 – نعني بخاصية الالتزام جبر الأفراد وإكراههم على احترام القاعدة القانونية تحت طائلة فرض الجزاء عليهم عند مخالفتهم لهذه القواعد، وهنا يقصد بالجزاء القوة المادية التي تمتلكها الدولة لقمع المخالفين للقانون أو لجبرهم على إصلاح الضرر وأداء تعويض عند الاقتضاء. أنظر: عجّة الجيلالي، مدخل للعلوم القانونية، الجزء الأول، برقي للنشر،الجزائر، 2009، ص56.

3 – أنظر في هذا الصدد المادة الأولى من ق.ع. ج.

غير أنّ هذا الاتجاه لم يسلم من النقد ، فبخصوص تعريف **دون باكر** فإن الربح لا يتحصل عليه دائما من هذه الجرائم كإتلاف المعطيات مثلا كذلك قد لا يكون عمديا إذ قد يحصل بطريقة غير مباشرة ، وقد لا يحصل الربح أبدا .

وعليه يمكن القول بأن الغرض من ارتكاب الجرائم الإلكترونية ليس هو دوما تحقيق الربح المادي لأن هناك دوافع كثيرة تحفز الجُناة على هذا السلوك الإجرامي، بمعنى آخر العائد المادي ليس بالضرورة هو الدافع للقيام بالاعتداء[1].

أما بخصوص تعريف خبراء البلجيك والذي أعتبر من البعض من أفضل التعريفات لشموليته بجملة من العناصر والخصوصيات التي ضمتها الجريمة الإلكترونية ، ولم تتناولها التعريفات السابقة ، إلا أن شمولية التعريف انتقدت على أساس إدراجها للأموال المادية في حين أن هذا النوع من الأموال محمي بموجب نصوص قانون العقوبات، وبالتالي فهي ليست بحاجة إلى قانون جديد [2].

ويرى أستاذ يونس عرب أنه وجب التفرقة بين الظاهرة الجُرمية والجريمة ، فظاهرة جرائم الكمبيوتر والتي نعني بها الجرائم الإلكترونية تعرف بأنها الأفعال غير مشروعة المرتبطة بنظم الحواسيب .

أما تعريف جريمة الكمبيوتر فإنها: "سلوك غير مشروع معاقب عليه قانونا صادر عن إرادة جرمية محله معطيات الكمبيوتر ".

فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل ، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجُرمية، ومعاقب عليها قانوناً لأن إصباغ الصفة الجُرمية لا يتحقق في ميدان القانون الجنائي إلا بإرادة المشرّع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للأخلاق ، ومحل جريمة الكمبيوتر هو دائما معطياته بدلالتها الواسعة ، بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة ، البرامج بأنواعها، المعلومات المستخرجة ، والمتبادلة بين النظر، وأما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزواج بين تقنية الحوسبة والاتصال بما في ذلك شبكات المعلومات .

1- سوف نرى ذلك بالتفصيل عند تطرقنا لدوافع ارتكاب الجريمة الإلكترونية في المطلب الثاني من المبحث الثاني من الفصل الأول من الباب الأول.

2 – محمود أحمد عبابنة، المرجع السابق ، ص19.

وفقا لكل ما سبق يمكن تعريف الجريمة الإلكترونية بأنها كل فعل أو امتناع من شأنه الاعتداء على الأموال المعنوية **(معطيات الحاسب)** يكون ناتجا بطريقة مباشرة وغير مباشرة لتدخل التقنية المعلوماتية.

والعلة في اختيار هذا التعريف يرجع إلى استناد هذا التعريف إلى أكثر من معيار لتحديد ماهية الجرائم الإلكترونية ، فالمعيار الأول تمثل في إيراد تعريف للسلوك المكون للواقعة الإجرامية والذي يجب أن يكون بصورة فعل ينهي عنه القانون أو امتناع عن فعل يأمر به القانون، أما المعيار الثاني فتمثل في طبيعة المحل أو موضوع الاعتداء **(الأموال المعنوية)** والمعيار الثالث هو اتصال السلوك بمحل الاعتداء عن طريق تدخل التقنية المعلوماتية، فهذا التعريف جاء شاملا لعدة معايير مجتمعة ، وبالتالي يعد تعريفا مطلوبا ولو إلى حين لأن هذه الجرائم في تطور مستمر الأمر الذي قد يؤدي إلى تصور مختلف غلى هذه الوقائع غير المشروعة .

أما عن موقف المشرع الجزائري من تعريف الجريمة الإلكترونية، فقد أطلق مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[1]، وتبنى في ذلك التعريف الذي جاءت به الاتفاقية الدولية للإجرام المعلوماتي، و بموجب أحكام المادة 02 من القانون 09- 04 [2] وعرفها على أنها :" جرائم

1- إن المشرع الجزائري لم يجد تجديدا من تعديل العقوبات لسد الفراغ القانوني في هذا المجال ،وكان ذلك بموجب قانون رقم 04 /15 المؤرخ في 2004/11/10 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات والذي أقر له القسم السابع مكرر منه تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات ، وجاء في عرض أسباب هذا التعديل أن التقدم التكنولوجي وانتشار وسائل الاتصال الحديثة أدى إلى بروز أشكال جديدة للإجرام ، مما دفع بالكثير من الدول إلى النص على معاقبتها، وأن الجرائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وبالتالي من شأن هذه التعديلات أن تستبد هذا الفراغ القانوني، ورأى المشروع الجزائري أن جوهر المعلوماتية هو المعطيات التي تدخل إلى الحاسب الآلي وتحول إلى معلومات بعد معالجتها وتخزينها، فقام بحماية هذه المعطيات من أوجه عدة .

2- القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، السابق الذكر.

المساس بأنظمة المعالجة الآلية للمعطيات[1] المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية . "

وبهذا يكون المشرع الجزائري تبنى تعريفا موسعا للجرائم الإلكترونية، واعتبر أنها تشمل بالإضافة إلى جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات من المادة 394 مكرر إلى المادة 394 مكرر 07 أي جريمة أخرى ترتكب أو يسهل ارتكابها بواسطة منظومة معلوماتية أو نظام للاتصالات الإلكترونية، وعليه لم يعد مفهوم الجريمة الإلكترونية في التشريع الجزائري يقتصر على الأفعال التي تكون فيها المنظومة المعلوماتية محلا للاعتداء بل توسع نطاقها لتشمل كذلك الأفعال التي تكون المنظومة المعلوماتية وسيلة لارتكابها[2].

يتضح مما سبق ذكره أن المشرع الجزائري قد اعتمد على الجمع بين عدة معايير لتعريف الجريمة الإلكترونية، أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكتروني، وثانيها معيار موضوع الجريمة والمتمثل في المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات، كما اعتمد على معيار رابع في تحيد نطاق الجريمة المعلوماتية وذلك من خلال إقراره بأن هذه الجريمة ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه وهو ما يوسع نطاق مجال الجرائم الإلكترونية في القانون الجزائري.

أمـــا المشرع الفرنسي فلـم يضع تعريفا شاملا وواضحا للجريمة الإلكترونية بل تولى هذه المهمة رجال الفقه.

المطلب الثاني : خصائص الجريمة الإلكترونية وأطرافها

إن محاولة ضبط خصائص الجريمة الإلكترونية ، والتي لم يعد أثرها يقتصر على النطاق الوطني بل تعداه بكثير إلى النطاق الدولي ، نتيجة لثورة التقنية العالية وتطور وسائل الاتصال وسهولتها بين

1- نظام المعالجة الآلية للمعطيات هو عبارة عن آلية وإجراءات منظمة تسمح بتجميع وتصنيف وفرز البيانات ومعالجتها ومن ثم تحويلها إلى معلومات يسترجعها الإنسان عند الحاجة ليتمكن من إنجاز عمل أو القيام بأية وظيفة عن طريق المعرفة التي يحصل عليها من المعلومات المستخرجة من النظام.

2- أول نص قانوني في مجال جرائم المعلوماتية (جرائم المساس بأنظمة المعالجة الآلية للمعطيات) ظهر في فرنسا سنة 1988. أنظر في هذا الصدد:

ANDRE (Lucas), JEAN (Dev rêve),JEAN(Frayssinet),Droit de T'informatique et de L'internet, édition Dallol, collection thémis (droit privé),France, 2001,P679.

دول العالم ، يسهل عمل المشرع ويمكنه من صياغة النصوص التشريعية الملائمة لمكافحة هذا النوع من الإجرام .

ونظرا لأن الجريمة الإلكترونية تتميز بطبيعة خاصة تميزها عن غيرها من الجرائم التقليدية لارتباطها بجهاز الحاسب الآلي وما يتميز به من تقنية عالية ، فقد أضفت هذه الحقيقة على الجريمة الإلكترونية عدد من السمات والحقائق التي انعكست بدورها على مرتكب هذه الجريمة الذي أصبح يعرف بالمجرم المعلوماتي، أي الجاني ولابد من وجود من يقع عليه الفعل وهو المجني عليه، أي أن الجريمة الإلكترونية كغيرها من الجرائم تحتاج إلى طرفين جاني ومجني عليه، إلا أن أطرافها يختلفون نوعا ما عن أطراف باقي الجرائم وعليه فجوهر البحث بهذا الصدد ينص على مصدر وجود الأفعال وتوجيهها ، ومما لاشك فيه أن الشخص الطبيعي هو الذي يهيئ فرصة استغلال الوسيلة المعلوماتية، ولكن هل يعد كذلك أيضا حين ترتبط شبكة المعلومات عموما بين حواسيب متعددة، يبدوا أن الأمر يختلف بعض الشيء فالمؤسسات العامة والبنوك وغيرها التي تحمل صفة الشخص المعنوي معرضة هي أيضا لاعتداءات عن طريق هذه الشبكة من المعلومات، فعلى الرغم من وسائل الحماية المتعددة إلا أنه ثبت عدم فعاليتها أمام قرصنة[1] شبكة المعلومات.

وأمام تعدد وتنوع أنماط هذه الجرائم وازدياد مخاطرها على أمن الدول سواء المتقدمة أو النامية وسواءا على مستوى الدولي أو الوطني، وكذلك على الأفراد، أصبحت تخترق خصوصياته وكذلك أمواله وتهدد حياته، نظرا لما تنفرد به من خصوصيات تميزها عن نظيرتها من بينها خصوصية مرتكبها الذي يعرف بالمجرم الإلكتروني وما يتمتع به من سمات لا مثيل لها لدى المجرم التقليدي.

لهذا سنحاول فيما يلي التطرق إلى خصائص الجريمة الإلكترونية في (الفرع الأول) وأطرافها في (الفرع الثاني).

1- تعرف القرصنة الإلكترونية: " بأنها عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الأنترنت غالبا لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب ، ويقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب وطرق إدارتها أي أنهم مبرمجون ذو ومستوى عال يستطيعون بواسطة برامج مساعدة اختراق حاسوب معين التعرف على محتوياته ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة ." أنظر : عماد مجدي عبد المالك، المرجع السابق ، ص 84.

الفرع الأول: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بسمات خاصة تميزها عن غيرها من الجرائم التقليدية وتمنحها طابعا خاصا نظرا لوقوعها في غالبية الأحيان في بيئة المعالجة الآلية للبيانات حيث تكون المعلومات محل الاعتداء[1]، ووقوع هذه الجريمة في بيئة المعالجة الآلية للبيانات يستلزم التعامل مع بيانات مجمعة ومجهزة لدخول الحاسب بغرض معالجتها إلكترونيا، بما يمكن المستخدم من إمكانية كتابتها في الحاسب الذي يتوفر فيه إمكانيات تصحيحها وتعديلها ومحوها وتخزينها واسترجاعها وطباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم، ولا بد من فهم الجاني لها، كما تكون أيضا البرامج محلا للاعتداء أو تستخدم وسيلة للاعتداء [2].

ولعل أبرز هذه الخصائص التي أثرت بشكل مباشر على التشريعات العقابية والإجرائية التقليدية القائمة ما يلي:

أولا: الجريمة الإلكترونية من الجرائم العابرة للحدود

عندما يكون الفعل أو الامتناع الذي يأتيه الإنسان بواسطة نظام معلوماتي معين اعتداء على حق أو مصلحة أو بيانات معلوماتية يحميها القانون أو إضرارا بالمكونات المنطقية للحاسوب أو بنظم الشبكات المتصلة به ماسّا بحدود أكثر من دولة نكون أمام جريمة عابرة للحدود[3] .

فأهم ما يميز الجريمة الإلكترونية، هي تخطيها للحدود الجغرافية، ومن تم اكتسابها طبيعة دولية ، أو كما يطلق عليها البعض أنها جرائم ذات طبيعة متعدية الحدود الآلية المتوزعة في مختلف دول العالم عبر شبكة المعلومات.

1- تعرف المعلومة كمحل للاعتداء بأنها: " مجموعة من البيانات التي قد تمت معالجتها وتحليلها وتلخيصها وتجريبها لتحقيق الأهداف المرجوة منها واستخدامها في المجالات المختلفة أي أنها البيانات المجهزة في شكل منظم ومفيد بتسلسل منطقي. " أنظر:

-Kenneth l'Auden, Jane l'Auden, " Manegement Information System – managing the digital firm ", Seventh édition , prentice bhall , inc,new jersey , USA , 2004 .P8 .

2- فتوح الشادلي، عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون- دراسة مقارنة-، منشورات الحلبي الحقوقية ، بيروت، لبنان، 2003 ، ص 34.

3- سامي جلال فقي حسين، المرجع سابق، ص 27.

فيمكن في بضع دقائق نقل كم هائل من المعطيات بين حاسب وآخر يبعد عنه آلاف الكيلومترات، كما يمكن أن تقع الجريمة من جان في دولة معينة على مجني عليه في دولة أخرى في وقت يسير جدا[1]، فالسرعة الهائلة التي يتم من خلالها تنفيذ الجريمة الإلكترونية وحجم المعلومات والأموال المستهدفة، والمسافة التي تفصل الجاني عن هذه المعلومات والأموال قد ميزت الجريمة الإلكترونية عن الجريمة التقليدية بصورة كبيرة .

ومن القضايا التي لفتت النظر إلى البعد الدولي للجرائم الإلكترونية، قضية عرفت باسم مرض نقص المناعة المكتسبة (**الإيدز**)، وتتلخص وقاعها عام 1989 في قيام أحد الأشخاص بتوزيع عدد كبير من النسخ بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أن هذا البرنامج في حقيقته كان يحتوي على فيروس (**حصان طروادة**) .[2]

وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلي عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يقوم الفاعل خلالها بطلب مبلغ مالي يرسل على عنوان حتى يتمكن المجني عليه من الحصول على مضاد للفيروس، وفي الثالث من فبراير سنة 1990 تم إلقاء القبض على المتهم (**جوزيف بوب**) في ولاية (**أوهايو**) بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب لتسليمه لها لمحاكمته أمام القضاء الانجليزي، حيث أن إرسال قد تم من داخل المملكة المتحدة ، وبالفعل وافق القضاء الأمريكي على تسليم المتهم وتم توجيه له إحدى عشر تهمة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات المتهم لم تستمر بسبب حالته العقلية فهذه القضية تتلخص أهميتها من

1- محمد خليفة، الحماية الجنائية المعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر، الاسكندرية، 2007 ، ص 37.

2- الفيروسات بصفة عامة عبارة عن برامج مشفرة مصّممة بقدرة على التكاثر و الانتشار من نظام إلى آخر إمّا بواسطة قرص ممغنط أو عبر شبكة الاتصالات، بحيث يمكنه أن ينتقل عبر الحدود من أي مكان إلى أخر في العالم، ومن أبرز الأمثلة المعرفة بحصان طروده ، مبرمج يعرف باسم Bakoufice ، الذي يصفه أحد خبراء الحاسوب الأمريكيان بأنه يمكن أن يدمر الكاميرا=

= التي يملكها، ويمكنه أن يفتح جهاز الميكرفون الخاص بك كما يمكنه أن ينسخ ملفاتك و أن ينقل كل ما يراه و يسمعه و يقرأه و يعيد إرساله.

ناحيتين : الناحية **الأولى** كونها المرة الأولى التي يتم فيها تسليم متهم في جريمة إلكترونية ، أما **الثانية** فهي المرة الأولى أيضا التي يتقدم فيها شخص فيها للمحاكمة بتهمة إعداد برنامج خبيث (فيروس)[1].

كذلك من الأمثلة على أن هذه الجرائم عابرة للحدود، أنه تمكن أحد الهواة في أوروبا من حل شفرة أحد مراكز المعلومات في البنتاجون (وزارة الدفاع الأمريكية)، ومن تم أصبح المجال أمامه مفتوحا للعبث ببيانات هذا المركز، وكذلك الحال عليه في إنتاج الفيروسات[2].

وعليه يمكن القول مما سبق ذكره أن الجريمة الإلكترونية تتميز بالتباعد الجغرافي بين الجاني والمجني عليه، ومن الوجهة التقنية التباعد بين أداة الجريمة ومحلها، وهذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة أو خارجها ليطال دولة أخرى يتواجد فيها نظام الحاسوب المحزّنة فيه المعلومات محل الاعتداء.

فالطبيعة الدولية لهذه الجرائم تشير العديد من الإشكالات القانونية كمشكلة السيادة أو الاختصاص القضائي[3]، ومسألة جمع الأدلة وقبولها في دولة ما أمام قضاء دولة أخرى [4]، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية وغيرها من المشاكل التي يمكن أن يثيرها الجرائم العابرة للحدود بشكل عام.

---

[1]-Glough(Brayn) and mango (Paul),approaching Zero :data crime and criminal under world,1992,P 136-146.

[2]- محمود أحمد عبابنة، المرجع السابق، ص 34.

1- نذكر في هذا المجال قضية (R.V Thompson) والتي تتخصص وقائعها في قيام مبرمج إنجليزي يعمل وبأحد البنوك في دولة الكويت بالتلاعب في معطيات نظام الحاسب الآلي الخاص بالبنك وذلك عن طريقة الخصم من أرصدة العملاء ثم إيداعها في حسابه الخاص، وبعد عودته إلى انجلترا طلب من البنك تحويل الحساب الخاص به إلى عدة حسابات بنكية في انجلترا وهو ما قام به البنك فعلا وقدم للمحاكمة أمام القضاء الانجليزي بتهمة الحصول على أموال الغير بطريق الاحتيال وحكم عليه بعقوبة السجن ، إلاّ أنه طعن في الحكم استنادا إلى عدم اختصاص القضاء الانجليزي لأن فعل السجن والإيداع كانا في الكويت وليس انجلترا، مشار إلى هذه القضية لدى محمد خليفة ، المرجع السابق، ص 37.

2- في هذا الصدد تنص المادة 15 من القانون رقم 04/09 على ما يلي :" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة خارج الإقليم الوطني، عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

لذلك بات من الضروري إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة الالكترونية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم بمعنى أن مكافحة هذه الجريمة تتطلب تعاونا كثيفا بين الدول وتوافقا كبيرا بين تشريعاتها، فيجب أن يشمل هذا التعاون تبادل المعلومات، تسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخرى والوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الاتفاقيات الدولية[1].

غير أن الوصول إلى إبرام هذه الاتفاقيات، كالاتفاقيات الخاصة بتسليم أو تبادل المجرمين يقتضي التنسيق بين قوانين الدول المختلفة لضمان تحقيق ما يسمى "مبدأ ازدواجية التجريم "، إلا أنها تقف أمام هذا المبدأ عقبات تحول دون تحققه لأن هناك العديد من القوانين لم يتم تعديلها حتى تتلاءم مع هذه الجرائم حتى يتسنى إدراجها ضمن الاتفاقيات الدولية الخاصة بتبادل المساعدة الجنائية في هذا النوع من الإجرام ألا وهو الجريمة الالكترونية.

والجدير بالذكر أن المشرع الجزائري في هذا الصدد خطى خطوة إلى الأمام، حيث نص في القانون رقم 04/09 على بعض القواعد الإجرائية الخاصة بالتفتيش والحجز في مجال هذه الجرائم، كما أنشأ المشرع هيئة وطنية للوقاية من الإجرام المتصل بتكنولوجيا الإعلام والاتصال ومكافحته وسنّ أحكام خاصة بالتعاون والمساعدة القضائية الدولية ناهيك عن القانون رقم 15/04 المعدل والمتمم للأمر 156/66 المتضمن قانون العقوبات والذي استحدث بموجبه أحكاما خاصة بالجرائم الماسة بالأنظمة المعلوماتية في المواد 394 مكرر إلى 394 مكرر7 .

ثانيا: الجريمة الإلكترونية تتطلب لارتكابها وجود كمبيوتر ومعرفة تقنية باستخدامه

لا يختلف إثنان في أنه يلزم لارتكاب الجريمة الإلكترونية الاستعانة بالكمبيوتر[2] (الحاسب الآلي) كوسيلة لتنفيذ هذه الجريمة، وما تجدر الإشارة إليه أن الكمبيوتر وإن كان موضوعا للاعتداء،

3- يمكن القول أنه لا غنى عن الاتفاقيات الدولية في مجال مكافحة هذه الجريمة وحتى المشرع الجزائري علق التعاون القضائي الدولي في مجال مكافحة الجرائم المتصلة تكنولوجيا الإعلام والاتصال على شرط احترام الاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل .

2- يقصد بالكمبيوتر: كل جهاز إلكتروني يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي لتنفيذ عمليات إدخال Data (impute)أو إخراج معلومات (information out put)، وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج Out put (devices) أو التخزين، والبيانات يتم إدخالها بواسطة مشغل الكمبيوتر (Opérator) عن طريق

كإتلاف أو سرقة الجهاز نفسه أو شاشة ، فلا تثور لدينا أية مشكلة ، وذلك لأن قانون العقوبات كفيل بردع الجاني، كون أن الحاسب لا يتعدى كونه من الأموال المادية المنقولة [1].

غير أن الإشكال يثور عندما يطال الاعتداء ما يمكن أن يسمى بفن الكمبيوتر ، كتدمير برامجه أو سرقتها أو تقليدها أو العبث ببيانات أو معلومات مخزنة، وبالتالي يطرح إشكال عن مدى انطباق النصوص القانونية عليها نظرا لصعوبة تحديد ما إذا كانت هذه الأموال مادية منقولة أم لها طابعا خاصا، والذي يهمنا هنا هو أن الكمبيوتر كوسيلة يعتبر من المتطلبات الرئيسية لارتكاب الجريمة الإلكترونية حتى تعتبر كذلك إضافة إلى ذلك فإن هذه الجريمة تتطلب إلماما كافيا بمهارات ومعارف فنية ، كالمعرفة التقنية بالكمبيوتر وكيفية تشغيله واستخدامه، ذلك أن مقترفي هذه الجريمة هم من المتخصصين في معالجة المعلومات آليا[2].

فالجاني في الجريمة الإلكترونية قد يكون شخصا طبيعيا يعمل لحسابه ،ويهدف إلى تحقيق مصلحة خاصة من وراء الجريمة التي يرتكبها ضد أحد نضم المعالجة الآلية للبيانات والمعلومات، أو عن طريق الاستعانة بها، ولكن يحدث كثيرا أن يقترف الشخص الطبيعي الفعل المؤثم جنائيا ليس لحسابه الخاص، وإنما لحساب أحد الأشخاص المعنوية كشركة عامة أو خاصة تقدم على السطو على أحد أنظمة المعلوماتية أو تحدث ضررا للغير عن طريق اللجوء لأحد نظم المعالجة الآلية للمعلومات.

وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية، وبعد معالجة البيانات تتم كتابتها على أجهزة الإخراج وهو يتكون من كيانين كيان مادي (hard ware) يضم الأجهزة المادية المختلفة والتي تشمل وحدات الإدخال والإخراج ووحدات التشغيل المركزية، وكيان معنوي (soft ware) يشمل على البرمجيات الجاهزة والبيانات والمعلومات المنطقية .

1 – يعتبر مصطلح المنقول من المصطلحات الشائعة في قانون المشرع بوجه خاص وفي اللغة القانونية بوجه عام ، ولكن رغم شيوع هذا المصطلح على لسان المشرع إلا أنه لم يعرفه تعريفا مباشر كما فعل في تعريف العقار بل اكتفى فقط بالعبارات التالية "كل شيء مستقر بحيّزه وثابت فيه ولا يمكن نقله منه دون تلف فهو عقار وكل ماعدا ذلك من شيء فهو منقول"م ،683 ق.م فالملاحظ أن المشرع الجزائري تأثر بنظيره المصري في عدم وضع تعريف إيجابي للمنقول عكس المشرع الفرنسي الذي عرف المنقول في المادة 528 ق م ف بقوله "أجسام corps يمكن نقلها من مكان إلى آخر سواء كانت تتحرك بنفسها مثل الحيوانات أم كان لا يمكن نقلها من محلها إلا بقوة أجنبية مثل الأشياء الجامدة " و الملاحظ أن المشرع الفرنسي يقصد بهذا التعريف أساس المنقولات بطبيعتها ، كأنظمة المعالجة الآلية للمعلومات والمعطيات المعلوماتية يعود طابعها المنقول إلى سهولة نقلها من حاسوب إلى آخر سواء عبر الأنترنيت أو شبكة الإكسترانيت. أنظر: عجة جيلالي ، مدخل للعلوم القانونية، الجزء الثاني، المرجع السابق، ص 271.

2 – محمود أحمد عبابنة، المرجع السابق، ص 36.

إذن تعتمد هذه الجرائم على قمة الذكاء في ارتكابها، إذ يصعب على المحقق التقليدي التعامل معها ومتابعتها والكشف عنها وإقامة الدليل عليها، فهي جرائم تتسم بالغموض والتحقيق فيها يختلف عن التحقيق في الجرائم التقليدية.

وتتناسب خطورة الجريمة الإلكترونية مع المعرفة التقنية تناسبا طرديا ، فكّلما تقدمت المعرفة التقنية لدى الأفراد كلما زادت احتمالية توظيف هذه المعرفة بشكل غير مشروع .

ثالثا: صعوبة اكتشاف وإثبات الجريمة الإلكترونية

نظرا لطابع الخاص الذي تتميز به الجريمة الإلكترونية [1] فإن اكتشافها وإثباتها يحيط به الكثير من الصعاب ويرجع ذلك لعدة أسباب نذكر منها:

1 – أن الجريمة الإلكترونية لا تترك أثار مادية ملموسة في المحيط الخارجي، بل ترتكب الجريمة في الخفاء دون أن تترك آثار تدل على مرتكب الجريمة عكس الجريمة التقليدية ذات النتيجة بمدلولها المادي، والتي يصطلح على تسميتها بالجرائم المادية ، كجرائم القتل و الجرح مثلا ،يكون دليل الإثبات فيها مرئيا لأنها تخّلف عند ارتكابها آثارا يمكن إدراكها بالحواس ، كنتيجة للوسائل التي استخدمها الجاني، فمن الممكن مشاهدة الجروح التي على جسم المجني عليه، وعلامات التسمم التي ظهرت على المجني عليه نتيجة استخدام الجاني المواد السامة في الجريمة القتل، أو ظهور دماء[2] على المجني عليه وغيرها من الآثار.

أما في الجريمة الإلكترونية فإن الأمر مختلف ، فمن حيث الوسيلة التي ترتكب بها هذه الجريمة إما عن طريق نقل المعلومات على شكل نبضات إلكترونية غير مرئية تنساب عبر أجزاء الحاسب الآلي

1– كون هذه الجريمة تقع على الكمبيوتر وشبكة الأنترنت ونظمها. أنظر: فريد منعم جبور، حماية المستهلك عبر الأنترنيت ومكافحة الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010، ص183.

2 – تعد وسيلة تحليل الدم من الوسائل العلمية التي تستخدم لكشف شخصية الجاني ، فالدم عبارة عن سائل حيوي يتكون من أجسام صلبة تسبح في سائل هو البلازما ، وتتمثل هذه الأجسام في كريات الدم الحمراء، كريات الدم البيضاء، الصفائح ، فالعثور على البقع الدموية أو أثار الدماء مثلا في مسرح الجريمة أو على ثياب المجني عليه أو الجاني أو على الأشياء الموجودة في مصرح الجريمة من شأنه أن يؤدي إلى ضرورة أخذ عينة من دم الأشخاص (جاني أو مجني عليه لا يزال على قيد الحياة)= =لضرورة ذلك فإنجاز عملية المضاهاة التي تتطلب المقارنة بين بقعة الدم التي تم العثور عليها ، ودم أحد الأشخاص وبصورة خاصة المتهم.

وشبكة الاتصال العالمية بصورة آلية مثل انسياب الكهرباء عبر الأسلاك أو يتم نقلها بالإشعاعات ، وغالبا ما يتم هذا عن طريق وحدات طرفية بعيدة ، وممكن جدا أن تكون هذه الوحدات لاسلكية الاتصال مما يصعب ضبطها [1] .

2- إن المجني في الجرائم الإلكترونية يحجم عن الإبلاغ عنها لعدة أسباب منها :

- افتقاره إلى القدرة الفنية التي تمكنه من اكتشاف الجريمة ، أو خوفا من الأضرار بمصالحه إذ ما أعلن عن تعرضه لاعتداء لا سيما إذا كان الاعتداء واقعا على مؤسسات مالية أو مصرفية أو تجارية كبيرة، فيؤدي الإعلان عن الإعتداء إلى إلحاق ضرر بالمركز المالي لها واهتزاز ثقة الجمهور بها، بحيث تصبح خسائر الإعلان عن الجريمة أكبر من خسائر الجريمة نفسها، لذلك يكون التكتم عليها أفضل من إعلانها [2].

لذلك فهي لا تقف عند حد الامتناع عن الإبلاغ عن الجرائم، إنما يمتد الأمر إلى أنها تمتنع عن تقديم الأدلة ، أو تقديم أي مساعدة لجهات التحقيق إن وقعت ، وقد علمت بها السلطات ، الأمر الذي يشكل صعوبة أمام الجهات ، ليس في اكتشافها فحسب بل وفي أثباتها أيضا ، والواقع العلمي يكشف عن الكثير من حالات عدم تعاون المجني عليهم في هذه الجرائم ، ولا يعود السبب فقط في عدم تعاون تلك الجهات ، بل يعود كذلك إلى أسلوب اكتشافها، فغالبا ما يتم اكتشافها بعد مضي فترة طويلة نسبيا على ارتكابها ، إلى جانب أن الصدفة [3] غالبا ما تكون السبيل إلى اكتشافها[4].

1- محمد حماد مرهج الهيتي، جرائم الحاسوب- ماهيتها - موضوعها - أهم صورها - والصعوبات التي تواجهها-، الطبعة الأولى ، دار المناهج للنشر والتوزيع ، عمان ، 2006 ، ص 214.

2- سامي جلال فقي حسين ، المرجع السابق ، ص 29 . محمد محمود عبابنة ، المرجع السابق ، ص 37.

3 - وما يؤيد ذلك أن دراسات مسحية متعددة أكدت على ذلك ففي دراسة مسحية قامت بها لجنة التدقيق في (إنجلترا) بشأن جرائم الاحتيال المعلوماتي ، وإساءة استعمال الحاسب ،شملت ستة آلاف مؤسسة تجارية ، وشركة من القطاع الخاص تعتمد في أعمالها على الحاسب الآلي ، فتبين أن نصف حالات الاحتيال التي تمت ضد هذه المؤسسات والشركات قد اكتشفت مصادفة المزيد من المعلومات أنظر: محمد حماد مرهج الهيتي ، جرائم الحاسوب - ماهيتها - موضوعها - أهم صورها - والصعوبات التي تواجهها، المرجع السابق، ص 217.

4- محمد حماد مرهج الهيتي، جرائم الحاسوب- ماهيتها - موضوعها - أهم صورها - والصعوبات التي تواجهها، المرجع نفسه، ص 218-219.

الأمر الذي أدى إلى اقتراح البعض في الولايات المتحدة الأمريكية بأن تفرض النصوص المتعلقة بجرائم الحاسبات التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يقع عليها من جرائم في هذا المجال متى وصل إلى علمهم مع تقرير جزاء في حالة إخلالهم بهذا الالتزام [1]، وعرض ذات الاقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة .

3 – قدرة الجاني في الجرائم الإلكترونية على تدمير أدلة إدانته:

من الأسباب الأساسية التي تقف وراء صعوبة اكتشاف الجرائم الإلكترونية هي قدرة الجاني على محو أو إزالة أدلة إدانته في زمن قياسي لا يستغرق أكثر من ثواني معدودة [2]، وذلك بتعريض البيانات المخزنة لديه على وسائل ممغنطة إلى مجال مغناطيسي قوي قادر على محوها في طرفة عين، أو بتزويد الحاسب ببرامج من شأنها تدمير وتخزين البيانات في حال استخدامه من قبل شخص غير مرخص له [3]، الأمر الذي لا يمكن على ضوئه القول بأن جرائم الحاسب الآلي شأنها شأن بقية الجرائم ذات الأدلة المادية ، حيث أن الجاني في مثل هذه الجرائم أيضا يتمكن من تدمير الأدلة ، بل غالبا ما

1 – محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنيت الطبقة الثانية، دار النهضة العربية، 2009، ص 40 .

2 – من الوقائع العلمية التي تؤيد ذلك قيام الجاني بالتوجه إلى أي مقهى انترنيت والدخول على أحد المواقع وإرسال رسالة على البريد الإلكتروني لآخر تحتوي على بيانات عبارات سب وقذف ، ويقوم بمحو الدليل وإرجاع كل شيء كما كان عليه والانصراف مع العلم أنه حتى فهده الحالة يمكن للمتخصصين استعادة تلك المعلومات طالما لم يتم إتلاف القرص الصلب الخاص بالجهاز أو إعادة تحميل البرامج عليه مند البداية " فرمطة" حيث أنه في الحالتين السابقتين يستحيل الوصول إلى البيانات المثبتة بذلك الجهاز والتي تحتوي على المعلومات التي تدين المتهم من قبل ، كذلك من الوقائع العلمية قيام أحد الجناة بإدخال تعديل على نظام الحاسب ، حيث ضمنه ، وفي نطاق التعليمات الأمنية لحماية ما فيه من معلومات مخزنة ، برنامج مهمته محو هذه المعلومات بشكل تلقائي ، إذا ما تم اختراق نظام المعلومات من قبل شخص غير مرخص له .

3 – محمد عبد الرحيم سلطان العلماء، جرائم الأنترنيت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والأنترنيت من 1–3 ماي 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، الطبعة الثالثة، 2004، ص 878.

يلي إلى ذلك ، فهو يحاول عندما يقتل أو يسرق يترك أثر في مسرح الجريمة ، بل ويدمر كل ما يمكن أن يتخلف عليه أثرا من آثاره ، الأمر الذي قد يفقد هذه الحجة أهميتها [1].

فطبيعة الجريمة الإلكترونية غير مرئية في الغائب لأنها تتعلق بمعطيات في شكل نبضات أو ذبذبات إلكترونية، وبالتالي يسهل على الجاني محو الأدلة المتعلقة بها وتدميرها في وقت وجيز لهذا وصفها بعض الفقهاء بأنها جريمة هادئة بطبيعتها لا تتطلب سوى عدد من اللمسات الخاطفة على لوحة المفاتيح حتى تؤدي إلى اختراق المعلومات المخزنة في الحاسب الآلي وهتك سريتها ومحوها أو تشويهها أو تعطيل الأنظمة التي تحتويها [2].

فالجريمة الإلكترونية من الجرائم المستحدثة التي لا تترك شهودا يمكن الاستدلال بأقوالهم ولا أدلة مادية يمكن فحصها، وبالتالي فهي صعبة الاكتشاف والإثبات لإدانة مرتكبيها، وهذا ما يشكل تحديا للمشرع والشرطة القضائية التي لن يكون بيدها حل وحيد هو استعمال نفس الوسيلة التي يستعملها المجرم المعلوماتي أي المعلوماتية [3] كالسبيل الوحيد لاكتشاف وإثبات هذه الجريمة .

4 – نقص الخبرة الفنية لدى المحققين يقف عائقا أمام إثبات هذه الجريمة ، لأن هذا النوع من الجرائم يتطلب خبرة فنية عالية، وإلماما واسعا باستخدام الحاسوب أو جهاز بإمكانه المعالجة الآلية للمعطيات المعلوماتية، كأجهزة فك الرموز المقرصنة التي يمكن استعمالها لسرقة الأموال من أجهزة التوزيع الآلي للنقود مثلا أو استعمالها بهدف الدخول الاحتيالي في نظام معلوماتي محمي تقنيا، ونتيجة لنقص الخبرة وعدم القدرة على التعامل مع هذا النوع من الجرائم ، فإن رجال الضبطية القضائية لا يبذلون

---

1 – محمد حماد مرهج الهيتي، جرائم الحاسوب – ماهيتها – موضوعها – أهم صورها – والصعوبات التي تواجهها–، المرجع السابق ، ص 212.

2 – محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع ، عمان، 2004، ص 165 .

3 – المعلوماتية مصطلح استخدمه لأول مرة ميخايلوف (Mikhailov) مدير المعهد الاتحادي للمعلومات العلمية والتقنية بالاتحاد السوفياتي وسماه "بعلم المعلومات العلمية " وتعني المعلوماتية ذلك العلم الذي يهتم بالموضوعات والمعارف المتصلة بتحصيل المعلومات وتجميعها وتنظيمها واختزانها واسترجاعها وتفسيرها وبثها وتحويلها واستخدامها كما يتضمن البحث عن تمثيل المعلومات في النظم الطبيعية والصناعية والإدارية ، واستخدام الرموز والمفاتيح في نقل الرسالة والتعبير عنها بكفاءة فضلا عن الاهتمام بدراسة أساليب معالجة المعلومات والأنظمة المعلوماتية ونظم البرمجة. لمزيد من التفاصيل أنظر: خثير مسعود ، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، 2010، ص 19.

عادة جهود كبيرة لكشف هذه الجرائم وإثباتها على الجاني ، إلى جانب ذلك فإن المحقق نفسه أحيانا يكون سببا في محو وإزالة الدليل، وذلك بسبب سوء تعامله مع تلك الأدلة بسبب نقص خبرته، ومعرفته الفنية والتي تمكنه من استخدام الدليل بشكل سليم ، فمعرفة المحقق بأساليب استخراج الدليل في الجرائم الإلكترونية يعتبر عامل مهم يمكن من خلاله إثبات الجريمة على الجاني ومحاسبته قضائيا [1].

وقد اتجهت بعض الدول إلى الاستعانة ببعض المجرمين الذين يطلق عليهم مصطلح الهاكرز [2] **(Hackers)** للتوصل إلى كشف غموض بعض الجرائم الإلكترونية ومن أجل ذلك بدأت بعض هذه الأجهزة في بعض الدول بتطوير أجهزتها المختصة بالتدريب المستمر على هذه التقنية وإنشاء مراكز متخصصة لهذا الغرض[3].

رابعا : وقوع الجريمة الإلكترونية أثناء المعالجة الآلية للبيانات

تقع الجريمة الإلكترونية أثناء عملية المعالجة الآلية للبيانات والمعطيات الخاصة بالكمبيوتر، ويمثل هذا النظام الشرط الأساسي الذي يتعين توافره حتى يمكن البحث في قيام أو عدم قيام أركان الجريمة الإلكترونية الخاصة بالتعدي على نظام معالجة البيانات ، ذلك في حالة تخلف ذلك الشرط تنتفي الجريمة الإلكترونية .

فبرغم من إمكانيات ارتكاب الجرائم الإلكترونية أثناء أية من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات (الإدخال– المعالجة – الإخراج) ، إلا أنه لكل مرحلة منها نوعية خاصة من الجرائم لا يمكن ارتكابها إلا في وقت محدد .

---

1 – سامي جلال فقي حسين، المرجع السابق، ص 30.

2 – الهاكرز هو شخص خبير بلغة البرمجة ويستطيع الدخول على غيره والتجسس عليهم ، وأول ما ظهر في عام 1984عندما استطاع ليكنس لوثر إنشاء مجموعة من القراصنة يقومون بدخول على أجهزة الآخرين ثم ظهرت عام 1990 مجموعة أخرى= =قامت بمنافسة ومحاولة كل طرف اختراق الآخر حتى سميت حرب الهاكرز واستمرت 4 سنوات انتهت بإلقاء القبض على بعضهم ويعتبر كيفن ميتنيك أشهر هاكر في التاريخ استطاع اختراق كمبيوتر شركة التي يعمل بها وسجن عام وخرج أكثر ذكاء ومارس هوايته وكانت أكبر قضاياه سرقة أرقام 2000 بطاقة انتماء .

3– محمد عبيد الكعبي، المرجع السابق، ص 43.

ففي مرحلة المداخلات تترجم المعلومات إلى لغة مفهومة من قبل الحاسب يسهل إدخال معلومات غير صحيحة ، وعدم إدخال وثائق أساسية ، وفي هذه المرحلة يرتكب الجانب الأكبر من الجرائم الإلكترونية .

أما في مرحلة المعالجة فإنه يمكن إدخال أي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في برامج الحاسب، كتشغيل برامج جديدة تلغي عمل البرامج الأصلية ، والجرائم المرتكبة في هذه المرحلة تتطلب أن يكون لدى الفاعل معرفة فنية عميقة و اكتشافها صعب ، وغالبا ما تقف المصادفة وراء اكتشافها، وفي المرحلة الأخيرة المتعلقة بالمخرجات يقع التلاعب في النتائج التي يخرجها الحاسب بشأن بيانات صحيحة أدخلت فيه و عالجها بطريقة صحيحة.

في الأخير يمكن القول بأنه رغم التطور السريع للجانب التشريعي والقضائي الفرنسي على التشريع الجزائري في مجال الإجرام المعلوماتي، إلا أن خصائص هذا النوع من الجرائم لقي نفسه في الدولتين وكذا الدول الأوروبية الأخرى لسبب الصعوبات التي تحيط بالجرائم الإلكترونية .

الفرع الثاني: أطراف الجريمة الإلكترونية

إن ارتباط الجرائم الإلكترونية بتكنولوجيا المعلومات كان وراء تمييزها عن الجرائم التقليدية، إذ أنّ الجريمة الإلكترونية كانت نتاج تزاوج بين انفجار المعلومات وتطور وسائل الاتصال، فهي نوع جديد من السلوكيات المنحرفة التي يتعرض لها كل من النظام المعلوماتي ومكوناته من البيانات أو المعطيات من خلال أشخاص مؤهلين وذوي خبرة علمية أو عملية في كيفية التعامل معه أو مع تلك المعطيات أو البيانات أو المستخرجات، فالجريمة الإلكترونية وكأية جريمة أخرى لها طرفان، الأول هو المجرم المعلوماتي والثاني هو الضحية المعلوماتية .

أولا : المجرم المعلوماتي

من الجوانب السلبية للمعلوماتية أنها أضافت عن غير قصد صنفا جديدا من الجناة إلى حياة البشر والذي أصطلح على تسميتهم بمجرمي المعلوماتية أو كما يسمون بالمجرم الإلكتروني الرقمي، والمجرم المعلوماتي قد يكون شخصا طبيعيا أي الإنسان وقد يكون شخصا معنويا كالمنظمات

الإرهابية والأجهزة الاستخبارية[1]، فمن مظاهر الخطورة التي تتجلى بها الجريمة الإلكترونية أن مرتكبيها يتسمون بالذكاء والدراية في مجال المعالجة الآلية للمعطيات والإلمام المهارات والمعارف التقنية، وإذا كان الشخص الذي يرتكب الفعل غير المشروع ويعتدي فيه على حق من حقوق الغير بالمعنى الواسع يعد في نظم القانون مجرما ويتعرض للعقاب، وكما هو معروف فإنه لا يمكن للعقوبة أن تحقق هدفها ما لم تضع في الاعتبار شخصية المجرم، إذا كنا في مجال الإجرام المعلومات، فيجب أن ننظر إلى المجرم المعلوماتي من حيث صفاته وسماته[2] .

كما أن هناك تفرقة تقليدية في دراسات علم الإجرام ، تقوم على التمييز بين الإجرام الطبيعي والإجرام المكتسب نادى بهذه التفرقة الفقيه "جاروفالو"، غير أن السؤال الذي يتبادر إلى أذهاننا: **أيّ الإجرامين ينتمي إليه المجرم الإلكتروني ؟**

يمكن القول في هذا الصدد أنه لا يوجد نموذج محدد للمجرم الإلكتروني[3]، بل هناك عدة نماذج للمجرمين قد يستخدمون الكمبيوتر في جرائمهم ، وقد يقومون بأفعال إجرامية ضد نظام الكمبيوتر نفسه، فعلى سبيل المثال هناك من يسرق النقود من البنك عن طريق الاستعانة بأنظمة الكمبيوتر، وهناك من يتحايل على الكمبيوتر عن طريق الاستعانة بكمبيوتر آخر يصدر منه الأمر إلى الجهاز الأول، وذلك لتحويل أموال إلى حساب آخر، كذلك لأجل التحاليل على كمبيوتر ثالث، وهناك من

1- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2013 ، ص 48.

2- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية ، رسالة ماجستير في العلوم الجنائي ، جامعة الحاج لخضر، باتنة ، 2012- 2013، ص 50.

3- يطلق فقهاء القانون الجنائي على المجرم الإلكتروني مصطلح ، "المجرم المعلوماتي " وهو الشخص الذي لديه مهارات تقنية أو دراية بالتكتيك المستخدم في نظام الحاسب الآلي الإلكتروني والقادر على استخدام هذا التكتيك لاختراق الكود السري لتغيير المعلومات أو لتقليد البرامج أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه" ، أما في الاصطلاح الإلكتروني فيطلق خبراء أمن المعلومات الإلكترونية مصطلح "هاكر" على من يخترق الحاسب الآلي ومصطلح كراكرز على الفئة التي لديها قدرة على الاختراق. أنظر : مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 143.

يرتكب جريمة التزوير عن طريق الاستعانة بالكمبيوتر، وذلك بتعديل البيانات المحفوظة فيه ، والتي يتم إخراجها في شكل محررات ورقية بعد ذلك وهكذا الأمر بالنسبة لصور أخرى من الجرائم[1].

لهذا ترجع الصعوبة في تحديد السمات الخاصة بالمجرم الإلكتروني[2] إلى تعدد الجرائم الإلكترونية وتنوعها، ورغم ذلك يمكن القول بأن شخصية المجرم الإلكتروني مرتكب الجريمة الإلكترونية تتميز بخصائص وسمات تختلف عن مرتكب الجرائم التقليدية، وهذا راجع لتميز شخصيته مرتكبي الجرائم الإلكترونية بالتقدم في مجال استخدام الحاسب الآلي، وهم غالبا على درجة علمية وثقافية عالية لكي يتمكنوا من استخدام أجهزة الحاسب الآلي في ارتكاب جرائمهم ، عكس المجرم العادي الذي غالبا ما يتميز بالقوة العضلية ونادرا ما يتميز بعضهم بعنصر الذكاء ، ومرتكب الإلكترونية إما أن يكون شخصا مستقلا أو يعمل من خلال جماعات تتميز هي الأخرى بمجموعة من السمات .

ومن السمات المشتركة بين جميع فئات مرتكبي الجرائم الإلكترونية مايلي :

1 – **الذكاء:** يعتبر الذكاء من أهم صفات مرتكب الجرائم الإلكترونية، لأن ذلك يتطلب منه المعرفة التقنية لكيفية الدخول إلى أنظمة الحاسب الآلي والقدرة على التعديل والتغيير في البرامج وارتكاب جرائم السرقة والنصب وغيرها من الجرائم التي تتطلب أن يكون مرتكب الجريمة على درجة كبيرة من

1– عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبيعة الأولى ، منشأة المعارف ، الإسكندرية، 2009 ، ص 95 .

2– يرمز الأستاذ Parker إلى الخصائص التي تميز المجرم الإلكتروني عن غيره من المجرمين بكلمة S.K.R.A.M وهي تعني المهارةSkills، المعرفة Knowledge ، الوسيلة Ressources ، السلطة Anthority وأخيرا الباعث Motives.
أنظر في هذا الصدد :
Parker (Donn), Figding computer crime anew Frame work for protecting information , 1998 , P 114 .
أما السلطة فيقصد بها الحقوق أو المزايا التي يتمتع بها المجرم الإلكتروني والتي تمكنه من ارتكاب جريمته وهذه السلطة إما مباشرة كالشفرة الخاصة بالدخول إلى النظام المعلوماتي التي تعطي للفاعل مزايا متعددة وقد تكون غير مباشرة كاستخدام شفرة الدخول الخاصة بشخص ما .
* الباعث لارتكاب الجريمة الإلكترونية لا يختلف كثيرا عن الباعث لارتكاب غيرها من الجرائم الأخرى ، فالرغبة في تحقيق الربح المادي بطريقة غير مشروع يظل الباعث الأول وراء ارتكاب هذه الجريمة ثم يأتي بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله وأخيرا الانتقام من رب العمل .
* الوسيلة: هي الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته، أما فيما يخص المجرم الإلكتروني فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسب الآلي تتميز نسبيا بالبساطة وبسهولة الحصول عليها حتى أنه يستطيع بمهارته ابتكارها.

المعرفة، لكي يتمكن من ارتكاب تلك الجرائم، لذلك عادة ما يذكر أن الإجرام المعلوماتي هو إجرام الأذكياء وذلك مقارنة بالإجرام التقليدي الذي يميل إلى العنف[1].

ويرى بعض الفقه أنه من السهل تصور الإجرام العنيف الموجه ضد النظام المعلوماتي ، والذي يتجسد في إتلاف الحاسب الآلي أو الدعائم المعلوماتي[2] لا يحتاج إلى سلوك عنيف ، فهو ينشأ من تقنيات التدمير الناعمة التي تتمثل في التلاعب بالمعلومات أو الكيانات المنطقية أو البيانات، ويكون ذلك عن طريق ما يعرف بالقنابل المنطقية[3] والفيروسات المعلوماتية[4]، بمعنى يكفي أن يقوم المجرم الإلكتروني بالتلاعب ببيانات وبرامج الحاسب الآلي لكي يمحوا أو يدمر هذه البيانات أو يعطل استخدام هذه البرامج، وبالتالي فهذا المجرم لا يمكن أن ينتمي إلى طائفة المجرمين الأغبياء، فمن يستعين مثلا بجهاز الحاسوب الآلي للاستيلاء على أسرار بنك لا بد أن يتميز بالذكاء حتى يمكنه أن يتغلب على كثير من العقبات التي تواجهه في ارتكاب جريمته .

2- **الخبرة والمهارة** : يتصف المجرم الإلكتروني بأنه على درجة عالية من الخبرة والمهارة في استخدام التقنية المعلوماتية ، وذلك لأن مستوى الخبرة و المهارة التي يكون عليها هي التي تحدد الأسلوب الذي يرتكب به تلك الجرائم، و المقصود بالمهارة في هذا المجال أن يكون المجرم الإلكتروني على درجة من العلم والدراية في التعامل في مجال المعالجة الآلية للمعلومات والإلمام بالمهارات والمعارف التقنية المتطلبة لتنفيذ العمل الإجرامي، والتي قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو

1- أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، بدون دار نشر، 2003 ، ص 243 . أنظر أيضا: رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الأنترنيت ، دار النهضة العربية، القاهرة ، 2013، ص 73.

2- يقصد بالإتلاف المعلوماتي (إتلاف برامج الحاسب الآلي ومعلوماتية) : إتلاف ومحو تعليمات البرامج أو البيانات ذاتها ويطلق عليها مصطلح تدمير نظم المعلومات Sabotage Informatique وعادة لا يستهدف مرتكب هذا الاعتداء فائدة لنفسه ، بل لمجرد إعاقة نظام المعلومات من الأداء بوظائفه وإحداث ضرر، وبالتالي نلاحظ أن هذا الإتلاف يوجه إلى الجانب المنطقي والمعنوي في الحاسب الآلي الذي بات يشكل قيمة اقتصادية عالية .

3- يقصد بالقنابل المنطقية Bombe logique " برنامج أو جزء من برنامج ينفذ في لحظة محدودة ، أو كل فترة زمنية منتظمة ، يوضع على شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل عمل غير مشروع. " أنظر : محمود أحمد عبابنة، المرجع السابق، ص 103-104 .

4- ضياء علي أحمد نعمان، المرجع السابق، ص 12.

عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين[1].

وعليه إذا كان الشخص مرتكب الجريمة على قدر ضئيل من مستوى الخبرة نجد أن الجرائم التي قد يرتكبها لا تتعدى ، الإتلاف المعلوماتي أو نسخ البيانات والبرامج ، أما إذا كان الشخص على درجة أعلى في المستوى المهاري فإن أسلوب ارتكابه للجرائم يختلف، إذ يمكنه عن طريق استخدام الشبكات بالدخول إلى أنظمة الحاسب الآلي وسرقة الأموال وارتكاب جرائم النصب وارتكاب جرائم التجسس وزرع الفيروسات وغيرها من الجرائم التي تتطلب مستوى مهاريا وخبرة كبيرة في ارتكابها[2].

إذن الجريمة الإلكترونية لا يقترفها إلا مجرم له طبيعة خاصة، تقتضيه عملية التغلب على المعلومات، وفك رموزها كونها موضوع جريمته سوءا كان برنامج أو معلومات مخزنة في الحاسب الآلي أو على أقراص أو أسطوانات، هي في حقيقتها معلومات مرمّزة أو مشفرة ، تحتاج من له الخبرة والدراية في فك رموزها ، أو حل تشفيرها ، إنما يدل هذا كذلك على تفاوت قدرة المجرم الإلكتروني على ارتكاب الجرائم بتفاوت قدراته ، ومعلوماته عن البرامج ، فمثلا محلل البرامج يستطيع أو ذو قدرة أفضل في ارتكاب الجرائم الإلكترونية ممن يستطيع أن يصمم هذه البرامج أفضل ممن يستخدم هذه البرامج، وهكذا وعليه بقدر اتصال الشخص وفهمه لعمل برامج الحاسب الآلي وكيفية تكوينها ، وتركيبها ، تزداد قدرته على ارتكاب الجرائم الإلكترونية[3].

كما أن المهارة التي يتميز بها المجرم الإلكتروني تمكنه من تكوين تصور كامل بجريمته ، إذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة ولو تكن في الحسبان من شأنها إفشال مخططاته أو الكشف عنها ، فعادة ما يلجأ هذا المجرم الإلكتروني إلى التمديد لارتكاب جريمته بالتعرف على المحيط الذي تدور فيه، وكذا

1- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012، ص 94.

2- أيمن عبد الحفيظ عبد الحميد سليمان ، المرجع السابق ، ص 244.

3- محمد حماد مرهج الهيتي، جرائم الحاسوب جرائم الحاسوب – ماهيتها – موضوعها – أهم صورها – والصعوبات التي تواجهها- ، المرجع السابق ، 137- 138.

الظروف التي تحيط بالجريمة المراد تنفيذها وإمكانيات نجاحها واحتمالات فشلها، ويساعد في كل هذا درجة المهارة التي يتمتع بها هذا الأخير[1].

3- **الميل إلى ارتكاب الجريمة** : يتميز المجرم الإلكتروني كذلك بوجود النزعة الإجرامية والميل إلى ارتكاب الجرائم لديهم، هذا على الرغم مما يكسبونه من مهارات في مجال التقدم التكنولوجي ، فمرتكب الجريمة الإلكترونية يتعلم ويتقن المهارات التكنولوجية لكي تساعده على ارتكاب الجريمة[2].

وتتكون تلك النزعة الإجرامية لدى الشخص لتأثره بعوامل عضوية وعوامل نفسية[3] صاحبت نشأته، ومع اقتران تلك العوامل بعنصر آخر جديد يساعد على استثارة الحالة الإجرامية ويزيد من قدر ضغوط عوامل الإجرام وتفوقها على موانع الإقدام ، وهذا العنصر قد يكون اكتساب الشخص للمهارات العلمية والتكنولوجية وتظل تلك العوامل السابقة بمثابة طاقة كامنة لدى الشخص، وعند استثارة تلك الطاقة لدى الشخص تبدأ في التحرر من مجرد طاقة كامنة إلى أن تبرز في شكل عمل إجرامي ، ويمكن إجمال تلك الحالة الإجرامية لدى الشخص طبقا للنظرية التالية :

حالة إجرامية كامنة + موقف إجرامي + قرار الحسم الإداري = سلوك إجرامي[4].

4- **المجرم الإلكتروني إنسان اجتماعي:**

إن المجرم الإلكتروني لا يضيع نفسه في حالة عداء سافر مع المجتمع الذي يحيط به بل إنه إنسان اجتماعي، ذلك أنه أصلا مرتفع الذكاء ويساعده على ذلك عملية التكيف الاجتماعي، وما الذكاء في رأي كثيرين سوى القدرة على التكيف ولا يعني ذلك التقليل من قيمة وشأن المجرم الإلكتروني، أن خطورة الإجرامية قد تزيد إذا زاد تكيفه الاجتماعي مع توافر الشخصية الإجرامية لديه[5].

1- نائلة عادل محمد فريد قورة ، جرائم الحاسب الآلي الاقتصادية ، الطبعة الأولى ، منشورات الحلبي ، 2005 ، ص 58.

2- أحمد ضياء ، الظاهرة الإجرامية بين الفهم والتحليل ، دار النهضة العربية ، القاهرة ، 2001، ص 294.

3- ضياء على أحمد نعمان، المرجع السابق ، ص 15.

4- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق ، ص 245.

5 -عبد الفتاح بيومي حجازي ، نحو صياغة عامة في علم الجريمة والجرم المعلوماتي، المرجع السابق، ص 100.

ويشير بعض الفقه باستثناء سرقة تقنيات المعلوماتية واستخدامها من قبل اللصوص، بأن الإجرام المعلوماتي بصفة عامة قد أثمر عن عوامل مستخدمة لي أذهان مرتكبيه ، حيث يلجأ العديد منهم إلى ارتكاب هذه الجرائم بدافع اللهو أو لمجرد إظهار تفوقهم على الآلة أو على البرامج المخصصة لأمن النظم المعلوماتي، ومن المألوف جدا من جهة أخرى ألا يحصلوا على منفعة مالية من جرائمهم ، ولكن يكتفوا بالتفاخر بأنفسهم وأن يظهروا لضحاياهم ضعف أنظمتهم[1].

وفي نفس السياق تشير إلى أن هناك تكييف اجتماعي ينشأ بين مجموعة لها صفات مشتركة ، فمثلا جماعة صغار نوابغ المعلوماتية لاشك أنهم يتكيفون في أفكارهم فيما بينهم وتنشأ بينهم صلات وروابط تساعدهم على ارتكاب جرائمهم وتتعدى تلك الروابط والصلات النطاق المحلي إلى المجال الدولي، بحيث تنشأ بينهم روابط دولية تتفق مع أفكارهم ومنهجهم في استثمار تلك المعرفة والتقدم العلمي [2].

فإحساس المجرم أنه محل ثقة من مجموعته، وشعوره أنه خارج إطار الشبهات قد يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تكتشف وإذا اكتشفت فإنها تواجه صعوبة في الإثبات ونقص الأدلة ونقص الخبرة لدى المحققين ولدى رجال القضاء، ونشير في الأخير إلا أن الجريمة الإلكترونية لها الوجه الإنساني بالنظر إلى أن مرتكبها إنسان اجتماعي، ولها الوجه الآخر في الآثار المترتبة عليها .

5-**الميل إلى التقليد** : يبلغ الميل إلى التقليد منتهاه حيث يوجد الفرد وسط آخرين متجمعين، إذ يكون عندئذ أسهل وأسرع انسياقا لتأثير سواه عليه ، ويظهر ذلك جليا في مجال الجريمة الإلكترونية، لأن

1- نذكر في هذا المجال مثال عن اعترافات متهم يبلغ في العمر 17سنة أمام القضاء الجنائي الألماني حيث نسب إليه ولوجه بطريق الغش في نظام الفيديو تكس Vidéotex الخاص ب Bumdaspost والمعروف بمصطلح BTX حيث دافع المتهم عن نفسه قائلا: تملكني إحساس قوي بأن أكون مفيدا في كشف عيوب BTX لذلك أرسلت في الحال إلى مجموعة عمل BTX كل العناصر التي اكتشفتها بالصدفة والتي أ ظهرت تشككها فيما يخص حماية البيانات ، لاسيما وأن غالبية ملاحظاتي لم تكن معروفة بعد لدى هؤلاء مما أرتاح الأمر إلى تلاشي هذه العيوب مضيفا أنه مولع بنظام BTX ويكرس نفسه له صباحا ومساءا ،لكنه ليس شريرا على الإطلاق ،كبعض الأشخاص القائمين على نظام BTX ولا يملكون أي كفاءة . أنظر: عبد الفتاح بيومي حجازي، نحو صياغة عامة في علم الجريمة و المجرم المعلوماتي، المرجع نفسه، ص100 -101.

2- ضياء على أحمد نعمان، المرجع السابق، ص 14.

أغلب الجرائم تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية التي لديه، مما يؤدي به الأمر إلى ارتكاب الجرائم، ولا شك أن ذلك يكون نتيجة لعدم الاستواء في شخصية الفرد الذي يتأثر بخاصية الميل إلى التقليد بسبب عدم وجود ضوابط يؤصلها الفرد في ذاته مما يحجم لديه غريزة [1].

أما فيما يخص السمات التي تتميز بها المجموعات عن الفرد المستقل في ارتكاب الجرائم الإلكترونية هي كالتالي:

1) **التنظيم والتخطيط** : تتميز الجريمة الإلكترونية عادة بوجود أكثر من فاعل لنشاط الإجرامي الواحد، إذ ترتكب أغلب الجرائم الإلكترونية من عدة أشخاص يحدد لكل شخص منهم دورا معين ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فمثلا تحتاج الجريمة نسخ برامج الحاسب الآلي إلى من يقوم بنسخ تلك البرامج، وقد يكونون مجموعة أشخاص، وتحتاج أيضا إلى من يقوم بعملية بيعها، كذلك هو الأمر بالنسبة لجريمة زرع الفيروسات فهي تحتاج إلى مجموعة من الأشخاص منهم المبرمج الذي يقوم بكتابة البرنامج ومنهم المستخدم الذي يقوم بعملية زرع الفيروسات داخل الأجهزة الأخرى ، وينتج عن هذا التنظيم صعوبة عملية كشف تلك الجريمة وإمكانية تنفيذها بدقة نتيجة للتخصص داخل تلك الجماعة في كل جزء من أجزاء الجريمة[2].

كما أنه من الملاحظ أن الأشخاص الذين يقومون بخلق أو تعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الإجرامي، فالجرائم الإلكترونية تتطلب عادة شخصين على الأقل أحدهما متخصص في الحاسبات الآلية يقوم بالجانب الفني من الشروع الإجرامي وشخص آخر من المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب[3]، وأحيانا أخرى يمكن تجنيد المجرم الإلكتروني القادر على اختراق نظم المعلومات ضمن عصابات الجريمة المنظمة عن طريق شبكة الأنترنيت ، و الأكثر من ذلك من خلال هذه الشبكة يمكن تبادل

1 – أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 245.

2– المرجع نفسه، ص 246.

3 –نائلة محمد فريد قورة ، المرجع السابق، ص 61.

معلومات وأفكار التطرف والإرهاب ، كما يمكن الاتفاق معه على اقتراف إحدى الجرائم الأخلاقية أو التلاعب في حسابات وأرقام بطاقات الانتماء وغيرها من الجرائم [1].

2)**التطور في السلوك الإجرامي** : إن وجود فرد في جماعة إجرامية مهما بلغت قدرتها العلمية أو المهارية إلى التأثير في قدرته العقلية وسرعة اكتسابه المهارة التقنية التي تؤدي به إلى التمرد الذاتي على محدودية الدور الذي يقوم به في تنفيذ الجريمة إلى محاولة الوصول لأعلى معدلات المهارة التقنية المتمثلة في إثبات قدرته على القيام بالدور الرئيسي في تنفيذ الجريمة، لذلك فإن وجود الفرد في جماعة يشكل خطورة عليه لأنه ليس فقط يكتسب المهارة التقنية والفنية ولكن يزيد أيضا لديه الملكة الإجرامية ومحاولة إثبات الذات والتفوق العلمي لديه مما يجعله يطور في أسلوب ارتكابه للجرائم فخطورة مرتكبي الجرائم الإلكترونية بأسلوب متطور لا تكمن فقط في قدرتهم على اختراق الأنظمة التقنية الفنية التي توضع لحماية المعلومات، إنما في كونهم أيضا ممن يعملون داخل المؤسسات [2]، وممن يعملون في مجال إدارة وتشغيل الحاسب الآلي وتكمن خطورتهم في أن الذي يعمل في المؤسسة قد يجعل أي نظام من أنظمة الحماية التي تستخدمه المؤسسة عديم القيمة والنفع، لأنه على دراية به وبأسلوب عمله ذلك يشجعهم على ارتكاب جرائمهم أولًا و سهولة وصولهم إلى مبتغاهم كونهم ممن يتعاملون مع الحاسب الآلي ثانيًا، الأمر الذي لا يجعل الشكوك تحوم حولهم وبسبب كون فرصهم أكبر من غيرهم سواء بالدخول إلى المعلومات السرية أو الإطلاع على الأسرار التجارية عليهم لارتكاب جرائمهم[3].

رغم كل ما قيل عن المجرم الإلكتروني في أنه متكيف اجتماعيا، وأنه مجرم غير عنيف وكل ما يمتاز به من صفات خاطئة إلا أنه في جميع الأحوال يبقى مجرمًا يتطلب توقيع العقوبة عليه.

---

1 –عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، المرجع السابق، ص 101- 102.

2 – في هذا الصدد يمكن القول بأن المجرم الإلكتروني معظم نشاطاته تتمركز على الإعتداء على الحقوق المالية للأفراد والشركات والمؤسسات المالية والاقتصادية بل في كثير من الأحيان هم لا يحاولون الإضرار بالأفراد بقدر ما يحاولون الإضرار بمؤسسات تتحمل الأضرار وتتجاوزها لما لديها من رصيد مالي عالي، ويعود السبب في التجائهم إلى اختراق جرائمهم ضد هذه المؤسسات في أنهم يسعون للكسب المالي الأمر الذي يحققه لهم هذا المجال أفضل من غيره.

3– محمد حماد مرهج الهيتي، جرائم الحاسوب جرائم الحاسوب –ماهيتها – موضوعها – أهم صورها – والصعوبات التي تواجهها ، المرجع السابق، ص 140.

ويمكن تصنيف مرتكبي الجرائم الإلكترونية[1]، إلى مجموعة من الطوائف ولا يعني بطبيعة الحال أن كل مجرم يندرج ضمن طائفة محددة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من طائفة أو فئة وسوف نتناولهم كما يلي:

1 / **فئة صغار مجرمي المعلوماتية** : كما يسميهم البعض صغار نوابغ المعلوماتية (pranksters) ويقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الآتية ، وكثيرا ما لفتوا لانتباه عن أفعال الانتهاك غير المسموح بها في العديد من ذاكرات الحاسوب ، وتقترف هذه الطائفة أفعالهم الإجرامية عن طريق استخدام حاسبات آلية إلكترونية خاصة بهم ، وليس هناك حدود جغرافية لأفعالهم التي تصل إلى أنظمة ومراكز معلوماتية توجد على آلاف من الكيلومترات من أماكن تواجدهم[2] .

ويطلق كذلك لفظ نوابغ المعلوماتية على المجموعات التي تميل للتحدي الفكري، وهو غالبا ما يكون في مرحلة المراهقة، وعلى الرغم من صغر سنهم إلا أنهم قادرون على اقتحام كافة أنواع الأنظمة المعلوماتية ، ويتميز هؤلاء المراهقون عن غيرهم من مرتكبي الجرائم التقليدية في أنهم لا يعتبرون أن ما يقومون به يعد جريمة لأنهم يعتقدون أن النظام غير قادر على حماية نفسه ليس من الخطأ اقتحامه، ولذلك فإنهم يعتبرون أنفسهم أبطالا لمساعدة المجتمع في تحديد نقاط الضعف

---

1 – هناك من يصنف المجرم الإلكتروني إلى أربع خانات رئيسية وهي:

أ– موظف العمل بمراكز الكمبيوتر، وهذا الصنف يمثل الغالبية العظمى من مرتكبي الجرائم الإلكترونية، وذلك بحكم سهولة اتصاله بالكمبيوتر ومعرفته الدقيقة باستخداماته التقنية.

ب– الموظف الساخط على مؤسسته والذي يستغل معرفته ببرامج الكمبيوتر الرئيسي للشركة لإيقاع الضرر بها عبر استخدام البيانات أو تسريبها أو مسحها

ج– هم من يصطلح على تسميتهم بالهاكرز أو الكراكز وهم فئة من المهووسين بالكمبيوتر يستغلون الحاسب من أجل اللهو والترفيه في أمور غير قانونية وليس بغرض التخريب.

د– هذه الفئة الأخيرة تهم الأفراد الذين يعملون في مجال الجريمة المنظمة عبر استخدام الحاسب ويشكل توقيت ومرحلة ارتكاب الجريمة الإلكترونية أحد أصعب النقاط في هذا النوع من الجرائم فقد ترتكب في أحد الأوقات التالية:

– عند إدخال البيانات مثلا كقيام المجرم الإلكتروني بتبديل أو تزوير البيانات كالتسلسل إلى برنامج طبع فاتورة الماء والكهرباء . – أثناء إخراج البيانات كسرقة بعض المعلومات الإلكترونية أو المتعلقة بمراقبة مخزون إحدى الشركات أو إنشاء معلومة خاصة بأحد الشركات. أنظر: الحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، مجلة الواحة القانونية، العدد الثاني، 2006 ص377– 378.

2 – ضياء علي أحمد نعمان، المرجع السابق، ص 18.

الخاصة بالبرنامج الذي تم اقتحامه[1] ، ويمكن رد الاتجاهات التقديرية لطبيعة هذه الفئة، وسمات أفرادها ومدى خطورتهم في نطاق الجرائم الإلكترونية[2] إلى ثلاث جهات :

أ- **الاتجاه الأول** : اتجاه لا يرى إصباغ أي صفة جرمية عليها أو على الأفعال التي تقوم بها، ولا يرى وجوب تصنيفه ضمن الطوائف الإجرامية ، استنادا إلى أن صغار السن لديهم ببساطة ميل للمغامرة والتحدي والرغبة في الاستكشاف، ونادرا ما تكون أفعالهم المحظورة غير شرعية، واستنادا إلى أنهم لا يدركون ولا يقدرون مطلقا النتائج المحتملة التي يمكن أن تؤدي إليها أفعالهم الغير المشروعة بالنسبة لنشاط منشأة أو شركة تجارية[3] .

ب-**الاتجاه الثاني** :هذا الاتجاه يحتفي بهذه الفئة ويناصرها ويعتبرها ممن يقدم خدمة لأمن المعلومات ووسائل الحماية ويصنفهم بالأخيار وأحيانا بالأبطال الشعبيين ، ويتمادى هذا الاتجاه في تقديره لهذه الفئة بالمطالبة بمكافئتهم باعتبارهم لا يسّببون ضررا للنظام ، ولا يقومون بأعمال احتيال ، وينسب إليهم الفضل في كشف الثغرات الأمنية في تقنية المعلومات.

ت- **الاتجاه الثالث** : يرى هذا الاتجاه إلى أن أفعال هذه الطائفة هي من الأفعال المحظورة والتي تطالها يد القانون، وبالتالي يصنفون ضمن مجرمي الحاسوب كغيرهم دون تمييز استنادا إلى أن تحديد الحد الفاصل بين العبث في الحواسيب وبين الجريمة أمر عسير من جهة ، و دونما أثر على وصف الفعل قانونا من جهة أخرى واستنادا إلى أن خطورة أفعالهم التي تتميز بانتهاك الأنظمة واختراق الحواسيب وتجاوز إجراءات الأمن والتي تعد من أكثر الجرائم

1- ضياء علي أحمد نعمان، المرجع نفسه، ص 19.

2- من أشهر الجرائم التي ارتكبت في الو.م. أ قيام مجموعة من طلبة المدارس العليا تتراوح أعمارهم بين 15 – 25 سنة يطلقون على أنفسهم أسرة المجموعة (414) في اختراق أنظمة نحو (60) حاسبا وذلك عام 1983 ، من بينها حاسبات وبنوك معلومات مختبر في لوس أنجلس وكذلك مركز شرطة Salan Kottring لعلاج الأورام في نيويورك ومعهد ماساشو سيتي للتقنية، وقاعدة ماك كليلان للقوات الجوية ، وأيضا جريمة مراهق لم يتجاوز 17 عاما يدعى "دينيسموران" والذي اختار لنفسه اسم "كوليو" حيث قام كو بشن سلسلة من الهجمات الإلكترونية على مواقع مهمة أنشأتها الحكومة الأمريكية على شبكة الإنترنيت ، ومنذ نهاية 1999= =وبداية سنة 2000 استطاع كوليو أن يحّول حياة المسئولين عن هذه المواقع إلى جحيم ، حيث دأب على مهاجمة موقع (DARE.ORG) المسؤول عن مواجهة مخاطر الإدمان ونقد عمليات تخريبية عليه.

3- عبد الفتاح بيومي حجازي ، نحو صياغة نظرية عامة في علم الإجرام والمجرم المعلوماتي، المرجع السابق، ص 106.

الإلكترونية تعقيدا من الوجهة التقنية، عوضا عن مخاطرها المدمرة ، ويدعم صحة هذا الاتجاه التخوفات التي تثيرها أصحاب الاتجاه الأول ذاتهم ، إذ يخشون من الخطر الذي يواجه هذه الطائفة ، والممثل في احتمال انزلاق من مجرد هاو صغير لاقتراف الأفعال غير المشروعة إلى محترف لأعمال السلب والاحتيال ، إضافة إلى احتمالية انضمامهم إلى أحضان منظمات أو أفراد غير شرفاء[1].

وفي الأخير يمكن القول أنه يمكن لجماعات صغار نوابغ المعلوماتية أن تتحول إلى فئة القراصنة، لأنه عندما يصبحون على درجة عالية وكبيرة من الخبرة والمهارة يتم استئجارهم واستغلالهم في أعمال ذات أهداف إجرامية.

2/ **فئة القراصنة** : يمكن تصنيف هذه الفئة إلى صنفين :

أ- **الهاكـــارز(les Hakers)**: الهــاكرز أو المتسلل هو شخص بارع في استخدام الحاسب الآلـي وبرامجـه ولديـه فضـول فـي استكشـاف حسـابات الآخـرين وبطـرق غيـر مشـروعة فـي الــهاكرز، وكما يدل على ذلك اسمهم ،هم متطفلون يتحدون إجراءات أمن نظم الشبكات من خلال الدخول إلى أنظمة الحاسبات الآلية غير المصّرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، وفي الغالب لا تتوفر لديهم دوافع حاقدة أو تخريبية وإنما ينطلقون من دوافع التحدي واثبات الذات، وتتألف هذه الطائفة أساسا من مراهقين وشباب (طلبة وتلاميذ الثانويات) وشباب عاطل عن العمل[2] ، وإذا ما واجهته حماية لا يستطيع تخطيها فهو ليس له علاقة بتكنولوجيا المعلومات[3].

ب-**الكراكـر (les Crakers)** : الكراكـــــر أو المقتحم هو شخص يقوم بالتسلل إلى نظم الحاسوب للاطلاع على المعلومات المخّزنة فيها أو لإلحاق الضرر أو العبث بها أو سرقتها،

1- محمود أحمد عبابنة، المرجع السابق، ص 42.

2- نسرين عبد الحميد نبيه، المرجع السابق، ص 40-41 . أنظر أيضا: عبد الصبور عبد القوي علي مهدي، الجريمة الإلكترونية ، الطبعة الأولى، دار العلوم للنشر والتوزيع ، 2008، ص 55.

3- ضياء علي أحمد نعمان، المرجع السابق، ص 20.

وذلك بدافع التحدي الإبداعي[1] ولقد تم استعمال هذا المفهوم سنة 1985 من طرف الطائفة الأولى ، طائفة الهاكرز للرد على الإستعمال السيئ للصحفيين لمصطلح الهاكرز [2].

وقد أثبت الواقع العلمي أنّ الهاكر يستعين بالكراكر إذا ما صادفه أي نوع من أنواع الحمـــاية، وغالبا ما يكون هدف هذه الفئة هو الحصول على المال أو بغرض الشهرة ، ومن السمات المميّزة لهذه الطائفة إستفادهم من التقنيات التي تطورتها فئة الهاكرز و بدؤوا يستخدمونها استخداما سيئا في اعتداءات تتم عن ميولات إجرامية، كذلك تبادلهم للمعلومات فيما بينهم، و في تطور حديث تنظم هذه الفئة نفسها بعقد مؤتمـرات لمخترقي الكمبيوتر يدعى الخبراء منهم للتشاور حول وسائل الاختراق ووسائل تنظيم عملهم[3].

3/ **فئة المحترفين** : يكتسب هذا النمط المستحدث من الأفعال غير المشروعة والمرتبط بالاستخدام التعسفي للحاسب الآلي خطورة خاصة ، نظرا لتقنيتها العالية من جهة ولغموض شخصية مرتكبيها من جهة أخرى .

وتعد هذه الفئة من أخطر الفئات التي ترتكب الجرائم، حيث تهدف اعتداءاتهم بالأساس إلى تحقيق الكسب المادي سواءا لهم أو للجهات التي كلفتهم لارتكاب الجرائم الإلكترونية، فضلا عن تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، إلى جانب ذلك تتميز هذه الطائفة بصيغة الخبرة والإدراك الواسع للمهارات التقنية والكفاءات العالية[4] .

1- تم إلقاء القضاء على أكبر هاكر يدعى كيفين متنيك عام 1995 حيث قام على مدار 20سنة بارتكاب عدد كبير من الجرائم الإلكترونية إذ كان بإمكانه الدخول إلى أي نظام معلوماتي مرتبط بأجهزة الكمبيوتر وتعلم كسر كلمة المرور بسلاسة فائقة و أتيحت له الفرصة للتبحر في مجال المعلومات والبيانات ليستولي على كل ما يريد، وكذلك يدمر كل ما يشاء بالإضافة إلى قدرته على زرع أي نوع من أنواع الفيروسات .

2- نسرين عبد الحميد نبيه، المرجع السابق، ص 21.

3- نسرين عبد الحميد نبيه، المرجع نفسه، ص 41.

4- تشير إحصائية قام بها معهد سنتانفورد على أن 25% من أفعال الاعتداء على نظم المعالجة الآلية قام بها المحللون ، و18% قام بها المجرمون ، 17% من الجرائم قام بها المستخدمون ، 16% قام بها الصرافون ، 11% المشغلون ، وأخيرا الأشخاص الأجانب عن المنشأة قاموا بـ 12% من مجموع هذه الجرائم . أنظر : محمود أحمد عبابنة ، المرجع السابق، ص 42.

وإلى تحقيق جانب المعرفة التقنية المميزة والتنظيم العالي والتخطيط بالأنشطة المنوي ارتكابها، فإن أفراد هذه الطائفة يتسمون بالتكتم فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة، ويحاولون ما أمكن عدم كشف طرقهم التقنية لارتكاب جرائمهم وحول الأعمار الغالبة على هذه الفئة فإن الدراسات تشير إلى أنهم الشباب الأكبر سنا وأن معظمهم تتراوح أعمارهم ما بين 25 – 40 سنة[1] .

ويتشابه مرتكبي هذه الأفعال مع المجرمين ذوي الياقات البيضاء[2] من حيث كونهم من أصحاب التخصصات العالية ولهم الهيمنة الكاملة على تقنية الإلكترونيات وعلى قدر من الذكاء.

4/**فئة الحاقدين:** هذه الطائفة يغلب عليها عدم توافر أهداف وأغراض الجريمة المتوفرة لدى غيرهم من الطائفة السالفة الذكر[3] ، فهم لا يسعون إلى إثبات المقدرات التقنية والمهارية وفي نفس الوقت لا يسعون إلى مكاسب مادية أو سياسية ، إنما يحرك أنشطتهم الرغبة في الانتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونون موظفين فيها، ولهذا فإنهم ينقسمون إما إلى مستخدمي للنظام بوضعهم موظفين أو مشتركين أو على علاقة ما بالنظام محل الجريمة ، وإلى غرباء عن النظام تتوفر لديهم أسباب الانتقام من المنشاة المستهدفة في نشاطهم[4] .

ولا يتسم أعضاء هذه الطائفة بالمعرفة التقنية الاحترافية، ومع ذلك يسعى الواحد منهم للوصول إلى كافة عناصر المعرفة المتعلقة بالفعل الذي ينوي ارتكابه ، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات الفيروسات والبرامج الضارة وتخريب النظم أو إتلاف كل أو بعض معطياته، أو نشاط إنكار الخدمة تعطيل النظام أو الموقع المستهدف إن كان من مواقع الأنترنيت[5].

1- نسرين عبد الحميد نبيه، المرجع السابق، ص 42 .

2 -مصطلح المجرمين ذوي الياقات البيضاء حديث نسبيا وأول من أطلقه هو عالم الاجتماع Suther lanc أين وضع أن هذه الجرائم ترتكب من قبل الطبقة الراقية في المجتمع وذوي المناصب الإدارية الكبيرة، وتشمل أنواعا مختلفة من الجرائم كسيل الأموال وغير ذلك من الجرائم التي يقوم بارتكابها وهم جالسون .

3- ضياء علي أحمد نعمان، المرجع السابق، ص 21.

4- نسرين عبد الحميد نبيه، المرجع السابق، ص 42.

5- نسرين عبد الحميد نبيه، المرجع نفسه، ص 43 .

أما فيما يخص أعمارهم فليس هناك أي ضابط محدد وهم الطائفة الأسهل من حيث كشف الأنشطة التي قاموا بارتكابها لتوفر ظروف وعوامل تساعد على ذلك فهم لا يفاخرون بأنشطتهم بل يعمدون على إخفائها .

إذن هذه هي أصناف مجرمي المعلوماتية، والذي تكمن خطورتهم في قدرتهم على اختراق الأنظمة التقنية والفنية التي توضع لحماية المعلومات ، وفي كونهم أيضا ممن يعملون داخل المؤسسات وممن يعملون في مجال إدارة وتشغيل الحاسب الآلي ، فالذي يعمل في المؤسسة قد يجعل أي نظام من أنظمة الحماية الذي تستخدمه المؤسسة عديم النفع والقيمة لأنه على دراية به وبأسلوب عمله ، ذلك يشجعهم على ارتكابهم جرائمهم أولا، وسهولة وصولهم إلى ما يبغون كونهم ممن يتعاملون مع الحاسب الآلي ثانيا، الأمر الذي لا يجعل الشكوك تحوم حولهم لأي سبب ، وكون فرصهم أكبر من غيرهم سواء بالدخول إلى المعلومات السرية أو الاطلاع على الأسرار التجارية فيسهل عليهم ارتكاب جرائمهم وإخفاء الأدلة التي تدينهم[1].

ثانيا : الضحية المعلوماتية

إن الجرائم عموما إنما تقع على المجني عليه، ولكن مع ذلك فإنه قد يتضرر من الجريمة أشخاص آخرون غير المجني عليه وهم من يطلق عليهم تسمية المتضرر من الجريمة وبناءاً على ذلك فقد أثارنا أن نطلق على الطرف الثاني في الجريمة الإلكترونية تسمية الضحية المعلوماتية ، لكي تشمل كلا من المجني عليه والمتضرر من الجريمة ، خصوصا وأن الإعلان العالمي بشأن المبادئ الأساسية المتعلقة بتوفير العدالة لضحايا الجريمة وإساءة استعمال السلطة الذي اعتمدته الجمعية العامة الأمم المتحدة بقرارها رقم 40/34 الصادر في 1985/11/29 قد أخذ بتسمية ضحايا الجريمة لتشمل كلا من المجني عليه والمتضرر من الجريمة[2].

1- عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، المرجع السابق، ص 121 .

2 -رغم اختلاف الفقه بشان ما إذ كان المجني عليه مضرورا أم لا في الوقت الذي تعتبر التفرقة بين المجني عليه والمضرور من الجريمة مهمة سواء كان ذلك في إطار القانون الجنائي الموضوعي كرضاء المجني عليه دون المضرور ذي الأثر الفعال في إباحة بعض الجرائم أو هدم أركانها في إطار القانون الجنائي الإجرائي كحق الشكوى كقيد على حرية النيابة العامة في تحريك الدعوى الجنائية يملكه المجني عليه دون المضرور. أنظر: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق ، ص 158.

ويقصد بالضحايا وفق الإعلان العالمي المشار إليه أعلاه الأشخاص الذين أصيبوا بضرر فردي أو جماعي بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية ، عن طريق أفعال أو حالات إهمال تشكل انتهاك للقوانين الجنائية النافذة في الدول الأعضاء بما فيها القوانين التي تحرم الإساءة الجنائية لاستعمال السلطة، كما يشمل المصطلح أيضا، حسب الاقتضاء العائلة المباشرة للضحية الأصلية أو فاعليها المباشرين و الأشخاص الذين أصيبوا بضرر من جزاء التدخل لمساعدة الضحايا في محنهم أو لمنع الإيذاء[1].

ويقصد بالضحية في الجريمة بصفة عامة كل شخص طبيعي أو اعتباري أصيب بخسارة أو بضرر أو بعدوان نتيجة ارتكاب جريمة تقليدية أو غير تقليدية ، وينتج الضحية سواءا من فعل أو امتناع عن فعل [2].

أما الضحية في الجريمة الإلكترونية فهو كل من أصابه ضرر مادي أو معنوي نتيجة الإستخدام غير مشروع للتقنيات الإلكترونية الرقمية [3].

وعموما ما يمكن تصنيف ضحايا الجرائم الإلكترونية إلى طائفتين رئيسيتين هما:

1 – **الطائفة الأولـــى: الأشخاص المعنوية**

تنقـسم الأشخاص المعنوية بدورها إلى قسمين:

أ- **الأشـخاص المعنويـة العامـة:** وتشمل جميع الدوائر الحكومية والمؤسسات المملوكة للدولة سواء كانت عسكرية أم مدنية كالوزارات والمطارات و البنوك المركزية، وكذلك المنشآت العسكرية والنووية، وتعد الجرائم الإلكترونية الواقعة على هذه الطائفة أخطر الجرائم من حيث

---

1 – مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 156.

2-إن الأعمال الإجرامية الإلكترونية تعد من الأعمال المستنكرة لأن العلاقة في الغالب بين المجرم الإلكتروني و الضحية مفقودة ، كما أن الأثر النفسي الذي تحدثه هو الهدف من الجريمة في كثير من الجرائم الإلكترونية خاصة البرامج الإلكترونية المتطفلة الضارة لإثبات الذات لدى الجاني و إرضاء شهوة التدمير و التخريب والأذى و الرغبة في نشر الدمار، لذلك لابد من ضرورة تحديد مفهوم الضحية في الجريمة الإلكترونية، وذلك من أجل إصدار قوانين تلتزم الدولة بمقتضاها بتعويض ضحايا تلك الجرائم .

3 – مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 159.

إضرارها بالدول العسكرية كجرائم التجسس المعلوماتي[1] على المواقع والمنشآت والمصانع والمختبرات العسكرية أو جرائم رصد البيانات المتعلقة بحجم القوات العسكرية وعدتها ونوعها وإمكانياتها .

ب- **الأشخاص المعنوية الخاصة** : تشمل هذه الفئة كافة المؤسسات الخاصة التي يملكها الأفراد مثل الشركات التجارية [2] والمصانع .....إلخ وأكثر ضحايا الجرائم الإلكترونية هم من هذه الطائفة، لما بها من أموال طائلة في أغلب الأحيان، كما أن البنوك تخسر سنويا مبالغ ضخمة من جراء الجرائم الإلكترونية وبالأخص الاحتيال المعلوماتي وسرقة أرقام بطاقات الانتماء[3].

1- نصت على هذه الجريمة المادة 3 من اتفاقية بودابست بقولها :" يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا لقانونه الداخلي واقعه الاعتراض العمدي، وبدون حق من خلال وسائل فنية للإرسال غير العلني لبيانات الحاسب في مكان الوصول في المنشأة أو في داخل النظام المعلوماتي، بما في ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات كما يمكن لأي طرف أن يستوجب أن ترتكب الجريمة بنية إجرامية أو ترتكب الجريمة في حاسب آلي يكون متصلا عن بعد الحاسب آخر ". نفس الأمر في المادة 7من الاتفاقية العربية = =لمكافحة جرائم تقنية المعلومات لسنة 2010 حيث اعتبرت الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات من قبيل التجريم ، إضافة إلى أن المادة 5 من ذات الاتفاقية" تلزم كل دولة من دول الأطراف بتجريم و الأفعال التي تم تجريمها وفقا للاتفاقية وذلك وفقا لتشريعاتها وأنظمتها الداخلية" . أما فيما يخص المشرع الجزائري فلم ينص على الاعتراض القانوني للمعلومات الإلكترونية بنص صريح رغم مصادقته على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بموجب المرسوم الرئاسي 14-252 المؤرخ في 8 سبتمبر (يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرر بالقاهرة بتاريخ 21ديسمبر 2010، جريدة رسمية عدد 57بتاريخ 28سبتمبر 2014)، وبالرجوع إلى نص المادة 394 مكرر 2 من ق.ع ، نجد بأنه تم تجريم التعامل في معطيات تم الحصول عليها عن طريق الاعتراض، بمعنى أنه جرم التعامل فيها ولكنه لم يجرم إعاقة أو اعتراض طريق نظام المعلومات أو المعطيات المرسلة عن طريق نظام المعلوماتية بصفة مباشرة ، كذلك تنص المادة 2/63 ق.ع على أن "الاستحواذ وسيلة على مثل هذه المعلومات أو الأشياء أو المستندات أو التصميمات بقصد تسليمها إلى دولة أجنبية أو إلى أحد عملائها " و من خلال هذه المادة نستطيع القول أن المشرع الجزائري جرم التجسس الإلكتروني ولكن حصره في المجال العسكري.

2 - تنص المادة 544 ق ت.ج على ما يلي :"يحدد الطابع التجاري لشركة إما بشكلها أو موضوعها تعد شركات التضامن وشركات التوصية و الشركات ذات المسؤولية المحدودة ، وشركات المساهمة ، تجارية بحكم شكلها و مهما يكن موضوعها.

3 - رشاد خالد عمر، المرجع السابق، ص56.

2 –الطائفة الثانية: الأفـــــــراد

وتشمل هذه الطائفة كل الأفراد المستخدمين لكمبيوتر وشبكة الإنترنيت و الهواتف المحمولة [1] ومن المنتظر أن تزيد نسبة الجرائم الإلكترونية الواقعة على هذه الطائفة نظرا لتزايد نسبة هؤلاء المستخدمين في العالم يوما بعد يوم ، وأغلب الجرائم الإلكترونية التي تتعرض لها هذه الطائفة تتمثل في جرائم الإحتيال المعلوماتي وسرقة أرقام بطاقات الائتمان وإرسال وزرع الفيروسات وجرائم التشهير بالأفراد عبر الانترنيت ، وأبرز مثال لهذه الجرائم الإلكترونية الواقعة على هذه الطائفة ستمثل بما حدث للكثير من مواطني الولايات المتحدة الأمريكية عقب أحداث 11سبتمبر 2001، حيث أستغل محتالون هذه الأحداث، وقاموا بإنشاء مواقع إلكترونية وهمية متخصصة لجمع تبرعات لضحايا هذه الأحداث عبر شبكة الانترنيت وطالبو المواطنين الأمريكيين بالتبرع لهؤلاء الضحايا عبر مواقعهم ، فقام الكثير من المواطنين بالتبرع لهم من خلال بطاقات الانتمان، إلا أن تلك المبالغ لم تصل إلى الضحايا وإنما وصلت لجيوب هؤلاء المحتالين[2].

على الرغم من إمكانية تعرض الجميع للجريمة الإلكترونية سواء كانوا أشخاص طبيعية أو معنوية، إلا أنه يمكننا الجزم بأنّ معظم الجرائم الإلكترونية ترتكب من أجل أمرين لا ثالث لهما وهما المال والمعلومات[3]، وخصوصا إذا كانت هذه المعلومات ذات أهمية بالغة وكان هدف المجرم المعلوماتي هو

1– الهاتف المحمول أو الهاتف النقال أو الهاتف الخلوي أو الهاتف السيّار: هو أحد أشكال أدوات الاتصال و الذي يعتمد على الاتصال اللاسلكي عن طريق شبكة من أبراج البث الموزعة ضمن مساحة معينة ، ومع تطور أجهزة الهاتف المحمول أصبحت الأجهزة أكثر من مجرد وسيلة اتصال صوتي بحيث أصبحت تستخدم كأجهزة كمبيوتر وتصفح الانترنيت و الأجهزة الجديدة يمكنها التصوير بنفس نقاء ووضوح الكاميرات الرقمية، وكذلك يمكن إرسال الرسائل القصيرة لأي مكان في العالم، ويعرف أيضا : "بأنه وسيلة اتصال سمعية لنقل الكلام باستخدام التيار الكهربائي" أنظر: طارق عفيفي صادق أحمد ، الجرائم الإلكترونية ، جرائم الهاتف المحمول ، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2015، ص 14–15.

2– رشاد خالد عمر، المرجع السابق، ص 56 .

3 – أصبحت المعلومات أحد الأنشطة المستهدفة بعد النقود إذ نشأ إلى جانب السوق الشرعي للمعلومات سوق سوداء لها يتم فيه بيع المعلومات المسروقة أو المقتبسة من أصحابها الحقيقيين والشرعيين مما أدى إلى ارتباط ذلك الإجرام بالأنشطة الاقتصادية والاجتماعية للجميع ويمكن تصوره بالنسبة للمعلومات الآتية :

أ/ المعلومات المالية : حيث تمس هذه الظاهرة المركز الحسابي والإداري ، وتنقلات الأموال و الاستثمارات سواءا في المنشآت العامة أو الخاصة .

الحصول على مقابل وعوض عن طريق المقايضة غير المشروعة لهذه المعلومات ، أو بيعها لغير أصحابها الشرعيين ، وسواءا كانت المعلومة مخزنة بذاكرة الحاسوب أو مدخلة في بنوك المعلومات، إذ يتم تشويهها وإظهارها على غير حقيقتها [1].

ففي هذا النوع من الجرائم يكون دور المجني عليه ضئيل وسلبي، إذ يفضل الكثير من المجني عليهم الإبقاء على ما لحقهم من الاعتداء سرا، أي يميلون إلى التكتم عما لحقهم من أضرار ناتجة عن الجريمة الإلكترونية والسبب في ذلك يرجع إلى رغبتهم في الحفاظ على مركزهم الاجتماعي أو سمعتهم التجارية فضلا عن عجز المجني عليهم في الإثبات المادي للجريمة وخشيتهم لاحتمالية المساءلة القانونية في الوقت الذي يقع عليهم واجب الإشراف على المعلومات المستهدفة وامتلاكهم السلطة اللّازمة لإمكان التقدير ووضع الإجراءات الضرورية في حالة حدوث أضرار ناشئة من إفشاء معلومات على قدر من الحساسية والخطورة [2].

المطلب الثالث: محل الجريمة الإلكترونية

تعتبر الجرائم الإلكترونية أحد أهم ثمار التقدم السريع في شتى المجالات العلمية ، فلقد صاحب التقدم الكبير في مجال العلوم والتقنية واستخداماتها لخير البشرية ، تقدم آخر مـــوازٍ في مجال

ب/المعلومات التجارية والصناعية : حيث تستهدف هذه الظاهرة الدراسات الخاصة بالأسواق و مشروعات الاستثمار و التصنيع و الإنتاج والتجارة و التوزيع والأسعار ومراكز البيع و القطاع الصناعي للإنتاج.

ج/المعلومات الشخصية: وهي تلك المخّزنة في ذاكرة الحاسبات الآتية وشركات التأمين ولدى المحامين والمستشفيات وأقسام الشرطة و الأحزاب و النقابات .

د/المعلومات العسكرية: تتمثل في أسرار الدولة والمشروعات النووية والتصنيع الحديث للأسلحة ويبدو أن هده المعلومات هي الأكثر رواجا في سوق المعلومات السوداء. أنظر: طارق فوزي الفقي ، الجوانب الإجرامية في الجرائم المعلوماتية ، رسالة دكتوراه ، كلية الحقوق ، جامعة المنوفية،2011، ص 21-22.

1 – صليحة علي صداقة ، الإبعاد القانوني و الأخلاقي للمعلوماتية الصحية ، دار المطبوعات الجامعية ، الإسكندرية ،2017، ص 220-221. أنظر أيضا : مدحت محمد عبد العزيز إبراهيم ،الجرائم المعلوماتية الواقعة على النظام المعلوماتي، الطبعة الأولى ، دار النهضة العربية ، القاهرة ،2015، ص 50.

2- صليحة علي صداقة ، المرجع نفسه ، ص 221.

الجريمة، فضلا عن أن التقدم أفرز وضعا جعل بموجبه المعلومات والمعرفة متاحة في متناول الجميع من خلال شبكة الأنترنيت، بحيث أصبح العالم بذلك قرية صغيرة يتم النفاد إليها بسرعة [1].

فقد تستهدف الجرائم الإلكترونية إما المعلومات المخزنة في جهاز الحاسب الآلي من خلال سرقتها أو تغييرها أو حذفها، كما قد ترتكب أضرار بجهاز الحاسب الآلي وبمكوناته المادية وغير المادية عن طريق نشر الفيروسات التي تدمر أنظمة الكمبيوتر وتعرقل كل الأنشطة المرتبطة به[2].

والجدير بالذكر هو أن العديد من الّدارسين أكدوا على أن الجرائم الواقعة على المكونات المادية للكمبيوتر تعتبر من قبيل الجرائم التقليدية، وهو الموقف الغالب إذ أنّ الجديد في القانون الجنائي وفيما أثير من مشكلات حول المسؤولية الجنائية عن الجرائم الكمبيوتر، إنما يتصل بالاعتداءات الموجهة إلى الكيانات غير المادية لنظام الكمبيوتر، والتي عّبر عنها بمعطيات الكمبيوتر، إذن فإن وقوع الجريمة على المكونات المادية لا تثير مشكلة على أساس أنها تتمتع بالحماية الجزائية وفقا لما ورد في قانون العقوبات بخلاف المكونات المعنوية ، رغم أن البعض يعتبرها ضمن جرائم الكمبيوتر، وهو رأي غير متفق عليه إذ تعتبر كذلك جرائم تقليدية [3].

وعليه فإن موضوع الجريمة الإلكترونية يتمثل في معطيات و المصلحة التي تهدرها والحق الذي تعتدي عليه هو الحق في المعلومات بذاتها، وبما تمثله من أموال أو أصول أو أسرار أو بيانات شخصية أولها قيمة بذاتها كالبرامج [4].

وعّرف الأستاذ **كاتالا** المعلومة بأنها "رسالة معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير، فهي تعبير تستهدف جعل رسالة قابلة للتوصيل إلى الغير، ثم هي قابلة للتوصيل بفصل علامة

---

1 – عبد الله عبد الكريم عبد الله، المرجع السابق ، ص17.

2– معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن ، مذكرة ماجيستر في العلوم القانونية التخصص قانون جنائي وعلوم جنائية ، جامعة الحاج لخضر، باتنة ، 2011–2012، ص 19.

3– عزيزة رابحي ، الأسرار المعلوماتية وحمايتها الجزائية، المرجع السابق ، ص110 .

4– علي حسن الطوالبة ، الجرائم الإلكترونية ، الطبعة الأولى ، جامعة العلوم التطبيقية ، مملكة البحرين ، 2008، ص82.

أو إشارة من شأنها أن توصل المعلومات للغير ، فالتعبير وتوصيله للغير يحقق وظيفة المعلومة وهي انتقال أو نقل المعرفة "[1].

وتعرف المعلومة أيضا " بأنها مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو المعالجة بواسطة الأفراد أو الأنظمة الإلكترونية ، وهي تتميز بالمرونة بحيث يمكن تغييرها ، وتجزئتها، وجمعها أو نقلها بوسائل وأشكال مختلفة [2].

كما عرفها المشرع الفرنسي لأول مرة في القانون الصادر في 29 يوليو سنة 1982 بشأن الاتصالات السمعية والبصرية بوصفها رنين صور الوثائق والبيانات أو رسائل من أي نوع وعلى هذا الأساس تعني المعلومة رمزا أو مجموعة رموز تخطو على إمكانية الإفضاء إلى المعني" [3].

هذا وعرفها المشرع الأردني في قانون المعاملات الإلكترونية لسنة 2001 بأنها" البيانات والنصوص والصور والأشكال والأصوات والرموز وقواعد البيانات وبرامج الحاسوب وما شابه ذلك"[4].

وتختلف المعلومات عن البيانات باعتبارها من المصطلحات التي ترتبط بها وجود أو عدمًا، وتعرف على أنها المعطيات الخام أو الأولية التي تتعلق بقطاع أو نشاط ما وتسمى العلاقة بينهما بالدورة الإستراتيجية للمعلومات إذ يتم تجميع وتشغيل البيانات والحصول على المعلومات ثم تستخدم هذه المعلومات في إصدار قرارات تؤدي بدورها إلى مجموعة إضافية من البيانات التي يتم تجميعها ومعالجتها مرة أخرى للحصول على معلومات إضافية يعتمد عليها في إصدار قرارات جديدة، وتعرف البيانات أيضا بأنها عبارة عن مجموعة من الحقائق التي تعبر عن مواقف وأفعال معينة، سواءا كان ذلك التعبير بالكلمات أو الرموز ولا تفيد هذه البيانات في شيء، وهي على صورتها الأولية ، لذلك فإن

---

1 - CATALA Pierre, Ebouche D'ume Théorie Juridique De L'information, D 1984, p,97.

2-أنظر: نهلا عبد القادر مومني ، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان – الأردن، 2008، ص 101. أنظر أيضا : Porker (Donnb), Op.Cit , P27

3 – عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات – دراسة مقارنة –، دار النهظة العربية، القاهرة ، 2000، ص 31.

4- عبد الرحيم بن بوعيدة ، ضياء علي أحمد نعمان ، موسوعة التشريعات الإلكترونية المدنية و الجنائية – التشريع المغربي و العربي و الفرنسي الاتفاقيات العربية و الأوروبية و الدولية، الجزء الثاني، الطبعة الأولى، المطبعة و الوراقة الوطنية، مراكش ، 2010، ص 55.

الأمر يستدعي تحليل هذه البيانات وإجراء العملية الحسابية والمنطقية عليها، أو بمعنى آخر معالجة البيانات للاستدلال منها على مجموعة من المعلومات إذن تتحول تلك البيانات إلى معلومات ، وبذلك تكون المعلومات هي النتيجة النهائية المترتبة على تشغيل البيانات وتحليلها أو استقراء دلالتها واستنتاج ما يمكن استنتاجه منها [1].

كما أن المعلومات هي ناتج معالجة البيانات تحليلا أو تركيب ،لاستخلاص ما تتضمنه البيانات أو تشير إليه من مؤشرات وعلاقات ومتعلقات وكليات وموازنات ومعدلات وغيرها[2]، فالبيانات هي مُدخلات الحاسب الآلي التي تمثل الخادمات التي يتم تشغيلها والمعلومات هي المخرجات بعد عملية المعالجة [3].

أما عن الفرق بين المعلومات والبرامج [4] باعتباره من العناصر الرئيسية للكيان المنطقي إلى جانب المعطيات لأي حاسوب ومن دونه يعتبر هذا الأخير مجرد مجموعة من معّدات فيكمن في الوظيفة التي يؤديه كل واحد منهما، فالغاية من وجود المعطيات تكمن فيها في حد ذاتها، إذ ليس لها دور معيّن في تشغيل الحاسب الآلي وإنما يعتبر هذا الأخير بمثابة المستودع الذي يتم فيه معالجة هذه المعطيات وتخزينها، ثم إتاحتها عند طلبها واسترجاعها وذلك للاطلاع عليها وتكوين معرفة أو دراية توفرها هذه المعطيات [5].

1- محمد محمد شتا ، فكرة الحماية الجنائية لبرامج الحاسب الآلي ، دار الجامعة الجديدة للنشر ،2012 ، ص 61.

2- محمد مصطفى الشقيري، السرية المعلوماتية ، ضوابطها وأحكامها الشرعية ، الطبعة الأولى، دار البشائر الإسلامية ، بيروت، لبنان 2008، ص 35.

3 – الموسوس عتو، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي و التكنولوجي –دراسة مقارنة– ، رسالة دكتوراه ، جامعة سيدي بلعباس ،2014–2015، ص، 31.

4 –للبرامج مفهومان أحدهما ضيق و الآخر واسع ، فالبرامج وفقا لمفهومه الضيق:" هو مجموعة من التعليمات و الأوامر الصادرة من الإنسان إلى الآلة أي إلى الكيان المادي للحاسب يسمح لها بأداء مهمته محددة "، أما المفهوم الواسع للبرنامج :" فهو يتضمن إضافة للمفهوم الضيق التعليمات و الأوامر الموجهة للعميل (مثل بيانات استعمال البرامج ، وكيفية المعالجة الإلكترونية للمعلومات)أي كل المعطيات أو البيانات أو المستندات الأخرى الملحقة بالبرامج والتي تساعد على تبسيط فهمه وتيسير تطبيقه. أنظر: محمد خليفة ، الحماية الجنائية لمعطيات الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية، 2007، ص 90.

5 – محمد خليفة، المرجع نفسه، ص 90.

أما البرامج فالغاية منه هو الوظيفة التي يقدمها، فليس مجرد الاطلاع على البرنامج وأخذ فكرة هو الهدف منه، بل أن وجوده بالحاسب له دور وهو القيام بمختلف العمليات التي يحتويها نظام الحاسب فهذا الأخير لا يقوم بعمله إلا عن طريق مجموعة من البرامج والتي تسمح بالقيام بمختلف العمليات عند إعطائها أوامر بذلك، فقيمته المعطيات والغاية منها تكمن فيما تحويه هي ذاته، أما قيمة البرامج فتكمن فيما يقوم به من وظائف في تشغيل الحاسب الآلي[1].

ونجد أن المشرع الجزائري عند تعريفه للمعطيات أدرج في مفهومها برامج الحاسوب حيث نصت المادة الثانية من القانون 04/09 السابق الذكر: "على أن المعطيات هي أي عملية عرض للوقائع أو المعلومات بما في ذلك البرامج المناسبة التي من شأنها أن تجعل المنظومة المعلوماتية تؤدي وظيفتها".

ولقد اختلف الفقهاء حول الطبيعة القانونية للمعلومات باعتبارها محلا يقع عليه الاعتداء كونها ذات طبيعة غير مادية ، فبينما يرفض جانب من الفقه اعتبار المعلومات كقيمة مالية إلا ما كان منها متعلقا لحقوق الملكية الأدبية أو الفنية أو الصناعية ، يرى جانب من الفقه الفرنسي بأن استبعاد المعلومات من طائفة الأموال لا يمنع عنها الحماية وفق قواعد المسؤولية التقصيرية [2] وذلك استنادا إلى نص المادة 1382 من القانون المدني الفرنسي أما الاتجاه الآخر فقد ذهب إلى إمكانية اعتبار المعلومات كقيمة مالية منهم الأستاذ الفرنسي **بيار كاتالا** ، الذي شبّه المعلومة بالسلعة، و أنها نتاج لعمل بشري وتنتمي إلى من يحوز العناصر المكونة لها بطريقة مشروعة وتكون في شكل يجعل منها صالحة للاطلاع عليها وتبليغها بشكل مفهوم، وعليه فيتوفر القيمة الاقتصادية لها المتمثلة لها في سعر السوق ، بالإضافة إلى تبعيتها لمالكها تصبح في ذاتها قيمة مالية بغض النظر عن الوسيط المادي الحامل لها بمعنى آخر، أن المعلومة ترتبط بصاحبها عن طريق علاقة قانونية وهي علاقة المالك بالشيء الذي يملكه[3].

---

1 – محمد خليفة، المرجع السابق، ص 90.

2– معتوق عبد اللطيف، المرجع السابق، ص 20.

3-LUCAS de Lyssac (Marie Paul),Une Information Seul Est-Elle Susceptible De Vol D'une Autre Atteinte Juridique Aux Bien . Dallozsiery ,1985,P43.

وأنظر أيضا: سامي جلال ففي حسين ، المرجع السابق ، 46.

ومن اللافت للنظر أن المعلومة الإلكترونية جديرة بالحماية عن المعلومات الورقية، وتظهر جدارة المعلومات المبرمجة آليا بالحماية الجنائية عن المعلومات التي تحتويها الملفات الورقية من ضعف النوع الأول من المعلومات ومن أهميته في آن واحد فالمعلومات المعالجة آليًا ضعيفة داخل النظام عنها داخل الملفات الورقية ، هذه الأخيرة يمكن إخفائها بسهولة عن المعلومات داخل النظام ، كما أن المعلومات المعالجة آليا تتميز بالضخامة و التنوع ، ومنها ما يتعلق بالحياة الخاصة للأفراد. كل هذه الاعتبارات دعت مشرعي كثير من البلاد إلى استحداث صور من التجريم لحماية المعلومات داخل الكمبيوتر من الاطلاع عليها، بينما لا يوجد مثيل لتلك النصوص بالنسبة للمعلومات المسجلة داخل الملفات الورقية [1].

كما أن المشرع يعلّق أهمية واضحة على حماية نظام المعلومات بالكمبيوتر الأمر الذي لم يوفره قانون العقوبات للملفات الورقية التقليدية التي تحتوي على معلومات من أهمية مماثلة .

ويرجع السبب في ذلك إلى أن من يدخل نظام الكمبيوتر غالبا ما يكون قد أخل بجرمه المكان دون أن يقوم بدخول هذا المكان في حالات كثيرة، يضاف إلى ذلك أن نظام الكمبيوتر يتيح التعرف على كمية هائلة من المعلومات بسهولة ويسر وفي وقت قصير، الأمر الذي لا يتوفر في حالة الملفات الورقية التقليدية [2].

المبحث الثاني: أساليب ارتكاب الجريمة الإلكترونية و دوافعها

عادة ما يسعى المجرم المعلوماتي إلى تحقيق مكاسب مادية من خلال إثبات مهارته الفنية الهائلة والمكتسبة لاختراق أنظمة محل الجريمة، وذلك عن طريق استعمال أساليب متنوعة في ارتكاب الجريمة الإلكترونية (المطلب الأول) فشغفه بالإلكترونيات هو ما يميزه عن غيره ، والكسب المادي والمعنوي أو حتى السياسي الغير المشروع هو الدافع، الباعث الحقيقي لارتكاب الجرائم الإلكترونية (المطلب الثاني).

1- شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 94.

2 - شيماء عبد الغني محمد عطا الله، المرجع نفسه، ص 94.

المطلب الأول: أساليب ارتكاب الجريمة الإلكترونية

تتنوع الوسائل التي تستخدم في العدوان على معطيات الحاسب الآلي، يستعمل من خلالها مجرمي المعطيات تقنيات مختلفة لتنفيذ جرائمهم، ولم يعد الحصول على هذه الأساليب حكرا على جهات أو أفراد معينين بل أصبحت متاحة للجميع ، حيث انتشرت الكثير من المواقع والكتب التي تتيح معرفة مختلف الأساليب التي يمكن استعمالها في هذه الجرائم، ولا يبقى معها لاقتحام باب الجريمة إلا التزود بالمعرفة اللازمة لهذا الاستعمال .

وتختلف الجريمة الإلكترونية باختلاف الهدف من وراء ارتكابها فقد تهدف إلى الأضرار بالحاسب وإعاقته عن أداء وظيفته، وقد تهدف أيضا إلى الحصول على منفعة من الحاسب الآلي كالاستيلاء على النقود أو الإطلاع على المعلومات، وهذه الجريمة ترتكب بإحدى الوسائل الآتية: الاختراق بأنواعه (الفرع الأول) والفيروسات بأنواعه[1] (الفرع الثاني).

الفرع الأول: الاخـــتراق

تـــعد جريمة الدخول غيَر المشروع لأنظمة المعالجة الآلية للمعطيات[2] من أهم جرائم الحاسب الآلـــي، إذ أن هذه الجريمة تعد منطلقا للعديد من الجرائم الأخرى وشرطا مفترضا لها، ويطلق على عملية الدخول غير المصّرح به لهذه الأنظمة تسمية الاختراق.

1- إضافة إلى الاختراق والفيروسات التي تعتبر من أهم الأساليب لارتكاب الجريمة الإلكترونية هناك أيضا طرق أخرى لارتكابها كتزييف البريد الإلكتروني، وإخفاء الشخصية على الانترنيت وما يسمى أيضا بالإغراق بالرسائل، وهذه الأساليب هدفها الأضرار بالمعطيات إما بهتك سريتها أو محوها أو تشويهها أو تعطيل أنظمة معالجتها. أنظر محمد خليفة، المرجع السابق، ص 56-58.

2 – نصت اتفاقية بودابست على هذه الجريمة في المادة الثانية تحت عنوان "الدخول غير قانوني "والتي تشير إلى أنه يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أي إجراءات يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقا للقانون الداخلي الولوج العمدي لكل أو جزء من جهاز الحاسب الآلي بدون حق كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن بغية الحصول على بيانات الحاسب أو أية نيّة إجرامية أخرى أو ترتكب الجريمة في الحاسب آلي يكون متصلا عن بعد لحاسب آلي آخر وجرّم السلوك أيضا القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات لعام 2004 في المادة الثانية بقولها : "كل من دخل عمدا وبغير وجه حق موقعا أو نظاما معلوماتيا يعاقب بالحبس ...والغرامة ...أو بإحدى هاتين العقوبتين " وأيضا نصت عليها المادة 6 منه، أما الشرع الفرنسي فجرم هدا الفعل في المادة 1/323 من القانون العقوبات الفرنسي.

فالجريمة الإلكترونية تتميز بارتكابها من طرف مجرمين يستعملون كل ما من شأنه خداع الحاسب الآلي و التحايل على أنظمته المعلوماتية ، وبالرغم من أن هذه الوسائل يمكن حصرها في الوقت الراهن ، إلا أنه لا يمكن التنبؤ بالوسائل الأخرى التي قد تستحدث في مجال تكنولوجيا المعلومات .

فالاختراق والمخترقون أو الهاكرز كلمة تخيف العديد من الناس، وخصوصا مستخدمي الانترنيت الذين يطمحون إلى حماية أسرارهم من هؤلاء الهاكرز، وكثيرا ما تكون عملية الاختراق عشوائية، بمعنى أن المخترق لا يعرف جهاز أحد الأشخاص بعينه ويقوم باختراقه [1].

أولا: تعريف الاختراق

الاختراق هو قدرة طرف على دخول إلى جهاز طرف آخر بغض النظر عما يلحقه به، ويتم ذلك بطريقة غير مشروعة أو بدون إذن الطرف الآخر (المخترقة).

والاختراق بشكل عام هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة.

والاختراق يمكن أن يتم بوصول المخترق نفسه إلى جهاز الضحية واطلاعه مباشرة على ما يحتوي عليه من معطيات، وإما أن يتم عن بعد، أي الوصول إلى تلك المعلومات عن طريق كمبيوتر آخر غير الكمبيوتر الضحية[2].

كما جرم المشرع الجزائري كلا من الفعل والنتيجة في المادة 394 مكرر من ق.ع.ج" فالفعل هو الدخول غير مصرح به و النتيجة تشديد المشرع للعقاب إذا ترتب على هذا الفعل حدوث أضرار بالمعلومات ونظم معالجتها ، حيث أن الدخول غير المشروع لأنظمة المعالجة الآلية للمعطيات هو إساءة استخدام الحاسب الآلي ونظامه عن طريق شخص غير مرخص له باستخدامه و الدخول إليه للوصول إلى المعلومات و البيانات المخّزنة بداخله لاستخدامها في غرض ما أو لمجرد التسلية و الرغبة في الاستطلاع ولإشباع الشعور بالنجاح في اختراق الحاسب الآلي رغم الاحتياطات الأمنية التي يحتويها نظامه للحيلولة دون ذلك .

1 – عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، المرجع السابق ، ص 124.

2– محمد خليفة ، المرجع ،السابق ، ص 40–41. أنظر أيضا: نسرين عبد الحميد نبيه، المرجع السابق ، ص 145.

فعملية الاختراق الإلكترونية تتم عن طريق تسريب البيانات الرئيسية و الرموز الخاصة ببرامج شبكة الأنترنيت وهي عملية تتم في أي مكان في العالم دون الحاجة إلى وجود شخص المخترق في الدولة التي يتم اختراق مواقعها، فالبعد الجغرافي لا أهمية له في الحد من الاختراقات المعلوماتية، ولا تزال نسبة كبيرة من الاختراقات لم تكشف بعد بسبب التعقيد الذي يتصف به نظم تشغيل الحاسبة الإلكترونية و الشبكات المعلوماتية [1].

ثانيا: أنواع الاختراق ووسائله

لقد تضاعفت حالات الاختراق وتدمير المواقع[2] بسبب اكتشاف المزيد من الثغرات الأمنية[3] في أنظمة التشغيل و البرامج المستخدمة في مزودات الأنترنيت، ويعد الاختراق من أهم وسائل ارتكاب الجريمة الإلكترونية.

1- علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، 2011، ص 87.

2- هناك عدة أسباب لوقوع عملية تدمير المواقع منها:

1/ ضعف الكلمات السرية فبعض مستخدمي الأنترنيت يجد أن بعض الكلمات أو الأرقام أسهل في الحفاظ فيستخدمها، مما يسهل عملية كسر وتخمين الكلمات السرية من المخترق.

2/ عدم وضع برامج حماية كافية لحماية الموقع من الاختراق أو التدمير وعدم التحديث المستمر لهذه البرامج و التي تعمل على التنبيه عند وجود حالة اختراق للموقع.

3/ إستضافة الموقع في شركات غير قادرة على تأمين الدعم الفني المستمر، أو تستخدم برامج و أنظمة غير موثوقة أمنيا ولا يتم تحديثها بإستمرار.

4/ عدم القيام بالتحديث المستمر لنظام التشغيل و الذي يتم في كثير من الأحيان اكتشاف المزيد من الثغرات الأمنية فيه،و يستدعي ضرورة القيام بسد تلك الثغرات من خلال ملفات برمجية تصدرها الشركات المنتجة لها امنع المخربين من الاستفادة منها.

5/ عدم القيام بالنسخ الإحتياطي للموقع للملفات و المجلدات الموجودة فيه، وعدم القيام بنسخ قاعدة البيانات الموجودة بالموقع مما يعرض جميع المعلومات في الموقع للضياع و عدم استرجاعها.

3- حذرت شركة مايكروسفت من وجود ثغرة في أدوات المساعدة في معظم إصدارات نظام ويندوز وتقول الشركة : إن هذه الثغرة يمكن أن تسمح للهاكرز بالتحكم في حواسيب المستخدمين، بينما صنفت الشركة الثغرة بأنها حرجة ودعت المستخدمين إلى تركيب برنامج ترقيمي لحل المشكلة أنظر : علي عدنان الفيل، الإجرام الإلكتروني، المرجع السابق، ص 91.

1- أنواع الإختراق:

للمخترق أسس و طرق يستطيع عبرها التطفل على أجهزة الآخرين فهو على دراية تامة بأهم الثغرات للولوج إلى بوابات الأجهزة عن طريق برامج خاصة معتمدة لفك أصعب الشفرات، وتتمثل أنواع الاختراق فيما يلي:

أ- **اختراق الأجهزة الخادمة:** ويتم عن طريق ما يسمى بالمحاكاة، وهي القيام بانتحال شخصية مسموح لها بالدخول إلى هذه الأجهزة، وذلك باستخدام طريقة تسمى مسارات المصدر، وفيها يتم إعطاء حزم عناوين "IP"[1] معينة لتبدو وكأنها صادرة من كمبيوتر مسموح له بالدخول إلى تلك الأجهزة .

وتعتبر وسيلة انتحال الشخصية [2] من أسهل الطرق المستخدمة في دخول إلى أنظمة الحاسب الآلي وهنالك وسيلتان لانتحال الشخصية هما: انتحال الشخصية باستخدام التقنيات غير عالية الكفاءة أو ما يطلق عليها الانتحال للشخصية بدائيا فقط، ويتم ذلك عن طريق استخدام المجرم البطاقة أو كارت خاص بشخص مسموح له بالدخول، وهذا النوع يعتبر بسيط من الناحية التقنية على الرغم مما يسببه من أخطار ونتائج ضار، و انتحال الشخصية باستخدام التقنيات العالية، أو ما يطلق عليها التنكر الإلكتروني بحيث ينتحل الشخص شخصية آخر باستخدام اسم هذا الشخص عن طريق إرسال بريد إلكتروني مدعيا أنه شخص آخر وهي من أسهل أنواع التنكر الإلكتروني.

1- Adress IP: يتطلب تشغيل نظم الاتصالات الكمبيوترية أن تكون هناك آلية من أجل عنونة الأجهزة سواءا المرسلة أو المستقبلة ،كما تتطلب أيضا أن تكون هناك آلية لضمان وصول أو التحقق من وصول الاتصال أو الرسالة للجهة المقصودة والتحقق من جهة الإرسال ويستخدم في تحقيق هذه الغاية بروتوكول الأنترنيت (IP)، أنظر: سعيداني نعيم، المرجع السابق، ص 57.

2- في هذا الصدد يمكن القول بأن انتحال شخصية الأفراد يكون الاستفادة من سمعتهم أو مالهم وصلاحيتهم، هذا الانتحال يمكنه القيام بذلك عن طريق المعلومات التي تتعلق بتلك الشخصية كالاسم والعنوان ورقم الهوية ويستغلها استغلالا سيئا والتي يحصل عليها من الأنترنيت ويمكن أن تؤدي هذه الجريمة إلى استنزاف رصيد الضحية في البنك أو الإساءة إلى سمعته، وقد تكون وسيلة= = المجرم إلى ارتكاب جريمة النصب مستفيدا من السمعة الطيبة لتلك الشخصية .أنظر : نبيلة هبة هروال، الجوانب الإجرائية لجرائم الأنترنيت في مرحلة جمع الاستدلالات ، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية ،2007، ص61.

وتتمثل خطورة هذه الوسيلة في عدم مقدرة جهاز الحاسب الآلي في التفرقة بين المستخدم الأصلي ومنتحل الشخصية [1].

ب- التعرض للبيانات أثناء انتقالها: وتستخدم هذه الطريقة للتعـرف على أرقام بطاقات الائتمان أثناء انتقالها من المشتري إلى موقع التسوق [2].

ت- اختراق الأجهزة الشخصية: وهي الطريقة الأكثر شيوعا نظرا لتوفر العديد من برامج الاختراق سهلة الاستخدام، ويشترط في الاختراق باستخدام البرامج وجود برنامجين أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم لأنه يأتمر بأوامر المخترق وينفذ المهام الموكلة إليه داخل جهاز الضحية، وبرنامج آخر يوجد بجهاز المخترق ويسمى بالبرنامج المستفيد، وأخطر هذه البرامج برنامج حصان طروادة لقدرته على الإختراق دون إمكانية كشفه وتتبعه و القضاء عليه واحتلال هذا البرنامج مكانا داخل النظام المخترق حتى ولو قام الضحية بحذفه فلا فائدة من ذلك، كما أنه يكفي لهذا البرنامج أن يعمل لمرة واحدة فقط حتى يقوم بمهامه يمكن إرساله للضحية عن طريق رسائل إلكترونية أو عن طريق برامج الدردشة[3].

ومن برامج أيضا التي تختص بكسر كلمة السر الخاصة بتشغيل الجهاز برنامج (Revelation) ومهمته تنحصر في كشف كلمة السر المخزنّة في نظام التشغيل والتي تتطلبها الشاشة عند بداية العرض عندما يطلب كتابة كلمة السر بحيث يضغط المستخدم على مفتاح (Enter) فقط، وبالتالي يستطيع الدخول إلى أنظمة الحاسب الآلي[4].

والتسلل إلى جهاز الضحية يحتاج إلى مجموعة من الأدوات الخاصة، هذه الأخيرة قد تكون بعض البرامج الموجودة داخل نظام التشغيل نفسه أو بعض البرامج التي صممت خصيصا لتسهيل عمليات الإختراق وتجنب استخدام العديد من الأوامر المعقدة.

1- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 313.

2- محمد خليفة ، المرجع السابق ، ص 41 . وأنظر أيضا : نسرين عبد الحميد نبيه، المرجع السابق، 145.

3- نعيم سعيداني، المرجع السابق، ص 57.

4 - محمد خليفة، المرجع السابق، ص41.

2- وسائل الإختراق :

وبالرغم من وسائل الأمان في البرامج المختلفة لأنظمة التشغيل إلا أنها تبقى نسبية أمام المنافذ السهلة والمتاحة لمرتكب الجريمة الإلكترونية، ليصبح الجهاز المخترق بعدها أداة بعدما كان هدف يأتي على شكل هجمات إلكترونية لا تتطلب خبرة كافية و تقنية عالية فهي ببساطة تعتمد على الخطأ البشري لكي تنجح.

أ- الاختراق عن طريق إستخدام نظام التشغيل :

لأن نظم التشغيل مليئة بالثغرات كما ذكرنا سابقا ، فإنه يتم استغلالها في عمليات الاختراق، ولكن الأهم هو القيام بذلك عن طريق البروتوكولات[1] التي يستخدمها النظام للتعامل مع شبكة الأنترنيت أو الشبكات الداخلية بأنواعها ويمر المتسلل بعده مراحل حتى يتمكن من اختراق الحاسب الآلي لغيره وهي :

يبحث المخترق أولا عن ضحيته، وذلك بمعرفة (IP)[2] الخاص به و البحث عن هذا الرقم يتم بمجموعة من الخطوات يقوم بها المخترق على جهازه ، لكن يجب أن يكون كذلك متصلا بجهاز الضحية عن طريق شبكة الأنترنيت أو شبكة داخلية ، وذلك في لحظة معينة ، لأن هذا الرقم يتغير دائما مع كل اتصال جديد بالأنترنيت[3]، و بعد تحديد IP يحدد المخترق إمكانية اختراق جهاز الضحية عن طريق مجموعة من الخطوات كذلك [4].

---

1 -البروتوكول هو نظام خاص بتنظيم تبادل البيانات داخل الشبكات بين مختلف الحواسب الالية المرتبطة ببعضها والتي تستخدم أنظمة تشغيل مختلفة مثلNT, UNIX WINDOWS 98 ، فيتدخل البروتوكول ليمكن من تبادل البيانات بينها بغض النظر عن أنظمة تشغيلها .

2- الـــــIP: هو اختصار لكلمة Internet Adress Protocol ، وهو رقم خاص يميز به الحاسب الآلي المتصل بشبكة الأنترنيت أو شبكة داخلية عن باقي الأجهزة المتصلة بها، وهو يتكون من أربعة أجزاء، وكل جزء يتكون من ثلاثة أرقام كحد أقصى منفصلة عن بعضها البعض بنقطة، وكل رقم لا يزيد عن 255.

3- محمد أمين الرومي، جرائم الكمبيوتر و الأنترنيت، دار المطبوعات الجامعية، الإسكندرية، 2003، ص 137.

4- محمد خليفة، المرجع السابق، ص 42.

ب-تشمم كلمات السر جمعها و التقاطها :

تعتبر كلمة السر خط الحماية الأول الذي يُعتمد عليه نسبة كبيرة من مستخدمي أجهزة الحاسب الآلي، ولذلك فإن أول خطوة يقوم بها القراصنة هي التعامل معها لكي يتمكنوا من الدخول إلى أنظمة الحاسب الآلي، وبالتالي يفتح الطريق أمامهم لارتكاب جرائمهم[1].

وإذا كانت أنشطة الاعتداء التي تتم باستعمال السر تتم غالبا عن طريق تخمين كلمات السر مستفيدة من ضعف الكلمات عموما وشيوعا اختيار الأفراد لكلمات سهلة تتصل بمحيطهم الأسري أو محيط العمل أو حياتهم الشخصية[2]، فإن جديد استخدام برمجيات يمكنها تشمم أو التقاط كلمات السر خلال تجوالها في جزء من الشبكة أو أحد عناصرها ومراقبتها ومتابعتها لحركة الاتصال على الشبكة، بحيث يقوم هذا البرنامج من حيث الأصل بجمع أول 128 بابت أو أكثر مثلا من كل اتصال بالشبكة التي تجري مراقبتها تتبع حركة الاتصال عليها، وعندما يطبع المستخدم كلمة سر أو اسمه فإن البرنامج (الشمام) يجمع هذه المعلومات وينسخها، إضافة إلى أن أنواعا من هذه البرامج تجمع المعلومات الجزئية وتعيد تحليلها وربطها معا، كما تقوم بعضها بإخفاء أنشطة الالتقاط بعد قيامها بمهمتها [3].

ت-المسح والنّسخ :

وهو أسلوب يستخدم فيه برنامج الماسح وهو برنامج احتمالات يقوم على فكرة تغيير التركيب أو تبديل احتمالات المعلومة ، ويستخدم تحديدا بشأن احتمالات كلمة السر أو رقم الهاتف الموزّع أو نحو ذلك، وأبسط نمط فيه عندما تستخدم قائمة الاحتمالات لتغيير رقم هاتف بمسح قائمة أرقام كبيره للوصول إلى أحدها الذي يستخدم موزع للاتصال بالأنترنيت، أو إجراء مسح الاحتمالات عديدة لكلمة

1- أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 310.

2 - يلجأ مستخدموا الأجهزة إلى استخدام كلمات السر القصيرة لضمان عدم نسيانها، ولذلك فإنّ المستخدم يلجأ إلى كتابة تاريخ ميلاده أو إسم زوجته أو أحد أبنائه ، فإن كان المخترق على معرفة بهذا الشخص فإن هذا يوفر عليه بعض من الوقت أما إذا كان غير ذلك لابد من التحّلي بالصبر لإمكانية معرفة كلمة السر.

3 -محمد خليفة، المرجع السابق، ص 44.

السر للوصول إلى الكلمة الصحيحة التي يمكن المخترق من الدخول للنظام، ومن جديد فإنّ هذا الأسلوب تقني يعتمد واسطة تقنية هي برنامج الماسح بدلا من الاعتماد على التخمين البشري[1].

ث- هـــجومات استغلال المزايا الإضافية:

الأمر هنا يتصل بواحد من أهم استراتيجيات الحماية فالأصل أن مستخدم النظام تحديدا داخل المؤسسة يحدد له نطاق الاستخدام ونطاق الصلاحيات بالنسبة للنظام، ولكن في الواقع العملي يحدث أن مزايا الاستخدام يجري زيادتها دون تقدير لمخاطر ذلك أو دون علم من الشخص نفسه أنه يحظى بمزايا تتجاوز اختصاصه رغباته في هذه الحالة، فإن أي مخترق للنظام لن يكون قادرا فقط على تدمير معطيات المستخدم أو التلاعب بها، من خلال اشتراكه أو عبر نقطة الدخول الخاصة به، وبـــكل بساطة سيتمكن من تدمير مختلف ملفات النظام حتى تلك غير المتصلة بالمدخل الذي دخل منه لأنه استثمر المزايا الإضافية التي يتمتع بها المستخدم الذي تم الدخول عبر مدخلة، وأعظم مثال على هذا الخطر في العالم المادي أنه يمكّن شخص من دخول غرفة مدير فندق لقصد سرقته فيجد في غرفته مفاتيح كافه قاصات الأمانات ، أو مفتاح الماستر الذي يفتح غرف الفندق جميعها ، ولهذا فتحديد الامتيازات و الصلاحيات قد يمنع في حقيقته من حصول دمار شامل و يجعل الاختراقات غير ذات أثر[2].

ح-الهندسة الاجتماعية :

الهندسة الاجتماعية هي أسلوب من الأساليب الاختراق التي تعتمد على العنصر البشري، وليس لها أية أبعاد تقنية، بحيث يستعمل فيها أساليب الخداع والكذب للحصول على معلومات ذات طابع تقني حتى أن أشهر الهاكرز كيفن ميتينك ذكر في كتاب ألفه بعنوان " **فن الخداع** " أن أكثر الاختراقات التي قام بها كانت باستخدام هذا الأسلوب [3].

1- محمد خليفة ، المرجع السابق، ص 44-45.

2 - محمد خليفة، المرجع نفسه، ص 45.

3-حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت- دراسة مقارنة -، دار النهضة العربية، القاهرة،2009، ص 341-342.

وفي هذه الطريقة يحصل المخترق على معلومات تهيأ له الاختراق من خلال علاقات اجتماعية، وذلك باستغلال الشخص أحد عناصر النظام –أشخاص بإيهامه بأي أمر يؤدي إلى حصوله على كلمة مرور أو على أية معلومات تساعد في تحقيق اعتدائه، كأنه يتصل شخص بأحد العاملين ويطلب منه كلمة سّر النظام تحت زعم أنه من قسم الصيانة أو قسم التطوير، وطبيعة الأسلوب الشخصي في الحصول على معلومة الاختراق سميّت بالهندسة الاجتماعية [1] .

خ–التفتيش في مخلفات التقنية:

وهو القيام بالبحث في مخلفات المؤسسة من القمامة و المواد المتروكة بحثا عن أي شيء يساعده على اختراق النظام ، كالأوراق المدون عليها كلمات السّر، أو مخرجات الكمبيوتر التي قد تتضمن معلومات مفيدة ، أو الأقراص الصلبة المرمية بعد استبدالها، أو غير ذلك من المواد المكتوبة أو الأقراص أو الملاحظات أو أي أمر يستدل منه على أية معلومة تساهم في الاختراق، وقد حدث أن بيعت من قبل وزارة العدل الأمريكية مخلفات أجهزة تقنية بعد أن تقرر إتلافها، وكان من ضمنها نظام كمبيوتر يحتوي قرصه الصلب على كافة العناوين الخاصة ببرنامج حماية الشهود، وبالرغم من أنه لم يتم فعليا استثمار هذه المعلومات، إلا أن مخاطر كشف هذه العناوين استدعى إعادة نقل كافة الشهود وتغيير مواطن إقامتهم وهوياتهم وهو ما ألحق تكلفة مالية باهضه[2].

ج–إنتحال شخصية المواقع :

هذا الأسلوب يعتبر حديثا نسبيا بين الجرائم الإلكترونية، ولكنه الأشّد خطورة و الأكثر صعوبة في اكتشافه من انتحال شخصية الأفراد، ويقوم الفاعل بهذه الجريمة من خلال وضع نفسه في موقع بيني بين البرامج المستعرض Browser للحاسب الخاص بأحد مستخدمي الأنترنيت وبين الموقع Web، ومن هذا الموقع البيني يستطيع حاسب المجرم أن يتصرف وكأنه صاحب الموقع الحقيقي، ويستطيع مراقبة أي معلومة متبادلة بين الضحية الذي يزور الموقع وبين الموقع نفسه، كما يستطيع سرقة هذه المعلومات أو تغييرها، ولكن القيام بهذه العملية حتى لو تم الاتصال بالموقع من خلال ما يسمى بنظم الاتصال الآمنة .

1–محمد خليفة، المرجع السابق، ص 46.

2– محمد خليفة، المرجع نفسه، ص 48.

وكل ما يحتاجه من يقوم بهذه العملية هو السيطرة على أحد المواقع التي تتم زيارته بكثير وتحويلها ليعمل كموقع بيني وتحتاج عملية التحويل هذه المهارة خاصته برمجة المواقع Web Programming أو إلى قيام المجرم باختراق موقع لأحد مقدمي الخدمة المشهورين، ثم يقوم بتركيب البرنامج الخاص به هناك ، وبمجرد أن يكتب مستخدم الأنترنيت اسم هذا الموقع فإنه يقع في المصيدة و يدخل إلى الموقع المشبوه الذي أعده المجرم إذ أن هذا الأخير قام بتغيير أحد الروابط في الوسط بين المستفيد والموقع الشهير، ويستطيع من ذلك أن يتلصص على المعلومات المتبادلة بينها[1].

ثالثا: الحماية الفنية من الاختراق:

هناك من يوصي بإجراءات وقائية لتجنب الاختراق، كإخفاء الملفات وإغلاقها بكلمات سريّة، وعدم ترك أي ملفات مهمة على الجهاز، بل تحفظ في أسطوانات خارجية وتُشغل عند الحاجة، فلا يجد المخترقون إليها سبيلا، لكن ليس هذا بالحل الأمثل لأنه كفيل بتجريد المستخدم من منافع الحاسب الآلي، والحل يكمن في حماية الحاسب بمجموعة من البرامج تثبت عليه، وهي تنقسم إلى قسمين، برامج مضادات الفيروسات والجدران النارية [2]، فأما الأولى فتقوم بمراقبة أي ملف يقوم المستخدم باستخدامه للتأكد من خلوه من الفيروسات لأنها تعتبر ملفات أحصنة طروادة بمثابة فيروسات، وتعطي المستخدم الخيار في استخدام الملف من عدمه، أما الجدران النارية فهي برامج صغيرة تثبت داخل النظام بغرض مراقبة المنافذ التي يتم من خلالها نقل البيانات من وإلى الجهاز أثناء التعامل مع شبكة الأنترنيت[3]، وذلك عن طريق مراقبة الحزم التي يتم إرسالها واستقبالها من الكمبيوتر الخاص

1- محمد خليفة، المرجع السابق، ص 48.

2- أخذ مفهوم الجدار الناري من الاستعداد الأمني القديم و المتمثل في حفر خندق حول قلعة، مما يمنع أي شخص من الدخول أو الخروج من جسر القلعة ويمكن تفتيشه من قبل المعنيين ، إذ يعمل الجدران النارية كالجسر الإلكتروني يراقب الدخول إلى الشبكة والخروج منها، ويعرف: بأنه مجموعة أنظمة توفر أساليب أمنية بين الانترنيت وشبكة المؤسسات أو الشركات وغيرها لكي تجبر جميع عمليات الدخول إلى الشبكة و الخروج منها أن تمر من خلال الجدران الناري الذي يقوم بصد اختراقات المستخدمين المتطفلين، وهو يوفر في ذات الوقت حواجز أمنية قبل الدخول الموقع المعني، مثل التحقق من المستخدمين المحليين والخارجيين ونظام الدخول والخروج. أنظر: وليد الزيدي، القرصنة على الأنترنيت والحاسوب، الطبعة الأولى، دار أسامة للنشر والتوزيع، عمان، الأردن، 2003، ص 101.

3- فوظيفة الجدار الناري تنحصر في أنه يوم يقوم بعملية مسح للمعلومات التي تصل إليه من شبكة الأنترنيت ويقوم بتحليلها وعندما يجد أي شك في المعلومات التي تصل إليه لمحاولة الدخول أو الاختراق إلى المناطق المؤمنة، فإنه

بالمستخدم، والحزمة هي الأجزاء الصغيرة التي يتم تجزئة الملفات إليها، وعند مراقبة الحائط الناري لهذه الحزم والمنافذ التي ترسل وتستقبل من خلالها فإن عليه السماح أو الاعتراض على دخول هذه البيانات أو خروجها، وتنبه المستخدم لذلك وإجباره بالمنفذ وإلى أي جهة يريد الخروج إليها، ليقوم المستخدم بالسماح بذلك أو عدم السماح به[1].

الفرع الثاني: الفيروسات

يعتبر فيروس الحاسب من أهم وسائل المساس بالأنظمة والمعطيات المعلوماتية ومن أخطر آفات الشبكات المعلوماتية، حيث يعد بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين، وفيروس الحاسب الآلي يشبه الفيروس الذي يصيب الإنسان إلى حدّ كبير فانتقاله من حاسب لآخر إلى حد كبير عدوى الفيروسات التي تصيب الإنسان وتنتقل من جسم لآخر، كما أنه يشبه الحاسب الآلي عبر مراحل عدّة وتظهر أعراض هذه الإصابة على الحاسب[2]، كما أن هذه الفيروسات عديدة ومتنوعة وقد أنشأت شركات ضخمة تقوم بتصنيع برامج للحماية منها.

وتتصف الفيروسات بعد تكاثرها داخل جهاز بقدرتها الفائقة على الانتشار في أجهزة الحاسب المتصلة والشبكات العامّة والخاصة والمتعلقة بالإتصال بين الحواسيب، الأمر الذي يؤدي إلى تدمير البرامج والمعلومات المخزنة داخل الجهاز وتعطيل الحاسب عن القيام بوظائفه الطبيعية، وتضليل مستخدميه وضياع بياناته وتحويله إلى آلة صماء لا فائدة منها[3] .

وعموما يستخدم الفيروس لتحقيق أحـــد الــغرضين:

- **الغرض الحمائي:** ويكون ذلك لحماية النسخة الأصلية من خطر النسخ غير المرخص به، فينشط الفيروس بمجرد النسخ ويدمر نظام الحاسوب الذي يعمل عليه، ويعد ذلك بمثابة عقوبة تلحق بالناسخ.

يقوم بمنع هذه المحاولة وطردها خارج الشبكة أما إذا كانت المعلومات عادية وآمنة فإن الجهاز يسمح لها بالمرور والدخول على أجهزة الحاسبات الآلية. أنظر: أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 394-395.

1- محمد خليفة، المرجع السابق، ص 48-49.

2- محمود أحمد عبابنة، المرجع السابق، ص101.

3- محمود أحمد عبابنة، المرجع نفسه، ص 101.

- **الغرض التخريبي:** ويتم إعداد هذه الفيروسات من طرف خبراء البرامج بهدف التخريب بحد ذاته[1]، أو إلى التخريب بهدف الحصول على منافع شخصية[2].

أولا: تعريف الفيروس وخصائصه:

تعددت تعريفات الفيروسات التي تصيب الحاسبات الآلية ومكوناتها المنطقية، التي تؤدي إلى إتلافها وتدميرها لدي المتخصصين في الجرائم الإلكترونية فمنهم من عرفها بأنها: "مجموعة من التعليمات المرمّزة ، تنتج لنفسها نسخا مطابقة تلحق من تلقاء ذاتها ببرامج التطبيقات ومكونات النظام المنفذ لتقوم في مرحلة معينة بالتحكم في أداء النظام الذي أصابته "، ومنهم من عرفها بأنها: "مجموعة من التعليمات التي تتكاثر بمعدل سريع جدا لدرجة تصيب النظام المعلوماتي بالشلل التام "، أو هي: " خلايا كهرومغناطيسية نائمة ومبرمجة بحيث تنشط في وقت محدد لتخريب البرنامج الأصلي، وتنتشر في الأجهزة الأخرى تضمها الشبكة بحيث تفسد ما تحتويه من معلومات "، ومنهم من عرف الفيروس أيضا بأنه: " برنامج حاسب مثل أي برنامج تطبيقي أخر، ولكن يتم تصميمه بواسطة أحد المخربين بهدف محدّد، وهو إحداث أكبر ضرر ممكن بنظام الحاسب، ولتنفيذ ذلك يتم إعطاءه القدرة على ربط نفسه بالبرامج الأخرى، وكذلك إعادة إنشاء نفسه حتى يبدو وكأنه يتكاثر ويتوالد ذاتيا ، وهذا ما يتيح له قدرة كبيرة على الإنتشار ببرامج الحاسب المختلفة، وكذلك بين مواقع مختلفة في ذاكرة حتى يحقق أهدافه التدميرية "[3].

وهناك فارق بين فيروس الحاسب الآلي و فيروس الأنترنيت ، حيث يتميز فيروس الأنترنيت بإمكانية إنتشار هائلة ، وغير محدودة ، كونه يستمر في الإنتشار ولو لم يتم إغلاق الحاسب أو النظام كله، كما يختلفان من حيث الدور الذي يلعبه كلا منهما، حيث يقوم فيروس الأنترنيت بدور

1- حيث أن الأوامر المكتوبة في البرامج تقتصر على أوامر تخريبية تلحق ضررا بنظام المعلومات أو البيانات. أنظر: عمرو عيسى الفقي، الجرائم المعلوماتية-جرائم الحاسب الآلي والأنترنيت في مصر والدول العربية-، المكتب الجامعي الحديث، مصر، بدون سنة نشر، ص 230.

2- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1993، ص 190. أنظر أيضا: نهلا عبد القادر المومني، المرجع السابق، ص 127.

3 -محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 159-160، وأنظر أيضا : سيف بن الراشد الحوسني، جرائم التجارة الإلكترونية- دراسة مقارنة-، السحاب للنشر والتوزيع، سلطنة عمان ، 2010، ص 66. وأنظر أيضا : محمد خليفة، المرجع السابق، ص 50.

المخرب والمختلس للمعلومات خلافا لفيروس الحاسب الذي يقتصر دوره على التخريب فقط، كما أن فيروس الأنترنيت يفوق قدرة فيروس الحاسب الآلي ، فالأول يقوم بدوره طالما أن شبكة الأنترنيت تعمل ولو تم إغلاق أجهزة الحاسب الآلي، في حين النوع الثاني يبقى في جهاز المصاب به ولا ينتقل إلى الجهاز الآخر، إلا بالعدوى عن طريق ملف أو برنامج ما من الجهاز المصاب إلى آخر أو ينتقل عن طريق القرص الصلب أو القرص الممغنط أو جهاز USB[1].

وعادة ما يقوم الفيروس بإصابة الحاسب دون أن يشعر المستخدم بذلك، حيث أن الأوامر المكتوبة في البرامج تكون بغرض إلحاق ضرر بالكمبيوتر أو السيطرة عليه [2].

والخطر الأساسي للفيروس المعلوماتي يكمن في إمكانية استجماعه سائر مقومات التخريب الموزعة على ماعداه من برامج ، وتغيير شكل و مضمون النسخ التي ينتجها من نفسه حتى تتكيف مع المحيط الذي تستقر فيه [3]، وسرعة انتشاره وإمكانية استخدامه في إحداث تغيير لوغاريتمي للبيانات أو محوها أو تدمير نظام الحاسب بأكمله كما سبق القول منذ قليل .

وعموما فإنه يمكن إجمال خصائص فيروسات الحاسب الآلي فيما يلي :

أ-**القدرة الفائقة على الاختفاء** : فالفيروس ما هو إلا برنامج له القدرة الفائقة على إخفاء نفسه على الضحية مستخدم جهاز الحاسب الآلي، ويستخدم في إخفاء نفسه وسائل متعددة منها مثلا: ارتباطه بالبرامج شائعة الاستخدام ، حيث أن كل مستخدم للحاسب الآلي تهتم بتوفير اكبر قدر ممكن من البرامج التي تمكنه من الاستفادة بخصائص حاسبة الشخص، وأغلب المستخدمين يقومون بنسخ هذه البرامج دون السؤال عن مصدرها، وعن تشغيلها ينتقل الفيروس إلى القرص الصلب، ويقوم بأداء أعماله التخريبية بل هناك من الفيروسات ما يدخل الحاسب الآلي كملفات متخفية بحيث لا يستطيع المستخدم ملاحظة وجودها على شاشات الحاسبات عن طريق فهرس الملفات، وبعض الفيروسات تقوم بالاستقرار في أماكن معيّنة يصعب على المستخدم ملاحظتها حتى تشير الساعة إلى تاريخ معين فتقوم بتشغيل نفسها وتنفيذ أعمالها التدميرية، كما أن بعض الفيروسات تقوم بإخفاء أي أثر يدل على

---

1 -الموسوس عتو، المرجع السابق، ص 135.

2- عبد الصبور عبد القوي علي مصري، الجريمة الإلكترونية، الطبعة الأولى، دار العلوم للنشر والتوزيع، القاهرة، 2008، ص 47.

3- محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 162.

وجودها، حيث تظل البرامج المحتوية عليها تعمل بكفاءة دون أخطاء ولمدة طويلة، وفي ذات الوقت يقوم الفيروس بالانتقال من برنامج إلى آخر بخفة وروية [1].

ب–الانتشار: لفيروس الحاسب الآلي قدرة فائقة على الانتشار تفوق قدرة الفيروس الحيوي أو البيولوجي، حيث أنّه يمكن لفيروس حاسب آلي أن ينتقل إلى الملايين من أجهزة الحاسبات الآلية الخاصة بالمستخدمين الضحايا في نفس الوقت، كما يمكن في ثواني معدودة أن ينتقل من قادة إلى أخرى .

ت–القدرة على اختراق: تتميز فيروسات الحاسب الآلي بقدرة فائقة على اختراق نظام البيانات المعلومات بالحاسب الآلي، وكذلك الموانع التي يقيمها المستخدم.

ث– القدرة على التدمير :عندما يدخل فيروس الحاسب الآلي[2] إلى جهاز الحاسب الخاص بالضحية، فإنه يظل ساكنا حتى تبدأ لحظة الصفر التي يبدأ عندها في النشاط والحركة، وساعة الصفر هذه إما أن تكون كلمة معينة يكتبها مستخدم الحاسب الآلي أو الجاني المعلوماتي، أو إشارة معينة، أو عند تاريخ معيّن في السنة، ويعمل الفيروس غالبا على مسح البيانات والمعلومات المخّزنة في ذاكرة الحاسب الآلي، أو على تدمير نظام الحاسب بأكمله[3].

1– محمد عبد الله أبو بكر سلامة، المرجع السابق، ص 163.

2 – تمر عملية إصابة الفيروس للحاسب الآلي بعدة مراحل تختلف باختلاف نوع الفيروس وهي كالتالي :

أ/ مرحلة الإصابة: وتتم عندما يقوم المستخدم بتشغيل الفيروس على الحاسب فيصيب ملفا واحد فيه على الأقل، وذلك عن طريق نقل المعطيات المصابة بالفيروس إلى الحاسب.

ب/ مرحلة الكُمون والانتشار: وتختلف من فيروس لآخر، فهناك من يظهر بمجرد إصابته للحاسب، وهناك من يمر بفترة حضانة تتراوح بين شهر وعدة أشهر، لا تظهر خلالها على الحاسب أي أغراض بينما ينتشر الفيروس ويصيب أكبر عدد ممكن من الملفات بدون أن يشعر به مستخدم الحاسب .

ج/ مرحلة الظهور: وفيها يعلن الفيروس عن وجوده، وينتقل من العمل السري إلى العمل العلني وله علامات معينة .

د/ مرحلة الاجتياح: وفيها يظهر الفيروس آثار التخريبية، ولكن الأمر يختلف كذلك من فيروس لآخر.أنظر: محمد خليفة، المرجع السابق، ص 51–52.

3– محمد عبد الله أبوبكر سلامة، المرجع السابق، ص 163.

ثانيا: أنواع الفيروسات

إن الفيروسات أخذت بالتزايد بشكل متسارع ويعود السبب في ذلك إلى وجود الشبكة العالمية للمعلومات (الانترنيت)، فقبل هذا الاستعمال المذهل لشبكة الانترنيت كان انتشار الفيروسات في جميع أنحاء العالم يستغرق عامين إلى خمسة أعوام، أما الآن فيستغرق الأمر ساعات محدودة، دون تلقي أي عوائق تمنع تنقلها.

فالفيروسات كثيرة جدا لولا يمكن عدها[1]، ومن أشهرها الموجهة ضد الحواسيب و الشبكات المعلوماتية:

أ. **فيروس الحب:**

يتمثل هذا الفيروس في شكل رسالة أو صورة مثيرة للإغراء، ترسل إلى البريد الإلكتروني للمستخدم لحثه على فتحها وتكون ملحقة برسالة عادية، ويتنكر الفيروس في شكل رسالة بريدية آمنة ، وبمجرد فتح الرسالة يقوم الفيروس بنسخ نفسه مرات عديدة، مما يضاعف قدرته على الانتشار لحذف الملفات أو إخفائها ويستبدلها بنسخ منه، ويقوم أيضا بإرسال رسالة بريد إلكتروني لكافة العناوين الإلكترونية الموجودة في سجل العناوين الإلكترونية[2].

1- يقسم الفقه الفيروسات التي تستخدم في التخريب المنطقي لبرامج وبيانات الحاسب المخزنة آليا من حيث تكوينها وأهدافها إلى ما يلـــي:

أ/ فيروس عام العدوى : وهو ذلك الفيروس الذي ينتقل إلى أي برنامج أو ملف معلوماتي.

ب/ فيروس محدد العدوى : وهو ذلك الفيروس الذي يستهدف نوعا محددا من النظم لينتقل إليه ويهاجمه، ويتميز هذا النوع عن السابق بأنه أبطأ في الانتشار وأصعب في الاكتشاف .

ج/ فيروس عام الهدف: وتتدرج تحت هذا النوع من الفيروسات الغالبية العظمى التي تم اكتشافها حتى الآن، ويرجع ذلك إلى سهولة إعداد تلك الفيروسات واتساع مدى تخريبها.

د/فيروس محدد الهدف: ويحتاج إعداده إلى درجة عالية من الكفاءة و المهارة ، والـــى دراية تامة بالتطبيق او الهدف أو الغرض الذي يستهدفه، وقد يجري هذا الفيروس تلاعبا ماليا أو يدخل تعديلات في تطبيق عسكري ، وبعضه قد ينتهي وجوده بعد تنفيذ هدفه وتكمن خطورة بعض الفيروسات من هذا النوع في أنها لا تؤدي إلى تعطيل عمل البرامج ، بل تبدل فحسب من هدفها. أنظر: محمد عبد الله أبوبكر سلامة، المرجع السابق ، ص 164-165. وأنظر أيضا: نهلا عبد القادر مومني، المرجع السابق، ص 128.

2- محمد سامي الشوا، المرجع السابق، ص 145.

ويعتبر فيروس الحب من الفيروسات التي ألحقت أضرارا فادحة، حيث لم يسبق أن تمكن فيروس من الانتشار بالسرعة والكثافة التي حققها فيروس الحب الذي انتشر في شهر أيار من عام 2000 عبر البريد الإلكتروني.

ويعتمد مبدأ عمل هذا الفيروس على الانتشار عبر البريد الإلكتروني إلى سجل العناوين الموجودة في دفتر العناوين، في برنامج (OTLOK) من مايكروسوفت، مسببا أضرارا متعددة، كتدمير بعض أنواع الملفات، ومحاولة تنزيل ملف باب خلفي باسم (WIN-BUGSFISX-EXE) من موقع انترنيت محدد إلى الجهاز المصاب وسرقة وإرسال كلمات السر الخاصة ببرنامج البريد الإلكتروني ومقدم خدمة انترنيت إلى عناوين بريد إلكتروني محددة، ويمكن لهذا الفيروس أن ينتقل عبر تقنية المنتشرة معتمدا على البرنامج الشهير MIRC ، وكان من أبرز ضحاياه وزارة الدفاع الأمريكية ووكالة الاستخبارات الأمريكية، وجهات حكومية بريطانية [1].

ورغم أن هدف الفيروس ليس الحصول على الأسرار المخزنة في الحاسب الآلي بل تدميرها، إضافة إلى أنه قد يهدد تلك الأسرار بطريقة غير مباشرة، حيث أننا نعلم حجم الأسرار التي تحملها هذه الحواسيب خاصة الشخصية الخاصة، فصاحبها لن يحس بالارتياح والإطمئنان إذا عرض حاسوبه على المُصلحّ، مما يجعل هذا الأخير مضطرا للاطلاع على ما كان يحمله الحاسوب من معلومات[2].

ب. دودة الأنترنيت:

هي فيروس تنتقل عبر شبكة الأنترنيت، ويعتمد على استخدام برنامج Out Look Express بشكل أساسي للقيام بعملية الانتشار وإصابة أكبر عدد ممكن من الأجهزة، ويقوم مصممه بزرعه داخل رسالة بريد إلكتروني، ويرسلها إلى عدد كبير من مستخدمي الشبكة وبمجرد قيامهم بفتحها يبدأ الفيروس في الحصول على دفتر العناوين Adress Book، الخاص بكل واحد منهم ثم إرسال هذه الرسالة للعديد من أصدقائهم فيفتحونها دون أدنى شك لمعرفتهم للمرسل فيقعوا ضحية هذا الفيروس، وهذا ما أدى إلى انتشاره بنسبة كبيرة في العالم[3].

1- محمود أحمد عبابنة، المرجع السابق، ص 102.

2- عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، المرجع السابق، ص 136.

3- محمد خليفة، المرجع السابق، ص 54.

وفيروس الدودة يصيب جزءا محددا من نظام المعالجة الآلية للبيانات[1] وهو الجزء الخاص بنظام التشغيل والذي يقصد به مجموعة البرامج التي تتحكم في إمكانيات الحاسوب وفي العمليات التي تستخدمها هذه الإمكانيات[2].

ويعمل هذا الفيروس على نسخ نفسه أوتوماتيكيا نسخا عديدة، فيقوم بوضع أصفار في الأماكن الموجودة بالذاكرة التي يمر عليها، أو يبدل محتويات مكان في الذاكرة مع محتويات المكان المجاور له، مما يجعل من الصعوبة اكتشافه، وعند إصابة الجهاز به، تستمر برامج هذا الجهاز بالعمل ولكن بقيم مختلفة عن المعطيات التي تعمل عليها القيم الأصلية نظرا لتحويل بعض منها إلى أصفار أو بتبديل أماكن المعطيات مع بعضها البعض، فيحصل مشغل البرنامج على نتائج زائفة دون أن يشعر بذلك ويتم على أساسها اتخاذ قرارات خاطئة[3].

ت- فيروس القنابل المنطقية:

يعمل هذا الفيروس كالقنبلة إذ يظل في حالة سكون حتى يتم تفجيره في الوقت المناسب، إذ يظل البرنامج موجودا و لا تأثير له حتى يجد بيانات مخزنة في مكان محدد لها قيمة معينة، أو بعد تشغيل البرنامج لعدة مرات معينة، وفي المرة التالية يبدأ الفيروس في العمل، و تأثير الفيروس يتراوح بين التغيير العشوائي لمحتويات مكان محدد على وسط التخزين أو في الذاكرة لجعل كل محتويات قرص التخزين الصلب غير قابلة للقراءة بأي حال من الأحوال.

1- ومن الأمثلة التي تشير إلى استخدام فيروس الدودة في إتلاف المعلومات وتدميرها قيام طالب جامعي ألماني في ديسمبر 1987 بإرسال بطاقة تهنئة من خلال إحدى الحاسبات وقد صمم لهذا الغرض برنامج دودة قاد على قراءة العناوين الموجودة بذاكرة الحاسوب، وقام بنسخ بطاقة التهنئة إلى نسخ كثيرة حيث أرسلها إلى كل العناوين التي قرأها البرنامج، الأمر الذي أدى بعد اختراقه لشبكة (VNET) التي تربط حاسبات 45 دولة إلى تغطية نصف مليون حاسوب خلال ساعتين فقط، مما أدى إلى تعطيلها لمدة 48 ساعة تقريبا. أنظر: نهلا عبد القادر مومني، المرجع السابق، ص 131.

2- نهلا عبد القادر مومني، المرجع نفسه، ص 131.

3- محمد خليفة، المرجع السابق، ص 54-55.

و فيروس القنابل المنطقية يؤدي إلى الإخلال بتشغيل الحاسب الذي قد يصل إلى تعطيله بصورة كاملة[1]، ويصمم لإصابة برامج محددة وتطبيقات معينة يوجه إليها، فهو ليس فيروسا عاما[2].

و تختلف القنبلة المنطقية عن القنبلة الزمنية في كون هذه الأخيرة تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة، ويتم إدخالها في برنامج وتنفذ في جزء من ثانية أو في بضع ثـــوان أو دقائق وفقا للتحديد اللاّزم، وقد يتم ضبطها لتنفجر بعد عام مثلا[3]، مثل الفيروس الإسرائيلي الذي يقوم بالتدمير في يوم الجمعة الثالث من شهر معين حالة نشاطه عند حدوث واقعة معينة كبدء تشغيل الجهاز مثل الفيروس الباكستاني[4].

وفي الواقع إنّ المجني عليه في معظم الأحيان لا يعرف من الجاني الذي صمم الفيروس، كما أنه قد لا يعرف لمدة طويلة برنامجه بالفيروس، كما أن المجني عليه قد لا يرغب في الإعـــــلان عن إصابة نظامه بهذا الفيروس خصوصا إذا كانت مؤسسة مالية.

ثالثا: آثار الإصابة بالفيروس:

ذكرنا سابقا أن الفيروس عبارة عن برنامج يكرر نفسه على نظام الكمبيوتر عن طريق دمج نفسه في البرامج الآخر، وكما أن الفيروسات خطيرة للإنسان لدرجة أنها قد تقضي عليه، فالفيروسات التي نتحدث عنها قد تقضي على الكمبيوتر، وقد تأتي في مختلف الأشكال والأحجام بـــل وإن بعضها لا يسمى فيروسا مثل الدود وأحصنة طروادة وبعض الفيروسات ليست خطيرة وإنما مزعجة.

1- هدى حامد قشقوش، الإتلاف غير العمدي لبيانات وبرامج الحاسب الإلكتروني، بحوث مؤتمر القانون والكمبيوتر والأنترنيت، المجلد الثالث، الطبعة الثالثة، جامعة الإمارات العربية المتحدة ، كلية الشريعة والقانون، من 01 إلى 03 ماي 2000، ص 898.

2- محمد خليفة، المرجع السابق ، ص 55.

3- محمود أحمد عبابنة، المرجع السابق، ص 104.

4- هدى حامد قشقوش ، المرجع السابق، ص 899.

كما أنها برامج خبيثة بطبيعتها فهي تؤثر سلباً في الحواسيب بشكل مباشر وفي غير الحواسيب بشكل غير مباشر، فالفيروس عندما يحذف ملفات مهمة للعملاء يتعدى الحاسوب إلى العملاء وسمعة الشركة[1].

وتختلف الآثار التي يخلّفها الفيروس بحسب نوعه، وهي تتدرج من أقلها ضررا إلى أكبرها كما يلي:

- البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا.
- عـــدم القدرة على تشغيل معظم التطبيقات، وظهور رسائل خطأ كلما تمت محاولة تشغيلها.
- مسح الملفات التنفيذية كالبرامج سواءًا المثبتة داخل نظام التشغيل أو التي يحتفظ بها داخل الحاسب، مما يسبب عدم القدرة على تشغيل هذه التطبيقات.
- حذف ملفات (FAT) مما يعني حـذف جميع المعطيات الموجودة داخل القرص الصلب، وهو الأمر الأكثر خطورة.
- إصابة أحد أجزاء المكونات الصلبة، كما يحدث مع فيروس تشير نوبل[2] الذي يصيب نظام الإدخال والإخراج الأساسية، مما يؤدي إلى توقف الحاسب بالكامل[3].

وعليه إثر الانتشار الواسع للفيروسات أنتجت العديد من الشركات برامج لمنع الإصابة بالفيروس شأنه في ذلك شأن السلاح، فكلما أنتج نـــوع أنتج معه النوع المضاد له، إذا لا بد من وجود هذه البرامج المضادة للفيروسات على جهاز الحاسب الآلي والقيام بتحديثها دوريا من الأنترنيت، حتى تلّم بكل جديد في عالم الفيروسات، لتكون رقيبا على أي ملفات جديدة تدخل للحاسب.

المطلب الثاني: دوافع ارتكاب الجريمة الإلكترونية

يعتبر الدافع (الباعث)، الغرض، الغاية، تعبيرات لكل منها دلالته الاصطلاحية في القانون الجنائي ،تتصل بما يعرف بالقصد الخاص في الجريمة ، وهي مسألة تثير جدلا فقهيا وقضائيا واسعا، لأن القاعدة القضائية تقرر أن الباعث ليس عنصر القصد الجرمي ، وأن الباعث لا أثر له في وجود

1- خالد بن سليمان الغثير ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مركز التأمين لأمن المعلومات، بدون بلد النشر، 2009، ص 66.

2- مصدر هذا الفيروس جنوب شرق آسيا حيث قام شخص باقتحام شبكة الأنترنيت وقام بإرسال هذا الفيروس يوم 26 أبريل 2000،حيث يقوم هذا الفيروس بمسح الملفات الأساسية المكونة للبرامج الموجودة على الجهاز وتتسبب في تعطيل الملايين من الأجهزة في مختلف أنحاء العالم، أنظر: طارق فوزي الفقي، المرجع السابق، ص 32.

3- محمد خليفة، المرجع السابق، ص 32.

القصد الجنائي، و إذا كان الاستخدام العادي للتعبيرات المشار إليها يجري على أساس ترادفها في الغالب فإنها من حيث الدلالة تتمايز [1] وينتج عن تمايزها آثار قانونية على درجة كبيرة من الأهمية ، وعليه فإن الجريمة تقوم بتحقيق عناصرها وأركانها أياّ كان الباعث من وراء ارتكابها وللجريمة الإلكترونية عدة دوافع لارتكابها [2] تتباين تبعا لطبيعة المجرم ومدى ثقافته وخبرته في مجال الحاسب الآلي، لأن المتهم يرتكب جريمته بناءا على ما لديه من مهارة وخبرة[3]، فيرجع البعض دوافع ارتكاب الجريمة الالكترونية إلى دوافع شخصية(الفرع الأول) والبعض الآخر يرجعها إلى دوافع خارجية (الفرع الثاني)، وكل هذه الدوافع لها مصدر واحد هو الرغبة الإجرامية .

الفرع الأول: الدوافع الشخصية

يقصد بالدوافع الشخصية تلك عوامل اللصيقة بشخصية المجرم الإلكتروني والذي تدفعه لارتكاب الجريمة الالكترونية، ويمكن رد الدوافع الشخصية لدى مرتكب الجرائم الالكترونية إلى دوافع مادية وأخرى دوافع ذهنية .

أولا: الـــــدوافع المادية

يعتبر الدافع المادي من أكثر الدوافع التي تحرك الجاني لارتكاب جريمته الالكترونية ،إلا أن الربح الكثير و الممكن تحقيقه من خلالها يدفع بالمجرم الالكتروني إلى تطوير نفسه حتى يواكب كل حديث

1- إن الدافع هو العامل المحرك للإرادة والذي يوجه السلوك الإجرامي كالمحبة، الانتقام، إذن هو قوة نفسية تدفع الإرادة إلى الاتجاه نحو ارتكاب الجريمة ابتغاء تحقيق غاية معينة، أما الغاية فهي الهدف البعيد الذي يرمي إليه الجاني بارتكاب الجريمة كإشباع شهوة الانتقام أو مثلا كسلب مال المجني عليه في جريمة القتل.

أما الغرض فهو الهدف الفوري المباشر للسلوك الإجرامي، يتمثل بتحقيق النتيجة التي انصرف اليها القصد الجنائي أو الاعتداء على الحق الذي يحميه القانون.

2 –يقول الدكتور Adam Graycar مدير المعهد الاسترالي لعلم الإجرام: بأن الجريمة تحتاج إلى أربعة عناصر رئيسية لتشجيع المجرم على ارتكابها وهي:

1/ دافع معين لارتكاب العمل.

2/ هدف ضحية محاسبته.

3/ القرصنة المواتية.

4/ غياب عيون الأمن.

3 –المتهم ذو خبرة في مجال البرمجة واستخدام شبكات الحاسب الآلي قد يكون هدفه مختلفا عن هدف المتهم الذي لا تتعدى خبرته مجرد تشغيل جهاز الحاسب الآلي.

يطرأ علي التقنية المعلوماتية ويقتنص الفرص ويسعى إلى الاختراق حتى يحقق أعلى المكاسب و بأقل جهد دون أن يترك أثرا وراءه.

فالدافع الذي يدفع الجاني لإرتكاب جرائمه ضد المؤسسات والشركات الاقتصادية هو الأضرار بهذه الشركات ، والحصول على نفع مادي سواءا بالمتاجرة بأسرارها الصناعية، أو الاعتداء على حقوقها في الإنتاج، أو الاعتداء على ذمتها المالية، وعليه يمكن القول بأن الدافع لارتكاب الجرائم الالكترونية هو النفع المادي سيحصل عليه الجاني من سيطرته على المعلومات[1].

فحب المجرم الالكتروني للمال هو عصب الحياة يدفعه للقرصنة أو السرقة أو الاختلاس، عن طريق الحاسوب للحصول على المال لتلبية حاجاته الأساسية والرغبة في الثراء السريع الغير مكلف[2].

فالمكسب المادي لا يكون هدفا فقط لمن يتمتع بالكفاءة الفنية العالية و المهارة في مجال التكنولوجي بل المكسب يكون هدفا أيضا لمن هم أقل في المعرفة التقنية وقد يكونون غير مؤهلين على الإطلاق في مجال المعلوماتي، لذلك يكون أسلوبهم لارتكاب الجريمة مختلفان كون الجريمة تكون متعلقة بالحاسب الآلي أو المعلومات، ولكن دون الدخول على أنظمة تلك الحواسب ويكون أسلوب ارتكابهم للجرائم محدودا في مجال معيّن لا يحتاج إلى خبرة أو مهارة [3].

ومند بداية الظاهرة فإن الدراسات أشارت إلى أن المحرك الرئيسي لأنشطة احتيال الكمبيوتر وفيما بعد احتيال الانترنيت هو تحقيق الكسب المالي ففي دراسة قديمة للفقيه **بـــاركـــر** الصادرة في إحدى المجلات المتخصصة (Sécurité Informatique) في موضوع الأمن ألمعلوماتي تبين أن :43 % من حالات الغش المرتبط بالحاسوب من أجل اختلاس الأموال،29 % ترتكب من أجل سرقة المعلومات،19% ترتكب من أجل الإتلاف و 15 % ترتكب من أجل سرقة وقت الحاسوب لأغراض شخصية.

1 – محمد حماد مرهج الهيتي، جرائم الحاسوب– ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها–، المرجع السابق، ص143.

2 –نسرين عبد الحميد نبيه، المرجع السابق، ص 44.

3–أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 249.

وإذا انتقلنا للدراسات الحديثة كالدراسات المسحية والدراسات الإحصائية والتقارير الصادرة عن مركز احتيال المعلومات الوطني في الولايات المتحدة الأمريكية N.F.I.C نجد أن هذا الدافع يسود على غيره من الدوافع، ويعكس استمرار اتجاه مجرمي التقنية إلى السعي لتحقيق مكاسب مادية شخصية.

وهناك فئة من مرتكبي الجرائم الالكترونية يرجع ارتكابهم لها للنجاة من غرق الديون المستحقة ، أومن المشاكل العائلية الراجعة إلى النقود أو من الخسائر الضخمة لألعاب القمار أو إدمان المخدرات، وقد تكون جميع الوسائل بالنسبة للبعض مشروعة في هذه المرحلة فالغاية تبرز الوسيلة[1].

وفي حالة نجاح المجرم الالكتروني في ارتكاب جريمته الالكترونية فإن ذلك يدر عليه أرباحا كبيرة في زمن قياسي، ويمكن أن نوضح مدى الأرباح المادية التي يحققها المجرم نتيجة اقترافه لهذا النوع من الجرائم من خلال أحدث خلاصة لإحدى الدراسات الواردة بالتقرير السادس لمعهد أمن المعلومات حول الجرائم الالكترونية، أين أجريت هذه الدراسة، بمشاركة 538 مؤسسة أمريكية تضم وكالات حكومية و بنوك ومؤسسات مالية ومؤسسات صحية وجامعات والتي أظهرت حجم الخسائر الناجمة عن الجرائم الالكترونية، فقد تبين أن 85% من المشاركين تعرضوا لاختراقات للأنظمة المعلوماتية و أن 64% لحقت بهم خسائر مادية جراء هذه الاعتداءات [2].

ثانيا: الدوافع الذهنية

تعتبر الدوافع الذهنية تلك العوامل النفسية اللصيقة بالمجرم الالكتروني تدفعه إلى ارتكاب الجريمة الالكترونية بهدف الرغبة في إثبات الذات وتحقيق انتصار على تقنية الأنظمة المعلوماتية، والرغبة في قهر النظام والتفوق على تعقيد الوسائل التقنية دون أن يكون له نوايا آثمة [3].

---

1 – ضياء أحمد علي نعمان، المرجع السابق، ص 11.

2– وضاح محمود الحمود ونشأت مفطي المجالي ، جرائم الانترنيت ، دار المنار للنشر، عمان ، 2005، ص 31.

3 – من أشهر القضايا التي وقعت قضية كان قد تعامل معها مكتب التحقيقات الفدرالية أطلق عليها اسم مجموعة الجحيم العالمي Global Hell، تتلخص وقائعها في تمكن مجموعة من الأشخاص من اختراق مواقع البيت الأبيض والشركة الفدرالية الأمريكية والجيش الأمريكي و وزارة الداخلية الامريكية ، وقد أدين 2 من هذه المجموعة جراء تحقيقات الجهات الداخلية في و. م .أ وقد ظهر من هذه التحقيقات أن هذه المجموعات تهدف إلى مجرد الاختراق أكثر من التدمير أو التقاط المعلومات الحساسة، وقد أمضى المحققون مئات الساعات في ملاحقة ومتابعة هذه المجموعة عبر

ويرجع ذلك إلى وجود عجز في التقنية التي تترك الفرصة لمشيدي برامج النظام المعلوماتي لارتكاب الجرائم، وعليه فإن البعض يرى بأن الدافع إلى ارتكاب الجريمة الالكترونية يغلب عليه قهر النظام أكثر من شهوة الحصول على الربح، مع أن الدراسات لا تظهر هذه الحقيقة على إطلاقها، إذ يظهر السعي إلى تحقيق الربح دافعا أكثر تحريكا للجرائم الالكترونية من الرغبة في قهر النظام إلا أن الدافع الأخير، يتجسد في نسبة مرتفعة من الجرائم الالكترونية خاصة ما يعرف بأنشطة الـ (Hackers) المتطفلين على النظام و المتجسدة في جرائم التواصل مع أنظمة الحاسب، والاستخدام غير المصرح به لنظام الحاسب، واختراق مواقع الانترنيت [1].

ويميل مرتكبي هذه الجرائم إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أي تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة يحاولون إيجادها، وغالبا ما يجدون الوسيلة إلى تحطيمها أو التفوق عليها بمعنى أصح ويتزايد شيوع هذا الدافع لدى فئة صغار السّن من مرتكبي الجرائم الالكترونية الذين يمضون وقتا طويلا أمام حواسيبهم الشخصية في محاولة لكسر حواجز الأمن لأنظمة الحواسيب وشبكات المعلومات ، لإظهار تفوقهم على وسائل التقنية[2].

و يعتبر هذا الدافع من أكثر الدوافع التي يجري استغلالها من قبل المنظمات الجُرمية (مجموعات الجريمة المنظمة) لجهة استدراج محترفي الاختراق إلى قبول المشاركة في أنشطة اعتداء معقدة أو استئجارهم للقيام بالجريمة.

بالإضافة إلى الدوافع الشخصية اللصيقة بشخصية المجرم الالكتروني هناك دوافع أخرى خارجية خارجة عن نطاق المجرم الالكتروني تدفعه لارتكاب الجريمة الالكترونية.

الشبكة وتتبع آثار أنشطتها، وقد كلف التحقيق مبالغ طائلة لما تطلبه من وسائل معقدة في المتابعة . أنظر: رشيدة بوكر، المرجع السابق ، ص 97.

1 – نسرين عبد الحميد نبيه، المرجع السابق، ص 135.

2– محمد محمود المكاوي، الجوانب الاخلاقية و الاجتماعية و المهنية للحماية من الجرائم المعلوماتية، الطبعة الاولى، المكتبة العصرية للنشر و التوزيع ، مصر، 2010، ص 52.

الفرع الثاني: الدوافع الخارجية

إن الإنسان يتأثر ويستسلم للمؤثرات و الدوافع الخارجية بارتكابه بعض الجرائم الالكترونية، نتيجة لوجوده في بيئة المعالجة الآلية للمعلومات، وتتعدد المؤثرات التي تدفع المجرم الالكتروني إلى اقتراف مثل هذا السلوك من بينها دافع الانتقام والتواطؤ على الإضرار برب العمل ودافع المنشأة.

أولا: دافع الانتقام وإلحاق الضرر برب العمل

هناك أثار سلبية في سوق العمل من جهة ، وفي البناء الوظيفي من جهة أخرى ، وقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ، يتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية ومن طبيعة علاقات العمل المنفردة في حالات معينة، وهذه العوامل قد تدفع إلى السرعة نحو تحقيق الربح، لكنها في حالات كثيرة مثلت قوة محركة لبعض العاملين لارتكاب الجرائم الالكترونية، باعثها الانتقام من المنشأة أو رب العمل وتحديدا جرائم إتلاف البيانات وربما تحتل أنشطة زرع الفيروسات وهناك عدة أمثلة، كان دافع الجناة فيها إشباع الرغبة في الانتقام، و التي تمثل الحقد على رب العمل الدافع المحرك لارتكاب الجريمة [1].

وبالتالي فإن دافع الانتقام يعد من أخطر الدوافع التي يمكن أن تدفع الشخص إلى ارتكاب الجريمة، وذلك إما لفصله من العمل أو تخطيه في الحوافز أو الترقية فيقوم هذا الشخص بالاستعداد مسبقا لمثل هذا الموقف كأن يقوم مثلا بزرع برنامج يحمل تعليمات بمسح كافة البيانات في حالة عدم وجود اسمه في كشف الموظفين بالشركة ويقوم عند فصله منها بالانتقام عن طريق تشغيل هذا البرنامج [2]، وكذلك عن طريق احتفاظه بكلمة السر لكي يتمكن من الدخول على نظام الحاسب الآلي الخاص بالشركة وارتكاب أي من الجرائم أو إعطائها لشركة أخرى منافسة لكي تتمكن من الدخول إلى أنظمة تلك الشركة والتجسس على البيانات الخاصة بها.

1 –محمد محمود المكاوي، المرجع السابق، ص51.

2– كذلك من الأمثلة على ذلك القيام موظف يعمل لدى إحدى شركات التامين لكي يحتفظ بوظيفته التي سبق أن فصل منها بحجز وحدة التخزين المركزية الخاصة بالشركة كرهينة ووسيلة تهديد لرئيسه لإرجاعه للعمل وهو ما حدث بالفعل.

ويمكن أن يصدر التصرف بغرض الانتقام من دولة معادية لدولة أخرى، وذلك عن طريق إما التجسس على المعلومات أو عن طريق زرع الفيروسات أو ارتكاب جرائم السرقة لأصول الأموال أو لمحاولة تسوية صورة هذه الدولة باستخدام الشبكة الدولية للاتصالات[1].

ثانيا: الدوافع الخاصة بالمنشأة

يقصد بالدوافع الخاصة بالمنشأة تلك العوامل الخارجية التي تسهل للجاني ارتكاب الجريمة داخل المنشأة باستعماله التقنية المعلوماتية الخاصة بالمؤسسة إذ تكون وسائل ارتكاب الجريمة المعلوماتية في متناوله،إذ يعتقد بعض المتخصصين في تقنية الأنظمة المعلوماتية أن العاملين في منشاة معينة أن من مزايا مراكزهم الوظيفية ومهارتهم الفنية استخدام الأنظمة المعلوماتية وبرامجها لأغراض شخصية أو ممارسة بعض الهوايات الدائرة في مجال التقنية ومن شأن ذلك أن يؤدي إلى تمادي بعضهم إلى استخدام الأنظمة بصفة غير مشروعة تصل إلى ارتكاب جرائم خطيرة لمصلحته الخاصة [2] لأن الشخص المسؤول عن المركز ألمعلوماتي هو بدون منازع في وضع يمكنه من استغلال نقاط الضعف المتمثلة بمركز المعالجة وتعد العلاقة بينة وبين الأنشطة التي يزاولها ومركز الثقة الذي يحوزه أفضل أسلحة له لارتكاب جريمته الالكترونية ومن أمثلة ذلك قيام مستشار لدى احد البنوك الكبرى يسمى STANLEY RIFKIN كان يتمتع بثقة مطلقة من جانب هذا البنك وقد سمحت اختصاصاته بالولوج والتحكم في مفتاحين الكترونيين من ثلاثة أساسية للتحكم في التحويلات الالكترونية للنقود من بنك إلى بنك آخر وقد تمكن بفضل قدراته في مجال المعالجة الآلية للمعلومات وتالفه الشديد مع النظام المعلوماتي من الوصول إلى المفتاح الثالث واستطاع أن ينقل 100مليون دولار إلى حساب بنكي فتح باسمه في سويسرا [3].

وفي الأخير نخْلص إلى القول أن هذه هي أبرز دوافع ارتكاب الجريمة الالكترونية لكنها ليست ثابتة ومعتمدة لدى الفقهاء و الباحثين ، لأن السلوك الإجرامي و الدوافع لارتكاب الجريمة تتغير وتتحول بسرعة من حالة العبث أو محاولة التحدي و التغلب على الأنظمة إلى تدميرها أو على الأقل تقدير حيازتها للقيام بعمليات الابتزاز ،أو استعمالها للحصول على الأموال ، ولذلك فالدافع لارتكاب

1-أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 250.

2-أحمد خليفة الملط، المرجع السابق، ص 91.

3- أنظر في هذا الصدد: ضياء علي أحمد نعمان، المرجع السابق، ص 18.

الجرائم الالكترونية قد لا يتوقف عند هذه الدوافع ، وخير دليل على ذلك أننا نجد في كل جريمة جديدة دوافع جديدة ، بل كثيرا ما نجد أن الجريمة الواحدة لها دوافع متخصصة خاصة إذا اشترك فيها أكثر من شخص وأكثر من جهة بحيث يسعى كل منهم لتحقيق مآربه الخاصة ، فمثلا يكون الدافع لمن يسعى للحصول على المعلومات تمثل أسرار تجارية هو المنافسة التجارية ، في حيث أن قسماً آخر يسعى في ممارسته لهذه الأنشطة تحقيق أهداف سياسية وإيديولوجية كتلك التي تمارس من قبل الدول.

الفصل الثاني: ماهية التحقيق الجنائي في الجرائم الالكترونية

إن ظهور الجريمة الإلكترونية فرض على جهات التحقيق تحديات عظيمة لم يسبق لها مثيل، نظرا للطابع الذي تتميز به هذه الأخيرة، مما أدى إلى إعادة النظر في وسائل المكافحة التقليدية للجريمة وأساليبها [1]وطرق الوقاية منها، وأصبح من الضروري وضع الخطط والبرامج الإستراتيجية لتحديد أجهزة العدالة الجنائية من حيث بنيتها المؤسسية وكوادرها البشرية، لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم ومواجهة مرتكبيها وضبطهم وتقديمهم للعدالة، فرجال التحقيق يواجهون صعوبات شديدة في ضبط وتوصيف الجرائم الإلكترونية وتعقب مرتكبيها، ويعود ذلك إلى كونها جرائم ترتكب في فضاء إلكتروني يتسم بالتغير و الديناميكية و الانتشار الجغرافي العابر للحدود، إلى جانب أن الطبيعة الفنية و التقنية الناجمة عن الجرائم الإلكترونية نتج عنها في مجال الإثبات الجنائي نوعاً جديدًا من الأدلة يطلق عليها الدليل الإلكتروني.

وتعتبر مسألة إثبات الجرائم الإلكترونية من أهم المواضيع القانونية، ذلك بالنظر إلى المشكلات الإجرائية التي أثارتها هذه الجرائم المستحدثة، والمتمثلة في سرعة ودقة تنفيذ الجريمة، وإمكانية إزالة آثارها، وإخفاء الأدلة الناتجة عنها عقب ارتكابها مباشرة، حيث يواجه التحقيق فيها إشكاليات كثيرة، تكمن في الطبيعة غير المادية للمعطيات المعلوماتية التي يكون لها دور في كشف الجريمة، فالتعامل في مسرح الجريمة سواءًا كان مادياً أو الكترونياً يتطلب إجراءات روتينية معينة متفق عليها لحماية الدليل وإبراز قيمته الاستدلالية، غير أن طرق حفظ الأدلة واستخلاصها تختلف من مسرح الجريمة المادي إلى مسرح الجريمة الإلكتروني.

هذا ما أوقع أجهزة التحقيق والعدالة أمام تحدٍ كبير ظهر فيه تفوق واضح لمرتكبي هذا النوع من الجرائم من حيث قدرتهم على التعامل مع هذه التقنيات الحديثة، و الولوج إلى مكوناتها المعقدة وتوجيهها نحو مقاصد جريمة لم تكن أجهزة التحقيق مستعدة لها، نظراً لافتقارها إلى الحد الأدنى من المعارف الفنية والعملية الخاصة بهذه التقنيات.

وعليه سنقسم هذا الفصل إلى مبحثين يتضمن الأول مفهوم التحقيق الجنائي في الجرائم الإلكترونية، أما الثاني فسنتناول فيه مفهوم المحقق الجنائي في الجرائم الإلكترونية.

---

[1] – يقصد بأسلوب ارتكاب الجريمة بيان الكيفية التي تمت بها بدءا من وجود السبب حتى الاختفاء والهروب بعد الانتهاء منها.

المبحث الأول: مفهوم التحقيق الجنائي في الجرائم الإلكترونية

يعتبر التحقيق الجنائي صراع بين المحقق والمجرم، الأول ينشد الحقيقة عن الجريمة والثان يحاول التضليل وطمس الحقائق حتى يفلت من العقاب، ولكن بقدر ما يكون للمحقق الجنائي من خبرة وفراسة وإلمام بالعلوم الجنائية والنفسية، وبقدر ما يتمتع به من كفاءة ومقدرة وسيطرة على المواقف التي يواجهها، بقدر ما تكون النتيجة في صالح التحقيق إرساءاً لقواعد الحق و العدل .

فالتحقيق في الجرائم الإلكترونية يمتاز بخصوصية تجعله يفترق عن التحقيق في الجرائم التقليدية، نظراً لتميز هذه الجرائم عن غيرها من الجرائم التقليدية الأخرى خاصة فيما يتعلق بطبيعة مسرح الجريمة، الأمر الذي يقتضي ضرورة تطوير أساليب التحقيق الجنائي بصورة تجعله يتلاءم مع هذا التميز، بحيث تمكن سلطة التحقيق من كشف غموض هذه الجرائم وتحديد شخص المتهم واثبات التهمة عليه.

كما أن التحقيق الجنائي الإلكتروني ليست مقتصرة فقط على الأجهزة الإلكترونية أو أدلة ملموسة، بل من الممكن أن تكون أيضا عملية تتبع لبعض الأدلة والأمور التي تم إجراءها أثناء أو بعد عملية الاختراق من خلال تحليل ملفات النظام وتتبع أثره والحركات التي قام بها أو يقوم بها في نفس اللحظة، وهذه الأمور جميعها تفيد في عملية التحقيق الجنائي في الجرائم الإلكترونية، ليس فقط لمعرفة الجاني، بل لمعرفة كذلك نقاط ضعف الموقع، من خلال تحليل الحركات التي قام بها المخترق أثناء عملية الاختراق[1].

ضف إلى ذلك رجال التحقيق في الجرائم الإلكترونية يحتاجون إلى مشاهدة وفحص الأدلة الجنائية، وهي غالبا ما تتميز بسهولة الاستخدام والبعد عن التعقيد، لأن الكثير من مستخدمي الحاسوب يستخدمونها كبرامج عرض الصو، وبرامج فك الملفات المضغوطة، ولذلك ينبغي على ضابط التحقيق أن يكون على وعي جيد بالجرائم الإلكترونية حتى يتمكن من مواجهتها.

وعلى المحقق كذلك إتباع أساليب متغيرة بحيث يعالج كل أسلوب منها في إحدى الحالات المعيّنة، أو يلجأ إلى استعمال عدة أساليب في حالات أخرى، وبذلك فهو يحتاج للوسائل المادية

[1]– محمد معسكر، مقال بعنوان تعريف لعملية التحقيق الجنائي الـــــرقمي، متوفر على الموقع الالكتروني: www.isecurity.org: http يوم الإطلاع 2017/2/22، الساعة 11:00.

والمعنوية ليستخدمها في تنفيذ التحقيق لأن التحقيق في الجرائم الإلكترونية يحتاج إلى معرفة تامة وإدراك لوسائل تثبت وقوع الجريمة والوصول إلى الجاني ونسبتها إليه[1].

لهذا سنقسم هذا المبحث إلى ثلاث مطالب، المطلب الأول نخصصه تعريف التحقيق الجنائي في الجرائم الإلكترونية، والمطلب الثاني لعناصر التحقيق في الجرائم الإلكترونية، أما المطلب الثالث سنتناول فيه وسائل التحقيق في الجرائم الإلكترونية.

المطلب الأول: تعريف التحقيق الجنائي في الجرائم الإلكترونية

لعل من أكثر الأمور صعوبة في الأبحاث الشرطية هو التوفيق بين مقتضيات كشف الحقيقة عند وقوع الجريمة، وبين حرية المتهم التي تصونها النظم القانونية باعتباره بريء إلى أن تثبت إدانته، مع الأخذ بعين الاعتبار ضرورة التحرك لجمع الأدلة دون إبطاء أو تأخير.

فوسائل التحقيق الجنائي في عصر المعلوماتية تطورت تطوراً ملموساً يواكب حركة الجريمة وتطور أساليب ارتكابها، بعد أن كان الطابع المميز لوسائل التحقيق العنف و التعذيب للوصول إلى الدليل، أصبحت المرحلة العلمية واستخدام الأنترنيت هي الصفحة المميزة و الغالبة.

كما أن طبيعة الجرائم الإلكترونية بعناصرها ووسائل ارتكابها قد تدفع المشرع الجزائي إلى أن يعيد النظر في كثير من المسائل الإجرامية، خاصة فيما يتعلق بمسألة الإثبات باعتبارها من أهم الموضوعات.

ضف إلى أن محاربة الجريمة الإلكترونية ومكافحتها، وذلك بالكشف السريع عنها وعن مرتكبيها، ومن تم محاكمتهم، وتنفيذ الحكم عليهم يعتبر من الأمور المهمة، لأن التحقيق الجنائي في هذه الجرائم له خصوصياته، و التحقيقات الجنائية عموما علوم تطبيقية تنطوي على دراسة الحقائق، وتستخدم للتحقق من وجود جريمة وإثبات ذنب المجرم[2].

وهو ما يدفعنا إلى إثارة عنصر الماهية أو الإطار المفاهيمي لموضوع دراستنا المتمثل في التحقيق الجنائي والذي يتطلب بالضرورة تعريفه (الفرع الأول) ثم شروط التحقيق في الجرائم الالكترونية (الفرع

[1]– خـالد عياد الحلبي، المرجع السابق، ص 203.

[2]– موقع الموسوعة الحرة : http://ar.wikipedia.org/wiki يوم الإطلاع 2017/03/05، الساعة : 19:00.

الثاني)، وخصائص التحقيق في الجرائم الإلكترونية (الفرع الثالث) وأخيرا أدوات التحقيق في الجرائم الإلكترونية (الفرع الرابع).

الـــفرع الأول: تعريف التحقيق الجنائي

تتعدد وتتنوع تعاريف التحقيق الجنائي إلا أن مضامينها واحدة ، وهو البحث عن الحقيقة بالوقوف على حقيقة الأمر سواءاً بالنفي أو الإثبات[1].

أولا: التعريف اللغوي والاصطلاحي للتحقيق الجنائي

التحقيق لـــغة :هو التصديق والتأكيد أو التثبيت، يقال في اللغة حقق الأمر أي أثبته وصدقه ويقال حقق الظن وحقق القول والقضية وحقق الثوب، أي أحكم نسجه وصنع الثوب صنعا تحقيقا مشبعا، وحقق مع فلان في قضية، أخذ أقواله فيها وجني جناية بمعنى أذنب، أي أن التعريف بالمعنى اللغوي للتحقيق هو إثبات التهمة على الجاني بإحكام[2].

التحقيـق اصطلاحـــا: فيعرف بأنه مجموعة الإجراءات التي يباشرها الجهاز القضائي المكلف بالتحقيق، قصد التثبت من الوقائع المعروضة عليه ومعرفة كل من ساهم في اقترافها ثم إحالة مرتكبيها إلى جهة الحكم لتوقيع الجزاء المناسب لهم عند الاقتضاء[3].

---

[1]– يـــرادف استعمال مصطلح التحقيق مصطلح البحث، غير أن كلا منهما يختلف عن الآخر حيث يدل معنى التحقيق (l'instruction) على مرحلة من مراحل سير الدعوة تجمع فيها المحكمة كل العناصر التي تسمح لها بالفصل في الطلب وذلك من خلال ادعاءات الأطراف، وتعد هذه المرحلة ضرورية في مواد الجنايات واختيارية في مواد الجنح، حيث يقوم ، بها قاضي التحقيق تحت رقابة غرفة الاتهام، وتسمح هذه الأخيرة بالتحقيق من وجود جريمة و تحديد ما إذا كانت الأدلة التي تم جمعها ضد أشخاص متابعين كافية لكي يتم اللجوء إلـــى الجهة القضائية لكي تبث فيها، أما مصطلح البحث (Enquête) فيرتبط بحالة التلبس بالجريمة (L'enquête de Flagrance) أين يجب على الشرطة القضائية إتحاد تدابير مستعجلة من اجل تجنب تلك الأدلة كما ينصرف إلـــى التحقيق الابتدائي (**L'enquête Préliminaire**) ليدل على البحث الذي يقام على اثر ارتكاب جريمة من طرف ضباط الشرطة القضائية من تلقاء أنفسهم أو بناءا على تعليمات وكيل الجمهورية وذلك قبل افتتاح التحقيق. أنظر: دليلة جلول، الأسس النفسية للتحقيق الجنائي، دارهومة، الجزائر، 2015، ص 12.

[2] – عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن– بين النظرية و التطبيق–، بدون بلد النشر، بدون سنة النشر، ص 11.

[3] – دليلة جلول، المرجع السابق، ص11.

وهناك من يعرفه أيضا على أنه: "علم يوضح للمحقق معالم الطريق ويرشده إلى كيفية البحث والسير في جمع الأدلة ".

أو بعبارة أخرى:"هو مجموعة الأعمال و الإجراءات المشروعة التي يتخذها المحقق الجنائي، للكشف عن الحقيقة وجمع الأدلة التي تؤدي إلى معرفة الجاني وشركائه"[1].

والتحقيق الجنائي أيضا هو العلم الذي يضم مجموعة من الإجراءات النظرية والعلمية التي يقوم بها محققي هيئة التحقيق والإدعاء العام، بما يوصله إلى الكشف عن الجريمة الإلكترونية وتوفير الأدلة الرقمية ضد مرتكبيها وتقديمهم للعدالة لمحاكمتهم[2].

كما عرف أيضا بأنه: "مجموعة من الإجراءات و الوسائل المشروعة قانونا والتي يقوم بها المحقق لاستجلاء غموض الحوادث الجنائية بصفة عامة، والجريمة الإلكترونية بصفة خاصة، والتوصل إلى الفاعل أو الفاعلين و توجيه الاتهام ضدهم[3] ".

كما أنّه مجموعة من الإجراءات التي يقوم بها المحقق للكشف عن الحقيقة الإجرامية مستندا إلى أهم فنيات ومهارات التواصل الاجتماعي قصد الوصول إلى المتهم.

فإلى جانب اعتبار التحقيق علم فهو فن كذلك أي يعتبر التحقيق الجنائي علم وفن لأنه لا يقتصر فقط على مجرد أسئلة يلقيها المحقق على المستجوب بل هو خبرة و دراسة، وفراسة، وتجربة ومهارة [4].

كما يعرف التحقيق الجنائي أيضا بأنه "عملية فنية يقوم بها المحقق عن طريق جملة من الإجراءات والأساليب تشير إلى كيفية السير في تحقيق من بدايته إلى نهايته وكيف يكتشف الجرائم الغامضة، ويتحرى حقيقتها ، ويجمع الأدلة فيها ، وكيف يتبع الجاني ويقتفي أثره إذا اختفى عن مسرح الجريمة،

---

[1]–عبد الواحد إمام مرسي، المرجع السابق، ص 11.

[2]–عبد الله بن الحسين أل حجراف القحطاني، تطوير مهارات التحقيق الجنائي والادعاء العام، مذكرة ماجستير، كلية الدراسات العليا، الرياض،2014، ص 13.

[3]– عبد الله بن الحسين أل حجراف القحطاني، المرجع نفسه، ص 13.

[4]–عبد الواحد إمام مرسي، المرجع السابق، ص 11.

ليتمكن من القبض عليه، واستكمال إجراءات التحقيق في الواقعة حتى أصبح بعض المفكرين ينظرون إلى التحقيق الجنائي أنه علم قائم بذاته[1].

استنباطا من التعريفين اللغوي و الاصطلاحي ، فإنّ التعريف الإجرائي للتحقيق الجنائي يشير إلى ذلك الموقف النفسي الذي يجمع بين المحقق والمتهم في إطار البحث عن الحقيقة الإجرامية، والتي يستند فيها المحقق إلى أهم فنيات ومهارات التواصل الاجتماعي، و إدارة الحوار تزامنا واستخدام المتهم لأهم الميكانيزمات الدفاعية التي تسمح له بإنكار ما نسب إليه من جرم واثبات براءته وتصنيف دائرة الشكوك والاتهامات التي تحوم حوله إذا كان على صلة بالجريمة .

ثانيا: تعريف التحقيق الجنائي في الجرائم الإلكترونية

التحقيق الجنائي في الجرائم الإلكترونية عبارة عن فحص جهاز الجاني أو المشتبه به من قبل المحققين فمثلا إذا تمت جريمة عن طريق الحاسوب أو الأجهزة الذكية المختلفة، يأتي المحقق المتخصص ليفحص ما به وذلك باستخدام أدوات خاصة ودراسات سابقة وكل ما هو ممكن والهدف منها جمع الأدلة المطلوبة.

و يعرف أيضا بأنّه: "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجرائم الإلكترونية الرقمية من فاعل ودليل الكتروني رقمي لتقديمهم إلى سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم لإقامة العدل[2]."

كما يعرف أيضا بأنه: "استخدام الطرق المثبتة علميا، لحفظ ، جمع ، عرض ، تحديد، تحليل ترجمة، توثيق والتحقيق من صحة الأدلة الرقمية المستخرجة من المصادر الرقمية، بهدف تسهيل أو تعزيز بناء الأحداث الجنائية، أوالمساعدة في إحباط العمليات غير الشرعية المرتقبة[3]."

عموما يعتبر التحقيق من أهم الإجراءات التي تتخذ بعد وقوع الجريمة، لماله من أهمية في التثبت من حقيقة وقوعها، و إقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما

---

[1] – خالد مختار الفار، إسماعيل بابكر محمد، المرجع السابق، ص15 .

[2] – مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 166.

[3] – محمد معسكر، مقال بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته، متوفر على الموقع الإلكتروني: http://www. Isecurity. Org. يوم الإطلاع 2017/03/25، الساعة: 18:00.

يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة و الثابت أن الدعوى الجزائية تمر على ثلاثة مراحل أساسية وهي مرحلة الاستدلالات ومرحلة التحقيق والمرحلة النهائية وهي المحاكمة، الأمر الذي يقودنا إلى معرفة المركز القانوني والموقع الإجرائي لقاضي التحقيق وتحديد صفة وصلاحياته وسلطاته، وبالرجوع إلى مختلف القوانين فأننا نجد أنها تسند مهمة التحقيق إلى الشرطة القضائية وهذه الجهة جمعت بين التحقيق و الإحالة أمام المحاكم، وكذلك بعض الأنظمة لم تعطي جهازا مطلقا لقاضي التحقيق وأن النيابة هي التي تقوم بالتحقيق، وذلك في الأنظمة الأنجلوسكسونية فإن صفة قاضي التحقيق تختفي تماما[1].

أما المشرع الجزائري المستمد من التشريع الفرنسي فإن قاضي التحقيق هو أول شخص يتولى التحقيق، وبقدر ما تزداد كفاءة المحقق وتضمن حياده واستقلاله بقدر ما يحافظ على الحريات، ونحن أمام أخطر دعوى جنائية تقام ضد شخص ينتمي إلى هذا المجتمع، أما بخصوص المشرع المصري، فإن التحقيق تقوم به النيابة العامة كأصل عام وقد قضت محكمة النقض المصرية بأن: "النيابة العامة شعبة من شعب السلطة القضائية خول الشارع أعضائها، من بين ما خوله لهم سلطة التحقيق والادعاء العام طبقا لنظامها ولائحته"[2].

وأننا نؤيد الرأي الذي يقسم التحقيق إلـــى:

- تحقيق أولي[3] والذي يناط به رجال الضبطية القضائية.

- تحقيق قضائي ويناط به رجال القضاء، وهذا التحقيق يقسم بدوره إلى تحقيق ابتدائي من اختصاص قاضي التحقيق، وتحقيق نهائي ويكون في مرحلة المحاكمة.

---

[1]- فضيل العيش، شرح قانون الإجراءات الجزائية النظرية و العملي، بدون طبعة، بدون دار نشر، الجزائر، ص 135.

[2]- سامح أحمد بلتاجي موسى، الجوانب الإجرامية للحماية الجنائية لشبكة الانترنيت، رسالة دكتوراه في الحقوق، جامعة الإسكندرية، مصر، 2010، ص 209.

[3]- فضلنا تسمية التحقيق الأولي تفاديا لأي التباس وتمييزا له عن التحقيق الابتدائي الذي هو تحقيق قضائي يقوم به قاضي التحقيق كما ذكرنا سابقا، فالمشرع لا يفرق بين التحقيق الأولي وهو ما يطلق عليه أيضا تحقيق جمع الاستدلالات والتحقيق الابتدائي و يبدوا ذلك جليا في نص المادة 63 ق.إ.ج التي تنص على أن: " ضباط الشرطة القضائية يقومون بالتحقيقات الابتدائية.."، في حين تنص المادة 66 ق.إ.ج أيضا الواردة في باب الثالث المتعلق بالأحكام الخاصة بقاضي التحقيق على أن:" التحقيق الابتدائي وجوبيا في مواد الجنايات..." وهو بذلك يعتبر أن التحقيق الذي يباشره سواءا رجال الضبطية القضائية أو قضاة التحقيق يعد تحقيقا ابتدائيا على حد سواء.

وتعد مرحلة جمع الاستدلال أو البحث التمهيدي من المراحل الهامة في بناء الدعوى الجنائية لأنها هي المرحلة التي تسبقها، ويطلق هذا المصطلح على الإجراءات التي ينفذها أعضاء الضبط القضائي عند ارتكاب جريمة معينة ، وذلك تمهيدا لوضع تم التوصل إليه بين يدي الجهة المختصة وهي النيابة العامة لتقرير ما تراه مناسبا بشأنها، ويقصد بمرحلة التحقيق التمهيدي مجموعة من الإجراءات التي يباشرها و ينفذها أعضاء الضبط القضائي عند وقوع جريمة ما وهذا تمهيدا لتحريك الدعوى العمومية.

ويعرفها الدكتور مأمون سلامة على أنها : " تلك الإجراءات التي تباشر خارج الدعوى العمومية وقبل البدء فيها بقصد التثبت من وقوع الجريمة، و البحث عن مرتكبيها[1]، و جمع الأدلة، و العناصر اللازمة للتحقيق".

ويرى الدكتور محمد الأخضر بأنّ مرحلة التحري هي:" مرحلة البحث عن الجرائم واكتشافها وإبلاغ النيابة العامة بها وقد خولها القانون صلاحية البحث عن مرتكبي الجرائم وجمع ما يتناهى إليهم من أدلّة إثبات إلى غاية فتح تحقيق قضائي".

أمّا الدكتور محمد علي سالم عياد الحلبي فيرى بأنّ: " مرحلة التحري والاستدلال هي إجراءات تمهيدية لإجراء الخصومة الجنائية ومستمرّة بعدها وضرورة لازمة لتجميع الآثار والأدلة والمعلومات، بهدف إزالة الغموض والملابسات المحيطة بالجريمة وملاحقة فاعليها".

ويعرفها الأستاذ أحمد غاي على أنها :" مجموعة الإجراءات الأولية التي يباشرها أعضاء الضبط القضائي بمجرد علمهم بارتكابها، والتي تتمثل في البحث عن الآثار الأدلة والقرائن التي تثبت ارتكاب تلك الجريمة و البحث عن الفاعل و القبض عليه وإثبات ذلك في محاضر تمهيدا للتصرف في الدعوى من طرف النيابة "[2].

---

[1]– إجراءات البحث والتحري لم يذكرها القانون على سبيل الحصر، بل وضع قاعدة عامة تخول لمأمور الضبط أن يقوم بأي إجراء من شأنه الكشف عن الجريمة ومرتكبيها وتعقبهم لتقديمهم للسلطة المختصة، بمعنى القيام بأي إجراء من شأن الكشف عن الجريمة ومرتكبيها وجمع الأدلة، وتتميز بعدم تعريضها للحقوق و الحريات ، فإجراءات الاستدلال ليس فيها تعرض لهذه الحقوق و الحريات، نظرا لطبيعتها شبه القضائية. أنظر: عبد الله اوهابية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق، دار هومة، الجزائر، 2004، ص 11-12.

[2] – أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، الطبعة الثالثة، دار هومة، الجزائر، 2011، ص 27.

هذه بعض التعريفات الفقهية[1].

أما مرحلة التحقيق الابتدائي فتعتبر أولى مراحل الخصومة، وهي المرحلة التي و إن كانت تسبق المحاكمة، فهي المرحلة التي تمهد لها، أي لمرحلة الفصل في الدعوى الجنائية، وقد وصف التحقيق في هذه المرحلة بأنه "ابتدائي"، لأن غايته ليست كامنة فيه، وإنما سيهدف التمهيد لمرحلة المحاكمة، وليس من شأنه الفصل في الدعوى لا بالإدانة ولا حتى بالبراءة، وإنما مجرد استجماع العناصرالتي تتيح لسلطة أخرى ذلك[2].

ومن خلال هذه المرحلة يتم تحريك الدعوى الجنائية، ويتم تمحيص الأدلة القائمة على نسبة الجريمة إلى فاعل معين و الكشف عن الحقيقة، ويثبت من خلال هذه المرحلة حق الدولة في العقاب، ومحاولة جمع أدلة جديدة تخدم تحقيق الجريمة التي وقعت، فيتم خلالها البحث عن الحقيقة قبل وصول القضية للمحكمة، وذلك من خلال إجراءات تملكها سلطة التحقيق[3] .عندما يتعلق الأمر بالجريمة الإلكترونية لأنها تعد حجر الزاوية الذي سيت عن مساسه بناء الدعوى برمتها فما يتم جمعه من معلومات وأدلة رقمية في المرحلة التي تعقب ارتكاب الجريمة مباشرة قد لا يبق متاحا بعد مرور قصير على ارتكابها، والسبب في ذلك يعود إلى الطبيعة التقنية في هذه الجرائم ففي الكثير من الجرائم

---

[1]– بالرجوع إلى النصوص القانونية في مختلف التشريعات، نلاحظ أنها لم تورد تعريفا خاص لمرحلة التحقيق التمهيدي، إلا أنها أشارت إلى مضمونها في المواد التي تحدد مهام الضبطية القضائية واختصاصاتها، حيث تنص 3/12 ق.إ.ج.ج على مايلي: "ويناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها بتحقيق قضائي. "

= وفي نفس السياق تنص المادة 14 ق.إ.ج.ف على أن: " اختصاص جهاز الشرطة القضائية لمهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات و القوانين المكملة له، لجمع الأدلة و البحث عن مرتكبيها مالم يفتح تحقيق قضائي بشأنها "

[2]– محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية، القاهرة، 1995، ص 105.

[3]– هدى أحمد العوضي، استجواب المتهم في مرحلة التحقيق الابتدائي، مذكرة ماجستير في الحقوق، تخصص قانون عام، جامعة المملكة، البحرين، 2009، ص 34. مشار اليها في الرابط الالكتروني :

https://www.policemc.gov.bh › mcms-store › pdf ، يوم الإطـــلاع 2017/10/05،الساعة :20:00.

الإلكترونية لم يترك الجاني وراءه سوى ذلك التعبير الذي يعتري وجوه القائمين على تعقبه والممزوج بالإعجاب والإحباط معا[1].

تعد مرحلة التحقيق الابتدائي أو ما يطلق عليها مرحلة جمع الاستدلالات مرحلة هامة في سبيل التحري عن الجرائم وتبلغ هذه المرحلة أعلى مستوياتها

ونظرا لخلو التشريعات من تعريف للتحقيق الابتدائي تاركة ذلك للشراح و الفقهاء من أهل القانون، لذا وجدت تعريفات كثيرة للتحقيق الابتدائي تتشابه في مضمونها وإن اختلفت من حيث الشكل .

فيعرفه البعض بأنه "مرحلة قضائية تتمثل في قيام المحقق بالتحقيق في القضايا الهامة التي أقيمت بها الدعوى، وهو مرحلة وسطى تلي مرحلة الأولى وتسبق مرحلة التحقيق النهائي أو المحاكمة "[2].

وعرفه البعض الآخر بأنه:" البحث الذي يتولاه الموظفون المختصون به لجمع أدلة الجريمة المنسوبة للمتهم وتقدير ما إذا كانت الأدلة كافية أم لإثباتها عليه "[3].

ويعرفه الأستاذ علي زكي العرابي بأنه:" دور من أدوار الدعوى العمومية سابق على رفعها، والغرض منه جمع الأدلة والتثبت من صحتها وكفايتها لإحالة الدعوى إلى المحاكمة، وينتهي إما بالأمر بحفظ الدعوى أو بأن لاوجه لإقامتها وإما بالإحالة إلى المحكمة"[4].

كما ذهب الأستاذ جندي عبد المالك إلى تعريفه بأنه : " جميع الإجراءات التي يراها قاضي التحقيق ذات فائدة لإظهار الحقيقة مادامت الإجراءات داخلة ضمن الإطار القانوني."

كما عرفه الأستاذ عاطف النقيب : "هو التحقيق الذي يقوم به قاضي التحقيق والهيئة الإتهامية في بعض الحالات لجمع الأدلة على الجرائم وفاعليها واتخاد القرار النهائي على ضوئها بإحالة الدعوى

---

[1]– محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011، ص 230.

[2]– عماد أحمد هاشم الشيخ خليل، ضمانات المتهم أثناء مرحلة الاستجواب، مذكرة ماجيستر في القانون الجنائي، كلية الحقوق، جامعة العالم الأمريكية، 2006، ص20، مشار إليها في الرابط الالكتروني:
www.riyadhalelm.com › researches › 64_zmanat_istjwab يوم الإطـــــــلاع 2017/10/05، الساعة:18:00.

[3]– فضيل العيش، المرجع السابق، ص 136.

[4] – عماد أحمد هاشم الشيخ خليل، المرجع السابق، ص 20.

على المحكمة إذا كان الجرم قائما، والأدلة كافية أو لمنع المحاكمة إذا كان الجرم قد سقط أو لم تكتمل عناصره، أو لم تتوافر الدلائل والقرائن بحق الدعوى عليه"[1].

ويعرفه الدكتور محمد زكي أبو عامر بأنه :" إجراءات تصدر عن سلطة معينة وفي شكل محدد ولغاية بذاتها"[2].

ونظرا لعدم الخلط بين جمع الاستدلال وبين التحقيق الابتدائي، فقد رأينا في هذا المقام أن نتعرض للتفرقة بينهما، ويمكن القول أن مواطن الاختلاف بين هاتين المرحلتين تتجلى في عدة نقاط وذلك على النحو التالي:

- لا يعد الاستدلال مرحلة من مراحل الدعوى العمومية بل هو مرحلة سابقة على تحريكها[3]، وفي ذلك ترى محكمه النقض المصريةأنه:" لا تنعقد الخصومة ولا تتحرك الدعوى الجنائية إلا بالتحقيق الذي تجريه النيابة العامة دون غيرها بوصفها سلطة تحقيق سواءا بنفسها أو بمن تندبه لهذا الغرض من مأموري الضبط القضائي أو برفع الدعوى أمام جهات الحكم، ولا تعتبر الدعوى قد بدأت بأي إجراء آخر تقوم به سلطات الاستدلال ولو في حاله التلبس بالجريمة[4]، أما التحقيق الابتدائي فهو مرحلة من مراحل الدعوى العمومية.

والتفرقة بينهما لا ترجع إلى اختلاف السلطة التي تباشر كلا منهما، فقد تقوم بالعملية سلطة واحدة، ولكن الذي يميز بينهما هو أن مرحلة الاستدلال تعد بمثابة تحضير للتحقيق، إذ يهدف أساسا إلى جمع عناصر الإثبات المادية لتحضير التحقيق الابتدائي[5]، أي أن أعمال الاستدلال لا تتولد عنها أدلة في مدلولها القانوني، لا يجوز أن يكون كل سند القاضي في حكمه محضر الاستدلال، ما عدا ما ورد في نص على سبيل الاستثناء، ولكن يجوز أن يكون الاستدلال أساسا للتحقيق يجرى في الجلسة وسيتخلص منه الدليل، والسبب في استبعاد نشوء الدليل عن أعمال الاستدلال أنه لا تتوافر فيها

---

[1] – فضيل العيش، المرجع السابق، ص 136.

[2] –عماد أحمد هاشم الشيخ خليل، المرجع السابق، ص 20.

[3]– عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر، ص 55.

[4]– سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص124– 125 .

[5]– عبد الرحمان خلفي، المرجع السابق، ص 125. أنظر أيضا: عماد أحمد هاشم الشيخ، المرجع السابق، ص، 35.

ضمانات الدفاع المتطلبة لنشوء الدليل، أما التحقيق فتتوافر فيه الضمانات اللازمة لحقوق الدفاع[1]، وهذا ما يجعل القاضي قد يبني حكمه بناءا على ما ورد في محضر قاضي التحقيق[2].

- أن الاستدلال مجرد جمع المعلومات، وهذا ما يجعله لا ينطوي على إجراءات القهر والإكراه التي تمس الحرية، عكس مرحلة التحقيق التي يمكن فيها قاضي التحقيق استعمال وسائل القهر كي تساعده على كشف الحقيقة[3].
- كما أن أعمال الاستدلال لا تقطع التقادم في الدعوى العمومية عكس إجراءات التحقيق[4]، وفي جميع أنواع التحقيق هذه يكون للقائمين عليه من ضبطية قضائية وقضاة صلاحية ممارسه إجراءات البحث والتحري وفقا لقانون الإجراءات الجزائية، وهو الأمر الذي يفهم صراحة من خلال استقراء نص المادتين 12و38 من ق.إ.ج.ج الواردتين في الباب الأول من هذا القانون تحت عنوان" في البحث والتحري عن الجرائم" ، حيث تنص المادة 3/12 ق.إ.ج.ج علي أنه "يناط بالضبط القضائي مهمته البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها تحقيق قضائي"، كما تنص المادة 38 ق.إ.ج.ج أيضا على أنه:" يناط بقاضي التحقيق إجراءات البحث والتحري، ولا يجوز له أن يشترك في الحكم في قضايا نظرها بصفته قاضيا للتحقيق و إلا كان ذلك الحكم باطلا....."

وعليه يمكن القول بأن إجراءات البحث هي من صلاحيات جهات التحقيق سواء كان أوليا أم ابتدائيا، وبهذا المفهوم فإن إجراءات البحث والتحري التي يباشرها رجال الضبط القضائي تصب في إطار التحقيق الأولى، بينما هذه الإجراءات عندما يباشرها قاضي التحقيق تعتبر تحقيقا ابتدائيا.

و بما أن التحقيق عموما يعتمد على ذكاء المحقق وفطنته وقوه ملاحظته وسرعة البديهة لديه، وأن يحاول بكل الجهد الممكن أن يقوم بالتحقيق في الجريمة ومتابعتها والبحث فيها وفي الأدلة والتنقيب عنها وصولا لإظهار الحقيقة، فإن التحقيق في البيئة الإلكترونية يستوجب بالإضافة إلى كل هذا

---

[1]– راجع نص المادة 100، 105 وما يليها من ق.إ.ج .

[2]– عبد الرحمان خلفي، المرجع السابق، ص، 55.

[3]–سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص 126.

[4]– عبد الرحمان خلفي، المرجع السابق، ص 55.

تطويرا لأساليبه، وتكليف جهات مختصة لممارسته من أجل مواكبة الجريمة و تطور أساليب ارتكابها في هذه البيئة[1].

الفرع الثاني: شروط التحقيق في الجرائم الإلكترونية

من المقرر والمعروف أن التحقيق في الجرائم الإلكترونية، بل وفي الجرائم التقليدية، يتطلب توافر عدة شروط أساسية، تلخص في مايلي:

أولا: أن يكون التحقيق بصدد جريمة (جناية أو جنحة)

يقصد بذلك أن تكون جريمة معاقب عليها في القانون، فلا شأن للمحقق بعمل لا يشكل جريمة، ويجري التحقيق واقعة توصف بأنها جناية أو جنحة، فبمجرد وقوع الجريمة يبدأ عمل المحقق للتأكد من وقوعها ومعرفه من ارتكبها؟ وما نوع هذه الجريمة؟ وما هو النص القانوني الذي ينطبق عليها؟ وبذلك يتم تكييفها تكييفا قانونيا سليما، حيث أنه في حالة عدم النص القانوني الذي ينطبق علي الجريمة المرتكبة، فيجب إصدار أمر بأن لا وجه لإقامة الدعوى أو يصدر أمر بحفظ الأوراق لعدم الجريمة، وذلك بناءا على أمر صادر من السلطة المختصة، ويعتبر هذا الشرط تطبيقا لمبدأ (لا الجريمة و لا عقوبة إلا بنص) ، وبناءا عليه لا يمكن توجيه اتهام ضد أي شخص مالم يكن منصوصا عليه قانونا.

فالمبدأ العام في القضايا الجنائية أن التحقيق فيها وجوبيا، وهذا ما نصت عليه المادة 66 من ق.إ.ج.ج فلا يجوز إحالة المتهم بجناية إلى جهات الحكم دون المرور عبر التحقيق، وذلك لخطورة هذا النوع من الجرائم والعقوبات المترتبة عليها من جانب، ولكون التحقيق فيها وسيلة دفاع المتهم، ووسيلة مساعدة لجنة الحكم في تقرير العقوبة أو التدبير الملائم للمتهم من جانب آخر.

ويعد فتح التحقيق في مواد الجنايات قاعدة من النظام العام يترتب على مخالفتها النقض، وعليه قاضي التحقيق ملزم بإجراء التحقيق حتى ولو كانت الحقيقة في شأن الجريمة والمسؤولية عنها واضحة جليا.

أما التحقيق في مواد الجنح يكون مطلوبا وضروريا كلما كانت القضية معقدة وخطيرة، وكلما تطلب الأمر اتخاذ إجراء من إجراءات التحقيق، يدخل طبيعيا في اختصاص قاضي التحقيق كاقتضاء وضع الشخص رهن الحبس المؤقت أو إجراء خبرة أو إنابة قضائية في الخارج.

[1]– نعيم السعيداني، المرجع السابق، ص 103.

كما أن فتح التحقيق يعد ضروريا أيضا إذا ما بقيّ مرتكب الجريمة مجهولا أو فارا أو أنهّ لجأ إلى خارج الوطن.

أما فيما يخص مواد المخالفات التي تعد أقلّ الجرائم خطورة فإن التحقيق فيها يكون دائما جوازياً بمعنى بإمكان وكيل الجمهورية طلبه إذا ما رأى ضرورة ذلك في القضية نتيجة غموض يكتنفها أو تشعب يحيط بالواقعة أو لإثبات حق أو إنشاء مركز قانوني محتمل[1].

ولكن ما تجدر الإشارة إليه هو وفقا للقانون فتح التحقيق في مواد المخالفات على شرط، بحيث أنّ طلب فتح التحقيق مقصور فقط على وكيل الجمهورية كممثل للنيابة العامة دون غيره.

وعليه يفهم من نص المادة (66 ق.إ.ج.ج) أنه من كان ضحية مخالفة لا يمكنه التأسس كطرف مدنيا بغرض تحريك الدعوى العمومية، وبالتالي فتح التحقيق غير أنه بالمقابل لا يوجد أي مانع يحول دون تأسسه كطرف مدني إذا ما فتح التحقيق بناءا على طلب وكيل الجمهورية[2].

و يكفي أن يتوافر في الجريمة محل التحقيق ركنها المادي[3] المكون لها، ومن القواعد العامة للركن المادي في الجريمة أن يحدد المشرع السلوك الإجرامي في كل جريمة ضيقا واتساعا على نحو يمكن القاضي من تكييف السلوك الإجرامي أو فعل الجريمة ورده إلى القاعدة القانونية أو النص التجريمي الذي يحكمه، وفي الجرائم الإلكترونية يتطلب القيام بالسلوك الإجرامي وجود حاسب آلي و أحيانا تتطلب الجريمة أن يكون متصلا بشبكة الأنترنيت، كما يتطلب أيضا معرفة بداية هذا النشاط والشروع فيه نتيجته.

فمثلا قد يقوم مرتكب الجريمة بتجهيز الحاسب الآلي لكي يحقق له حدوث الجريمة، فيقوم بتحميله ببرامج اختراق، أو يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل

---

[1]–عمارة فوزي، قاضي التحقيق، أطروحة دكتوراه العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2009–2010، ص39.

[2]– عمارة فوزي، المرجع السابق، ص 39.

[3]– يعرف الركن المادي للجريمة التقليدية أنه سلوك إجرامي معين يتطلبه القانون كمناط للعقاب على هذه الجريمة، على أن تتحقق نتيجة ضارة لهذا السلوك الإجرامي، كشرط بذاته يتعين قيامه حتى يعاقب على الجريمة،كما يجب أن يرتبط النشاط أو السلوك الإجرامي والنتيجة الضارة بعلاقة السببية أو ما يعرف بالإسناد المادي. أنظر: رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، الطبعة الثالثة، دار الفكر العربي، القاهرة، بدون سنة النشر، ص 188 وما يليها.

مواد مخلة بالآداب العامة وتحميلها على الجها، كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها[1].

والسلوك الإجرامي في الجرائم المعلوماتية يختلف حسب نوع الجريمة فأحيانا، يكون نشاطا واحدا في الجرائم البسيطة كفعل الدخول غير المصرح به إلى نظام المعالجة الآلية للمعطيات الذي يتحقق بفعل الدخول غير المشروع، إذ أن عدم مشروعية الفعل تقترن بكون الدخول غير مصرّح به، بينما يكون السلوك الإجرامي في جريمة السرقة المعلوماتية و الإتلاف العمدي للمعلومات والبرامج، أو جريمة القرصنة أو الاحتيال المعلوماتي سلوك إجرامي متعددا ينطلق من الدخول إلى نظام الحاسب الآلي، أو إلى موقع ما على شبكة الأنترنيت بوجه غير شرعي ثم القيام بالتلاعب بمحتوياته، هذا التلاعب الذي ينطوي على عدة أنشطة إجرامية من إدخال لبيانات غير صحيحة أو محوها أو تدمير لمحتويات هذا النظام، أو نشر لمواد مخلّة بالنظام ولآداب العامين[2].

كما أن السلوك الإجرامي في الجرائم الإلكترونية قد يكون وقتيا أي يبدأ وينتهي بمجرد تمامه مثل جريمة السرقة المعلوماتية، وقد يكون مستمرا مثل إنشاء مواقع تحريض القصر على الفسق والدعارة أو مواقع معادية بغرض الترويج للإرهاب.

أما الركن المعنوي في الجريمة الإلكترونية ويمكن القول بأنها جرائم عمدية، يستوجب المشرع فيها توفر القصد الجنائي بركنيه العلم و الإرادة، إذ يجب أن تتجه إرادة المجرم إلى ارتكاب سلوك يحظره القانون، كالاعتداء على نظام المعالجة الآلية معطيات، بما يشمله من صور كفعل الإدخال للبيانات أو المحو أو التعديل، أو إلى نسخ البرامج بوجه غير شرعي من موقع على شبكة الأنترنيت أين يقوم القراصنة بفك_شفيرة الموقع أو تخريبه للحصول على البرمجيات، إما للمنفعة المادية أو لإيقاع الضرر بالشركة المعتدى على منتجها.

و يختلف الركن المعنوي في الجرائم الإلكترونية من جريمة إلى أخرى، فجريمة الدخول غير المصرّح به إلى نظام الحاسب الآلي تتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة، أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرّح به يعد جريمة، باعتبار حماية المشرع محل الحق وهو جهاز الحاسب الآلي بما يتضمنه من معلومات وبرامج، وعلى

[1]– عبد اللطيف معتوق، المرجع السابق، ص23 .

[2]– عبد اللطيف معتوق، المرجع نفسه، ص23 .

هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهوا[1] ينفى عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله الغير الشرعي.

وفي جريمة الاحتيال المعلوماتي التي بدورها تعتبر جريمة عمدية، يتطلب المشرع قصدا جنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترك في جريمة الاحتيال المعلوماتي هو القصد الجنائي العام والخاص (نية التملك)[2].

فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيّته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع.

أما فيما يخص جريمة إتلاف المعلومات فاشترط المشرع توفر القصد الجنائي العام فقط، حيث يكفي علم الجاني بأنه يقوم بأعمال من شأنها أن تؤدي إلى إتلاف المعلومات أو محوها[3].

فالبحث في مسؤولية الجاني عن الواقعة غير المشروعة، يبحثها القاضي بمناسبة الدعوى الجزائية، ويلزم أن تكون تلك الجريمة من جرائم تقنية الحاسوب و الأنترنيت.

ثانيا: أن تكون الجريمة قد وقعت فعلا أو ترجح وقوعها

العبرة في اتخاذ الإجراءات في شأن الجرائم الإلكترونية أن تكون الجريمة محل التحقيق قد وقعت فعلا أو ترجح وقوعها، فلا يجري التحقيق بشأن جريمة محتملة، و إلا كان الإجراء باطلا.

وفي هذا الصدد يثور التساؤل حول أمرين:

- الأول: الإجراءات السابقة على مباشرة التحقيق والتي تجري لكشف جريمة ثم الإعداد أو التخطيط لارتكابها.
- والثاني: إجراءات الضبط الإداري التي تتخذ للعمل على منع وقوع الجريمة.

---

[1]– يعني إذا دخل الشخص صدفه في نظام المعالجة الآلية، فلا يعاقب على ذلك. وعليه يجب أن يكون مرتكب الجريمة على علم بأنه دخل إلى النظام المعلوماتي بطريقه غير عاديه أي انه على علم بان الدخول إلى هذا النظام ممنوع، الجريمة لا تكون مؤسسة أمام القاضي الجزائي إلا بإثبات عمليه الدخول.

[2]– محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011، ص 180.

[3]– عبد اللطيف معتوق، المرجع السابق، ص 24.

و مما لا شك فيه أن لمأمور الضبط القضائي أن يباشر إجراءات الاستدلال وجمع التحريات بشأن وجود دلائل كافية على وجود جريمة قامت الدلائل الكافية على وقوعها، كأن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على ارتكابه جريمة في الجنايات عموما دون تحديد لنوعها [1].

كما أن التحري والاستدلال بشأن الجرائم تقليدية أم تقنية، من صميم عمل مأمور الضبط القضائي، وقيام هذا الأخير بضبط جريمة في حاله تلبس بناءا على هذه التحريات يكون صحيحا، ولا يعتبر تحريضا على الجريمة[2].

وحول مدى تحقق صور الجريمة المشهودة في نطاق المعلوماتية، فيرى البعض أن بالإمكان تحققها، في حال أن يكتشف مأمور الضبط القضائي أو المجني عليه أثناء قيامه باختراق شبكة، أو نظام معلوماتي، أو قاعدة بيانات تابعة للمجني عليه، ويكون لديهما الإمكانية الفنية لمطاردة الجاني وتتبعه بقصد معرفته.

ومثال ذلك قيام شركة (AOL) وهي شركة خدمات أنترنيت (ISP) بالولايات المتحدة الأمريكية باكتشاف أنشطة دعارة وترتيب لقاءات جنسية مع أطفال أثناء قيامها بمراقبة أنشطة

---

[1]– سرحان حسن المعيني، التحقيق في جرائم تقنيه المعلومات، الفكر الشرطي، المجلد عشرون، العدد الرابع، رقم 79، الشارقة، الإمارات العربية المتحدة، 2011، ص48.

[2]– نصت المادة 41 ق.إ.ج.ج على حالات التلبس بقولها" توصف الجناية أو الجنحة بأنها في حالة تلبس إذا كانت مرتكبة في الحال أو عقب ارتكابها"،كما تعتبر الجناية أو الجنحة متلبسا إذا كان الشخص المشتبه في ارتكاب إياها في وقت جدا من وقت وقوع الجريمة قد تبعه العامة بالصياح أو و جدت في حيازته أشياء أو وجدت أثار أو دلائل تدعوا إلى افتراض مساهمته في الجناية أو الجنحة.

وتتسم بصفة التلبس كل جناية أو جنحة وقعت و لو في غير الظروف المنصوص عليها في الفقرتين السابقتين، إذا كانت قد ارتكبت في منزل و كشف صاحب المنزل عنها عقب وقوعها و بادر في الحال باستدعاء أحد الضباط الشرطة القضائية لإثباتها"

يفهم من نص المادة على وجود قرائن تدل على مساهمته، كذلك نصت المادة 30 من ق.إ.ج.م على حالة التلبس بالجريمة بقولها " تكون الجريمة متلبسا بها حال ارتكابها أو عقب ارتكابها ببرهة يسيرة ، و تعتبر الجريمة متلبسا بها إذا اتبع المجني عليها مرتكبيها أو تبعته العامة مع الصيّاح إثر و وقوعها، أو إذا وجد مرتكبيها بعد وقوعها بوقت قريب حاملا آلات أو أسلحة أو أمتعة أو أوراق أو أشياء أخرى يستدل منها على أنه فاعل أو شريك فيها أو إذا وجدت في الوقت آثار أو علامات تفيد ذلك"

المشتركين لديها، وعلى الفور قدمت أسماء المشتبه بهم للمباحث الفدرالية الأمريكية التي تمكنت من القبض على العشرات منهم بعد مراقبة أنشطتهم[1].

وأيضا يمكن مشاهدة الجريمة حال حدوثها من خلال الأنترنيت إذا شاهد مأمور الضبط القضائي أو الغير الجريمة حال ارتكابها، ففي مثل هذه الحالة تتحقق صورة الجريمة المتلبس بها بالمشاهدة عن بعد وعبر موجات كهرومغناطيسية، مثلها مثل المشاهدة المادية الملموسة التي نصت عليها القوانين التقليدية.

ومثال ذلك ملاحظة صاحب مقهى الأنترنيت لشخص يقوم ببث صورا إباحية لفتاة عبر الانترنيت مستخدما حاسب آلي في المقهى، فيقوم على الفور بإخطار السلطات المعنية بوجود جريمة ترتكب داخل مقهى الأنترنيت المملوك له، لأن وزارة الداخلية المصرية تلزم أصحاب مقاهي الأنترنيت بالإخطار الفوري لأية جرائم يلاحظونها من مرتادي تلك المقاهي، و إلاّ تعرضوا لعقوبات إدارية قد تصل لحد غلق المقهى، وانتقلت السلطات المعنية بناءا على إخطار صاحب مقهى الأنترنيت، فيشاهد مأمور الضبط القضائي الجريمة حال ارتكابها[2].

و يمكن أيضا أن تتحقق صورة مشاهدة الجريمة عقب ارتكابها ببرهة يسيرة[3]، و مثال ذلك قيام صاحب إحدى محلات الأنترنيت بمراجعة الحاسوب عقب انتهاء العميل من استخدامه، ملفات غريبة وبالإطلاع عليها يجد أنها تحتوي على صور دعارة تم إنزالها أثناء عمل العميل الذي ينتظر دفع الحساب، وهنا تكون حاله التلبس قائمة، أما في حالة ما إذا غادر هذا الأخير مقهى الأنترنيت وابتعد عنه ويترتب على ذلك عدم قيام حالة التلبس.

ومع تطابق قيام التلبس في الجريمة التقليدية في حاله تتبع المجني عليه للجاني أو الغير عقب ارتكاب الجريمة مع الصّياح، إلا أن الصيّاح في الجريمة الإلكترونية غير متصور حدوثه، لأن الملاحقة تتبع اللتان تتم إنما هي إجراءات افتراضية، ومع ذلك فيوجد رأي بعدم اشتراط الصيّاح أثناء

---

[1]- فايز محمد راجب غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني أطروحة الدكتوراه، كليه الحقوق، فرع القانون الجنائي و العلوم الجنائية، جامعه الجزائر (1)، 2010-2011، ص288.

[2]– أحمد سعد محمد الحسني، الجوانب الإجرائية الناشئة عن استخدام الشبكات الإلكترونية، أطروحة الدكتورة، كلية الحقوق، قسم القانون الجنائي، عين شمس، 2012، ص 42.

[3]– يقصد بذلك أن تكون الجريمة قد وقعت منذ لحظة أو لحظات قصيرة، وتمت بالفعل لكن آثارها لازالت بادية تبني عن وقوعها ونارها لم تخمد بعد.

التتبع والملاحقة في الجريمة التقليدية، وذلك في حالة أن يكون المجني عليه أخرص أو لا يستطيع الصيآح لأي سبب كان.

غير أن قيام حالة الجريمة المتلبس بها تعترضها بعض المشكلات منها لزوم كشف حالة التلبس بالمشروعية[1]، بمعنى أن الإجراء اللازم لكشف حالة التلبس يجب أن يكون مشروعا، وهذا يكون محل صعوبة في مجال الجريمة الإلكترونية نظرا لحداثتها وعدم وجود نصوص قانونية لتنظيمها، أضف إلى ذلك تداخل القيام بالإجراء مع موضوع الحرية الشخصية التي يجب أن تكون مصانة بالقدر اللازم والضروري للحفاظ على حقوق الأفراد وحرياتهم، وبالتالي يجب أن يكون الإجراء منصوصا عليه في القانون.

وفي هذه المسألة تثار مشكلة مشروعية التخفي عبر الأنترنيت من قبل القائم بعمل التحريات، سواء بهدف الكشف عن جريمة محددة حدثت، أم بغرض التوصل إلى البحث عن الجرائم ومرتكبيها بشكل عام، فغالبا ما يقوم عناصر من التحريات في بلد ما بالتخفي واتخاذ أسماء وهمية ومن تم الولوج إلى الأنترنيت، والدخول إلى غرف المحادثات وحلقات النقاش، وتبادل الحديث مع الغير بقصد التوصل إلى نتائج غير محددة تتمثل في التوصل إلى مرتكبي جرائم معينة، كما قد يتم التوصل إلى نتائج غير محددّة بهدف البحث عن الجرائم ومرتكبيها[2].

كما توجد مشكلة أخرى في حال حساب الزمن اللازم لقيام حالة التلبس والتي غالبا ما يترك أمر تحديدها لمأمور الضبط القضائي شريطة عدم تجاوزها مدّة محددة، حيث أن المدة بالنسبة للجريمة التقليدية قد قدرها البعض بساعات وفي الغالب بيوم أو يومين والمهم أن لا يكون في تقدير الزمن إسراف، بخلاف مدة التلبس في الجريمة الإلكترونية والتي يصعب تحديدها إذا كان في الأمر مطاردة[3].

---

[1]– لا يكفي أن يكون التلبس سابقا من حيث الزمان على الإجراءات المخولة للضبطية القضائية في حاله التلبس و أن يشاهدها بنفسه، بل يلزم أن يكون اكتشافها قد تم بطريق مشروع، ويقصد بذلك أن تكون وسيلة الكشف عن الجريمة مشروعة و قانونية، فإن تم الاكتشاف بالمخالفة للطرق القانونية كان الإجراء باطلا ولا ينتج عنه أي اثر قانوني. أنظر: عبد الرحمان خلفي، المرجع السابق، ص 61-62.

[2]– فايز محمد راجب غلاب، المرجع السابق، ص 290.

[3]– فايز محمد راجب غلاب، المرجع نفسه، ص 290.

غير أنه لتوضيح كيفية قيام المطاردة عبر الأنترنيت، يتم اللجوء لبرمجيات دقيقة لتعقب الهكرة ومجرمي المعلوماتية عبر الأنترنيت، ويمكن لهذه البرمجيات تعقب المجرم بجدارة، ذلك أن الجاني يترك وراءه وبصمة تسمى البصمة الإلكترونية.

ولقد تم تطوير تقنية المطاردة والتتبع عبر الأنترنيت، بحيث أمكن التوصل إلى برمجيات يمكنها تتبع أولى محاولات المجرم المعلوماتي، مثل برمجية أتيكسATICD التي يمكنها التوصل إلى أول بصمة الكترونية للمجرم عبر الأنترنيت.

وبعد تحديد الجهاز المستخدم في ارتكاب الجريمة الإلكترونية، يمكن الوصول إلى مكانه و محل إقامة مستخدمه عن طريق (IP Adress) حيث يوجد في البريد الالكتروني رقم (IP) الخاص بكل جهاز متصل بالأنترنيت في خانة Header، فيقوم رجال الضبط القضائي بالذهاب إلى Mail option ، ثم General Préférence، إضافة Header ، ثم يقوم باختيار Show all Header On Inconing Message ثم يذهب إلى الرسالة المرسلة فيجب الـ (IP) المرسل المكون من أربعة أرقام يفصل بينهما نقطه في: X-Originating- IP، وبعد التوصل إلى (IP) الخاص بالجهاز المستخدم الذي يمكننا من تحديد الموقع الجغرافي، ومزود الخدمة و خط التليفون الأراضي أو شبكة (ADSL) [1] لمستخدم الجهاز الذي تم التوصل إلى(IP) الخاص بجهازك، ويمكننا بالتالي من تحديد محل إقامة مالكه[2].

فإن هذه الوظيفة تباشر وقوع الجريمة بهدف الحيلولة دون وقوعها، إلا أن ذلك لا يعني إنتهاء الضبط الإداري بوقوع الجريمة إذ يستمر الضبط الإداري مباشرة نشاطه لمنع تفاقم أثار الجريمة [3].

في هذا السياق يتميز الضبط القضائي في مجال كشف الجريمة عن الضبط الإداري الذي يسعى إلى حماية النظام العام بصورة وقائية من خلال مايلي :

1. الضبطية الإدارية تختلف عن الضبطية القضائية في طبيعتها و غايتها:

---

[1]– يعرف خط الاشتراك الرقمي غير المماثل (ADSL) بأنه: تقنية الشبكة التي تنقل البيانات بسرعة على خطوط الهواتف النحاسية التناظرية ANALOG و بشكل غير مماثل، حيث تتحرك البيانات في اتجاه واحد و بسرعة أكبر من الاتجاهات الأخرى.

[2]– أحمد سعد محمد الحسيني، المرجع السابق، ص59.

[3]– طارق فوزي الفقي، المرجع السابق، ص 36.

فرجال الضبط القضائي هم أشخاص خولهم القانون هذه الصفة و أعطاهم سلطات معيّنة تبدأ بعد وقوع الجريمة لمعرفة ظروف وملابسات المتعلقة بارتكابها وجمع الاستدلالات اللاّزمة لكشف الحقيقة، في المقابل يقوم أعضاء الضبطية الإدارية بحفظ الأمن العام واتخاذ الاحتياطات اللازمة لحماية المجتمع ومنع وقوع الجرائم ومراقبة المشتبه فيهم وترصدهم، وتنفيذ اللوائح و التقيد بها.

وهذه الوظيفة الرئيسية الموكلة لرجال الضبطية بحيث تنتهي لتبدأ مهمة الضبطية القضائية عند وقوع الجريمة والبحث عن فاعليها وتقديمهم للنيابة العامة[1].

2. رجال الضبط الإداري يتميزون عن رجال الضبط القضائي من حيث المسؤولية:

رجال الضبط الإداري يخضعون للقضاء الإداري ورقابته عن طريق قضاء الإلغاء والتعويض، أما رجال الضبط القضائي فيخضعون في ما يتعلق بعملهم ومدى صحته أو بطلانه للقضاء العادي.

3. الضبطية الإدارية تتميز عن الضبطية القضائية من حيث الهدف خلال ممارسة كل منهما لعملها:

فالضبطية الإدارية تسعى للمحافظة على الأمن العام لمنع وقوع الجرائم والحوادث، وتوفير الاستقرار والهدوء من خلال منع الحالات التي تخل براحة المواطنين.

أما بالنسبة لإجراءات الضبط الإداري التي تتخذ للعمل على منع الجريمة فيمكن القول أن هناك علاقة وطيدة بين الضبط الإداري والجريمة، ومبعث تلك العلاقة تتأثر من خلال سعي الضبط الإداري إلى منع وقوع تلك الجريمة وذلك باتخاذ الإجراءات و الوسائل التي تقلل من فرص ارتكابها، ومن تلك الوسائل التي تحقق للضبط الإداري غرضه في منع ارتكاب الجرائم مراقبة المشتبه فيهم وعمل الدوريات على النحو الذي يرتدع به المجرمين[2].

وقد صدر في إيطاليا سابقا قانون أطلق عليه قانون الجبُر على منع الجريمة مفاده أنه عندما تعلم الشرطة من خلال التحريات بأن هناك جريمة سوف ترتكب، فأنه يتعين عليها العمل على منعها[3] .

ويميز الفقه بين نوعين من الضبط: الضبط القضائي والضبط الإداري:

---

[1]– ممدوح حسن مانع العد، ضمانات المتهم أثناء التحقيق ومدى مراعاة مبادئ القانون الدولي لحقوق الإنسان في المجال الجنائي، رسالة الدكتوراه في القانون، كليه الحقوق، جامعه الإسكندرية، 2009، ص120. أنظر أيضا: عبد الرحمان خلفي، المرجع السابق، ص47.

[2]– طارق فوزي الفقي، المرجع السابق، ص38.

[3]– سرحان حسن المعيني، المرجع السابق، ص 38.

- فالضبط القضائي: يقصد به الإجراءات التي تتخذها السلطة الضبطية القضائية في التحري عن الجرائم بعد حدوثها، في سبيل القبض على مرتكبي ،هذه الجرائم، وجمع الأدلة اللّازمة لتحقيق و إقامة الدعوة لمحاكمة المتهمين، وإنزال العقوبة على من ثبتت إدانته وفق إجراءات غاياتها علاج أثار الجرائم وردع مرتكبيها بعد حدوثها، فالضبط القضائي لا يتحرك إلا بعد وقوع انتهاك للنظام العام، لمعالجة أثار هذا الانتهاك على خلاف الضبط الإداري الهادف النظام العام من الانتهاك قبل وقوعه[1]، وهو يمارس تحت السلطة الإدارية المتمثلة في وزارة الداخلية بالنسبة للشرطة وهدفه الوقاية من الجرائم[2].

- أمـا الضبط الإداري: فيعرف بأنه حق جهة الإدارة في فرض قيود تحد بها من الحقوق والحريات التي يتمتع بها الأفراد بقصد حماية النظام العام، الضبط الإداري وظيفته معينة أي أنها تستهدف حماية النظام العام من الإخلال بتوقي الجرائم و من تم فإن هذه الوظيفة تباشر قبل وقوع الجريمة بهدف الحيلولة دون وقوعها، إلا أن ذلك لا يعني إنتهاء الضبط الإداري لوقوع الجريمة إذ نجد أنفسنا أمام استمرار الضبط الإداري في مباشرة نشاطه لمنع تفاقم أثار الجريمة.[3]

أما رجال الضبط القضائي فإن عملهم يبدأ بإجراءات التحري والاستدلال و تعقب المجرمين، حيث منحهم القانون صلاحيات أوسع في مضمونها من صلاحيات رجال الضبط الإداري، فعملهم يتسع إلى حد القبض والتفتيش في حالات التلبس، ولخطورة هذه المهمة الموكلة لرجال الضبطية القضائية حرصت معظم التشريعات على حصرها بفئة معينة وعدم إعطائها لرجال الضبطية الإدارية[4].

ورغم أن الصلاحيات الممنوحة للقائمين بتنفيذ كل من الضبط الإداري والضبط القضائي، إلّا أنه قد تجتمع الوظيفتين معا في شخص واحد، كما لو قام مأمور الضبط القضائي بأعمال من قبيل الضبط الإداري، وتكشف له خلال ذلك أن هناك جريمة، فمن حق رجل الضبط القضائي في هذه الحالة اتخاذ الصلاحيات التي يمنحها له القانون، كما هو الحال في التفتيش الذي يجريه مأمور الضبط القضائي على أجهزه الحاسب في مقهى الأنترنيت أو في إحدى المؤسسات أو

---

[1]– عبد الغني بسيوني عبد الله، النظرية العامة في القانون الإداري، منشأة المعارف، الإسكندرية ، 2003، ص391.

[2]-JACQUES Leroy،Procédure Pénale Librairie Général de Droit et de Juris Prudence،L'extenso éd . Paris cedex 2009، P76.

[3]– طارق فوزي الفقي، المرجع السابق، ص 36.

[4]– ممدوح حسن مانع العد، المرجع السابق، ص122.

الشركات للتأكد من صلاحية البرمجيات، فيتبين عدم صلاحية البرمجيات المذكورة أو وجود صور منافية للآداب العامة، فاستخدامه صلاحية الضبط الإداري لا تعرفي من التحول إلى صفة الضبط القضائي، هذا و إن كان من الممكن اجتماع صفتي الضبط الإداري والضبط القضائي في شخص واحد، فإنّه من المتصور توافر الضبط الإداري دون الضبط القضائي مثل مزودوا الدخول وخدمات الأنترنيت إذ أن القانون يمنحهم الرقابة عبر المزود عن سير حركة العمل ومدى الخضوع للنظام قانون من قبل العاملين والمتعاملين بالأنترنيت، فإنه إذا ما اكتشف جريمة ما، لا يكون لرجل الضبط الإداري سوى التحفظ على أدلة الجريمة إلى حين حضور رجال الضبط القضائي[1] .

وتقوم الشرطة في نطاق القواعد العامة بأعمالها الإدارية من خلال الأعمال التنظيمية التي تصدرها الإدارة تنفيذا للقوانين، إذ تقوم بتنفيذ الأحكام الصادرة ضد المتهمين، و إيداعهم السجون، وتنفيذ النظام القانوني المعمول به في السجن كما تقوم بمنع بعض الأشخاص من السفر للخارج كإجراء وقائي في حدود اختصاصاتها[2] .

ومن أعمال الضبط الإداري ما تقوم به مصالح الدرك الوطني ببلادنا المختصة بالجرائم الإلكترونية، أو ما يطلق عليهم بدركي الأنترنيت من حرص و يقظة وتأهب وعمل على استباق الإجرام المعلوماتي حتى قبل وقوعه[3].

كما تقوم الهيئات المختصة في بعض الدول بأنشطة خادعة على الأنترنيت، كعرض صور فتيات غير حقيقية، لتلقي طلبات المهووسين بارتكاب جرائم الجنس على الأطفال، وتتبعهم لاتخاذ الإجراءات الكفيلة بردعهم.

و هذا لا يعني أن تقوم هذه الجهات المختصة بالتحريض على ارتكاب الجريمة لإلقاء القبض على أصحابها، فذلك مسلك منتقد، ويتنافى مع قرينه البراءة، وينتج عنه بطلان الدليل المبني على هذا الإجراء المعيب.

ومن تطبيقات ذلك ما حكمت به محكمه باريس بإبطالها تقرير التحقيق أولى للضبطية القضائية، ليس فقط لأن التنصت لم يتم وفقا للإجراءات القانونية الصحيحة، من أجل ذلك

---

[1]– طارق فوزي الفقيه، المرجع السابق، ص36–37.

[2]– إيهاب فوزي السقا، الحماية الجنائية و الأمنية بطاقات الإئتمان، دار الجامعة الجديدة، الإسكندرية، 2007، ص379.

[3]– عبد الحميد كرود، التسول النصب والاحتيال، عبر الانترنت، مجله الـــــدركي، العدد 16 ، 2008، ص 49.

الحصول على ترخيص من قاضي التحقيق، بل وأيضا لأن الشرطة دفعت بالمتهم طيلة شهرين على ارتكاب الجريمة عن طريق تحريضه على ذلك[1].

ثالثا: أن يجري التحقيق في مواجهة متهم معين بارتكاب الجريمة أو للبحث عنه

يتطلب ذلك معرفة من هو المتهم [2] بارتكاب الجريمة، سواء كانت إلكترونية أم تقليدية، وينصرف اصطلاح المتهم إلى الشخص الذي يوجه إليه الاتهام بارتكاب إحدى الجرائم المنصوص عليها في قانون العقوبات أو في أحد التشريعات الجنائية الخاصة كقانون مكافحة تقنية المعلومات، سواءا بوصفه فاعلاً أم شريكا فيها[3].

فالمتهم هو المدعى عليه في الدعوى الجنائية، و إجراءات الدعوى ينبغي أن تتخذ ضد شخص معين كونه هو الغاية التي تسعى إلى تحقيقها الدعوى الجنائية وهي إدانته بما توافرت لديها من أدلة يقينية.

لذا يعرف البعض المتهم هو كل شخص تحرك الدعوى الجنائية ضده لشبهة ارتكاب جريمة أو اشتراكه فيها.

ويعرف المتهم أيضا متى توافرت ضده أدلة وقرائن قوية كافية لتوجيه الاتهام إليه وتحريك الدعوى الجنائية قبله .

ونجد في كلا التعريفين فرقا واضحا وهو أنه في التعريف الأول تحرك الدعوى الجنائية ضد الشخص ويعتبر متهما لمجرد الاشتباه في ارتكابه الجريمة أو اشتراكه فيها، أما التعريف الثاني فتحرك الدعوى الجنائية ضد الشخص ويعتبر متهما إذا توافرت ضده أدلة وقرائن قوية وليس لمجرد الاشتباه به، وعليه فإن التعريف الثاني هو الأوفر حظا في القبول.

---

[1]- JACQUES Leroy،Op Cit،P 77.

[2]– المتهم لغة: من اتهم اتهاما أي رماه بالتهمة وظنه بها،شك في صدقة، و وقعت عليه التهمة، والتهمة أصلها الوهَم من الوهمْ ، ويقال اتهمته افتعال فيه، يقال اتهمت فلانا،على بناء افتعلت ،أي أدخلت عليه التهمة و التهمة الظن ، واتهم الرجل و اتهمه و أوهمه، أدخل عليه التهمة أي ما يتهم عليه ، واتهم الرجل ، إذا صارت به الريبة ، و اتهمته، ظننت فيه ما نسب إليه. أنظر: ابن منظور عبد الله العلايلي، لسان العرب ، المحيط ، المجلد الثالث ، الجزء الثاني، دار لسان العرب، بيروت، لبنان، بدون سنة نشر، ص 994.

[3]– سرحان حسن المعيني، المرجع السابق، ص 49.

كما أن المتهم هو كل شخص تثور ضده شبهات ارتكابه فعلا إجراميا، فيلتزم بمواجهه الادعاء لمسؤوليته عنه والخضوع للإجراءات التي يحددها القانون، وتستهدف تمحيص هذه هي الشبهات وتقدير قيمتها ثم تقرير براءته أو إدانته[1].

كما تم تعريف المتهم أيضا: بأنه شخص تفترض إدانته بجنحة أو جريمة فتح بصددها تحقيق، ومصطلح المتهم لا يطلق إلا على الشخص الذي وجه له اتهام وتحركت ضده الدعوى أم تم رفعها عليه بحسب الأحوال، فهذه الصفة تبدأ بتوجيه الاتهام وتنتهي بصدور مقرر حفظ أو أمر بأن لا وجه للمتابعة بعد اتهامه نهائيا، أما إذا صدر حكم بالإدانة فإن صفه المحكوم تحل محل صفه المتهم[2].

كما يعرف المتهم أيضا بأنه كل إنسان طبيعي على قيد الحياة صالح لاتخاذ إجراءات التحقيق معه أسند إليه الاتهام بجناية أو جنحة وتحركت بناء عليه الدعوى الجنائية [3].

ولقد جاءت التشريعات باصطلاحات مختلفة لتمييز المتهم عن غيره ممن يعترضون لذات الإجراءات[4]، وهذا ما يدعونا إلى التطرق لمعرفه المقصود بالمتهم في التشريعات العربية والتشريعات الأجنبية.

1- تعريف المتهم في التشريعات العربية:

لم تعرف بعض التشريعات العربية المتهم تعريفا واضحا، و جاءت هي الأخرى خالية من تعريف محددا له.

أ_ المقصود بالمتهم في التشريع المصري :

إن المشرع المصري لم يعرف المتهم سواءا في نصوص قانون العقوبات أو قانون الإجراءات الجنائية، رغم استخدامه للفظ متهم في كل مراحل الدعوى الجنائية ابتداءا من حاله اشتباهه في ارتكاب

---

[1]- هدى أحمد العوضي، استجواب المتهم في مرحلة التحقيق الابتدائي، مذكرة ماجستير في الحقوق، تخصص قانون عام، جامعة المملكة، البحرين، 2009، ص 18.

[2]- دليلة جلول، المرجع السابق، ص 26.

[3]- أحمد مهدي، أشرف الشافعي، التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها، الطبعة الأولى، دار الكتب القانونية، مصر، 2005، ص53.

[4]- إذا كان من السهل تعريف المتهم وغيره من المسميات كالمشتبه فيه والشاهد، إلا أنه من الصعب التفرقة بينهم خاصة في فتره جمع الاستدلالات، حيث توجد إجراءات في هذه المرحلة تتخذ ضد أشخاص لم ينسب إليهم بعد ارتكاب أية جريمة، كالتي تتخذ ضد من ينسب اليه ارتكاب الجريمة، الاستدعاء والاستيقاف والقبض والتحفظ وهي جميعها اجراءات يخضع لها المتهم والمشتبه فيه وشاهد اثناء مرحله الاستدلال مما يصعب معهم التفرقة بينهم.

الجريمة بما في ذلك مرحله الإستدلالات، ثم مرحله التحقيق الابتدائي ثم مرحله التحقيق الجنائي النهائي.

وهذا ما يلاحظ من نص المادة 29 ق.إ.ج.م و التي تنص على أنه: " لمأموري الضبط القضائي أثناء جمع الاستدلالات أن يسمعوا أقوال من لديهم معلومات عن الوقائع الجنائية ومرتكبيها وأن يسألوا المتهم عن ذلك"، ففي هذه المادة أطلق المشرع المصري المتهم على الشخص وأجاز سؤاله وهو خارج مرحلة الاتهام، وما يمكن ملاحظته أيضا أن المشرع لم يبيّن المقصود من المتهم، وإنما حدّده بالشخص الذي يجوز لمأمور الضبط القضائي أن يقبض عليه في حالة وجود دلائل كافية على اتهامه، حتى لو لم تؤدي هذه الدلائل لإثبات الواقعة ويكفي مجرد وجود الشبهة في وقوعها.

وهذا ما نصت عليه المادة 34 من ق.إ.ج.م بأنه : " مأمور الضبط القضائي في أحوال التلبس بالجنايات والجناح التي يعاقب بالحبس لمدة تزيد على ثلاثة أشهر، أن يأمر بالقبض على المتهم الحاضر الذي توجد دلائل كافية على إتهامه."

ب- المقصود بالمتهم في التشريع الأردني:

إن المشرع الأردني سار على خطى المشرع اللبناني وهذا ما يلاحظ من خلال نص المادة 4 من ق.إ.م.ج.إ التي تنص على أنه: " كل شخص تقام عليه دعوى الحق العام فهو مشتكي عليه ويسمى ظنينا، إذ ظنّ فيه بجنحة ومتهما إذا اتهم بجناية"، فالمشرع الأردني أطلق إسم المتهم على الشخص الذي ارتكب جنحة، على غرار المشرع اللبناني إلا أنه تختلف المسميات فعند إسناد الجريمة إليه يكون مشتكى عليه وليس مدعي عليه.

ت- المقصود بالمتهم في التشريع الكويتي:

لم يعرف قانون الإجراءات الجنائية الكويتي المتهم رغم استعماله بهذا اللفظ في أكثر من موضع وفي جميع مراحل الدعوى الجنائية، فبالرجوع إلى نص المادة 42 من قانون الإجراءات الجنائية الكويتي والتي تنص على أنه: " يثبت رجل الشرطة أثناء تحرير محضر التحري يبديه المتهم من أقوال وما يتقدم به من دفاع و إذا كانت أقوال المتهم تتضمن اعترافا بارتكاب جريمة فرجل الشرطة تدوينه مبدئيا في محضره ويحال المتهم إلى المحقق لاستجوابه والتثبت من صحة هذا الاعتراف" ، يتضح أن المشرع الكويتي إعتبر وصف المتهم يلحق الشخص حتى في مرحلة التحرّي، وكذلك ما نصت عليه المادة 43 من نفس القانون على أن:" لرجل الشرطة إذا شهد ارتكاب جناية أو جنحة..... أن يقوم بتفتيش المتهم ومسكنه."

ويذهب البعض إلى أن المشرع الكويتي فضل استعمال تعبير المتهم لسببين:

- السبب لأول: أن رجل الشرطة له صلاحيات واسعة منها القبض على الأشخاص إذا قدر كفاية الدلائل على ارتكاب الجريمة.
- السبب الثاني: أن المشرع يقرر عدة ضمانات للمتهم وهذه الضمانات منها ما يمكن أن يستفيد منها المتهم حتى في مرحلة التحري مع أن هذه الضمانة لا توازي اعتبار الشخص خارج دائرة الاتهام في هذه المرحلة، فالقول بإمكان الاستفادة من الضمانات المقررة للمتهم في هذه المرحلة يقابله عدم إمكان اتخاذ أي إجراء ضده في حالة عدم تمتعه بوصف المتهم ولا شك في أفضلية الوضع الثاني على الوضع الأول.

ث- المقصود بالمتهم في التشريع البحريني:

استخدام المشرع البحريني اللفظ المتهم غير أنه لم يقم بتعريفه، حيث تنص المادة 50 ق.إ.ج.ب على أنه" لمأمور الضبط القضائي أثناء جمع الاستدلالات أن يجروا المعاينات اللازمة وأن يسمعوا أقوال من لديهم معلومات عن الجرائم ومرتكبيها وأن يسألوا المتهم عن ذلك وللمتهم والمجني عليه والمدعى بالحقوق المدنية والمسئول عنها ولوكلائهم أن يحضروا هذه الإجراءات كلما أمكن".

وأيضا نصت المادة 55 من نفس القانون على ما يلي:" لمأمور الضبط القضائي في الجنايات والجنح المتلبس بها التي تزيد مدة الحبس فيها ثلاثة أشهر أن يقبض على المتهم الحاضر الذي توجد دلائل كافية على اتهامه، وما يمكن قوله في هذا الصدد أنه على المشرع البحريني إعطاء تعريف محدد وواضح للمتهم، حيث أطلق وصف المتهم على الشخص وهو في مرحلة جمع الاستدلالات دون تحديد وصف مناسب لهذا الشخص في جميع مراحل الدعوى الجنائية.

ج- المقصود بالمتهم في التشريع الجزائري:

استعمل المشرع الجزائري مصطلح المتهم في المادة 46 ق.إ.ج.ج والتي تنص على ما يلي:" يعاقب بالحبس من شهرين إلى سنتين و بغرامة تتراوح بين2.000 إلى20.000 دينارا كل من أفشى مستندا ناتجا من التفتيش أو إطلع عليه شخصا لا صفه لها قانونا في الإطلاع عليه وذلك بغير إذن المتهم أو من ذوي حقوقه أو من الموقع على المستند أو من المرسل إليه، مالم تدع ضرورات التحقيق إلى غير ذلك، فأطلق المشرع مصطلح المتهم على كل شخص تحرك ضده الدعوى العمومية دون

تمييز بين مراحلها في حين أطلق على من يكون محلا لإجراءات البحث والتحري بواسطة الشرطة القضائية مصطلح المشتبه فيه ويظهر ذلك في المواد 42- 45- 58 ق.إ.ج.ج[1].

وبهذا يكون المشرع قد ميز بين مصطلح المتهم والمشتبه فيه[2]، واعتبر أن الشخص المشتبه فيه هو الشخص الموجود محل التحريات الأولية التي تباشرها الضبطية القضائية، ولم يكن بعد محل إجراء تحريك الدعوى العمومية.

وعلى رغم من عدم إعطائه تعريفا محددا لهما، إلا أنه استند في التفرقة بينهما على المرحلة الإجرائية الموجودة فيها الشخص محل المتابعة.

2- تعريف المتهم في التشريعات الأجنبية:

أ- المقصود بالمتهم في التشريع الفرنسي:

وفقا للمادة 111 من المرسوم الصادر في 1903/05/20 قسّمت الشخص المتهم إلى ثلاث فئات:

- **الفئة الأولى:** وهو (l'accusé) للدلالة على كل شخص اتخذت حياله إجراءات اتهامه بارتكاب جناية.
- **الفئة الثانية** : وهو(le prévenu) ويطلق على كل شخص اتخذت حياله إجراءات بجنحة أو مخالفه وذلك في المرحلة التي تلي انتهاء أو قفل الإجراءات ضده والتي تتمثل في التحقيق الأولي وذلك في الجرائم المتلبس بارتكابها، و التحقيق الابتدائي، و بالبحث عن هذه الكلمة يتضح أنها تعني المتهم قبل أن يصبح مدانا.
- الفئة الثالثة : وهو (inculpé) يطلق هذا المصطلح أنا على كل شخص يكون موضوعا أو محل اتهام بارتكاب جريمة في مرحله التحقيق الابتدائي، وتعني المدان[3].

---

[1]- تنص المادة 42/ف4 ق.ا.ج.ج على أنه: "و أن يعرض الأشياء المضبوطة على الأشخاص المشتبه في مساهمتهم في الجناية للتعرف عليها ".وتنص المادة 45 من ق.إ.ج.ج:".... إذا وقع التفتيش في مسكن شخص يشتبه في أنه ساهم في ارتكاب الجناية.....". وتنص المادة 58 ق.ا.ج.ج على انه:" يجوز لوكيل الجمهورية في حاله الجناية المتلبس بها إذا لم يكن قاضي التحقيق قد ابلغ بها بعد أن يصدر أمرا بإحضار المشتبه في مساهمه في الجريمة."

[2]- يعرف المشتبه فيه بأنه" الشخص الذي تتوفر ضده قرائن تجعله محل شبهه بأن له علاقة بارتكاب الجريمة كافيه ليكون محل إجراءات تحريات الأولية ثم لم تحرك ضده الدعوى العمومية." أنظر: أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، المرجع السابق، ص 43.

[3]- هدى أحمد العوضي، المرجع السابق، ص 22.

ولقد أدرج قانون الإجراءات الجنائية الفرنسي على استخدام ذلك التقسيم حتى اصدر المشرع الفرنسي مرسوما في 1958/08/22 متضمنا لفظ المشتبه فيه (soupçonne) وهذا اللفظ مستمد من المادة 305 من مرسوم سنة 1903 السابق الذكر، وقد استقرّ قانون الإجراءات الجزائية الفرنسي على استخدام هذا اللفظ أثناء جمع الاستدلالات، ويقصد به الشخص الذي أحاطت به دلائل يمكن أن تسوغ اتهامه أو تشير إلى أن له دور في ارتكاب الجريمة دون أن تتأكد هذه الشبهات، وهو يعد كذلك حتى ولو كان في حاله تلبس ولا يطلق عليه متهم بالرغم من قوة الدلائل في حاله التلبس، ويسأل في هذه الحالة بوصفه شاهدا[1] وليس مشتبهاً فيه.

والمشرع الفرنسي قام بالتمييز بين المتهم والمشتبه فيه في المادة التمهيدية المضافة لقانون الإجراءات الجزائية موجب القانون 2000-516 و المؤرخ في 2000/06/15 لتدعيم حماية قرينة البراءة[2] حيث نصت الفقرة الثالثة منها على أن" كل شخص مشتبه فيه كان ملاحقا يفترض أنه بريء ما لم تثبت إدانته، كما عبّر عنه بعبارات أخرى عند تناوله سلطات الشرطة القضائية تفيد تمييزه عن المتهم[3].

ب- المقصود بالمتهم في التشريع الإنجليزي:

لا يوجد أيضا في التشريع الإنجليزي تعريفا محددا للمتهم، غير أن القاعدة الثانية من قواعد القضاء الصادر عام 1906 لإرشاد الشرطة أبرزت التفرقة بين المشتبه فيه والمتهم، حيث نصت على أنه: " عندما يكون قد استقر رأي الشرطة على اتهام شخص بارتكاب جريمة ما، فإنه يجب تحذيره بعدم إلتزامه بالإجابة التهمه الموجهة إليه ما لم يرغب في ذلك و أن كل ما سيقوله سيدون كتابه، ويقدم ضده وقد يستخدم دليلا لإدانته"، يفهم من هذه المادة أن التحذير الذي يوجهه ضابط الشرطة إلى الشخص المستجوب بحقه في الصمت الحد الفاصل بين مرحلة الاشتباه و مرحلة الاتهام، حيث تنتهي

---

[1]- يقصد بالشاهد ذلك الشخص الذي لديه معلومات تفيد في كشف الحقيقة في شأن واقعة ذات أهمية في الدعوى الجنائية، وقد تكون الشهادة مؤيده لتهمة وقد تكون نافية لها، وبالتالي فإن الشاهد بعيد كل البعد عن دائرة الاشتباه أو الاتهام، غير أن لديه معلومات مفيدة قد تساعد جهات الاستدلال و التحقيق في كشف الحقيقة.

[2]- تعني قرينة البراءة افتراض براءة كل فرد مهما كان وزن الأدلة أو قوة الشكوك التي تحوم حوله أو تحيط به، فهو بريء هكذا ينبغي أن يعامل و هكذا ينبغي أن يصنف طالما أن مسؤوليته لم تثبت بمقتضى حكم صحيح و نهائي صادر عن قضاء المخفض. أنظر: عبد الرحمان خلفي، المرجع السابق، ص 27.

[3]- حسيبة محي الدين، ضمانات المشتبه فيه أثناء التحريات الأولية، مذكره التخرج لنيل شهادة الماجستير، كليه الحقوق، جامعه الإسكندرية، مصر، 2010، ص 14.

عند المرحلة الأولى لتبدأ به المرحلة الثانية ويسمى المشتبه فيه (Suspect Person) بينما يطلق على المتهم (Accused Person) أو المدعى عليه جنائي Criminal Defendant [1] .

فالمشرع الإنجليزي توسع في فتح اختصاص الاتهام إلى أجهزه الشرطة القضائية وهو الاختصاص المقصور على النيابة العامة في النظام اللاتيني، في إنجلترا إذا تبين أثناء التحريات الأولية التي تتولاها أجهزه الشرطة أن هناك دلائل ترجح إتهام شخص يكون محل البحث، وفي حاله ما إذا اقتنع ضابط الشرطة القضائية بذلك فأنه يبادر تبليغ المشتبه فيه في أنه أصبح متهما وهذا التبليغ شفويا، وعندئذ تتحول صفة شخص من مشتبه فيه إلى متهم[2].

ج- المقصود بالمتهم في التشريع الأمريكي:

إن الولايات المتحدة الأمريكية فرقت بين المشتبه فيه (Suspect) والمتهم (Assused) أو (Crimimal défendant) وتكمن التفرقة في الإجراءات التي تتخذ مع كل منهما فلم ستوقف (Stopped) بشأن توجيه الأسئلة و تفتيشه تفتيشا سطحيا (Firsk) وحجزه وفقا للمادة الثانية من قانون القبض الموحد الصادر عام 1941، حيث يعتبر مشتبها فيه، و لا يجوز استيقافه أكثر من ساعتين، ثم يستجوبه ضابط الشرطة، فإما أن يوجه إليه اتهاما و إما يطلق سراحه.

ويذهب البعض إلى القول بأنه وعلى الرغم من خلو التشريعات الأمريكية من نصوص صريحة تتطلب على وجه الخصوص تحذير المشتبه فيه بحقه في الصمت، إلاّ أن ممثلي الاتهام يميلون في توجيه هذا التحذير للمشتبه فيه عند توجيه الأسئلة إليه ، وذلك خشيه الطعن في هذه الأقوال لكونها قد صدرت من غير إكراه، كما أن بعض مراكز البوليس تقوم بهذا التحذير كنوع من حسن المعاملة، الأمر الذي لا يجعله قاعدة ينبغي العمل بموجبها[3]، غير أنا المحكمة الأمريكية العليا حسمت هذا الموقف في نقضها في قضية (Miranda) عام 1966 المؤسّسة على اعتراف المشتبه فيه بعد إلقاء القبض عليه، حيث بررت نقضها لهذا الحكم بعدم تحذير المشتبه فيه بحقه في الصمت، والإنكار عليه بحقه في الاستعانة بمحامي، فقد جاء في تحذيرات Miranda بالتحذير الثاني بها أنه يجب أن ينّبه

---

[1]- هدى أحمد العوضي، المرجع السابق، ص 23.

[2]- منصف خطابي، ضمانات المشتبه فيه أثناء التحريات الأولية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الدفعة السابعة عشر، الجزائر، 2006-2009، ص 10.

[3]- هدى أحمد العوضي، المرجع السابق، ص 23.

المشتبه فيه عند توقيفه في مركز الشرطة أن من حقه التزام الصمت، وأن ما سيقوله يمكن أن يستعمل كبيّنة ضده في الملاحقة الجزائية وأن من حقه أن يستعين بمحامي يعينه أو يعين له[1].

رغم أننا بينـــاّ مدلول المتهم غير أنّ ذلك يستلزم بيان الشروط التي ينبغي أن تتوافر فيه، حيث هناك شروط يجب أن تتوافر في الشخص حتى يكتسب وصف المتهم، وباكتمالها يمكن أن تتحرك الدعوى العمومية ضده وتوجيه الاتهام إليه من قبل السلطة ذات الاختصاص و بالتالي يمكن استجوابه[2]، ومن هذه الشروط مـــا يلي:

1- أن يكون المتهم شخص طبيعي على قيد الحياة:

ترفع الدعوى الجنائية على الإنسان الطبيعي[3] ولا ترفع على الحيوان ولا الجماد، غير أنه يجوز رفع الدعوى المدنية على مالك الحيوان إذا حدثت إصابة للغير نتيجة إهماله بالمحافظة عليه للمطالبة بالتعويض.

فالإنسان وحده الذي يملك الإرادة التي تقف وراء الفعل وهو الذي يستجيب لأهداف المجتمع من تطبيق الجزاءات الجنائية وعدم العودة للجريمة مرة أخرى.

أما الشخص المعنوي فحيث أنه ليس له كيان مادي و إرادة معتبرة تصدر عنها الجريمة، فهو لا يقوم بتصرفاته بنفسه وإنما يقوم به ممثله القانوني الأمر الذي قد يثير صعوبة بشأن إقرار مساءلته ومن ثم إمكان استجوابه، إلا أن إقرار جواز تحريك الدعوى الجنائية اتجاهه، التي تمر عبر تحريك الدعوى الجنائية تجاه ممثله بصفته لا بشخصه، و التي يتم عبرها مساءلة الشخص المعنوي جنائيا، الأمر الذي يبرره إنتشار مختلف المنشآت والهيئات والنقابات الشخصية المعنوية وخروج بعضها على

---

[1]- هدى أحمد العوضي، المرجع السابق، ص 23.

[2]- يقصد بالاستجواب مواجهه المتهم بالتهمة المنسوبة إليه أو مطالبته إبداء الرأي فيها ثم مناقشته تفصيليا في أدله الدعوى إثباتا أو نفيا ، وهو إجراء إجباري إذا كانت الأفعال الموجهة للمتهم تشكل جناية، أما إذا كانت هذه الأفعال تشكل جنحة فهو إجراء جوازي يلجأ إليه قاضي التحقيق عاده في حاله إنكار المتهم للوقائع الموجهة إليه أثناء الاستجواب عند الحضور الأول أو إذا تمسك أثناءه بحقه في اختيار محامي قبل استجوابه. أنظر: محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الأولى، دار هومه، الجزائر،2006، ص 96. و أنظر أيضا: فضيل العيش، المرجع السابق، ص 169.

[3]- هناك شخص طبيعي وشخص معنوي، الأول: يتمثل في الإنسان والثاني: يتمثل في الشركات، المؤسسات وغيرهما.

القانون يوجب تقرير تلك المسؤولية، ومن ثم إمكان استجوابه باعتباره هو من يمثل إرادة الشخص الذي يمثله[1].

وحتى ترفع الدعوى الجنائية يجب أن يكون هذا الإنسان على قيد الحياة، فلا يجوز رفعها على إنسان ميت، وسبب في ذلك أن الدعوى الجنائية بها عقوبة شخصيا ومن غير المنطق فرضها على إنسان غادر الحياة، وعلى أساس ذلك تم الإقرار بتأثر الدعوى الجنائية بالوفاة، فإذا حدثت الوفاة قبل تحريك الدعوى العمومية تأمر النيابة بحفظ أوراق القضية، وإذا حدثت الوفاة بعد تحريك الدعوى العمومية وقبل صدور حكم فيها فلا يمكن السير فيها و تصدر الجهة المعروضة عليها القضية أمرا بأنه لا وجه للمتابعة[2] أو بانقضاء الدعوى العمومية إذا كانت على مستوى التحقيق القضائي، وتصدر حكم بانقضاء الدعوى العمومية إذا كانت خلال مرحلة المحاكمة، أما إذا حدثت الوفاة بعد صدور الحكم فأن الحكم يسقط وتسقط معه العقوبة[3]، حيث تنص المادة 1/6 من ق.ا.ج.ج على ما يلـــــي:" تنقضي الدعوى العمومية الرامية إلى تطبيق العقوبة بوفاة المتهم و بالتقادم و العفو الشامل وبإلغاء قانون العقوبات وبصدور حكم لقوة الشيء المقضي فيه"، وتنص المادة 14 من ق.ا.ج.م. كذلك على أنه:" تنقضي الدعوى الجنائية بوفاة المتهم ولا يمنع ذلك من الحكم بالمصادرة في الحالة المنصوص عليها بالفقرة الثانية المادة (30) من قانون العقوبات إذا حدثت الوفاة أثناء نظر الدعوى."[4]

2- أن يكون الشخص معينا:

يقصد بذلك أن يكون المتهم معينا بذاته أو بصفاته فلا يجوز رفع الدعوى ضد مجهول، ولا يشترط أن يكون المتهم معروفا باسمه كاملا، فقد يضبط الشخص متلبسا بارتكاب جريمة ويرفض الإفصاح عن اسمه أو أن يتسمى باسم شخص آخر، كما قد يكون المتهم فاقد النطق فذلك لا يمنع من رفع الدعوى الجنائية ضده والحكم عليه، كما أنه لا يشترط أن يكون الشخص حاضرا، فغيابه أو مثوله أمام

---

[1]- هدى أحمد العوضي، المرجع السابق ،ص 36.

[2]- يعرف الأمر بأن لا وجه للمتابعة أو الأمر بانتفاء وجه الدعوى: بأنه أمر قضائي تقرره بمقتضاه جهات التحقيق عدم السير في الدعوى العمومية لتوافر سبب من الأسباب تحول دون ذلك. أنظر: عبد الرحمان خلفي، المرجع السابق، ص 201.

[3]- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، المرجع السابق، ص 16. أنظر أيضا: عبد الرحمان خلفي، المرجع السابق، ص 128- 129.

[4]- أنظر المادة 13 من قانون الإجراءات الجنائية القطري، و المادة 15 من قانون الإجراءات الجزائية العماني، والمادة 20 من قانون الإجراءات الجزائية الإماراتي، و المادة 22 من قانون الإجراءات السعودي.

المحكمة لا أهمية له في هذا الصدد وفي حالة عدم معرفة المتهم، يجوز للنيابة العامة حفظ الأوراق أو تقرر بأن لا وجه لإقامة الدعوى، ذلك لأن هذا الإجراء تطالب فيه النيابة باقتضاء حق الدولة في العقاب من شخص معين هو مرتكب الجريمة و ذلك لابد أن يكون معينا، والسبب من تعيين المتهم هو التحقق من شخصيته ومن إثبات براءته أو إدانته من خلال جملة من الإجراءات من بينها الاستجواب[1].

وما تجدر الإشارة إليه في هذا المجال هو أنه يجب التفرقة بين حالتين:

- الحالة الأولى : مرحلة جمع الاستدلالات، ففيها لا يشرط أن يكون الشخص معينا بل قد يكون مجهولا وهو الأصل ويسعى القائمون على الإجراءات فيها إلى الكشف عن شخصية مرتكب الجريمة.
- الحالة الثانية : هي مرحلة التحقيق القضائي وفيها يشترط أن يكون المتهم معينا بشخصه وذاته، إذ لا يجوز في هذه المرحلة مباشرة الإجراءات ضد مجهول بل لابد أن يكون معلوم الهوية (الاسم ، اللقب ، تاريخ و مكان الازدياد ... الخ) وغيرها، لأن الهدف فيها الوصول إلى حكم بالبراءة أو الإدانة، وهو أمر غير متصور إلا بالنسبة إلى شخص معين، ولا يشترط هنا أن يكون المتهم معينا باسمه بل يكفي أن يكون معينا بذاته .

3- تمتع المتهم بالأهلية الإجرائية :

يجب أن يتمتع المتهم بالقدرة اللازم من الإمكانيات البدنية والذهنية لكي يتمكن من الدفاع عن نفسه، أي أن يكون متمتعا بالأهلية الإجرائية، و هي الأهلية الإجرائية لمباشرة نوع من الإجراءات ضده على نحو يعد معه هذا الإجراء صحيحا أو منتجا لأثاره القانونية، أي أن يكون متمتعا بصحة عقلية تمكنه من إدارة دعواه بأفضل الطرق وخصوصا استعماله الحق في الدفاع عن نفسه في جميع مراحل الخصومة الجنائية[2].

وعلى هذا الأساس ينبغي أن يبلغ الشخص السن القانونية التي تمكنه من المسائلة الجنائية وبالتالي يكون أهلا لرفع الدعوى الجنائية عن الجرائم التي يرتكبها بغض النظر عن الجزاء الذي سيوقع عليه والمحكمة التي تنظر في الدعوى.

---

[1]- هدى أحمد العوضي، المرجع السابق، ص 37. و أنظر أيضا: عماد أحمد هاشم الشيخ خليل، المرجع السابق، ص16.

[2]- عماد أحمد هاشم الشيخ خليل، المرجع نفسه، ص18.

إلا أن عدم بلوغ الشخص السن القانوني لا يعني عدم إمكان اتخاذ الإجراءات ضده، إذ كما يمكن أن تكون المحكمة المختصة هي المحكمة العادية، يمكن أن تكون المحكمة المختصة محكمه أحداث[1].

كما أنه إذا طرأت على المتهم عاهة في عقله[2] بعد وقوع الجريمة توقف إجراءات الخصومة ضده حتى يعود إليه رشده، فأي خلل في تمييز المتهم و إدراكه سواء حصل أثناء التحقيق أو المحاكمة سيكون موجبا لوقف النظر في الدعوى إلى أن يسترجع ملكاته المفقودة[3].

4- أن ينسب للشخص المساهمة في الجريمة:

الدعوى الجنائية لا ترفع إلا على من ارتكب الجريمة بسلوكه الشخصي أو ساهم بنشاط يجعله مساهما فيها، فيشترط في الشخص الذي يعد متهما أو يكون منسوباً إليه المساهمة في الجريمة بصفته فاعلا أصليا أو شريكا[4].

ومن المعلوم أيضا أن الدعوى الجنائية لا ترفع عن جريمة يرتكبها صغير أو مجنون لما هو مقرر بصدد ذلك قانونا و قضاءا، ولكن هذا لا يمنع من إقامة الدعوى المدنية وعندئذ ترفع بحق الولي أو الوصي أو القيم[5]، وإنما ترفع الدعوى على مرتكب الجريمة ذاته، بينما ترفع عليهم الدعوى المدنية بتعويض الضرر في حين ترفع الدعوى الجنائية على مرتكب الجريمة لأنه هو المتهم فيها[6].

---

[1]- هدى أحمد العوضي، المرجع السابق، ص40.

[2]-المادة 1/339 من قانون إ.ج.م.

[3]- هدى أحمد العوضي، المرجع السابق، ص 40.

[4]- تنص المادة 41 من قانون.ع.ج على أنه" يعتبر فاعلا كل من ساهم مساهمه مباشره في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو تهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي" و تعرف المادة 42 من ق.ع.ج الشريك بقولها:" يعتبر شريكا في الجريمة، من لم يشترك اشتراكا مباشرا، ولكنه ساعد بكل الطرق، أو عاون الفاعل أو الفاعلين على ارتكاب الأفعال التحضيرية والمسهلة أو المنفذة لها مع علمه بذلك."

[5]- الـــولي: هو الشخص الذي يعهد إليه بالولاية على أموال القاصر أو الصغير غير المميز و تثبت للأب والجد.
أمـــا الوصي: شخص يعهد إليه بالولاية على أموال القاصر أو الصغير غير المميز و تثبت لغير الأب والجد=
= أمـــا القيم: فهو الشخص الذي يتولى إدارة أموال المحجور بسبب الجنون أو السفه أو العته.

[6]- هدى أحمد العوضي، المرجع السابق، ص 39.

5- وجود دلائل كافية على ارتكاب الشخص للجريمة أو الاشتراك فيها:

لابد من وجود دلائل كافية لاكتساب الشخص صفه المتهم، لأن كفاية الأدلة تعد ضمانا هاما يقي الأفراد من الوقوع ضحايا اتهامات قد تكون تعسفية.

و على مستوى الفقه هناك تفرقة من حيث القوه بين الدلائل الكافية، لكي يكتسي الشخص صفه المتهم وبين التي يمكن إحالته بها إلى سلطات المحاكمة، إذ يكفي في الأولى بالشكوك المعقولة، أما الثانية فيشترط أن تكون من القوه بحيث ترجح الإدانة على البراءة[1].

و بناءاً عليه يمكن القول بأنّ الدلائل الكافية تعد شرطا جوهرياً لأي إجراء فيه مساس بالشخص وأن وجودها يجعل الإجراء صحيحاً حتى ولو تبين فيما بعد أنها كانت مجرد شبهات ظالمة، لا أساس لها في واقع الأمر، طالما كان لها ما يبررها في ذهن الجهة التي أمرت بالإجراء لأن الأصل في الأعمال الإجرائية حسب تعبير محكمة النقض أنها تجري على حكم الظاهر وهي لا تبطل بعد زوال ما ينكشف من أمر الواقع وذلك تيسيرا لتنفيذ أحكام القانون وتحقيقا للعدالة حتى لا يفلت الجناة من الجزاء[2].

والواقع أنه من الصعب وضع تعريف جامع مانع للدلائل الكافية،لأن الأمر يختلف تبعاً لظروف الحال التي تؤسس عليها الأدلة الكافية للإتهام و يجب أن تؤخذ كل الظروف أو الملابسات في الاعتبار ووزنها بميزان حساس عادل حتى نحدد ما يعتبر من الدلائل الكافية وما لا يعتبر كذلك.

الفرع الثالث: خصائص التحقيق في الجرائم الإلكترونية

يتميز التحقيق الجنائي في الجرائم الإلكترونية بسمات وذاتية تميزه عن التحقيق الجنائي في الجرائم التقليدية وترجع هذه الذاتية للأسباب التالية:

- أن مرتكبي الجريمة الإلكترونية لديهم قدره إلكترونية قادرة على سرعة إتلاف وتشويه وإضاعة الدليل الالكتروني في وقت قصير.
- هذه النوعية من الجرائم الإلكترونية الرقمية لا تترك أثرا ماديا في كثير منها في مسرح الجريمة.
- إن التحقيق في الجريمة الإلكترونية ذات البنية الرقمية يحتاج لإمكانيات مادية و قواعد وإجراءات تختلف عن التحقيق في الجرائم التقليدية سواء من حيث طبيعة السلوك الإجرامي الالكتروني أو

[1]- عماد أحمد هاشم الشيخ خليل، المرجع السابق، ص 15.

[2]- عماد أحمد هاشم الشيخ خليل، المرجع نفسه، ص 15.

من حيث طبيعة الدليل الالكتروني أو وسائل وآليات كشف الجريمة والوصول إلى الدليل الالكتروني[1].

كما يتميز التحقيق أيضا باعتباره عملاً قضائيا بمجموعة من الخصائص الأخرى منها:

أولا: الكتابة أو التدوين

يعتبر التدوين من القواعد الأساسية في الاجراءات الجزائية، والمقصود به هو إثبات إجراءات التحقيق عن طريق الكتابة التي تعد حجةتبنى عليها النتائج، ودونها يفترض عدم مباشرة التحقيق استنادا إلى مبدأ مالم يكتب لم يحصل، فهي قاطعة للشك، ويستوي أن يكون التدوين في محضر واحد أو عدة محاضر، فجميع المحاضر التي يثبت فيها المحقق ما قام به من إجراءات تعتبر من أوراق الدعوى الجزائية وتكتسب حجتها متى كانت مستوفية للشروط القانونية.

فالكتابة قاعدة عامة تشمل جميع الإجراءات بوجه عام سواءا كانت أثناء التحقيق أو عند انتهائه، حتى يكون حجة في ما أثبته وفيما يستفاد منه من نتائج، ذلك أنّ ذاكرة المحقق لا يمكن الاعتماد عليها لمعرفه ما تم من إجراءات و الكيفية التي تمت بها، و يتفرع عن ذلك أنه لا يجوز إثبات حصول الإجراء بغير المحضر الذي دوّن فيه، أي استبعاد طرق الإثبات الأخرى في هذا الشأن[2].

ونص المشرع الجزائري على وجود كتابة محاضر التحقيق عن طريق كاتب ضبط تابع للمحكمة المختصة حتى يتم الرجوع إليه عند الحاجة، وهذا ما نصت عليه المادة 2/68 من ق.إ.ج بقولها:" تحرر نسخة عن هذه الإجراءات وكذا جميع الأوراق ويؤثر كاتب التحقيق أو ضابط الشرطة القضائية المنتدب على كل نسخة مطابقتها للأصل وذلك مع مراعاة ما أشير إليه في الفقرة الخامسة من هذه المادة، وكذلك ما نصت عليه المادة 2/24 من ق.ا.ج.م و التي تنص على ما يلي" يجب أن تثبت جميع الإجراءات التي يقوم بها مأمور الضبط القضائي في محاضر موقع عليها منهم يبين فيها وقت اتخاذ الإجراءات و مكان حصوله ويجب أن تشمل تلك المحاضر زيادة على ما تقدم توقيع الشهود والخبراء الذين سمعوا و ترسل المحاضر إلى النيابة العامة مع الأوراق و الأشياء المضبوطة ".

[1]– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 166 – 167 .

[2]– أحمد سعد محمد الحسيني، المرجع السابق، ص 62.

على أنه لا يكفي مجرد كتابة الإجراءات بل يجب أن تتم هذه الكتابة بواسطة كاتب من كتاب المحكمة يستصحبه المحقق في جميع الإجراءات[1]، وأن يكون التدوين معاصرا لمباشرة الإجراء.

هذا وقد نص المشرع المصري على ذلك في المادة 73 من ق.إ.ج والتي تقضي بأن " يستصحب قاضي التحقيق في جميع إجراءاته كاتبا من كتاب المحكمة ويوقع معه على المحاضر، وتحفظ هذه المحاضر مع باقي الأوراق في قلم المحكمة."

غير أنه في الحالة التي لا يكون فيها من يصاحب المحقق من الكتبة لأي سبب من الأسباب، أو قد ينتقل عضو النيابة قبل وصول الكاتب، فلا يمكن أن تتعطل إجراءات التحقيق و إنما تبدأ مباشرتها على أن يستعين المحقق بأخذ الأفراد غالبا ما يكون من رجال الضبط القضائي كأمين شرطة ويحلفه عضو النيابة المحقق اليمين القانونية[2] والتي تكون بالصيغة الآتية:" اقسم بالله العظيم أنا أؤدي أعمال التحقيق بالصدق والذمة والأمانة" وتثبت هذه الواقعة في المحضر.

و ينبغي على المحقق أن يشرف إشرافاً كاملا على الكاتب في توجيه لقصور خبرته أو انعدامها، وفي حال حضر كاتب التحقيق المختص وتولى هو إتمام المحضر على أن يثبت وجوده، كما يجوز لعضو النيابة مباشرة بعض الإجراءات بنفسه حتى حضور كاتب التحقيق إذا كانت طبيعة الإجراء أو دواعي الحال تقتضي ذلك، فيجوز له مثلا أن يقوم بمعاينة محل الحادث وإثبات ما يرى إثبات حالته[3].

غير أن ضابط الشرطة القضائية إذا ندب للقيام بعمل من أعمال التحقيق فهو غير ملزم بالاستعانة بكاتب يحرر المحاضر له فهو يحررها بنفسه وله الاستعانة بمساعديه من الأعوان.

---

[1]– أحمد سعد محمد الحسيني، المرجع السابق، ص 62.

[2]– يقصد باليمين: إشهاد الله تعالى على صدق ما يقوله الحالف أو على عدم صدق ما يقوله الخصم الأخر ولما كانت اليمين عملا دينيا فإن لمن يكلف حلف اليمين أن يؤديها وفقا للأوضاع المقررة في ديانته إذا طلب ذلك ويكون أداؤها بان يقول الحالف (أحلف) و يذكر الصيغة التي أقرتها المحكمة وتكون اليمين إما لتوكيد القول أو للتوكيد الوعد.

فاليمين للتوكيد القول: هي اليمين التي تؤدي لتوكيد انجاز وعد أخذه الحالف على نفسه مثل ذلك اليمين التي يخلفها القضاة ورجال النيابة والخبراء والشهود على أن يؤدوا أعمالهم بالأمانة والصدق أو أن يقرروا الحق فيما يشهدون. أنظر: محمد صبري السعدي، الواضح في شرح القانون المدني،الإثبات في المواد المدنية و التجارية، دار الهدى، الجزائر،2009، ص 261.

[3]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009، ص 20.

والهدف من تدوين إجراءات التحقيق ووجود اصطحاب قاضي التحقيق لكاتب التحقيق يقوم بعملية التدوين إلى تفرغ القاضي المحقق فكريا وذهنيا للعمل الفني المتمثل في التحقيق نفسه، لما يقوم به من إجراءات ومناقشة أطراف الدعوى بسؤالهم وأجوبتهم مما ييسّر عليه تكوين عقيدته واقتناعه والتي يقوم كاتب التحقيق بتدوينها في محضر التحقيق، كما يتمكن الخصوم في الدعوى العمومية من الإطلاع على أوراقه ومناقشة ما تم منها، وعليه فالتدوين شرط لوجود محضر التحقيق، وبالتالي كل إجراء من إجراءات التحقيق يتضمنه المحضر، ويجب أن يكون محضراً مستوفيا شروطه الشكلية، موقعاً عليه من طرف قاضي التحقيق والكاتب والشاهد إن وجد[1].

ويجب أن يكون خالياً من أي تحشير بين السطور[2]، و المصادقة على كل شطب أو تخريج من القاضي والكاتب الشاهد و المترجم كلما كان هناك داع لذلك[3].

ثانيا: سرية التحقيق:

من خصائص التحقيق ما يعرف كذلك بسرية التحقيقات التي تحّرص عليها أغلب القوانين الجزائية بهذا الشأن، أي جعل التحقيق ذا طبيعة سرية بالنسبة للجمهور أو الغرباء عن الدعوى العمومية القائمة[4].

و يقصد بالسرية كذلك عدم العلانية أي إجراء التحقيق في جو من السرّية والكتمان بالنسبة للجمهور و هذا ما نصت عليه المادة 11 ق.إ.ج بقولها : " تكون إجراءات التحري والتحقيق سرّية ما لم ينص القانون خلاف ذلك ، ودون إضرار بحقوق الدفاع....". وكذلك ما نصت عليه المادة 75 من قانون إ.ج.م :" تعتبر إجراءات التحقيق ذاتها والنتائج التي تسفر عنها من الأسرار ويجب على قضاة التحقيق و أعضاء النيابة العامة ومساعديهم من كتاب وخبراء وغيرهم ممن يتصلون بالتحقيق أو يحضرونه بسبب وظيفتهم أو مهنتهم عدم إفشائها...".

---

[1]– عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري– التحري والتحقيق–، المرجع السابق، ص317.

[2]– تنص المادة 95 من قانون.إ.ج على ما يلي:" لا يجوز أن تتضمن المحاضر تحشيرا بين السطور، ويصادق التحقيق و الكاتب و الشاهد على كل شطب أو تخريج فيها، ومن المترجم أيضا إذا كان ثمة محل لذلك، وبغير هذه المصادقة تعتبر هذه الشطوبات أو التخريجات ملغاة و كذلك الشأن في المحضر الذي لم يوقع عليه توقيعا صحيحا أو في الصفحات التي لا تتضمن توقيع الشاهد."

[3]– عبد الله أوهايبيه، شرح قانون الإجراءات الجزائية الجزائري– التحري والتحقيق–، المرجع السابق، ص 317 .

[4]– أحمد سعد محمد الحسيني، المرجع السابق، ص64.

وعليه فإنّ القانون يلزم كل من ساهم في التحقيق ، قاضي التحقيق وكل من يتصل بالتحقيق بطريق أو بآخر، كأعضاء النيابة العامة والضبط القضائي والخبراء والمترجمين، بحضور إجراءات التحقيق والاطلاع على أوراقه بموجب كتمان السّر المهني، بعدم إذاعة أسرار التحقيق وإلا تعرض المفشي للسر للعقوبات المقررة في القانون، فتنص المادة 2/11 من قانون.ع.ج " وكل شخص يساهم في هذه الإجراءات ملزم بكتمان السّر المهني بالشروط المبينة في قانون العقوبات وتحت طائلة العقوبات المنصوص عليها فيه".

هذا ما أكدته أيضا محكمه النقض الفرنسية في قرارها الصادر بتاريخ 1978/10/09 تحت رقم 76-92- 075[1] . و قد استثنى نص المادة 11 من قانون.إ.ج.ج واجب كتمان السّر المهني المعاقب على إفشائه بموجب المادة 301 من ق.ع.ج و المادة 310 من ق.ع.م[2] ممثل النيابة العامة أو ضابط الشرطة القضائية المرخص له فسمح لهما باطلاع الرأي العام على بعض المعلومات تفاديا لانتشار معلومات غير كاملة أو غير صحيحة أو لوضع حد للإخلال بالنظام العام.

و الغرض من ذلك واضح وضوح بين وهو أن سرية التحقيق[3] من شأنها عدم الإساءة و التشهير بالمتهم قبل إدانته والحكم عليه من قبل المجتمع، الأمر الذي يؤدي إلى امتداد تلك الإساءة والتشهير

---

[1] - Cour de cassation : Chambre Criminelle Lecture de 9 Octobre 1978, N° 76 .92.075 publier au bulletin.
(Attendu d'une part, que l'article 378 de code pénale ne vise que les faite parvenus à la connaissance d'une personne dans l'exercice d'une profession ou d'une fonction aux actes de laquelle la loi, dans un intérêt général et d'ordre public, à imprimé le caractère confidentiel, ou dans le cas où les mêmes faits lui en été confiés sous le sceau de secret en raison d'une semblable profession ou fonction.
Attendu, d'autre part, qui si , selon, l'article 11 de code de procédure pénale, toute personne qui concourt à la procédure de l'instruction est tenu au secret professionnel, dans les conditions et sous les peines de l'article 378 du code pénale, tel n'est pas le cas de la partie civile)

نقلا عن نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، الطبعة الأولى، دار هومة، الجزائر، 2015- 2016، ص62.

[2]- نصت المادة 301 من ق.ع.ج على ما يلي:" يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة من 20.000 إلى 100.000 دج، الأطباء و الجراحين و الصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم و أفشوها في غير الحالات التي يوجب عليهم فيها القانون إفشائها ويصرح لهم بذلك...."

و تنص المادة 310 من ق،ع،م على ما يلي:" كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعا إليه بمقتضى صناعته أو وظيفته سر خصوصي ائتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مده لا تزيد على ستة شهور أو بغرامه لا تتجاوز خمسمائة جنيه مصري....".

[3]- إن سرية إجراءات التحري على مستوى الضبطية القضائية وإجراءات التحقيق القضائي هي ما يميز النظام التنقيبي، والإجراءات في هذا النظام تمتاز بالكتابة والسرية وعدم الوجاهية، بخلاف الإجراءات في مرحله المحاكمة التي تسير

إلى عائلته وأهله، مما يؤدي إلى ترك أثرا سيئا في النفوس، ولا سيما إذا تبّين بعد ذلك براءته من الواقعة، ذلك أن الاتهام الموجه للمتهم لا يشكل في بداية الأمر سوى وقائع ماديه أو قانونيه نسبت له على خلاف الأصل الذي يتمتع به كل فرد، والذي جوهره أنه بريء انسجاما مع قرينة البراءة[1].

كما أن السرية التي تحيط التحقيق الجنائي تحمل الكثير من الفوائد بالنسبة للمجتمع، حيث أنّ من فوائدها عدم انتشار الشائعات بين أفراد المجتمع، الأمر الذي يدفعهم للتنبؤ بأحداث القضية والمبالغة في الوقائع المنسوبة، فيكون بالتالي رأي عام، من الممكن أن يتأثر به القضاء ومن ثم ينحرف كتب عن الرأي العام.

و بخلاف مبدأ السرية المقرر للجمهور أقر علانية التحقيق بالنسبة لأطراف الدعوى القائم التحقيق بشأنها بمعنى حضور إجراءات التحقيق تعني كل من له مصلحه فيه كالمتهم والمدعي المدني ووكلائهما والنيابة العامة، حيث أوجب القانون إخطار هؤلاء بمواعيد التحقيق، اليوم والساعة ومكان مباشرة إجراءات التحقيق. وللمتهم حق اصطحاب محاميه ليحضر معه التحقيق وهذا ما نصت عليه المادة 100 من ق.إ.ج.ج [2] والمادة 77 من ق.إ.ج.م[3] الفقرة الأخيرة منها وتتعلق المادة 100 من ق.إ.ج بمحضر استجواب المتهم عند الحضور الأول و مادام المتهم قد ورد اسمه تحديدا في الطلب الافتتاحي لوكيل الجمهورية فليس بإمكان قاضي التحقيق إلا أن يوجه له الاتهام بخلاف الوضع في قانون الإجراءات الجزائية الفرنسي أين يمكن لقاضي التحقيق أن يسمعه كشاهد مساعد و هو مركز

وفقا للنظام الاتهامي ، الذي تمتاز الإجراءات أثناءه بالشفوية و الوجاهية و العلنية، وبذلك فالنظام القضائي الجزائري قد أخذ بنظام مختلط قوامه النظام التنقيبي في مرحلتي التحري والتحقيق، والنظام الاتهام أثناء المحاكمة.

[1]– أحمد سعد محمد الحسيني، المرجع السابق، ص 64.

[2]– تنص المادة 100 من ق.إ.ج.ج على ما يلي:" يتحقق قاضي التحقيق حين المثول المتهم لديه لأول مرة من هويته، ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه وينبهه بأنه حر في عدم الإدلاء بأي قرار، وينوه من ذلك التنبيه في المحضر، فإذا أراد المتهم أن يدلي بأقوال تلقاها قاضي التحقيق منه على الفور، كما ينبغي للقاضي أن يوجه المتهم بان له الحق في اختيار محام عنه فان لم يختر له محاميا عين له القاضي محاميا من تلقاء نفسه إذا طلب منه ذلك أن ينتبه المتهم إلى وجوب إخطاره بكل تغيير يطرأ على عنوانه، ويجوز للمتهم اختيار موطن له في دائرة اختصاص المحكمة".

[3]– تنص المادة 77 من ق.إ.ج.م على ما يلي:" .... وللخصوم دائما الحق في استصحاب وكلائهم في التحقيق".

وسط بين الشاهد و المتهم بحيث يسمع المعني دون أداء اليمين ويمكنه أن يستعين بمحام حسب نص المادة 113-1 ق.إ.ج.ف[1].

ويعلل ذلك بالدور الرئيسي الذي صار المدافع وخاصة مدافع المتهم يحتله في الإجراءات الجنائية، وهذا الدور لا يحتاج له أدائه إلا إذا علم بإجراءات التحقيق.

كما يعلل أيضا بأن حضور المحامي إجراءات التحقيق يمثل نوعا من الرقابة على المحقق بما يحول بينه وبين التورط في مخالفة القانون، وبالإضافة إلى ذلك فهو يمد المتهم بالشعور بالطمأنينة يتيح له أن يحسن عرض وجهة نظر نظره، وفي ذلك مصلحه للتحقيق[2].

ويظهر لنا أهمية الاستعانة بمحامي في مجال الجرائم الإلكترونية في القضية و التي تتلخص وقائعها في قيام طالب في كليه الهندسة، بإنشاء موقع على شبكة الأنترنيت لإحدى الفتيات، متضمنا صورا منافية للآداب وألفاظا خارجة تمس عرض تلك الفتاه وسمعة عائلتها، فقامت الفتاة على إثرها بتحرير محضر بالواقعة في الإدارة العامة للمعلومات والتوثيق، التي قامت بدورها بإجراء التحريات التي جاء بها ،أن ذلك الموقع تم إنشاءه عن طريق جهاز حاسب ألي مربوط على رقم تليفون معين، وتم تحديد منزل المتهم وتحرير محضر تحريات فنية، ألقــّي القبض عليه، وقدمته النيابة العامة للمحاكمة بتهمه السب والقذف و إساءة استعمال أجهزة الاتصالات.

إلا أن الدفاع تقدم بمذكرة طلب فيها ندب خبير في الدعوى لإعادة بحث عناصرها من جديد للأسباب التالية:

- السبب الأول : مسألة إثبات **(IP)** الخاص بكل لرسالة يوصل في النهاية إلى تليفون المتهم محل شك ومرتبطة بمحضر التحريات الفنية، لا يمكن التحقق من هذه دون الرجوع إلى خبير فني متخصص من خبراء وزارة العدل.
- السبب الثاني : محرر التحريات الفنية لا يعد خبيرا لأنه لم يندب من النيابة العامة، ومحضر التحريات الفني لا يعد دليل فنيا يصلح سندا للإدانة ، بل لا بد من ندب خبير من السلطة القضائية، حيث أنه لو اعتبرنا أن محضر التحريات تقريرا فنيا فأن ذلك يعني أنه يمكن للشخص أن يكون

[1]- ART 113 -1 de C.P.P.F « Tout personne nommément visée par un réquisition introductif (L N° 2004-204 du 09 Mars 2004 art. 95 I, en vigueur le 1 ère Oct 2004) » « ou par un réquisitoire supplétif » et qui n'est pas mise en examen ne peut être entendue que comme témoin assisté »

[2]- أحمد سعد محمد الحسيني، المرجع السابق، ص69.

خصما وحكما في آن واحد وهو ما يجافي القواعد الأصولية التي تحكم الإجراءات الجنائية، وبالتالي فإن محضر التحريات الفني هو مجرد إجراء استدلالي عادي وليس دليل قضائي أو دليل فني.

- السبب الثالث: حدد المشرع جهات الخبرة، ليس منها التقارير الفنية التي تصدر عن مأموري الضبط القضائي[1].

كما يحق كذلك لوكيل الجمهورية حضور استجواب المتهمين ومواجهتهم وسماع أقوال المدعي المدني، ويوجه ما يراه مناسبا من الأسئلة وهذا ما نصت عليه المادة من ق.إ.ج.ج و بناءا على ما تقدم نجد أن القاعدة العامة بالنسبة للخصوم لا سرية في التحقيق، ومع ذلك فقد أورد المشرع عليها استثنائيين عاد فيهما إلى أصل السرية بالنسبة للخصوم وهمـــا حالة الضرورة و حالة الإستعجال.

- **حالة الضرورة:** يجوز فيها لقاضي التحقيق الخروج على الأصل العام الموجب لحضور الخصوم إجراءات التحقيق، بالسماح له بالتحقيق في غيابهم، وهذا ما نصت عليه المادة 99 من ق.إ.ج.ج بقولها:" إذا تعذر على شاهد الحضور انتقل إليه قاضي التحقيق لسماع شهادته أو اتخذ لهذا الغرض طريق الإنابة القضائية، فإذا تحقق من أن الشاهد قد ادعى كذبا عدم استطاعته الحضور جاز له أن يتخذ ضدّه الإجراءات القانونية طبقا لأحكام المادة 97" ، وكذلك نصت المادة 1/77 من ق.إ.ج.م " أن لقاضي التحقيق أن يجري التحقيق في غيبتهم متى رأى ضرورة ذلك لإظهار الحقيقة أو بمجرّد انتهاء الضرورة يبيح لهم الاطلاع على التحقيق".

وتظهر الضرورة التي تبرر فرض السرّية في احتمالية أن يفسد حضور المتهم أو غيره من الخصوم جهود المحقق للتنقيب عن الدليل، أي أن الحكمة من السرّية هو الخشية من أن يؤدي هذا الحضور إلى إحباط جهود المحقق في إظهار الحقيقة.

و تحدد حالة الضرورة هذا الإجراء وكذلك الخصم الذي يمتنع عليه الحضور، فيجب ألّا يتجاوز المحقق الحكمة من منع الخصوم وهي حالة الضرورة ويقوم بإجراء لا يتوافر فيه تلك الصفة، كما أن المنع يجب أن يقتصر أيضا على الخصم الذي في عدم حضوره تتحقق الغاية من المنع وهي إظهار الحقيقة، ويستوي بعد ذلك أن يكون الخصم هو المتهم أو المسؤول عن الحقوق المدنية أو المجني

[1]– أحمد سعد محمد الحسيني، المرجع السابق، ص 72–73.

عليه، ولذلك يباشر الإجراء في غيبة الخصوم الذين يرى المحقق ضرورة مباشرة هذا الإجراء في غيابهم ولا يجب أن يتعداها إلى آخرين لا تتوافر بالنسبة لهم حالة الضرورة هذه [1].

ولقد أوجب المشرع على سلطة التحقيق بمجرد الانتهاء من حالة الضرورة التي من أجلها باشرت الإجراء في غيبة الخصوم، أن تبيح لهم الإطلاع على التحقيق فلا يجوز منعهم من حضور إجراءات التحقيق وحرمانهم في الوقت ذاته من الإطلاع على ما فاتهم من إجراءات في غيبتهم.

- **حالة الاستعجال:** أجاز المشرع فيها للمحقق أن يجري بعض إجراءات التحقيق في غيبة الخصوم، وهذا ما نصت عليه المادة 101 من ق.إ.ج.ج بقولها: " يجوز لقاضي التحقيق على الرغم من مقتضيات الأحكام المنصوص عليها في المادة 100 أن يقوم في الحال بإجراء استجوابات أو مواجهات تقتضيها حالة استعجال ناجمة عن وجود شاهد في خطر الموت أو وجود أمارات على وجه الاختفاء ويجب أن تذكر في المحضر دواعي الاستعجال"[2].

وهي حالة من شأنها أن تعفي قاضي التحقيق من واجب الإخطار المقرر قانونا، فتسمح له عند تبليغه مثلا بحالة احتضار الشاهد أو المجني عليه وكل من يفيد في إظهار الحقيقة أو معاينة تلك الأمارات بالانتقال فورا و اتخاذ الإجراءات المناسبة في غياب المعنيين.

وعليه فإن الاستعجال كما هو مقرر في القانون لم ترد حالاته على سبيل الحصر بتحديده تحديدا دقيقا، و إنما هي حالات واردة على سبيل المثال، مما يترك للقاضي المحقق تقدير مدى وجود حالة الاستعجال من عدمها فكلما رأى أن هناك حالة يخاف منها على ضياع الحقيقة بسببها، بادر باتخاذ أي إجراء يراه مناسبا، كالإنتقال دون ما التزام بواجب إخطار الأطراف[3].

و تظهر لنا أهمية مبدأ سرية التحقيقات في مجال الجرائم الإلكترونية، حيث أن معظمها إما جرائم متعلقة بالأعراض أو بالأموال، ومثال ذلك القضية التي تتخلص وقائعها في تلقي إدارة مكافحه جرائم الآلي و شبكة المعلومات بلاغا من فتاة تبلغ من العمر 31 سنه، تعمل مدرسة موسيقى بمدرسة (شرق القاهرة)، تعرفت عبر موقع زواج في الانترنيت على شاب يدعى حسام، وبعد فترة قصيرة أرسل لها صورته و أرسلت له صورتها، واتفاقا على سرية أن يتقابلا في مطعم بفندق شهير بمصر الجديدة،

---

[1]– أحمد سعد محمد الحسيني، المرجع السابق، ص66. وأنظر أيضا: عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري– التحري والتحقيق–، المرجع السابق، ص314 .

[2]– أنظر أيضا نص المادة 77 من ق.إ.ج.م.

[3]- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري– التحري والتحقيق–، المرجع السابق، ص315.

بهدف التعرف على بعضهما أكثر طالما اتفقا مبدئيا على الاختيار والارتباط ، و يوم الحادث وصلت إلى المطعم، وبعد جلوسها أمطرها بكلمات غزل و أصر على تناول الغذاء، وبعد فترة بدأ الحديث عن الشبكة ومكان شرائها، ثم طلب منها هذا الشاب خلع بعض المشغولات الذهبية التي ترتديها بحجة أن ذوقها رائع وليرى جمال نقوشها، وما هي إلا لحظات حتى كانت هذه القطعة في يده في الوقت الذي رن فيه جرس هاتفه المحمول، ثم بدأ الحديث في المحمول وهو يتمشى في إرجاء المطعم حتى اختفى وفي يده المشغولات الذهبية التي تقدر بمبلغ 9 آلاف جنيه.

توافرت للمباحث معلومات محددة أن الشاب كان يدخل على الموقع من مقاهي إنترنيت عديدة، وتم تحديد نطاق المتهم ما بين منطقتي بشتيل ومدينه 6 أكتوبر.

تم التعرف بأحد استوديوهات التصوير بمدينه 6 أكتوبر على صورة الشاب، وقال أنه يسكن في المجاورة السادسة واسمه رجب وليس حسام، و أنه دائما ما يتردد عليه لعمل مونتاج لصورته الشخصية ليخفي به مرضه الذي أصيب به في رأسه، وأقر أن هذا المرض هو الثعلبة الجلدية.

تم وضع أكمنة حول أماكن تردد المهتم بالجريمة حتى ألقي القبض عليه و أقر المتهم بالجريمة وأنه أوقع ما لا يقل عن 10 فتيات مثقفات في شباكه، جميعهن تتراوح أعمارهن بين 28 و 33 سنه، وهن لديهن إحساس بأن قطار الزواج قد يفوتهن، لذالك نجد لهفتهن وسذاجتهن تدفعهن للثقة فيه، كما أن الشيء المثير في القضية أنه وجد الضحايا لا يقمن بإبلاغ الشرطة خوفا من الفضيحة أو خجلا أمام عائلاتهن[1].

وفي قضيه أخرى ، تتلخص وقائعها في تلقي إدارة مكافحة جرائم الحاسبات الشبكات المعلومات المصرية بلاغا من طالة جامعية، ضد مجهول يقوم بتوزيع صورها وهي شبه عارية وفي وضع مثير علي جميع عناوين البريد الالكتروني لزملائها وأقاربها، وهي ابنة أستاذ جامعي شهير والنجم الدائم لحوارات الفضائيات، كما أن والدتها مسؤولة مرموقة لوزارة الصحة، أصرّت على أن الصورة الفاضحة هي صورة ليست حقيقية ولكنها تسببت لها في إساءة شديدة منعتها من الخروج من المنزل أو التوجه لكلياتها.

[1]– أحمد سعد محمد الحسيني، المرجع السابق، ص67.

و بالفحص المهني والفني من الخبراء، تبيّن أن الرسائل مرسلة من جهاز كمبيوتر يستخدمه عده أشخاص، أحدهم طالب جامعي يدرس بنفس الكلية و نفس تخصص صاحبة الشكوى، و لكنها تركته بعدما تعرفت على شاب آخر مما اثأر حفيظته، خاصة بعدما فشلت كل محاولاته لعوده علاقتهما ثانية، وعلى الفور تم استئذان النيابة العامة لضبطه، وكانت المفاجأة أثناء التحقيق معه عندما تبين أن الصورة الفاضحة صورة الفتاة الحقيقية وكانت تحتفظ بها على بريدها الالكتروني، حيث اعترف بذلك الطالب الذي قال بأنه هو الذي أنشأ لها بريدها الالكتروني، وبحكم علاقتهما العاطفية كان يعرف كلمة المرور السريّة التي استخدمها بعد مقاطعتها له في الدخول على بريدها والاطلاع عليه، حيث قام بسحب هذه الصورة و قام بإرسالها على جميع عناوين أصدقائها والمسجلة أيضا على بريدها الخاص.[1]

الفرع الرابع: أدوات التحقيق في الجرائم الإلكترونية

تعتبر أدوات التحقيق من الأدوات التي ينبغي على محقق الجرائم الإلكترونية التسلح بها وتتمثل هذه الأدوات فيما يلي:

أولا: برنامج التفتيش (Computer Scorch Warrant program) :

هو برنامج قاعدة بيانات يسمح بإدخال كل المعلومات الهامة لترقيم الأدلة وتسجيل البيانات عنها، ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين، أو طرف ضبط هذا الدليل ويجب أن يكون هذا البرنامج مع المحقق على قرص مرن أو قرص صلب محمول.

ثانيا: قرص بدء تشغيل الحاسب (Bootable Diskette) :

يجب وجود قرص تشغيل الحاسب مع المحقق لإمكان تشغيل الحاسبات[2] إذا كان نظام التشغيل فيها محميا بكلمة مرور، ويجب أن يكون القرص مزودا ببرنامج مضاعفة المساحة (Double Space) فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب[1].

---

[1]- أحمد سعد محمد الحسيني، المرجع السابق، ص68-69.

[2]- تنقسم الحاسبات من حيث التقنية إلى ثلاثة أنواع:

أ- حاسب آلي رقمي (Digital): وفيه يتم تمثيل البيانات بطريقة رقمية.

ب- حاسب آلي تناظري أو قياسي Analogue: وهو جهاز قياسات مثل كمبيوتر الأوزان والسرعة والحرارة، فلا يقوم بمهمة التخزين، ويعتمد في تنفيذ البيانات الداخلية على المتغيرات الفيزيائية مثل: الضغط الجوي ودرجة الحرارة.

ثالثا: برنامج (X Tree Pro Gold)

وهو برنامج معالجة ملفات ممتاز يمكن العثور على الملفات في أي مكان على الشبكة، أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الخاص بالمتهم أو الأقراص المرنة المضبوطة، ويستخدم لقراءة البرامج في صورتها الأصلية كما يستخدم أيضا للبحث عن كلمات معينة، أو عن أسماء ملفات أو غير ذلك مما له صلة بالأمر[2].

رابعا: برنامج (Laplink)

وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الحاسب الخاص بالمتهم ونقلها إلى قرص آخر من خلال المنفذ المتتالي أو المنفذ المتوازي، وهذا البرنامج مفيد جدا للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم[3].

خامسا: برنامج كشف الفيروسات وتدميرها

أي برنامج من برامج مكافحة الفيروسات يمكن أن يؤدي الغرض وتكمن أهمية مثل هذا البرنامج في ضمان حماية جهاز الحاسب الخاص بالمحقق[4]، لأن الفيروس كما هو معروف يعتبر من أحد أنواع برامج الحاسب الآلي إلا أن الأوامر المكتوبة في هذا البرنامج تقتصر على أوامر تخريبية ضارة بالجهاز محتوياته، فيمكن عند كتابة كلمة أو أمر ما أو حتى مجرد فتح البرنامج الحامل لفيروس أو الرسالة البريدية المرسل معها الفيروس إصابة الجهاز به ومن تم قيام الفيروس بمسح محتويات الجهاز أو العبث بالملفات الموجودة به[5] .

سادسا: برنامج (Ana Disk/ viewDisk)

جـ- حاسب آلي مختلط Hybride: يجمع بين خصائص الحاسب الرقمية التناظرية ويستخدم في أبحاث الفضاء والاستشعار عن بعد، وأبحاث الكشف عن الثروات الطبيعية، ويجمع بين خاصيتي التخزين والاسترجاع.

[1]- حسن طاهر داوود، جرائم نظم المعلومات، الطبعة الأولى، الرياض، 2000، ص228.

[2]- محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، الفكر الشرطي، المجلد 20، العدد الرابع، رقم 79، الشارقة، الامارات العربية المتحدة، 2011، ص45.

[3]- حسن طاهر داوود، المرجع السابق، ص229.

[4]- محمد حسان السراء، المرجع السابق، ص45.

[5]- محمد محمد الألفي، العوامل الفاعلة في إنشاء جرائم الارهاب عبر الأنترنيت، أعمال المؤتمرات حول مكافحة الجريمة عبر الأنترنيت، المنظمة العربية للتنمية الادارية، القاهرة، مصر، 2010، ص11.

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن مهما كان أسلوب تهيئته، وهذا البرنامج توجد منه نسخة عادية تصلح للأفراد العاديين، ونسخة خاصة لرجال الشرطة أو محققي الحاسب الآلي ويمكن الحصول عليه من شركة (Software Sydex).

سابعا: برامج الدمج وفك الدمج: (PKZIP)

ويستخدم لفك دمج البرامج، فربما كان المتهم قد قام بدمج برامجه، وفي هذه الحالة لا يمكن الإطلاع عليها إلا بعد فك الدمج[1].

ثامنا: برنامج اتصالات

مثل (Lantastic) وهو برنامج يستطيع ربط جهاز حاسب المحقق بجهاز حاسب المتهم لنقل ما به من معلومات، وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

المطلب الثاني: عناصر التحقيق في الجرائم الالكترونية

لا تختلف الجريمة المعلوماتية عن الجريمة الكلاسيكية في الأركان المتعارف عليها، إلا أن الأولى لها خصوصية تختلف عن الجريمة الثانية، لذلك يجب على المحقق أن يستظهر الركن المادي(الفرع الأول)، والركن المعنوي للجريمة محل التحقيق(الفرع الثاني)، وتحديد وقت ومكان ارتكاب الجريمة الإلكترونية(الفرع الثالث) بالإضافة إلى علانية التحقيق (الفرع الرابع).

الفرع الأول: إظهار الركن المادي للجرائم الإلكترونية

إن النشاط أو السلوك المادي في جرائم الأنترنيت يتطلب وجود بيئة رقمية واتصالات بالأنترنيت[2]، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته فمثلا يقوم مرتكب الجريمة بتجهيز

---

[1]– حسن طاهر داوود، المرجع السابق، ص229.

[2]– الأنترنيت أو الشبكة العالمية للمعلومات هي توصيات تعاونية لعدد من شبكات الحاسبات الآلية وهي مكونة من كلمتين (Inter Connections) وكلمة (Net.Work)، وهذا يعني أن مئات الشبكات المربوطة مع بعضها البعض مكونة من حاسبات آلية مختلفة وكذلك تكنلوجيا مختلفة، تم توصيلها ببعضها البعض بطريقة بسيطة وسهلة بحيث تبدوا وكأنها قطعة واحدة أو نظام واحد دون إحساس أي من الأطراف بأنه يختلف فنيا عن الآخر. أنظر: عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والأنترنيت في القانون العربي النموذجي، المرجع سابق، ص80–81. أنظر أيضا: سهيل محمد العزام، الوجيز في جرائم الأنترنيت، الطبعة الأولى، مكتبة الجامعة الأردنية، 2009، ص6.

الحاسبة الإلكترونية لكي يحقق له حدوث الجريمة، فيقوم بتحميل الحاسبة الإلكترونية ببرامج اختراق، أو أن يقوم بإعداد هذه البرامج بنفسه، وكذلك قد يحتاج إلى تهيئة صفحات تحمل في طياتها مواد داعرة أو مخلة بالآداب العامة وتحميلها على الجهاز المضيف (Hosting Server) كما يمكن أن يقوم بجريمة إعداد برامج فيروسات تمهيدا لبثها[1].

لكن ليس كل جريمة تستلزم وجود أعمال تحضيرية، وفي الحقيقة يصعب الفصل بين العمل التحضيري والبدء في النشاط الاجرامي في نطاق الجرائم الإلكترونية حتى ولو كان القانون لا يعاقب على الأعمال التحضيرية، إلا أنه في مجال تقنية المعلومات الأمر يختلف بعض الشيء، فشراء برامج اختراق وبرامج فيروسات، ومعدات لفك الشفرات وكلمات المرور، وحيازة صور دعارة للأطفال فمثل هذه الأشياء تمثل جريمة في حد ذاتها[2].

الفرع الثاني: إظهار الركن المعنوي للجرائم الإلكترونية

الركن المعنوي هو الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني، وقد تنقل المشرع الأمريكي في تحديد الركن المعنوي للجريمة بين مبدأ الارادة ومبدأ العلم، فهو تارة يستخدم الارادة كما هو الشأن في قانون العلامات التجارية في القانون الفيدرالي الأمريكي، وأحيانا أخرى أخذ بالعلم كما هو قانون مكافحة الاستنساخ الأمريكي[3].

الفرع الثالث: تحديد وقت ومكان ارتكاب الجريمة

تثير مسألة النتيجة الإجرامية في الجرائم الإلكترونية مشاكل عدة، فعلى سبيل المثال مكان وزمان تحقق النتيجة الاجرامية، فلو قام أحد المجرمين في أروبا باختراق جهاز خادم[4](SERVER) أحد

---

[1]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص52.

[2]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2012، ص66.

[3]– خالد ممدوح إبراهيم، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع نفسه، ص53. وأنظر أيضا: محمد حسن السراء، المرجع السابق، ص36–37.

[4] – يستخدم الحاسب الخادم لتبادل البيانات بين قواعد البيانات الضخمة ومئات وآلاف من المستخدمين المرتبطين به عبر حواسيب شخصية، حيث يمكن لمثل هذا الحاسب الخادم معالجة كم كبير من البيانات وربما يشغل عدة جيجابايت من الذاكرة وآلاف الجيجابايت من مساحات التخزين الثانوية بالإضافة إلى إجراءات ضمان الحماية ضد الفقدان

البنوك في العراق، وهذا الخادم موجود في البرازيل فكيف يمكن معرفة وقت حدوث الجريمة هل هو توقيت بلد المجرم أم توقيت بلد البنك المسروق أم توقيت الجهاز الخادم في البرازيل، وهذا بالتالي يثير مشكلة أخرى، وهي مكان ارتكاب الجريمة الإلكترونية، ويثير أيضا إشكاليات القانون الواجب التطبيق في هذا الشأن حيث أن هناك بعد دولي في هذا المجال ذلك أن الجريمة المعلوماتية جريمة عابرة للحدود[1].

الفرع الرابع: علانية التحقيق

إن علانية التحقيق من الضمانات اللازمة لتوافر العدالة، ولهذا قيل أن العلانية في مرحلة المحاكمة لا يقتصر فيها الأمر على وضع الاطمئنان في قلب المتهم، بل أن فيها بذاتها حماية لأحكام القاضي من أن تكون محلا للشك أو الخضوع تحت التأثير، كما أن فيها اطمئنان للجمهور على أن الإجراءات تسير في طريق طبيعية[2].

والعلانية المقررة للتحقيق في الاجراءات الجنائية هي من بين الضمانات الخاصة به ، وهي تختلف في مرحلة التحقيق الابتدائي عنها في مرحلة المحاكمة، ففي مرحلة التحقيق الابتدائي تعتبر العلانية نسبية أي قاصرة على الخصوم في الدعوى الجزائية، بينما العلانية في مرحلة المحاكمة هي علانية مطلقة، بمعنى أنه يجوز لأي فرد من افراد الجمهور الدخول الى قاعة الجلسة و حضور المحاكمة.

كما أنه يجوز في المرحلتين، مرحلة التحقيق الابتدائي ومرحلة التحقيق النهائي مباشرة الإجراءات في غير علانية، فيصدر القرار بجعله سريا، ولما كان هذا استثناء يأتي على قاعدة عامة أصلية، كان

العرض للبيانات لذلك فهي غالية الثمن، مثال ذلك: الموجود في المؤسسات العامة والخاصة والوزارات، ويكون لهذا الحاسب وحدة معالجة مركزية مرتبط بها عدد من النهايات الطرفية في مواقع العمل والمنافذ المختلفة. أنظر: مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، الطبعة الأولى، بدون دار نشر، 2001، ص30-31.

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص67.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص54.

لابد من أن يتم تحديد الاحوال التي يجوز فيها جعل التحقيق سريا، وهذه على كل حال رخصة لا يحسن الالتجاء إليها إلاعند الضرورة [1].

وإذا كانت الامور التي تجري سرا من شأنها ان تولد الشك في القلب، وتبعث في النفس عدم الاطمئنان فإن هذا الاثر كما يتحقق لدى المتهم، فهو الجائز ان يقوم في نفس الشاهد وأقواله من الأدلة الجنائية الهامة، ولهذا كان القرار يجعل التحقيق سريا موجها للجمهور عامة و للشهود خاصة بأهمية و خطورة الواقعة التي يجري التحقيق فيها، وينعكس هذا الأثر في صورة اضطراب وتردد بل قد يصل الأمر إلى إنكار المعلومات من جانب الشاهد[2].

ولذلك فإن ظروف مثل هذا التحقيق ينبغي أن تكون محل تقدير دقيق حين الإستشهاد بأقوال الشاهد، فرغم أن العلانية النسبية في التحقيق الابتدائي تجعل حضور إجراءاته قاصرا على من له علاقة بالدعوى الجزائية، إلا أن هؤلاء بذاتهم قد يكون لهم اعمق الأثر في نفسية الشاهد، وهناك بعض المسائل التي تتصل بعلانية التحقيق لها أهمية عملية خاصة، هي اختيار مكان التحقيق، و حضور الخصوم اثناء التحقيق، و القواعد التي ينبغي مراعاتها في معاملة الحضور[3].

المطلب الثالث: وسائل التحقيق في الجرائم الالكترونية

عند القيام بالتحقيق في جريمة ما، فإنّه يتعين على المحقق الالتزام بقوانين و تشريعات و لوائح مفسّرة، وقواعد فنية تحقق الشرعية، وسهولة الوصول إلى الجاني، وحيث أن للجرائم الالكترونية طابعها الخاص المميز لها، فإن التحقيق فيها يحتاج إلى معرفة تامّة وإدراك لوسائل وقوع الجريمة، وبالتّالي حل لغزها والوصول إلى الجاني، وتوجد ثمّة وسائل تساعد على ذلك وهي الوسائل المادية (الفرع الأول) والوسائل الإجرائية (الفرع الثاني) .

---

[1]– علي عدنان الفيل، إجراءات التحري وجمع الادلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص67-68.

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 55 .

[3]–علي عدنان الفيل إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق ص 68. وأنظر أيضا: خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع نفسه، ص 55.

الفرع الأول: الوسائل المادية

وهي الأدوات الفنية التي غالبا ما تستخدم في بنية نظـــم المعلومات و التي تثبت وقوع الجريمة وتساعـد على تحديد شخصية مرتكبها ومن أهمها:

أولا: عناوين (IP) و البريد الالكتروني، و برامج المحادثة

عنوان الإنترنيت هو المسؤول عن تراسل حزم البيانات عبر شبكة الانترنيت و توجيهها إلى أهدافها، و هو يشبه الى حد كبير عنوان البريد العادي، حيث يتيح للموجات و الشبكات المعنية نقل الرسالة و هو يوجد بكل جهاز مرتبط بالأنترنيت، و يتكون من أربعة أجزاء كل جزء يتكون من أربع خانات فيكون المجموع اثنتا عشر خانة كحد اقصى، حيث يشير الجزء الأول من اليسار وإلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الالية المرتبطة، والرابع يحدد جهاز الحاسبة الإلكترونية الذي تم الاتصال منه[1].

وفي حالة وجود أي مشكلة أو أية أعمال تخريبية فإن أول ما يجب أن يقوم به المحقق هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال غير القانونية، ويمكن لمزود خدمة الانترنت أن يراقب المشترك كما يمكن للشبكة التي تقدم خدمة الاتصال الهاتفي أن تراقبه أيضا إذا ما توافرت لديها أجهزة وبرامج خاصة لذلك.

هذا وتوجد أكثر من طريقة يمكن من خلالها معرفة هذا العنوان الخاص بجهاز الحاسبة الالكترونية في حالة الاتصال المباشر، منها على سبيل المثال ما يستخدم في حالة العمل على نظام التشغيل (Windows) حيث يتم كتابة (WIN.PCFG) في أمر التشغيل ليظهر مربع حوار يبين فيه عنوان(IP)، مع ملاحظة أن عنوان الأنترنت قد يتغير مع كل اتصال بشبكة الأنترنت [2].

أما في حالة استخدام أحد البرامج التحادثية كأداة للجريمة، فإنه يتطلب تحديد هوية المتصل، كما حدد رسالة البريد الإلكتروني عنوان شخصية مرسلها حتى ولو لم يدون معلوماته في خانة المرسل،

[1]– حسين بن سعيد الغافري، المرجع السابق، ص 511.

[2]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع سابق ص70.

شريطة أن تكون تلك المعلومات التي وضعت في مرحلة إعدادات البريد الإلكتروني معلومات صحيحة.[1]

والسؤال الذي يمكن طرحه في هذا الصدد ماذا يكشف رقم (IP) ويمكن لذلك الاستفادة منه في التحقيق الجنائي؟

يمكن القول في هذا الصدد أنه عندما يزور شخصا موقعا ما على الشبكة يسجل الموقع (IP) العائد للكمبيوتر الذي اتصل به، وعند إرسال رسالة إلكترونية، يمكن لمستلم الرسالة معرفة عنوان (IP)، للكمبيوتر المرسل أيضا، فإذا كان يستخدم برنامج الأوتلوك مثلا، فيكفي أن ينقر على أوبشن بعد أن يفتح الرسالة ليطلع على عنوان (IP)[2]، لكن هل يحدد عنوان الكمبيوتر المتصل بدقة ؟

إذا كان الكمبيوتر المتصل ينتمي إلى شبكة مرتبطة بخط خاص مؤجر كما هو الحال بالنسبة للعديد من شبكات المؤسسات المتوسطة و الكبيرة، فسوف يكشف عن اسم تلك المؤسسة، ورقم الكمبيوتر المتصل، أما إذا كان الكمبيوتر يتصل عن طريق طلب رقم هاتف عادي فلا يكفي رقم (IP)، لتحديد الجهة المتصلة بالموقع أو التي بعث برسالة، إذا سيكشف القسمان الأول والثاني من الرقم، بدءا من اليسار، عن اسم مزود خدمات الأنترنت الذي يشترك لديه المتصل، فيما يحدد القسمان الثالث والرابع، رقم مجموعة الكمبيوترات، ولكن ما هو الحل إذا كان والكمبيوتر المتصل لدى مزود خدمة واحدة لدية عنوانين متطابقة، اذا جرى الاتصال في أوقات مختلفة، كيف يمكن اكتشاف المتصل او مرسل الرسالة في هذه الحالة ، إن ارتكب مخالفة قانونية؟

يمكن ذلك عن طريق مزود خدمة (ISP) الذي تحتفظ كمبيوتراته بسجلات عن كافة الاتصالات، تضم حقلا لرقم وحقلين لكل من تاريخ وزمن الاتصال وحقلا لاسم المشترك، ويكفي أن تزود الجهة المتضررة بقيمة الحقول الثلاثة الأولى (تكون عادتا مسجلة لديها) كي يكتشف اسم المشترك، ويمكن

---

[1]– حسين بن سعيد الغافرين، المرجع سابق، ص512.

[2]– ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006، ص71.

بالتعاون مع مؤسسة الهاتف الوصول الى الرقم الذي تم عن طريقه الاتصال، لكن هذه الإجراءات تتطلب تدخلا من قبل الجهات الرسمية المشرفة على تطبيق القانون[1].

وتستخدم معظم المواقع نظام او بروتوكول الكوكز (Cookies)[2] والفائدة منه هو في الحقيقة تسريع الدخول الى المواقع ويرجع السبب الرئيسي في وجوده الغاية التجارية، فبهذا النظام تستطيع المواقع أخذ بعض البيانات الخاصة مثل كم مرة تم زيارة الموقع وما نوع الجهاز المستخدم؟ ويلاحظ أن بعض البرامج الموجودة في جهاز الكمبيوتر تقدم هذه المعلومات، كما أن تلك المواقع تقوم بإرسال ملف صغير الى الهارد دسك عن طريق استخدام الكوكز[3].

ويلاحظ أنه توجد على شبكة الانترنت عدة مواقع تؤمن السرية لتحركات المستخدم، فموقع www.anonymizer.com مثلا يوفر للمستخدم من خلال خدمة إمكانية إخفاء رقم (IP) عن المواقع التي يرغب في زيارتها ويوصله إليه، بدون أن يمكنه من تسجيل أي معلومات حقيقية عنه حيث سيبدو للموقع الذي يزوره، أنه قادم من عنوان أخر، وتقدم هذه الخدمة إما مجانا بسرعة بطيئة نسبيا أو بمقابل مع سرعة جيدة، ومزايا أفضل في الخدمة.

ويوفر الموقع أيضا، إمكانية إخفاء هوية المستخدم عن مزود خدمة انترنت الذي يشترك لديه المستخدم، من خلال مزود خدمة آخر يقود تصرفات المستخدم على الشبكة، باستخدام تقنيات تشفير متطورة (128 بت) فلا تشفر هذه الخدمة، كل مزود الخدمة قادرا على معرفة أسماء المواقع التي يزورها المستخدمين، أو الكلمات التي يبحث عنها، لذا تضمن أيضا سرية إرسال رسائل البريد الالكتروني، والدردشة عبر الأنترنت، وتوفر بعض البرمجيات المجانية مثل Ghost mail إمكانية

---

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص72.

[2]– الكوكي أو Cookie : تشير إلى ملف أو سجل البيانات، يسجل على القرص الصلب للكمبيوتر بوسطة كمبيوتر أخر خلال اتصالك بها، وتتيح البيانات المدونة في الملف Cookies للمزود الذي تتصل به معرفة المواقع التي زرتها في الآونة الأخيرة، ومعلومات أخرى عنك، وحيث أن القليل من المزودات في الأنترنيت تخبرك أنها ستسجل معلومات تخصك في الملف Cookies، فإن الكثيرين يعتبرونها انتهاكا لحرمة خصوصياتهم، وظهرت العديد من البرمجيات المضادة للكوكي Anti-cookies التي تبادر إلى محو أية بيانات تسجل في الملف Cookies فورا. أنظر: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص208.

[3]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 72.

ارسال رسائل الكترونية بدون الكشف عن عنوان (IP) الخاص بالكمبيوتر[1] المتصل، ويمكن جلب البرنامج من الموقع (www.er.uqam.ca/merlin/fg591543/gm).

ولكن هل يضمن الاشتراك بالخدمات المذكورة، إخفاء الهوية بشكل كامل أثناء استخدام الانترنت؟

بطبيعة الحال لا، فالجهة الوسيطة التي تقدم هذه الخدمات، تحتفظ بسجل عن كافة تحركاتك، لكنها لا تكشفه، إلا في حال وقع اعتداء معين، مصدره الكومبيوتر الذي يستخدم، كان يرسل رسائل تهديد الى الاخرين، أو قنابل بريدية، أو يقوم بتصرفات أخرى تخالف القوانين والتشريعات المعمول بها.

ثانيا: البروكسي(proxy)

البروكسي[2] عبارة عن حلقة وصل بين الخص وبين الأنترنت على الرغم من أن بعض الناس ترى مشاكل في استعمال البروكسي، إلا أن فوائدها تفوق مشاكلها بكثير[3].

ويعمل البروكسي كوسيط بين الشبكة ومستخدميها كما ذكرنا سابقا بحيث تضمن الشركات الكبرى المقدمة لخدمة الاتصال بالشبكات قدرتها لإدارة الشبكة، وضمان الأمن وتوفير خدمات الذاكرة الجاهزة (Cashe Memory)، وتقوم فكرة البروكسي على تلقي مزود البروكسي طلبا من المستخدم للبحث عن صفحة ما ضمن ذاكرة (Cashe) المحلية المتوفرة فيتحقق البروكسي فيما إذا كانت هذه الصفحة قد جرى تنزيلها من قبل فيقوم بإعادة إرسالها إلى المستخدم بدون الحاجة إلى إرسال الطلب إلى الشبكة العالمية، وفي هذه الأخيرة يعمل البروكسي كمزود زبون ويستخدم أحد عناوين(IP)، ومن أهم مزايا مزود البروكسي أن ذاكرة (Cashe) المتوفرة لديه يمكن ان تحتفظ بتلك العمليات التي تمت

---

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 71.

[2]– البروكسي (Proxy): كلمة انجليزية تعني الوكيل وتقوم مزودات بروكسي بدور الوسيط بين المشتركين لدى احدى شركات تقديم خدمة الانترنيت، وبين المواقع الموجودة على الشبكة العالمية، او بدور الوكيل عن هؤلاء المشتركين في طلب المعلومات من تلك المواقع، ونستطيع أن نتخيل مزودات البروكسي كذاكرات كاش كبيرة الحجم، مهمتها تسريع الحصول على المعلومات من مواقع ويب، وأداء بعض الوظائف الأخرى المفيدة. أنظر: ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص83.

[3]– أشرف صلاح الدين، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة، أعمال مؤتمرات حول مكافحة الجريمة عبر الأنترنيت، المنظمة العربية للتنمية الإدارية، القاهرة، 2010، ص203.

عليها، مما يجعل دوره قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة[1].

فالمهمة الرئيسية لمزودات البروكسي هي الحصول على المعلومات في أسرع وقت ممكن، حيث يستطيع البروكسي قراءة المعلومات من مواقع ويب بسرعة أكبر مما يستطيعه جهازك، فيما لو اتصل بذلك الموقع مباشرة، وقال مدير احدى شركات تقديم خدمة انترنيت في لبنان: بينت سجلاتنا في الأشهر الستة الماضية ان 60% من المواقع التي يرتادها المشتركون، يتكرر طلبها، وأن مزود البروكسي يمكنه أن يوفر على المشتركين 50% من وقتهم، وسيطا وعندما تستخدم البروكسي تعود الفائدة عليك وعلى بقية المشتركين أيضا[2].

ولكن ماهي الوظائف الأخرى للبروكسي ؟

طورت تقنية البروكسي في البداية لاستخدامها كحواجز نارية (fireWalls) لأنترنيت، والحاجز الناري عبارة عن نظام أمين يفرض توليد جميع الرزم المرسلة أو الواردة الى الشبكة الداخلية لمؤسسة ما، من خلال جهاز وحيد، واذا أراد المستخدمون جلب وثيقة ما من شبكة انترنيت، فعليهم أن يطلبوا ذلك من مزود البروكسي الذي يقوم بالمهمة ويمررها لهم من خلال الحاجز الناري[3].

كما أن هناك ثلاثة وسائل تستطيع من خلالها خوادم البروكسي تحسين نوعية الخدمة عن طريق الذاكرة المختبئة[4]:

- الوسيلة الأولى: الذاكرة المخبئة توفر المساحة المتاحة للنقل بصورة أفضل في الشبكة.
- الوسيلة الثانية: هي أن الذاكرة المخبئة تقلل من الوقت اللازم لتحميل الصفحات من الانترنيت على أجهزة الكمبيوتر التابعة للزبون.

---

[1]– حسين بن سعد الغافري، المرجع السابق، ص513.

[2]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص84.

[3]– أشرف صلاح الدين، المرجع السابق، ص211. وأنظر أيضا: ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص84.

[4]– حيث تعمل الذاكرة المخبأة على الاحتفاظ بالصفحات التي تمت زيارتها بواسطة أي مستخدم على نفس الشبكة للمؤسسة، وعندما يريد شخص آخر زيارة نفس الصفحة أو الموقع فإن صفحات الموقع قد تم خزنها في الذاكرة المخبئة ولذلك فإن عملية تنزيلها تصبح أسهل وأسرع. أنظر: أشرف صلاح الدين، المرجع نفسه، ص212.

- من خلال الذاكرة المخبئة فإن صفحة الويب تكون موجودة على خادم البروكسي حتى إذا تم توقف عمل المصدر الرئيسي.

واشتهرت مزودات البروكسي في الآونة الأخيرة، بسبب امكانياتها في تسريع الوصول الى شبكة الأنترنيت، وتخفيض استهلاك عرض حزمة الناقل، ولأنها تؤمن تدابير أمنية جيدة للتحكم بعمليات الاتصال بالأنترنيت، فمن السهل باستخدام مزود بروكسي، تعريف الأشخاص المسموح لهم الاتصال بالأنترنيت وتحديد الخدمات التي يمكنهم استخدامها(تصفح، بريد الكتروني) ويمكن لمدير الشبكة أن يحدد أيام الأسبوع والساعات المسموحة للاتصال بالأنترنيت وأن يمنع الاتصال ببعض المواقع نهائيا[1].

غير أن السؤال الذي يتبادر الى أذهاننا ماهي مساوئ البروكسي؟

يمكن من خلال البروكسي منع الوصول إلى صفحات معينة، وبالإضافة إلى هذا، فإن السلبية الرئيسية للبروكسي، هي الحصول على صفحات قديمة أو ناقصة أحيانا من قاعدة بياناته، ويمكن الالتفاف إلى هذه المشكلة بإعادة تحميل الصفحة (بالنقر على زر Relouad) في برنامج التصفح، غير أن هذه الطريقة لا تنجح دائما.

و تحدث المشكلة عندما ينقطع الاتصال خلال عملية جلب البروكسي لصفحة ما، أو عندما يلغي المستخدم طلبه، ففي هذه الحالة يخزن جزء من الصفحة في قاعدة بيانات البروكسي ولكن يعتبرها البروكسي كاملة ، ويرسلها الى أي مستخدم بطلبها، ويتم تنظيف قاعدة بيانات البروكسي وإعادة تنظيمها يوميا، حيث تسمح الصفحات التي يكون الطلب عليها في حده الأدنى، مما قد يعني بقاء بعض الصفحات الناقصة في الكاش لعدة أيام، وربما لاحظ مستخدمي الأنترنيت في بعض الدول ظهور الرسالة (Transfer interruptif) على شاشتهم كلما حاولوا زيارة الموقع www.microsoft.com وهذا مثال عما يحدث عندما يخزن البروكسي صفحة ناقصة لديه، ولحسن الحظ هذه المشكلات مؤقتة، ويتم إيجاد حلول لها[2].

و الحقيقة أن مزود البروكسي يمنع الوصول الى بعض المواقع، لكن هذا الدور الرقابي هام ويجب أن تقوم به السلطات المعنية، ولكن الاعلام للأسف سلط الضوء على موضوع الرقابة فقط، متجاهلا

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص85.

[2]– ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص86.

كافة الفوائد الأخرى لمزودات البروكسي، وهذا الأخير يفيد ضباط الشرطة القضائية عن طريق ضبط ذاكرة الكاش لكل مستخدم والرقابة عليها أو فحصها عند وقوع الجرائم الالكترونية.

ثالثا: برامج التتبع

يقوم هذا البرنامج بالتعرف على محاولات الاختراق التي تتم مع تقديم بيان شامل بها الى المستخدم الذي تم اختراق جهازه، ويحتوي عذا البيان على اسم الحدث وتاريخ حدوثه وعنوان(IP) الذي تمت من خلاله عملية الاختراق، واسم الشركة المزودة لخدمة الانترنيت المستضيفة للمخترق، وأرقام مداخلها ومخارجها على شبكة الانترنيت ومعلومات أخرى[1].

ومن الأمثلة على هذه البرامج برنامج (hack tracer vl2) وهو يتكون من شاشة رئيسية تقدم للمستخدم بيان شامل بعملية الاختراق التي تعرض لها جهازه، يحتوي على اسم وتاريخ الواقعة وعنوان (IP) التي تمت من خلاله عملية الاختراق واسم الدولة التي تمت منها محاولة الاختراق، واسم الشركة المزودة لخدمة الانترنيت المستضيفة للمخترق، ورقم المنفذ و البوابة الخاصة، وبيانات الشبكي التي تتبعها الشركة المستفيضة للمخترق بما فيها أرقام هواتفها والفاكسات الخاصة بها، وأخر تحديث قامت به في أجهزة الخدمة الخاصة بها، وغيرها من المعلومات[2].

رابعا: نظام كشف الاختراق (Intrusion Détection System):

ويرمز له اختصارا بالأحرف (IDS) وهذه الفئة من البرامج تتولى مراقبة بعض العمليات التي يجرى حدوثها على أجهزة الحاسب الآلي أو الشبكة مع تحليلها بحثا عن أية إشارة قد تدل على وجود مشكلة قد تهدد أمن الحاسوب او الشبكة[3].

ويتم ذلك من خلال تحليل رزم البيانات اثناء انتقالها عبر الشبكة ومراقبة بعض ملفات نظام التشغيل الخاصة بتسجيل الاحداث فور وقوعها في جهاز الحاسب الآلي أو الشبكة مقارنة نتائج التحليل بمجموعة من الصفات المشتركة للاعتداءات على الأنظمة الحاسوبية، والتي يطلق عليها أهل

---

[1]– حسين بن سعيد الغفاري، المرجع السابق، ص 513.

[2]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص71.

[3]– حسين بن سعيد الغفاري، المرجع السابق، ص513– 514.

الاختصاص مصطلح التوقيع، وفي حال اكتشف النظام وجود أحد هذه التواقيع يقوم بإنذار مدير النظام بشكل فوري وبطرق عدة ويسجل البيانات الخاصة بهذا الاعتداء في سجلات حاسوبية خاصة، والتي يمكن أن تقدم معلومات قيّمة لفريق التحقيق تساعدهم على معرفة طريقة ارتكاب الجريمة وأسلوبها وربما مصدرها[1].

خامسا: نظام جرة العسل(Honey pot)

وهو نظام حاسوبي مصمم خصيصا لكي يتعرض لأنواع مختلفة من الهجمات عبر الشبكة، دون أن يكون عليه أية بيانات ذات أهمية، ويعتمد على خداع من يقوم بالهجوم و إعطائه انطباعا خاطئا بسهولة الاعتداء على أي جهاز آخر في الشبكة، في الوقت الذي يتم جمع أكبر قدر ممكن من المعلومات عن الأساليب التي يتبعها المهاجم في محاولة الاعتداء، وتحليلها وبالتالي اتخاد اجراء وقائي فعال، وهذه المعلومات التي تم جمعها تفيد في تحليل أبعاد الجريمة في حال وقوعها ويهتم فريق التحقيق بالعديد من البيانات التي توضح معالم الجريمة.

سادسا: أدوات تدقيق ومراجعة العمليات الحاسوبية(Auditing Tools)

وهي أدوات خاصة تقوم بمراقبة العمليات المختلفة التي تجري على ملفات ونظام تشغيل حاسوب معين وتسجيلها في ملفات خاصة يطلق عليها (Logs) والكثير من هذه الأدوات تأتي مضمنة في أنظمة التشغيل بعد إعدادها للعمل، وكل ما يحتاجه الأمر هو قيام مدير الشبكة أو النظام بتفعيلها أو إعدادها للعمل في وقت مبكر وسابق لارتكاب الجريمة حتى يمكن أن تقوم بتسجيل المعلومات التي قد يكون لها علاقة بالحادثة وربما ساعدت في كشف أسلوب الجريمة وشخصية مرتكبيها[2].

ومن الأمثلة على هذه الأدوات أداة(Event veiwer) لبيئة النوافذ وأداة (syslogd) لبيئة يونكس.

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص71- 72. وأنظر أيضا: خالد عياد الحلبي، المرجع السابق، ص208- 209.

[2]- خالد عياد الحلبي، المرجع نفسه، ص 210. أنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص73.

سابعا: أدوات الضبط

تحتاج جهات التحقيق وجمع الاستدلالات الى ضبط الجريمة وإثبات وقوعها والمحافظة على الأدلة حتى نسبتها الى الجاني، لتقديمها الى النيابة العامة لكسب اعترافه، والذين بدورهم يقدمون تلك الأدلة محفوظة الى القضاء للمحاكمة، وأدوات الضبط تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة الإلكترونية منها على سبيل المثال: برامج الحماية وأدوات المراجعة، وأدوات مراقبة المستخدمين للشبكة، وبرامج التصنت على الشبكة، والتقارير التي تنتجها نظم أمن البيانات، ومراجعة قاعدة البيانات، وبرامج النسخ الاحتياطي التي تستخدم لعمل نسخة مطابقة تماما للأقراص الصلبة الموجودة في الحسابات الالكترونية محل التحقيق وعلى مستوى (Bit Stream Bac kop)، بغرض الفحوصات الجنائية عليها دون تعريض الأقراص الأصلية لأي تغير في البيانات الموجودة كما يمكن استخدام أغلب الأدوات المستخدمة في الجريمة كأداة ضبط مثل أدوات جمع المعلومات عن الزائرين للموقع كبرمجيات (Java Appllets) أو (Java)[1] والبرامج الأخرى.[2]

ثامنا: الوسائل المساعدة للتحقيق

من هذه الوسائل الأدوات المستخدمة في استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمات المرور، وبرامج الضغط وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية وبرامج تشغيل الحاسبة، وبرامج نسخ البيانات، أيضا من الأدوات المهمة والتي تساعد في عملية التحقيق برامج منع الكتابة على القرص الصلب وذلك بعد ارتكاب الجريمة، مما ساعد في المحافظة على مسرح الجريمة، وهناك البرامج التي تساعد على استرجاع الملفات والمعلومات التي قد يلجأ الجاني إلى

---

[1]– جافا لغة: برمجة تستخدم " الكائنات" (OOP)، ومستقلة عن منصة العمل (العتاد ونظام التشغيل)، طورتها شركة صن، ولا تزال جافا تسير بخطوات سريعة نحو النضج والاكتمال، وتتضمن بعض صفحات ويب، وصلات إلى برمجيات جافا مثل أي أمر (HTML) آخر، وعندما يستلم متصفح يدعم جافا، صفحة تتضمن وصلات إلى برمجيات جافا، فإنه يجلب تلك البرمجيات مباشرة من أنترنيت وينفدها على جهازك. أنظر: ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص86.

[2]–خالد عياد الحلبي، المرجع السابق، ص210.

حذفها نهائيا من الحاسبة الإلكترونية، ومن أشهرها على سبيل المثال (Get Free) لبيئة النوافذ وبرامج (Extractor) لبيئة يونيكس[1].

وهناك أيضا برمجيات تحرير الملفات الست عشر (Hexadecimal Editors) وهي برامج يمكن المحقق من الاطلاع على محتوى كل ملف حاسوبي بشكله الثنائي، متيحة له المزيد من القدرة على تحليل الملف والتعرف على طبيعة البيانات التي يحتويها، خاصة وأن بعض الأنظمة قد لا تستطيع تحديد إلى أية فئة من الملفات ينتمي هذا الملف، وقد يتطلب الأمر استخدام هذا النوع من برامج التحرير التي تعتمد على أنّ الكثير من الملفات تحتوي على مجموعة من الرموز ذات الدلالة تتواجد في بداية الملف، ويستطيع الخبير الحاسوبي من خلالها تحديد نوع الملف بدقة[2].

ومن أشهر هذه البرمجيات برنامج (Gander) وهناك برمجيات البحث عن المفردات النصية والتي تستخدم في البحث عن البيانات، وتلك الملفات التي تحتوي على مفردات معينة عادة ما يكون لها علاقة بالقضية ومن الأمثلة عليها برنامج (Et Search) و برنامج (Starting Search)[3].

كذلك توجد برمجيات استعراض الصور والتي تستخدم في عرض الصور الرقمية على شاشة الجهاز وبالتالي فهي تقدم خدمة جيدة للمحقق من خلال تمكينه من مشاهدة واستعراض الصور الرقمية المخزّنة داخل أجهزة الحاسب الآلي أو وسائط التخزين الخارجية، حيث تبرز الحاجة لهذه البرمجيات في الجرائم الإباحية نشر مواد ذات طابع إباحي.

---

[1]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص74.

[2]– حسين بن سعيد الغافري، المرجع السابق، ص517.

[3]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص75.

تاسعا: أدوات فحص ومراقبة الشبكات

هذه الأدوات تستخدم في فحص بروتوكول الأنترنيت (TCP/IP)[1] (Transmission Control Protocol/ Internet Protocol) و ذلك لمعرفة ما قد يصيب الشبكة من مشاكل، ومعرفة العمليات التي تتعرض لها ومن تلك الأدوات التي يمكن استخدامها على النحو التالـــــي:

1- **أداة ARP** : و وظيفتها تحديد مكان الحاسب الآلي فيزيائيا على الشبكة، وهو يحتفظ بجميع أرقام كروت الشبكة MAC ، ولـه عدد من المداخل المستخدمة معه التي تحدد وتعرض كل جدول ARP للتعرف على عناوين (IP) هل أسندت بشكل صحيح أم لا؟ ، و وظيفته الأخرى معرفة رقم كرت الشبكة عند تعيين(IP) خاص لشخص ما.

2- **برنامج (Visual Route)** : هو عبارة عن برنامج يلتقط أي عملية فحص عملت ضد الشبكة، فيقوم بتقديم أجوبة تبيّن المعلومات التي حدث فيها مسح والمناطق التي مر فيها الهجوم، وبعد معرفة عنوان **(IP)** أو اسم الجهة، يرسم البرنامج خط يوضح من خلاله مسار الهجوم بين مصدره والجهة التي استهدفها ذلك الهجوم[2].

3- **أداة (Tracer)**: تقوم هذه الأداة برسم مسار بين جهازين تظهر فيه كل التفاصيل عن مسار الرزم والعناوين التي زارها الجاني وتوجه من خلالها والوقت والفترات التي قضاها، وهي تسمح برؤية المسار الذي اتخذه (IP) من مضيف إلى آخر وتستخدم هذه الأداة الخيار (Time to Live)، (TTL) التي تكون ضمن (IP) لكي تستقبل ن كل موجة رسالة وبذلك يكون هو العدد الحقيقي للوثبات.

---

[1]- بروتوكول **TCP/IP** يعتبر من أشهر البروتوكولات المستخدمة في شبكة الأنترنيت والاتصالات، فهي جزء أساسي من الأنترنيت ويتكون هذا البروتوكول مما يلـــــي:

1) بروتوكول : User Datagsam Protocol UDP

2) بروتوكول : Transport Control Protocol TCP

3) بروتوكول : Internet Protocol IP

وتعمل هذه البروتوكولات الثلاثة معا لـنقل المعلومات الخاصة بالمستخدم طبقا لنظام هيكلة تبادل المعلومات المعروف باسم .TCP/IP WITH OSI

[2]- خالد عياد الحلبي، المرجع السابق، ص210-211.أنظر أيضا: حسين سعيد الغافري، المرجع السابق، ص518.

ويتم بذلك تحديد وبشكل دقيق المسار التي تسلكه الرزمة، وهذه الأداة تستخدم في الأساس للمسح الميداني للشبكات المراد التخطيط للهجوم عليها، إذ أنه يبيّن الشبكة وتخطيطها والجدران النارية المستخدمة، ونظام الترشيح ونقاط الضعف، ولكن يمكن أيضا من خلالها معرفة مكان الخلل والمشاكل التي تعرضت لها الشبكة والاختراقات التي وقعت عليها[1].

4- **أداة (Net Stat):** هي أداة لفحص حالة الاتصال الحالي للبروتوكول (TCP/IP) ولها عدد من المهام أهمها عرض جميع الاتصالات الحالية، ومنافذ التنصت، وعرض المنافذ والعناوين بصورة رقمية، وعرض كامل لجدول التوجيه.

الفرع الثاني: الوسائل الاجرائية

يقصد بها تلك الاجراءات التي باستخدامها يتم تنفيذ طرق التحقيق الثابتة والمحددة والمتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبيها ومنـــها:

أولا: اقتفاء الأثـــر

من أخطر ما يخشاه المجرم الإلكتروني تقصي أثره أثناء ارتكابه الجريمة فهناك الكثير من الوثائق التي يتم نشرها في المواقع الخاصة بالمخترقين تحمل بين جنباتها العديد من النصائح، أولاهما نصيحة هي قم بمسح آثارك (Cover Your Tracks)، فلو لم يقم المخترق بمسح آثاره، فمؤكد أنه سيتم القبض عليه حتى و إن كانت عملية الاختراق قد تمت بشكل سليم، ويمكن تقصي الأثر بطرق عدة سواءا عن طريق البريد الالكتروني تم استقباله أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بعملية الاختراق[2].

ثانيا: الاطلاع على عمليات النظام المعلوماتي وأسلوب حمايته

ينبغي على المحقق الاطلاع على نظام المعلوماتي ومكوناته من شبكات وتطبيقات وخدمات تقدم للعملاء، كما ينبغي عليه الاطلاع على عمليات النظام والمستفيدين والملفات والإجراءات وتضيف الموارد العامة، ومدى مزامنة الأجهزة، ومدى توزيع الصلاحيات للمستفيدين، وإجراءات أمن العامين،

---

[1]- علي عدنان الفيل، اجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص76.

[2]- حسين بن سعيد الغافرين، المرجع السابق، ص519.

وأسلوب النسخ الاحتياطي، والاستعانة ببرامج الحماية، كمراقبة المستفيدين والموارد والبرامج التي تعالج البيانات وتسجيل الوقائع وحالات فشل الدخول إلى النظام، بالإضافة إلى معرفة نوعية برامج الحماية وأسلوب عملها والاستفادة من التقارير التي تنتجها نظم أمن البيانات وتقارير جدران الحماية.[1]

و في هذا الصدد يجب على قائد فريق التحقيق التأكد من حرص جميع أعضاء فريق التحقيق على الأمور التالية أثناء تعاملهم مع الأدلة الرقمية على وجه الخصوص:

1) عدم القيام بأي عمل من شأنه إحداث تعديل أو تغيير أي دليل.

2) عدم تنفيذ أية برامج على الحواسيب الموجودة في موقع الجريمة خصوصا البرامج ذات الصلة بأنظمة التشغيل.

3) ضرورة عمل نسخة مطابقة للأقراص الصلبة، ومن تم عمل الفحوصات الجنائية على هذه النسخة فقط، سواءا تم ذلك داخل مسرح الجريمة أو خارجها، وهنا يجب التأكيد أنه لا تكفي نسخة احتياطية من البيانات المراد فحصها، وإنما يجب عمل نسخة مطابقة تماما لكامل القرص الصلب، وهي مستوى البت Blt [2] وهي أصغر وحدة لقياس كم البيانات الرقمية وهذه الطريقة تعرف باسم (Bit Stream Back-up)، بل أنه من الأفضل عمل نسخة احتياطية ثانية من النسخة الاحتياطية الأولى وعلى مستوى البت أيضا، ومن تم إجراء الفحوصات الجنائية على النسخة الثانية، بحيث تظل النسخة الأولـــى دون أن تطالها أية تعديلات[3].

ثالثا: الاستعانة بالذكاء الصّناعي.

أثبتت تقنية الحاسبة الإلكترونية نجاحها في جمع الأدلة الجنائية وتحليلها واستنتاج الحقائق منها، كما يمكن الاستعانة بالذكاء الصنّاعي في حصر الحقائق والاحتمالات والأسباب والفرضيات ومن تم

---

[1]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص77.

[2]– بت (BIT): عبارة عن رقم ثنائي يشير إلى أصغر وحدة من معلومات الكمبيوتر يتم نقلها كنبضة واحدة مضيئة ON أو كمطفأة OFF ويرمز لها بالواحد أو الصفر. أنظر: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي، المرجع نفسه، ص203.

[3]– حسين بن سعيد الغافري، المرجع السابق، ص520.

استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية، وفق برامج صممت خصيصا لهذا الغرض[1].

المبحث الثاني: مفهوم المحقق الجنائي في الجريمة الإلكترونية

لا يوجد بين المهن المختلفة أفضل من مهنة المحقق الجنائي أو أمتع منها فإن السعادة التي يدركها المرء والثقة والرضاء الذي يملأ النفس وهي جادة باحثة ساعية متجهة صوب إحراز العدالة، هي خير ما يعوض المحقق عن كده وجهده وعنائه وخير ما يجعله فخورا دائما بعمله واثقا من نفسه، شديد الإيمان برسالته[2]، تحقيقا لقوله تعالـــى: " وَإِذْ قَالَ رَبُّكَ لِلْمَلَائِكَةِ إِنِّي جَاعِلٌ فِي الْأَرْضِ خَلِيفَةً قَالُوا أَتَجْعَلُ فِيهَا مَن يُفْسِد فِيهَا وَيَسْفِكُ الدِّمَاءَ وَنَحْن نُسَبِّح بِحَمْدِكَ وَنُقَدِّس لَكَ قَالَ إِنِّي أَعْلَمُ مَالَا تَعْلَمُونَ"[3] وتطبيقا لقوله تعالـــى:" إِنَّا عَرَضْنَا الْأَمَانَةَ عَلَى السَّمَاوَاتِ وَالْأَرْضِ وَالْجِبَالِ فَأَبَيْنَ أَن يَحْمِلْنَهَا وَأَشْفَقْنَ مِنْهَا وَحَمَلَهَا الْإِنسَانُ ۖ إِنَّهُ كَانَ ظَلُومًا جَهُولًا"[4].

فالمحقق الجنائي يقوم بأهم وأخطر المهام على الإطـــلاق ألا وهي تحقيق العدالة، لذا فإنه يتعين أن يكون ذات صفات معينة وعزيمة جبارة وجلد عظيم وأن يكون شديد اليقظة والانتباه والحزم ذا قدرة على استخلاص المعلومات والنتائج، وعليه أن يقدر دوما ما ستعترضه من عوائق وظروف تتطلب شجاعته والتضحية في كثير من الأحيان بكل ما هو غالي من نفس ونفيس، كذلك يجب أن يكون ملما بأكثر من لغة مما يساعده على النجاح.

والمحقق في سبيل أدائه لمهامه يجب عليه بذل العناية الواجبة فيما يعرض عليه من تحقيقات وشكاوي والتزام الحيدة والنزاهة فيما يتخذه من إجراءات، والحرص على إنزال حكم القانون صحيحا عليها، ومراعاة ملائمة التعرف للوقائع والأدلة القائمة في الأوراق رعاية لقدسية مهمته وتأكيد السيادة القانون[5]، وعلى هذا لابد أولا من دراسة تعريف وأنواع المحقق الجنائي في الجريمة الإلكترونية (المطلب الأول)، ثم تبيان صفات المحقق الجنائي في الجريمة الإلكترونية (المطلب الثاني)، وعيوب

---

[1]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي، المرجع السابق، ص78.

[2]– عبد الواحد إمـــام مرسي، المرجع السابق، ص23.

[3]– الآية 30 من سورة البقرة.

[4]– الآية 72 من سورة الأحـــزاب.

[5]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص85.

المحقق الجنائي في الجريمة الإلكترونية في (المطلب الثالث) وبعدها نتطرق إلى أهم الصعوبات التي تعترض المحقق الجنائي في التحقيق (المطلب الرابع).

المطلب الأول: تعريف وأنواع المحقق الجنائي في الجرائم الإلكترونية

إن التحقيق كإجراء مرتبط بالقضايا الناشئة عن وقائع إجرامية حرّكت وبوشرت بشأنها دعوى عمومية، لا ينطوي فقط على جانب شكلي إجرائي، وإنما هناك جانب إنساني للعملية يجسده التفاعل بين المحقق والمحقق معه وما يحقق حوله[1]، فالمحقق يقوم بالتحقيق عن طريق جملة من الإجراءات والأساليب تشير إلى كيفية السير في التحقيق من بدايته إلى نهايته.

الفرع الأول: تعريف المحقق الجنائي في الجريمة الإلكترونية.

يعرف المحقق الجنائي في الجرائم الإلكترونية بأنه: " الشخص المكلف بالبحث عن الحقيقة في الجرائم الإلكترونية لكشف مرتكبها، وتجميع أدلة الإدانة أو البراءة ضدهم لإحالتهم للقضاء، فالمحقق هو المكلف بتنفيذ إجراءات القانون المطبق كل حسب اختصاصه، سواءا كان في دائرة اختصاصه المكاني أم على مستوى الدولة"[2].

وفي تعريف آخر هو " كل من عهد إليه القانون بتحري الحقيقة في البلاغات والحوادث الجنائية وتحقيقها وسيهم بدوره في كشف غوامضها وصولا إلى معرفة حقيقة الحادث وكشف مرتكبه لمحاكمته أو بصدد المحاكمة التي تجريها المحكمة"[3].

كما تم تعريفه أيضا بأنّه:" من يتولى التحقيق من رجال الضبط القضائي أو أعضاء النيابة أو رجال القضاء"[4].

وعرف أيضا بأنّه: " ذلك الشخص الذي عهد إليه قانونا باتخاذ كافة الاجراءات القانونية والوسائل المشروعة فيما يصل علمه من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة"[1].

للمحاكمة"[1].

---

[1]– دليلة جلول، المرجع السابق، ص14.

[2]– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص253.

[3]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص86.

[4]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع نفسه، ص87.

وعليه فالمحقق الجنائي بصفة عامة هو الشخص القائم بأعمال التحقيق الجنائي، ولا يختلف تعريف المحقق في الجرائم التقليدية عن تعريفه في الجرائم الإلكترونية فالفرق في نوعية الجريمة وليس في المحقق، ويبقى المحقق دائما شخص قانوني حدده القانون على وجه التحديد، وحدد واجباته ووظائفه، أي أنه يعمل في إطار من القانون وبالقانون ومن خلاله.

ويحدد قانون كل دولة من لهم وظيفة التحقيق وكذا اختصاصهم المكاني والنوعي، ويتولى التحقيق في مصر حسب كل مرحلة: مأمور الضبط القضائي، أعضاء الإدعاء العام، قاضي التحقيق، مستشار التحقيق، مستشار الإحال ، المحكمة بيد أن المحكمة تتولى التحقيق النهائي في الدعوى الجنائية[2].

ويتولى التحقيق في الكويت كـــل من: محققوا الشرطة ،أعضاء الادعاء العام، و ضباط الشرطة[3].

أمّا في الجزائر فإنّ إجراء التحقيق منوط بعدّة أشخاص حسب المسار الذي تعرفه الدعوى العمومية، فنجد رجال الضبطية القضائية وهم يباشرون التحريات تحت إشراف وكيل الجمهورية المختص إقليميا و هذا ما نصّت عليه المادة 12 و14[4] من ق إ ج ج. ويمكن ندب خبراء لهذا الغرض إذ تعلق الأمر بمسألة تقنية أو فنية، كما نجد قاضي التحقيق إذ يحتل مركزا هاما على الصعيدين الإجرائي والقضائي بما له من الصلاحيات والسلطة وبدليل تسميته قاضي التحقيق وهو ما يهمنا بالدرجة الأولى، ولا يعني ذلك إقصاء رجال الضبطية القضائية القائمين بالتحري أو المعهود

---

[1]– عبد الواحد إمام مرسي، المرجع السابق، ص23.

[2]– راجع في هذا الصدد المواد 11-1/24- 25-65-199، 200 ق.إ.ج.م.

[3]– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 253- 254.

[4]– تنص المادة 12 من ق.إ.ج.ج علـــى ما يلي: "يقوم بمهمة الضبط القضائي رجال القضاء والضباط والأعوان والموظفون المبيّنون في هذا الفصل.

و يتولى وكيل الجمهورية إدارة الضبط القضائي ويشرف النائب العام على الضبط القضائي بدائرة اختصاص كل مجلس قضائي، وذلك تحت رقابة الغرفة الاتهام بذلك المجلس.

ويناط بالضبط القضائي مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات و جمع الأدلة عنها والبحث عن مرتكبيها مادام لم يبدأ فيها بتحقيق قضائي."

أما المادّة 14 من ق.إ.ج.ج علـــى فتنص علـــى ما يلي:" يشمل ضبط القضائي:

1)ضباط الشرطة القضائية.

2)أعوان الضبط القضائي.

3) الموظفون والأعوان المنّوط بهم قانونا بعض مهام الضبط القضائي".

إليهم بالتحقيق في مسألة بأمر من قاضي التحقيق أو الخبراء الفنيين من نفسانيين وأطباء و تقنيين أو السادة القضاة الجلوس أو غرفة الاتهام، بل إن هذه الخصائص التي سوف نتحدث عنها لاحقا في شخص قاضي التحقيق ستكون نموذجا يحتذى به لدى من ذكرناهم من القائمين بالتحقيق .

الفرع الثاني: أنواع المحققين في الجرائم الالكترونية

توكل مهمة التحقيق في الجرائم الإلكترونية إلى نوعين من المختصّين:

أولا: الخبرة الفنية

هم النخبة المتخصّصة في مجال الأجهزة الإلكترونية وشبكات الاتصالات من حاسبات آلية وموبيلات ولابتوب وبلاك بيري...إلخ و يتم الاستعانة بهم لاكتشاف وضبط الجرائم الإلكترونية وجمع الأدلة والتحقيق مع المتهمين فيها وتقديمهم للمحاكمة[1].

ثانيا: الكـــــفاءة المــهنية

وهم المختصون في مجال التحقيق الجنائي، حيث أنّ أخذ أقوال الشهود واستجواب المتهمين يعتمد على قواعد مهنية وقدرات لا تتوافر في خبراء الحاسب الآلي، فطريقة توجيه الأسئلة وترتيب أولوياتها واستنتاج الحقائق من الطريقة التي يتحدث بها المتهم وقراءة لغة الجسد لديه، أمور مهنيّة لا يوفيها حقّها إلاّ المحققين الذين لديهم خبرة ومعرفة علمية يطبقونها[2].

لذلك يجب الجمع في التحقيق الجنائي في الجرائم الإلكترونية بين النوعين:الخبرة الفنيّة والكفاءة المهنية للقيامة بإجراءات التحقيق مع الأشخاص من ذوي العلاقة بالجريمة الإلكترونية.

وعلى المحقق الجنائي الإلكتروني القراءة باستمرار في مجال التقنية الالكترونية الرقمية وشبكة الأنترنت و التعليم والتدريب لاكتساب الخبرة التقنية وتحقيق التوازن الفكري الإلكتروني[3]، ويتمكن من

---

[1]– فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2012، ص 626 .

[2]– مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 254.

[3]– يقصد بالتوازن الفكري الإلكتروني الثقافة الالكترونية، والثقافة المعنية هنا مجموعة التصورات الذهنية التي تستقر في أعماق كل انسان ومن بينهم رجل مكافحة الجريمة وتنعكس بالتالي على سلوكهم مع النّاس والأشياء، وبهذا المفهوم يمكن الحديث عن العلاقة بين رجل مكافحة الجريمة والثقافة الأمنية، فالثقافة الأمنية تطور رجل مكافحة الجريمة، كما

التفوق في تحديد أهدافه وتحقيقها، وبالتالي ينخفض القلق لديه من التعامل مع تلك النوعية من الجرائم الإلكترونية، وكذلك على المحقق تحقيق التوازن الاجتماعي الإلكتروني[1]، والتوازن الجسماني الالكتروني[2]، وكذلك التوازن الاقتصادي الإلكتروني المتمثل في توفير مصدر مالي مستمرّ لتوفير نفقات التقنية الإلكترونية الرقمية المستخدمة في التحقيق[3].

المطلب الثاني: صفات المحقق الجنائي في الجرائم الإلكترونية

يتطلب في المحقق الجنائي في الجرائم الإلكترونية تقريبا ذات الصفات الواجب توافرها في أي محقق جنائي، بمعنى ذلك الجانب من أخلاقه وطباعه وتصرفاته التي يتصل بالمهمّة الملقاة على عاتقه، ومن تم يخرج منها كل ما يتعلق بالصفات العادية بوصفه أحد أفراد المجتمع، كما أنّ التطور التقني والتكنولوجي الذي صاحب الجريمة الإلكترونية، جعل التحقيق فيها لا يعتمد على التدريبات الجسدية التي يتلقاها عادة رجال الضبطية القضائية وإنّما يعتمد هذا الأخير على البناء العلمي والتكنولوجي الواجب توافره في المختصين بالتحقيق في هذا النوع من الإجرام المستحدث.

فبقدر ما يتحلى المحقق الجنائي من صفات بقدر ما يوفق في تحقيق هدفه ويخرج من الصراع الذي بينه وبين المجرم منتصرا، حيث أن الأول ينشد الحقيقة والثاني يجتهد في تضليل العدالة وطمس الحقائق، فالتحقيق ليس أسئلة تلقى وإجابات تدوّن، لكن فن ودراسة، خبرة وفراسة، صراع بين الحقيقة

أن رجل مكافحة الجريمة = =يطور الثقافة الأمنية. أنظر: مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، الطبعة الأولى، بدون دار نشر، 2001، ص 28.

[1]– يقصد بالتوازن الاجتماعي الإلكتروني: إقامة العلاقات الاجتماعية المختارة التي تتفق وطبيعة العمل وأهدافه من خلال استخدام الكمبيوتر وتقنية الاتصال(الهاتف المحمول وشبكة الأنترنيت). أنظر: مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، المرجع السابق، ص134.

[2]– يقصد بالتوازن الجسماني الإلكتروني: تناسب الطول مع الوزن مع تلافي أمراض مهنة استخدام الحاسب الإلكتروني الرقمي و ملحقاته ويتحقق بمعرفه أمراض ومتاعب استخدام الحاسب الآلي وأعراضها وكيفية تلافيها، ومن أعراض أمراض استخدام الحاسب الآلي: آلام في اليدين، فقد القدرة على التحكم في اليدين وتنظيم حركتها، خشونة والتهاب في اليدين والمرفق والأصبع والكوع للمحترفين، فقد جزء من الإحساس في اليدين والأصابع مع الشعور بالبرودة في هذه الاجزاء. أنظر: مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، المرجع السابق، ص 118– 119.

[3]– فهد عبد الله العبيد العازمي، المرجع السابق، ص 627.

والخيال، بين الصدق والضلال، وكم ضاعت الحقيقة في الصحف فقضى ببراءة مجرم آثم أو إدانة بريء نتيجة لتحقيق خاطئ أو لقصور فيه[1].

الفرع الأول: أن يكون هدف المحقق الوصول إلى الحقيقة

إنّ الشرط الأساسي في نجاح المحقق في أداء رسالته هو إيمانه بها، أي أن يكون اعتقاده الذي يمتلئ به ضميره هو أنّ الوصول إلى الحقيقة هدف أساسي لا عدول عنه، وهذا ليس بالهين اليسير، ذلك أنّ العدالة من صفات الله سبحانه وتعالى، فإن آمن بها المحقق فإنّه لن يخل بواجباته[2].

وإيمان المحقق برسالته يقتضيه ابتداء أن يجرد نفسه من كل تأثير يقع عليه من جراء الحادث الذي يقوم على تحقيقه، فعليه أن يباشر إجراءاته على أساس انّه خالي الذهن عن أي علم سابق على اول اجراء يبدا به، ثم يسير في طريقه متجها الى سبيل الحق، وبالتالي يجب على المحقق أن يلتمس و يتحسس لا أن يسير بخطى ثابتة أكيدة، فهو أن حدد لنفسه مقدما طريق السير نحو اتهام شخص معيّن بأنه مقترف الجريمة كثيرا ما ينتهي به المطاف إلى اكتشاف براءة هذا الشخص، ذلك لأنّ التوصل إلى الجاني إنمّا يكون في نهاية التحقيق لا قبل ذلك[3].

الفرع الثاني: قوة الملاحظة والسرعة في الإنجاز

تعد قوة الملاحظة مفتاح حل للكثير من الغموض في الحوادث، وقوّة الملاحظة هي المعرفة الدقيقة والسريعة لتفاصيل الأشياء التي تقع تحت إحدى الحواس، والملاحظة شأنها شأن أي صفة للإنسان تنمو بالتمرين المستمر والتعود والممارسة وعلى المحقق المبتدئ أن ينمي هذه الصفة في نفسه، وعليه أن يتبين مايدور حوله من أشياء ووقائع ويعرف تفاصيلها[4]، ولا يدع أمرا يمّر به دون أن يقف عنده بالتأمل و التفكير والتمحيص والتحليل.

---

[1]– عبد الواحد إمام مرسي، المرجع السابق، ص28.

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص95. وأنظر أيضا: دليلة جلول، المرجع السابق، ص18.

[3]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع نفسه، ص96.

[4]– خالد مختار الفار، اسماعيل بابكر محمد، المرجع السابق، ص17.

كذلك يجب أن تتوافر في المحقق السرعة في إنجاز أعماله، فعليه أن ينتقل فورا إلى مكان الجناية إثر إخطاره بوقوعها لأنّ عامل الزمن له أثره في ضياع الأدلّة أو تغيير معالمها أو حتى طمسها، فكلما فات الوقت على وقوع الجريمة إلا وحاول الجاني وأفراد عائلته أو أصدقائه التلفيق والعبث بكل ما يؤدي إلى معرفه الفاعل وسبب إجرامه[1].

فالدقة وسرعة الإنجاز يتطلبان منه تحقيق الواقعة تحقيقا وافيا وشاملا والتصرف فيها بشرط أن لا يؤدي ذلك إلى الإخلال بحقوق الدفاع، ولقد حاول المشرّع التوفيق بين السرعة والفعالية المطلوبتين في الدعوى الجنائية و بين حقوق الأفراد، مراعيا في ذلك مصالح المجتمع والدفاع، لتمكين الجهات المكلفة بالتحقيق بإنجازه في آجال معقولة و بسرعة معتدلة لا تهدر حرّية و حقوق الأشخاص و لا تساعد الجاني على إفلاته من يد العدالة، ويتجلى ذلك خصيصا في المادة 60 من ق إ ج ج[2] فبموجبها يجوز لقاضي التحقيق في حالة الجنحة أو الجناية المتلبس بها أن ينتقل الى مكان وقوع الجريمة و يباشر بنفسه أعمال مأموري الضبط القضائي أو يكلف أحدهم بمواصلتها[3].

الفرع الثالث: حياد المحقق أثناء إجراءات التحقيق

يعني حياد المحقق عدم انحيازه إلى أحد أطراف الدعوى الجنائية أو تحيّزه ضدّه، وإنّما تحري الحق أينما كان سواءا أدّى إلى إقامة دليل قبل المتهم أو إلى نفي اتهام يقع على عاتقه[4].

لذلك يجب على المحقق الجنائي القيام بما يـــلي:

– تحري حقيقة الدعوى، بالبحث عن الأدلة كاملة، ما كان منها ضد المتهم وما كان منها في صالحه.

---

[1]– دليلة جلول، المرجع السابق، ص20 .

[2]– تنص المادة مـــن 60 ق.إ.ج.ج علـــى مـــا يلي: "إذا حضر قاضي التحقيق لمكان الحادث فإنّه يقوم بإتمام أعمال ضباط الشرطة القضائية المنصوص عليها في هذا الفصل وله أن يكلف أحد ضباط الشرطة القضائية في متابعة تلك الإجراءات، ويرسل قاضي التحقيق عند انتهاء الإجراءات جميع أوراق التحقيق إلى وكيل الجمهورية ليتخذ اللازم بشأنها.

وإذا وصل وكيل الجمهورية وقاضي التحقيق إلى مكان الحادث في آن واحد، جاز لوكيل الجمهورية أن يطلب من قاضي التحقيق الحاضر افتتاح محضر تحقيق قانوني."

[3]– دليلة جلول، المرجع السابق، ص20.

[4]– عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2009، ص548.

– لترجيح بين الأدلّة في حيدة تامة و موضوعية مطلقه وتجرّد من أي رأي مسبق.

– التزام النّزاهة في عمله، وعدم اللجوء إلى الغش أو الخديعة او الإكراه لحمل المتهم على الاعتراف تحت ضغط و إكراه.

– البعد عن كافة الوسائل غير المشروعة عند جمع الأدلّة خلال التحقيق[1].

مؤدى ما تقدم ضرورة حياد المحقق بين طرفي الدعوى الجنائية أوبالأحرى بين الاتهام و المتهم، فليس له أن ينحاز إلى طرف ضد طرف آخر[2].

ولذلك يمكن القول أن المحقق الجنائي يجب أن يتحلى بالحياد التام في مباشرة مهامه، وتعتبر هذه الخاصية ضمانة من ضمانات التقاضي أمام المحاكم الجنائية[3].

و ما يمكن استخلاصه ممّا سبق أن المحقق الجنائي هو في واقع الحال قاضي التحقيق يتحرى الحقيقة، وهذا يستلزم منه أن يكون محايدا في جميع أعماله دون تأثر بما تقدمه له أجهزة الضبطية القضائية عن الحدث، وكذلك ما قد يدفع به المتهم عن نفسه، فغالبا ما تكون المظاهر خادعة ومضللة للشخص، فبالتالي عليه أن يطمئن ضميره ويقرّ في وجدانه من واقع ما بين يديه من أدلّة عن المتهم الماثل أمامه هو المرتكب للجريمة من عدمه.

الفرع الرابع: عدم التأثر باتجاهات الرأي العام.

إعجاب المحيطين بشخص المحقق من زملاء وأصدقاء بل ووسائل الإعلام، قد يصيبه بالغرور، لذا ينبغي على المحقق أن يبتعد عن أي مؤثرات من شأنها التأثير على سير العدالة، كما ينبغي على المحقق التجرد من نزعاته الشخصية وألا تكون للعاطفة تأثير قوي على عمله، وأن يكون همّه الوحيد هو سعيه لتحقيق العدالة، وتأثر المحقق قد يجعله قاسيا عنيفا كذلك قد يجعله متعاطفا ودودا في تعاملاته مع المجني عليه أو الجاني[4].

---

[1]– خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، المرجع السابق، ص106.

[2]– خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، المرجع نفسه، نفس الصفحة.

[3]– عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص549.

[4]– خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، المرجع السابق، ص112.

ويعتبر الغرور من الصفات القاتلة التي من شأنها أن تؤخر ولا تقدّم، لذا ينبغي على المحقق لكي يكون ناجحا أن يعلم أنّ ما يحققه من نجاح هو بفضل الله تعالى وتوفيقه أولا، وبفضل تعاون فريق كامل من رؤساء ومرؤوسين وليس لشخصه فقط[1].

الفرع الخامس: العلم التام بأحكام القوانين الجنائية.

يجب على المحقق أن يكون على علم تام بأحكام القانون الجنائي، وبعلم الإجرام وبعلم العقاب، فعلم الإجرام يهدف إلى تقصي أسباب الجريمة ابتغاء مكافحتها سواءا تعلقت تلك الأسباب بطبيعة تكوين الجاني أو نفسيته أو المجتمع الذي يعيش فيه، ومن ثم يدخل فيه علم الطبائع الجنائية ويتناول دراسة الفرد من ناحية تكوينه الجسماني لمعرفة أثر هذا التكوين في قيام اسباب الجريمة ، ويدرس علم النفس الجنائي تلك الأسباب من ناحية نفسية المجرم وعواطفه وانفعالاته، وعلم الاجتماع الجنائي يتناول أسباب الجريمة من حيث تعلقها بالمجتمع الذي يوجد فيه الفرد[2].

أمّا علم العقاب فيبحث في أنواع العقوبات وما يحقق غايتها بأقل قدر ممكن منها، وهو ما يشمل أيضا وسائل الأمن والتدابير الاحترازية التي تتخذ حيال من تثبت خطورتهم على المجتمع، ولا تطبق عليهم العقوبة أو على من يبدوا خطرهم عملا على منع الجريمة قبل وقوعها.

كذلك يجب على المحقق أن يكون على دراية بمبادئ الطب الشرعي الذي يساعد على اكتشاف الحقيقة في بعض الجرائم، ولا يشترط فيه أن يلم بكافة أحكام هذه العلوم وإنمّا يكون على دراية بمبادئها الأساسية حتى يستعين بها عند ندب الخبراء لاستظهار الحقيقة، أي أن يكون منهجيا[3].

إضافة إلى بعض الصفات الواجب توفرها فيه كالاستقامة في حياته الشخصية، العمل بروح الفريق، البعد عن الصغائر والشبهات، أن يكون قدوة لمرؤوسيه، و يتصف بجمال الخلق، واحترام الذات ، وقوة الشخصية وحسن المظهر وسمو الشعور والإدراك، وأن يكون صبورا هادئا يتحلى بالشجاعة والاعتماد

---

[1]– عبد الواحد إمام مرسي، المرجع السابق، ص38.

[2]– خالد ممدوح إبراهيم، فن التحقيق في الجرائم الإلكترونية، المرجع السابق، ص117. وأنظر أيضا: خالد مختار الفار، إسماعيل بابكر محمد، المرجع السابق، ص25.

[3]– دليلة جلول، المرجع السابق، ص20.

على النفس وحسن المعاملة حتى يكتسب ثقة الخصوم ويرسخ اعتقاد النّاس في سلامة إجراءات التحقيق.

كل الصفات التي سبقت الاشارة إليها لازمة في كل محقق جنائي، غير أنّ هناك بعض المهارات الإضافية في المحقق في الجرائم الإلكترونية، كون أنّ هذه الأخيرة النابعة من التطور الإلكتروني أضافت أعباء جديدة على أجهزة التحقيق لما يتطلبه التصدي لهذه الجرائم من قدرات فنيّة لم يألفها رجال الضبطية القضائية ولم يتعودوا عليها، ما يستلزم ضرورة توفير الإمكانيات والمهارات المطلوبة في هذا المجال.

ولكي يتمكن المحقق من التعامل مع هذه الجرائم لابد له من التعرف على علوم أخرى كعلم الكمبيوتر والأدلّة الرقمية أي الاستخدام الأمثل للحاسب الآلي ونظمه وبرامجه، ووسائل الاتصال الإلكترونية الرقمية.

وإذا كانت مهارات التعامل مع مسرح الجريمة، والتحفظ على الأدلة ومناقشة الشهود وغيرها تعتبر من أساسيات التحقيق التي لا يتوقع أحد عدم توافرها لدى المحقق، إلا أنه يلزمه عند مباشرته التحقيق في الجريمة الإلكترونية معرفة العديد من الجوانب الفنية ليقوم بعمله على أحسن وجه وندكر منها:

أولا: التعرف على المكونات المادية للحاسوب وآلية عمل الشبكات

يجب التعرف على المكونات الحاسوب لأن التحقيق وجمع الأدلة في الاجرام الإلكترونية يتطلب مهارات فنية وتقنية من أجل التعامل مع كافة الجوانب والمكونات المادية والمعنوية للحاسوب، ومعرفة كيفية التعامل مع مكونات هذه الأجهزة ومعطياتها وطريقة عملها و كيفية تخزين هذه المعطيات ووسائط تخزينها[1].

وإن معرفة أجهزة الحاسوب المختلفة، وأجهزة الاتصال التي تشكل الشبكة الدولية للمعلومات المرتبطة بالأنترنيت وطرق تخزين البيانات الرقمية يساعد المحقق عند وصوله إلى مسرح الجريمة، ومعاينة هذه الأجهزة من سرعة تحديد كيفية وقوع الجريمة وارتباطها بالأنظمة المعلوماتية (الحاسوب

[1]– خالد عياد الحلبي، المرجع السابق، ص184.

والأنترنيت وسهولة التعرف على مكوناتها، والأقراص الصلبة وما حوزته من بيانات ذات الصلة بارتكاب الجريمة[1].

ولا بد من أن يعلم المحقق بجميع أشكال الحاسوب وملحقاتها ووسائط التخزين بصفتها أدلة محتملة، وهذا ماتهدف إليه الدورات التدريبية لرجال التحقيق، حتى يتم الإلمام بالمعرفة اللازمة لمكونات الحاسوب واكتساب المهارات الفنية اللازمة[2]، والحرص على عدم تعريض وسائط التخزين كالأقراص المرنة أو المدمجة، لأية مؤثرات خارجية كالقوى المغناطيسية أو موجات المكروويف حتى لا تتلف محتوياتها .

وكذلك يتوجب على المحقق معرفة آلية عمل شبكات الحاسوب والأنترنيت لأن الشبكة الدولية للمعلومات تربط ملايين أجهزة الحاسوب ببعضها البعض، مما ساهم بشكل كبير في نشوء أنماط إجرامية لم تكن معروفة، حيث أتاحت هذه الشبكات لمحترفي الإجرام إلى تطوير أساليب الإجرام ، وارتكاب جرائمهم بعيدا عن مسرح الجريمة .

إن الكثير من الجرائم الإلكترونية يتم ارتكابها من خلال شبكة الأنترنت ، ولذا وجب على المحقق أن يلم بمبادئ الاتصال وأنواعه، و كيفيه انتقال البيانات من جهاز لآخر على شكل حزم عن طريق الشبكات.

وتبرز أهمية فهم المحقق لمبادئ عمل الشبكات في كونها ضرورة لتصوير كيفية ارتكاب الفعل الإجرامي في القضاء_السيبراني من اختراق للشبكات والحواسيب، واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس عليها وتحويل مسارها، كما أنها تعطي المحقق تصورا جيدا عن مدى امكانية متابعة مصدر الاعتداء على الشبكة والمعوقات التي تحول دون ذلك[3].

---

[1]– خالد عياد الحلبي، المرجع السابق، ص184.

[2]– حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، متوفر على موقع الالكتروني شبكة القوانين شرق www.eastlaw.com، ص2.

[3]– حسين بن سعيد الغافري, التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكه الحاسوب، المرجع السابق، ص 2.

ثانيا: تمييز أنظمة تشغيل الحاسوب المختلفة ومعرفة صيغ معطيات الحاسوب

يتوجب على المحقق أن يستطيع التمييز بين الأنظمة المختلفة لتشغيل الحاسوب، وأن يلم المحقق بجميع الأنظمة التشغيلية لأجهزة الحاسوب وما تتسم به من خصائص ومميزات لكل نظام على حدة، لأنه ملزم بالتعامل معها، وكذلك أنظمة الملفات التي يعتمدها كل نظام، حتى يتمكن من إجراء التحقيق في جرائم الحاسوب والأنترنيت في كشف الجناة، ومعاينة مسرح الجريمة، وإجراء التفتيش والتمكن من ضبط الأدلة الجرمية [1].

إن التعامل المباشر مع هذه الأنظمة، والقيام بفحصها ورفع الأدلة الجنائية الرقمية الموجودة فيها، يعتبر مهمة الخبير الجنائي في الحاسوب والشبكات الموجودة ضمن فريق التحقيق، إلا أن معرفة المحقق الجنائي الأولية لهذه الأنظمة ضرورية لكي يشارك في متابعة فحص وتفتيش مسرح الجريمة، وأحيانا يجد قائد الفريق نفسه أمام قرار فني صعب يجب أن يتخذه بالتشاور مع خبير الحاسوب، ودون توافر الحد الأدنى من المعرفة التقنية لهذا القائد فإن القرار سيكون للخبير وحده، مثال ذلك وجود حواسيب ضمن مسرح الجريمة وهي في وضع التشغيل، ويكون القرار الواجب اتخاذه هو هل سيتم إيقاف عملها حتى لا يكون بداخلها برامج تعمل على محو أدلة الإدانة أو على استمرارية تنفيذ جريمة ما، أم يتم الابقاء عليها في حالة عمل خشية أن يتسبب بقفلها عن العمل، ضياع بعض الأدلة الموجودة في ذاكرة الحاسوب أو في نظام الملفات على القرص الصلب، وربما يتسبب في تشغيل أداة خفية لتدمير كافة محتويات القرص الصلب، تم إعدادها من قبل المجرم وذلك دون أن ينتبه خبراء الحاسوب لوجودها[2].

و يتعين على المحقق كذلك التعرف على معطيات الحاسوب المختلفة ليصبح قادرا على معرفة صيغ الملفات وما يمكن أن تحتويه من معطيات، ومعرفة لأهم التطبيقات التي يمكنه من خلالها قراءة أو مشاهدة محتوى هذه الملفات يعد أمرا في غاية الأهمية لأن هذه الملفات هي الوعاء الحقيقي لأدلة الإدانة في كثير من القضايا ذات الصلة بالحاسوب والأنترنيت بما تحتويه من معلومات، علما بأنه يتم حفظ البيانات الرقمية داخل الحاسوب على شكل مجموعات أو كتل من البيانات، تمثل وحدة واحدة

[1]– خالد عياد الحلبي، المرجع السابق، ص186.

[2]– خالد عياد الحلبي، المرجع نفسه، ص187.

تسمى الملفات، حيث يتميز كل ملف ببنية محدد من المحتوى، كأن يحتوى الملف على بيانات تمثل صورة أو صوت أو فيديو أو مستند خطي أو غير ذلك[1].

ويلعب الأنترنيت دورا رئيسيا كمصدر للمعلومات، حيث يتيح الاطلاع على كم هائل منها من جميع أنحاء العالم بسرعة وسهولة، وهي بالنسبة للمحقق تمثل أداة جمع تحريات مناسبة، فقد خلقت الأنترنيت مجتمعا افتراضيا شبيها إلى حد ما بالمجتمعات الحقيقية، ويدور في مجتمع الأنترنيت هذا الكثير من الحديث الذي قد يفيد المحقق في توضيح غموض بعض الجرائم[2].

ومن الضروري أن يستخدم رجال التحقيق الحاسوب والأنترنيت، حتى يستطيعوا التصدي لجرائم الحاسوب والأنترنيت والنظم المعلوماتية، بما لديهم من معرفة بالبرمجيات المستخدمة في المواقع الإلكترونية، وتبادل الرسائل البريدية ونقل الملفات وكافة الخدمات التي تتيحها شبكة الأنترنيت، حيث من الممكن استخدامها كأداة تعليمية للإطلاع على جرائم الحاسوب والأنترنيت وطرق التصدي لها[3].

ثالثا: معرفة الأساليب المستخدمة في ارتكاب جرائم الحاسوب وتقنيات الأمن المعلوماتية

إن معرفة رجال التحقيق بالأساليب المستخدمة في ارتكاب جرائم الحاسوب والأنترنيت والإلمام بكيفية استخدامها من الأمور المهمة التي تساعدهم في معرفة الجناة وموقع ارتكاب الجريمة، ومن أي طرفية إلكترونية صدر السلوك الجرمي، وكذلك في مناقشة الشهود واستجواب المتهمين ومحاصرتهم بالأسئلة التي تتعلق بكيفية ارتكاب الجريمة وطرق ارتكابها، والتفاهم مع خبراء الحاسوب عند التوصل إلى الأدلة عن طريق ارتكاب الجريمة وعن الأدوات التي ساعدت في ارتكابها[4].

ولأن جرائم الحاسوب والأنترنيت كثيرة ومتعددة، يستخدم مرتكبوهاأ مستجدة وأدوات تجريمية متطورة لتساعدهم على ارتكاب هذه الجرائم، وهذه الوسائل وتلك الأدوات من التجدد وسرعة التطور بحيث أنه لا يمكن أن يحيط بها أي برامج تدريبية يستهدف رجال التحقيق، ولا حل إلا بالمتابعة المستمرة و

---

[1]– حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص508.

[2]– خالد عياد الحلبي، المرجع السابق، ص 188.

[3]– حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكه الحاسوب، المرجع السابق، ص3.

[4]– حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص509.

الاطلاع على النشرات الأمنية التي تصدرها منظمات رسمية وغير رسمية ذات مصداقية من خلال الأنترنيت.

إن الإلمام بتقنيات الأمن المعلوماتية والحاسوبية من الأمور المهمة التي لابد للمحقق في جرائم الحاسوب والأنترنيت من معرفتها واستيعابها، لأنها تساعده في معرفة مجريات التحقيق، لأن المحقق عندما يباشر التحقيق في جريمة اختراق شبكة الحاسوب التابعة لمؤسسة ما يسأل القائمين على الشبكة عن نوع برامج الحماية المستخدمة وكيفية إعدادها، والكيفية التي تفاعلت بها مع الحدث محل التحقيق[1].

وهناك الكثير من التقنيات التي تستخدم في أمن الحاسوب والشبكات، والتي تكون وثيقة الصلة بالتحقيق، ويكون فهم المحقق لوظائفها وأسلوب عملها وطرق استخدامها عاملا مساعدا له عند قراءته للتقارير الجنائية التي يعدها خبير الحاسوب، والتي تعتبر من أهم الوثائق التي يرجع إليها المحقق ويعتمد عليها في تحقيقه، والتي ترفق بمحاضر التحقيق ويرتكز عليها توجيه الاتهام عند اللزوم.

ومن أهم هذه التقنيات الجدار الناري وأنظمة كشف الاختراق وأنظمة الخادم الوكيل وأدوات تتبع مصدر الاتصال الشبكي، وأدوات ومراجعة الأدوات الحاسوبية، والتي بالرغم من أن استخدامها يتم من قبل خبير الحاسوب الجنائي، إلا أنه من الضروري أن يمتلك المحقق فهما جيدا لأساسيات عملها، ليكون قادرا على التحقيق في القضية والتواصل مع الخبير فيما يختص بعلاقة هذه التقنيات بها[2].

غير أن المشكلة الأساسية التي تواجه المحققين في الجرائم الإلكترونية هي خلفية المحقق نفسه فمتى تخصصوا في الحاسب الآلي قد تكون لديهم المعرفة التقنية اللازمة ولكنهم ليسوا مدربين على تفهم دوافع الجريمة وجمع الأدلة لتقديم المتهم للمحاكمة، و في كثير من الحالات نجد أن متخصص الحاسب يعتقد أن لديه الدليل الحاسم حول جريمة إلكترونية ما، ولكن من الناحية القانونية يتبين فيما بعد أن هذا الدليل لا يصلح لإقامة الدعوى، بينما المحققون ذوي الخلفية القانونية قد تكون لديهم خبرة

[1]– خالد عياد الحلبي، المرجع السابق، ص189.

[2]– خالد عياد الحلبي، المرجع نفسه، ص190.

واسعة في التحقيق ولكنهم يفتقدون المعرفة الكافية بتقنيات الحاسب الآلي التي يستخدمها المجرمون في هذا النوع من الجرائم[1].

المطلب الثالث: عيوب المحقق الجنائي في الجرائم الإلكترونية

للمحقق الجنائي عيوب يمكن أن تشوب عمله أثناء التحقيق في الجرائم الإلكترونية، فقد تكون هناك عيوب متعلقة بأسلوب تحقيق المحقق (الفرع الأول)، وقد تكون عيوب ترجع إلى شخص المحقق (الفرع الثاني)، أو عيوب ترجع إلى رؤساء المحقق (الفرع الرابع).

الفرع الأول: عيوب متعلقة بأسلوب تحقيق المحقق

قد تشوب أعمال المحقق أثناء التحقيق في الجريمة المعلوماتية بعض المثالث والعيوب التي من شأنها أن تسيء إلى مهمة إظهار الحقيقة.

أولا: عدم الانتقال الفوري لمعينة مسرح الجريمة الإلكترونية

قد لا ينتقل المحقق فور تلقي الأخطار بوقوع الجريمة الالكترونية، إما لكثرة شواغل المحقق بسبب عدم وجود العدد الكافي من المحققين ، وإما لعدم توافر أسباب السرعة في المواصلات، فتتطرق يد العبث إلى الآثار التي خلفتها الجريمة الإلكترونية، أثناء فترة تأخر المحقق عن الوصول إلى مسرح الجريمة فور وقوعها[2].

فقد يقوم شخص ما بإلغاء أو تعريف رسائل البريد الإلكتروني الموجودة على جهاز الكمبيوتر الخاص بالمتهم والمتعلقة بموضوع الجريمة، أو يقوم بتغيير الرقم السري الخاص بالكمبيوتر لمنع تشغيله[3]، أو بمسح برنامج خاص بالتجسس أو الاختراق ويكون قد استخدم في ارتكاب الجريمة، مما يؤدي إلى صعوبة اكتشاف الجريمة[1].

---

[1]– نعيم سعيداني، المرجع السابق، ص115.

[2]– خاد مختار الفار، إسماعيل بابكر محمد، المرجع السابق، ص29.

[3]– في هذا الصدد يمكن القول بأنها ظهرت هناك العديد من البرمجيات التي تساعد على كسر كلمات السر سواءا تعلق الأمر بملفات محمية، أو كشف كلمة سر حافظ الشاشة أو حتى كشف كلمة سر مدير الشبكة وهذا الأمر يفيد في التحقيق والبحث عن الأدلة حيث ظهرت ثلاث شركات متخصصة في إنتاج هذه البرمجيات هي Access Data Corporation و Professional Help Crack Software، فهي تقدم سلسلة من البرامج تحمل الإسم Pass Out لكشف

ثانيا: إغفال الدقة في فحص وحصر الأدلة التي خلفها المجرم المعلوماتي.

من عيوب التحقيق كذلك إغفال المحقق الدقة الواجبة في فحص وحصر ووصف الأدلة التي خلفها المتهم في مسرح الجريمة، أو إغفال ملاحظة ما وعدم تسجيلها اعتقادا منه أنها غير ذات قيمة، ولكنها في الواقع قد تكون ذات ثقل في استظهار الحقيقة مثال ذلك عدم ذكر اسم الدومين الخاص بالبريد الإلكتروني بالمتهم والذي قد يكون مرتبط بجهة عمله أو جهة المجني عليه، أو عدم إثبات جهاز الكمبيوتر المتهم المستخدم في ارتكاب الجريمة مزود ببرنامج Software خاص باختراق بعض النظم المعلوماتية[2].

ثالثا: الاكتفاء باعتراف المتهم دون إثبات باقي أدلة الجريمة الإلكترونية.

قد يرى المحقق الاكتفاء باعتراف المتهم المعلوماتي بارتكاب الواقعة، وغض النظر عن تسجيل وإثبات كافة الآثار المادية أو الأدلة الإلكترونية التي خلّفها المتهم على مسرح الجريمة، مثل عدم وجود جهاز طابعة[3] ، أو وجود ماسح ضوئي[4]، أو وجود أسطوانات مدمجة، أو عدم إثبات اتصال جهاز الكمبيوتر بشبكة الأنترنيت أو وجود جهاز للاتصال بشبكة الأنترنت عن بعد، في حين أن كل هذه

كلمات سر ملفات بعض التطبيقات وقواعد البيانات العاملة في بيئتي ويندوز وماكنتوش، وهناك أيضا شركة Sand Boy Software التي تعمل على إنتاج برامج خدمية = =لبيئته ويندوز 95 لكنها قدمت برنامجا مجنيا متواضعا يكشف الكلمات المخزنة في ذاكرة كاش ويندوز 95 على القرص الصلب. أنظر: ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص73-74.

[1]- خالد مختار الفار، إسماعيل بابكر محمد، المرجع السابق، ص29.

[2]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص129.

[3]- الطابعة هي أداة نحصل منها على نسخ ورقية مطبوعة للمعلومات المخرجة من الحاسب بوساطة الطابعات ومن أشهرها وأكثرها شيوعا طابعات الليزر (تنتج المخرجات بدمج الجزيئات الصغيرة جدا من الحبر بالورق، ويستخدم ليزر صغير جدا في هذه العملية وهذا هو أصل التسمية)، والطابعات النافثة للحبر(تنتج مخرجات برش القطرات الصغيرة جدا من الحبر على الورق ويمكن استخدامها لإنتاج الصور الملونة بدقة تتجاوز 2000 نقطة لكل بوصة أفقيا، وهي مثالية لطباعة الصور الملونة).

[4]- الماسح الضوئي يستخدم في إنشاء ملف صورة، من وثيقة مطبوعة أو صورة، وبعد ذلك ندخلها إلى الحاسب الآلي الرقمي، ويمكن استخدام تلك الصور مباشرة في الوثائق الأخرى أو تعالج في معالج الصور، ويمكن أن تحول صورة النص الناتجة عن المسح الضوئي إلى ملف المستند باستخدام التعرف الضوئي على الحروف (OCR). أنظر: مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص39.

الأجهزة لازمة لتأكيد صّحة الاعتراف أو لإظهار كذبه بالإضافة إلى احتمال العدول عن الاعتراف أمام المحكمة.

رابعا: إخلاء سبيل المجرم المعلوماتي قبل استكمال إجراءات التحقيق

قد يقوم المحقق وقبل انتهاء إجراءات التحقيق بإخلاء سبيل المتهم، سوآءا بضمان مالي أو بضمان محل إقامته، وهذا قد يؤثر على حسن سير التحقيق، إذ قد يجري المتهم اتصالاته بشهود الإثبات ليؤثر على شهادتهم، أو يحاول إعداد شهود مجاملين لينفوا عنه ما ارتكبه من أفعال، وإذا كان المتهم أجنبي أو يحمل جنسية دولة أخرى فإن احتمال هروبه خارج البلاد وارد[1].

خامسا: عدم إعطاء الجريمة الإلكترونية التكييف القانوني الصحيح

في بعض الحالات قد لا يستطيع المحقق أن يضع التكييف القانوني الصحيح للجريمة الإلكترونية و ربما يكون ذلك بسبب حداثة هذا النوع من القضايا، أو بسبب أنّ هذا الأخير حديث العهد غير ذي خبرة و لا يستعين برأي من هم أقدم منه في العمل، فعلى سبيل المثال في قضايا بطاقات الائتمان الصادرة من البنوك قد يدق الأمر بين وصف الواقعة انتحال صفة استخدام بطاقة الائتمان وبين اعتبارها واقعة احتيال على البنك مصدر البطاقة الائتمانية.

أما في مجال العمل الشرطي فإنه قد يلجأ بعض رؤساء المحقق لمحاسبته عن عدد الجرائم التي وقعت، وتوجيه اللوم الشديد له، أو التحقيق معه بسبب زيارة نسبة هذه الجرائم، الأمر الذي يجعل بعض المحققين يعمد إلى التقليل من هذه الجرائم بعدم قيدها مطلقا، أو التخفيف من وصفها القانوني وهو ما يعرف في الحياة العملية (التجنيح) أي يجعل الجناية جنحة، وهذه الظاهرة على قدر من الخطورة لأنّ من شأنها أن تؤدي إلى مساعدة المجرم على الإفلات من العقاب والخاسر من تلك العملية المواطنين والمجتمع.

لذلك فإنّ قيادات جهاز الشرطة على اختلاف درجاتها تشدّد على تلك الظاهرة وبالتالي توقع أقصى العقوبات والجزاءات على المحققين الذين يرتكبونها، حيث أنه يجب على المحقق أن يعلم أنّ الزيادة

[1]– خالد ممدوح ابراهيم،فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص130. وأنظر أيضا: خالد مختار الفار، إسماعيل بابكر محمد، المرجع السابق، ص30.

السكانية والمناطق العمرانية العشوائية والحالة الاقتصادية كل تلك العوامل وغيرها من شأنها زيارة الحوادث، وأنّه لابد أن يعمل على مواجهة هذه الزيادة بالأساليب والإجراءات المناسبة لا بالتهاون منها بالتقليل من أهميتها.

وبالتالي يجب على المحقق الحرص على إنزال حكم القانون صحيحا عليها، ومراعاة ملائمة التصرف للوقائع والأدلّة القائمة في الأوراق رعاية لقدسية مهمته وتأكيد سيادة القانون[1].

الفرع الثاني: عيوب ترجع إلى شخص المحقق

هذه العيوب ترجع إلى المحقق نفسه، ويمكن أن يتفاداها بالابتعاد عنها وعدم القيام أو الإتيان بها من بين هذه العيوب :

أولا: الإرهاق في العمل

لما كان في عمل المحقق الجنائي متعة خاصّة ورغبة أكيدة في سرعة كشف غموض الحادث وجلاء وكشف طلاسمه وضبط فاعله قد تدفع المحقق الى العمل المتواصل الأمر الذي يصيبه بإرهاق بدني وذهني، مما يؤثر على تفكيره وسيره في إجراءات التحقيق، لذا فإنه ينبغي على المحقق متى استشعر ذلك أن يتوقف لينال قسطا من الراحة بالقدر الذي يجعله يستعيد نشاطه ولا يؤثر على التحقيق، وعليه أن يختار الوقت المناسب[2]، ويتذكر قول الرسول صلى الله عليه وسلم:"ولبدنك عليك حق."

ثانيا: التأثر بالمركز الاجتماعي لأحد الخصوم

قد يتأثر عمل المحقق بالمركز الاجتماعي المرموق لأحد أطراف الخصومة الأمر الذي قد يؤدي الى تراخ المحقق في أداء عمله أو الانحياز لذلك الطرف دون سواه، لذلك يجب عليه أن يكون عادلا في معاملة الخصوم عند مباشرة التحقيق بأن لا يفرق بينهم في المعاملة مهما تفاوتت مراكزهم الاجتماعية

[1]– خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص131–132.

[2]– عبد الواحد امام مرسي، المرجع السابق، ص 39.

أو مظاهرهم الشخصية، كما يجب عليه أن يستمع لتوجيهات رؤسائه في ذلك المجال وأن يؤدي واجبه كاملا وفقا لما يمليه عليه ضميره والقانون[1].

ثالثا: تأثر المحقق بمشاكله و أموره الخاصة

من العيوب الخطيرة التي من شأنها إعاقة المحقق عن أداء عمله بسهولة ويسر وضياع تركيزه وصفاء ذهنه، تأثر المحقق بمشاكله الشخصية والأسرية، لذا ينبغي عليه أن يحاول الاعتياد على نسيان مشاكله بمجرد التواجد في عمله، وإذا لم يتيسر له ذلك لضخامة المشكلة أو نوعها و ارتباطها به فعليه أن يعرض ذلك على رؤسائه بأمانة مطلقة، ويترك الواقعة محل البحث والفحص لزميل آخر لكي يكمل مسيرته، فإنّ ذلك أفضل له وللعمل[2].

رابعا: التشبث بوجهة نظره

من العيوب الذاتية و الشائعة في الحياة العملية، تشبث وتمسك المحقق برأي محدد واتجاه في السير نحو تحديد الفاعل، ظنا منه أنّه السبيل الوحيد لتحقيق هذا الهدف، ويسلك في سبيل ذلك كل الطرق المؤدية و المؤيدة لوجهة نظره، وقد يكون لهذه العقيدة والرأي أسبابه، إلاّ أنّه عند الوصول إلى النتيجة النهائية لهذا الرأي يتبيّن عدم صحّته، يكون قد ضاع من المحقق الجهد الكثير و الوقت الثمين، وأعطى المتهم فرصة لتدبير أمره وهروبه، وقد يصاب المحقق بإحباط شديد، لذا يجب على المحقق أن يضع أمامه كافة الاحتمالات، ويسير فيها بخطوط متوازنة ومتوازية حتى تنتهي هذه الاحتمالات الى الخط الصحيح والذي يؤدي الى ضبط الفاعل[3].

ويلجأ بعض المجرمين إلى وضع شرك للمحقق لتضليله، وذلك بالعمل على إتيان بعض التصرفات التي توهم المحقق بأشياء أخرى غير السبب أو الدافع الرئيسي للواقعة، مثال ذلك أن يقوم الجاني بالقتل بقصد السرقة ثم يعمل على نزع ملابس المجني عليه للإيهام بأنّ الغرض من الواقعة كان بقصد الانتقام للشرف أو وجود عملية جنسية على خلاف الحقيقة، ولتلافي ذلك الخطأ يجرى العمل في

---

[1]– عبد الواحد إمام مرسي، المرجع السابق، ص 39. وأنظر أيضا: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 553.

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 133 – 134.

[3]– عبد الواحد إمام مرسي، المرجع السابق، ص 40.

الحياة العملية في القضايا الهامّة بتشكيل فريق بحث من مجموعة الضباط الأكفاء تجمعهم دائما و بصفة مستمرّة قيادة واحدة يتم من خلالها فحص كافة الاحتمالات والتشاور الدائم الأمر الذي يمنع الوقوع في هذا العيب[1].

لذلك يجب على المحقق عند مباشرته للتحقيق أن يلتزم بضبط النفس ولا يستسلم للغضب أو لسيطرة الميول والغرائز، وأن يتحلى بالصبر والمثابرة في الكشف عمّا يعظم من أمور التحقيق، وأن يتأنى في الحكم على قيمة الدليل مقلبا الرأي على مختلف وجوهه متى يتيقن من مطابقته لمقتضى الحال دون التزام بالتأثير الأول الذي يتبادر الى ذهنه عن الحادث.

الفرع الثالث: عيوب ترجع إلى رؤساء المحقق

هناك بعض العيوب التي تلصق بالمحقق الجنائي و إن كانت ناتجة لأسباب غير خاصة به وإنّما تعود لرؤسائه.

أولا: استعجال الانتهاء من التحقيق

قد يعمد بعض رؤساء المحقق إلى استعجال الانتهاء من التحقيق في القضايا المعروضة على المحقق، وهو الأمر الذي يؤدي به إلى التسرع في الإجراءات، ممّا يجعله يقدم المتهم بأدلّة ناقصة وغير صحيحة، كما يعطي فرصة للمتهم في الإدلاء بأيّة أقوال واتخاذ الحيطة من المحقق، ممّا يجعل التحقيق مهيئا لعيب البطلان.

ويحدث ذلك بصفة خاصّة في فترة إعداد الكشوف السنوية أو الشهرية التي يوافي بها تفتيش النيابات، حيث يعمد عضو النيابة إلى السعي جاهدا إلى الانتهاء من التحقيق في القضايا المعروضة عليه، وبصفة خاصّة تلك المقيدة بدفتر حصر القضايا، سواء بإحالتها إلى محكمة الجنايات أو الجنح أو بحفظها، أو بإصدار أمر بألاوجه لإقامة الدعوى الجنائية قبلها، ولا شك أن مثل هذا التصرف يخنق الحقائق مانعا إياها من الظهور ويميت المظلومين كمدا، ويهدر مهمّة المحقق الأساسية التي تتمثل في العمل الدّائب سعيا وراء إظهار الحقيقة[2].

[1]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 135.

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع نفسه، ص 135– 136.

لذلك يجب على المحقق أن يتسم بعدم التباطؤ في جمع الأدلّة وألا يتردّد في مباشرة الإجراء الذي يراه سليما حتى لا تضيع الفائدة من اتخاذه، وأن يتصف بسرعة التصرف دون المساس بالعدالة تحقيقا لاستقرار مراكز الخصوم.

ثانيا: توزيع التحقيق بين أكثر من محقق

قد يلجا بعض رؤساء المحقق إلى إسناد إجراءات التحقيق لعدّة محققين، وذلك نتيجة لبعض الظروف مثل الإجازات والنقل والندب الأمر الذي من شأنه تشتت إجراءات التحقيق بين أكثر من محقق بأن يعاين واحد، ويقوم آخر بسؤال بعض الشهود، ويقوم ثالث بإجراء عملية التفتيش، ممّا يؤدي الى صعوبة الوصول إلى الفاعل.

ولتلافي ذلك العيب في الحياة العملية يكون من الأفضل أن يتولى عملية التحقيق محقق واحد من بداية وقوع الجريمة حتى انتهاء التحقيق فيها بالكامل، إذ تكون صورة الواقعة ومراحل تحقيقها راسخة في ذهنه موحية له تلقائيا بما يلزم أن يتخذه من خطوات جديدة توصلا إلى الحقيقة[1].

وفي إطار الجرائم الإلكترونية يوجد في بعض الدول تخصص في هذا الشأن كما هو الحال في نيابة جرائم الحاسب والاتصالات في الولايات المتحدة الأمريكية، وهي مشكلة من مجموعة من أعضاء النيابة العامة وتلقوا تدريبات مكثفة على نظام المعالجة الآلية للبيانات وتم منحهم صلاحيات كبيرة في مجال الاستعانة بغيرهم من خبراء وزارة العدل خاصة قسم جرائم الحاسوب والعدوان على حقوق الملكية الأدبية والفكرية CTC، يعدون خبراءتكنولوجيا المعلومات في مجال الجريمة ويتضمن عملهم البحث في تطوير المعلومة القانونية بحيث تتفاعل مع التطور في مجال تكنولوجيا المعلومات، وهم مرتبطون بنظان تدريبي مستمر دون توقف عند مرحلة معينة ويتم رصد الأموال بشكل مستمر لبرامج تدريبهم أيضا لكي يكون ممارستهم لعملهم منطلقا من كل جديد يبرز في مجال تكنولوجيا المعلومات.

فالتخصص مفيد في تنفيذ التشريعات المتعلقة بتكنولوجيا المعلومات حيث يتولى المتخصصون القيام بمتابعة برنامج تدريبي يرتبط بتنفيذ مهام التحقيق واستيعاب القضايا المتعلقة بتكنولوجيا المعلومات وكيفية بناء عريضة الاتهام قبل تقديمها للمحكمة لكي يتم هيكلة االاتهام بشكل صحيح، فلا ينجوا مجرم بفعلته.

[1]– عبد الواحد إمام مرسي، المرجع السابق، ص42– 43.

لذلك فإن منطق التخصص في مجال قانون تكنولوجيا المعلومات من قبل سلطات التحقيق والاتهام والسلطة القضائية في القانون المقارن لم يتسع مداه بحيث يمكن أن يتفرع عنه أبعد مما هو مقرر من حيث تخصص هذه الجهات بكافة أعمال تكنولوجيا المعلومات.

ثالثا: تنازع الاختصاص بين جهات التحقيق

هذا العيب ذائع وشائع جدّا من العيوب الخطيرة التي تضر بالمواطنين وتفيد المتهم ولا تقل خطورة عن العيب السابق.

والمقصود به أن كثير من الحوادث تقع في الحدود الفاصلة للحدود الإدارية لأقسام الشرطة، بل أنّه في حالات كثيرة يلجأ بعض المحققين إلى تغيير معالم الجريمة بتغيّر مكان العثور عليها لتغيير الاختصاص، الأمر الذي لا يفيد سوى المتهم بإفلاته من العقاب، والمحقق الكسول الذي لا يرغب في العمل.

ولتلافي ذلك العيب يكون بإخضاع كل مجموعة من أقسام الشرطة المتجاورة لقيادة موحدّة بمسميات مختلفة مثل فرقة أو قطاع، لذا فإنّه ينبغي على المحقق أن ينقل فور الإبلاغ بالواقعة وأن يثبتها على ما هي عليه، ويعمل كأنّها تقع في نطاق اختصاصه ثم يقوم بالتنسيق مع المحقق الذي يختص بها توصلا للفاعل الحقيقي[1].

رابعا: عدم التخصص في نطاق التحقيق في الجرائم الإلكترونية

تجدر الإشارة بداية إلى أن تخصص المحقق لتحقيق الجرائم الإلكترونية لا يؤدي إلى سحب اختصاصه بشأن باقي الجرائم، فسيظل مختصا بالتحقيق في كافة أشكال الجرائم وليس هناك ما يفيّد قيامه بالتحقيق في جرائم ليست من تخصصه، وإنما تقع في إطار تقسيم العمل من اختصاص غيره دون أن يكون ذلك منه سوى تنفيذا لصحيح القانون.

ففي إطار الجرائم الإلكترونية يوجد في بعض الدول تخصص في هذا الشأن كما هو الحال في نيابة جرائم الحاسب والاتصالات في الولايات المتحدة الأمريكية، وهي مشكلة من مجموعة من أعضاء النيابة العامّة وتلقوا تدريبات مكثفة على نظام المعالجة الآلية للبيانات وتم منحهم صلاحيات كبيرة في

[1]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص138.

مجال الاستعانة بغيرهم من خبراء وزارة العدل خاصّة قسم جرائم الحاسوب والعدوان على حقوق الملكية الأدبية والفكرية CTC، يعدون خبراء تكنولوجيا المعلومات في مجال الجريمة، ويتضمن عملهم البحث في تطوير المعلومة القانونية، بحيث تتفاعل مع التطور في مجال المعلوماتي، وهم مرتبطون بنظام تدريبي مستمر دون توقف عند مرحلة معيّنة ويتم رصد الأموال بشكل مستمر لبرامج تدريبهم أيضا لكي يكون ممارستهم لعملهم منطلقا من كل جديد يبرز في مجال تكنولوجيا المعلومات.

فالتخصص مفيد في تنفيذ التشريعات المتعّلقة بتكنولوجيا المعلومات حيث يتولىّ المتخصصون القيام بمتابعة برنامج تدريبي يرتبط بتنفيذ مهام التحقيق واستيعاب القضايا المتعلّقة بتكنولوجيا المعلومات وكيفية بناء عريضة الاتهام قبل تقديمها للمحكمة لكي يتم هيكلة الاتهام بشكل صحيح، فلا ينجوا مجرم بفعلته[1].

لذلك فإنّ منطق التخصص في مجال قانون تكنولوجيا المعلومات من قبل سلطات التحقيق والاتهام والسلطة القضائية في القانون المقارن لم يتّسع مداه بحيث يمكن أن يتفرع عنه أبعد ممّا هو مقرّر من حيث تخصص هذه الجهات بكافة أعمال تكنولوجيا المعلومات.

المطلب الرابع : صعوبات التحقيق في الجرائم الإلكترونية

لا يمكن مناهضة جريمة أو سلوك منحرف إلاّ من خلال مواجهتها بكافة الطرق الممكنة لدى المجتمع ومعالجة ما ينتج عنها من آثار، ومن أهم طرق هذه المواجهة، الطريق القانوني من خلال إقرار عقوبات رادعة على من تسوّل به نفسه إتيان هذه الأفعال، إلاّ أنّ هذه الآلية لن تأتي بثمارها ما لم يتم اكتشاف الجريمة، واستطاعت السلطات القائمة على التحقيق إثباتها في حق مرتكبيها من خلال ما يتوافر لها من أدلّة يقبلها القاضي.

ومن هنا تبرز مهمّة القاضي الجنائي في إطار هذه الجرائم، إذ يجب أن يكون مستعدّا لتقبل وتفهم فحوى الدليل المستمدّ من الحاسوب، ولا نجد أي معوق قانوني يمكن أن يقف عائقا أمام القاضي في هذا الأمر طالما كفل له النظام القانوني للدولة مبدأ الإثبات الحر وحريته في تكوين قناعته الشخصية في المواد الجنائية.

[1]– طارق فوزي الفقي، المرجع السابق، ص75– 76.

وقد أظهر التطبيق العملي مجموعة من المشكلات والصعوبات تشكل تحديا أمام مكافحة هذه النوعية من الجرائم، كون هذه الأخيرة ترتكب في فضاء إلكتروني (بيئة افتراضية)، تختلف عن البيئة الطبيعية التي يسهل فيها تجميع أدلّة الجريمة وتتبع أثارها الأمر الذي يصعب مهمّة القاضي أو المحقق في التماس وجه الحقيقة بشأنها، ويؤدي من ناحية أخرى إلى حتمية البحث عن أدلّة تتناسب مع الطبيعة التقنية لهذه الجرائم.

وفي هذا الصدد سنحاول بيان هذه الصعوبات والمتمثلة في: عوائق التحقيق في الجرائم الالكترونية (الفرع الأول) والحصول على الدليل الإلكتروني (الفرع الثاني).

الفرع الأول: عوائق التحقيق في الجرائم الإلكترونية

يتسم التحقيق في الجرائم الإلكترونية وملاحقة مرتكبيها جنائيا بالعديد من الصعوبات التي يمكن أن تعرقل عملية التحقيق، بل يمكن أن تؤدي بها إلى الخروج بنتائج سلبية تنعكس على نفسية المحقق بفقدانه الثقة في نفسه وفي أدائه، وعلى المجتمع بفقدانه الثقة في أجهزة تنفيذ القانون الغير قادرة على حمايته من هذه الجرائم وملاحقة مرتكبيها، وانعكاسها على المجرم نفسه، حيث يشعر أنّ الجهات الأمنية غير قادرة على اكتشاف أمره وأنّ خبرة القائمين على المكافحة والتحقيق لا تجارى خبرته وعلمه، الأمر الذي يعطيه ثقة كبيرة في ارتكاب المزيد من هذه الجرائم التي قد تكون أكثر فداحة وأشد ضررا على المجتمع المحلي أو المجتمعات الأخرى[1].

ومن أهم العوائق التي تواجه القائمين على مكافحة الجرائم الإلكترونية والتحقيق فيها، عوائق تتعلق بالجريمة، وعوائق تتعلق بالجهات المتضررة، وعوائق تتعلق بجهات التحقيق.

أولا: عوائق تتعلق بالجريمة الإلكترونية

تتمثل عموما المعوقات المتعلقة بالجريمة الإلكترونية فيما يلي:

1- إخفاء الجريمة وغياب الدليل المرئي الممكن بالقراءة فهمه، حيث أنّ الجرائم التي تقع على الحاسبات أو بواسطتها، في أكثر صورها، مستترة خفية، لا يلاحظها المجني عليه غالبا أو يدري حتى بوقوعها، والإمعان في حجب وإخفاء السلوك المكون لها ونتائجها عن طريق التلاعب غير المرئي

[1]- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص521.

في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها، ليس عسيرا في الكثير من أحوالها بحكم توافر المعرفة والخبرة الفنيّة في مجال الحاسبات غالبا لدى مرتكبها.

فاختلاس المال عن طريق التلاعب في منظومات الحاسبات ومحتوياتها غالبا ما يجري في مخرجات الحاسب تغطيته وستره، والتجسس على ملفات البيانات المختزنة أو استنساخها، وكذلك اعتراض وتفريع البيانات التي يجري عبر الشبكات الاتصالية نقلها، تقل إلى حد كبير فرص المجني عليه في التفطن إليه أو إثباته.

ولا يختلف الحال عند اغتصاب جهد الحاسب أو خدماته، واختراق قواعد البيانات وتغيير بعض محتوياتها بدس برامج خاصة ضمن برامجها قد لا يشعر به القائمون على تشغيلها، والتخريب المنطقي للأنظمة يمكن تمويهه ليبدوا كما لو كان خطأ مصدره البرامج أو الأجهزة أو نظام التشغيل أو التصميم الكلي للنظام المعلوماتي.

ونتيجة لهذه الصعوبة، بات لإمكانية إخفاء الجريمة الإلكترونية عن طريق التلاعب في البيانات مصطلحا يستخدم في دراسات علم الاجرام الأمريكية هو الطبيعة غير الأولية لمخرجات الحاسب المطبوعة[1].

أما فيما يخص غياب الدليل المرئي الممكن بالقراءة فهمه ، فإن أكثر ما تتيحه النظم المعلوماتية من أدلة على الجرائم التي تقع عليها أو بواسطتها تتمثل في بيانات غير مرئية، لا تفصح عن شخصية معيّنة عادة، مسجلة إلكترونيا، بكثافة بالغة، وبصورة مرمزة غالبا، على دعائم أو وسائط للتخزين ممغنطة، لا يترك التعديل فيها أي أثر ولا يمكن للإنسان قراءتها، وإن كانت قابلة للقراءة من قبل الآلة نفسها.

وكشف وتجميع أدلة هذا شأنها لإثبات وقوع الجريمة والتعرف على مرتكبها، هو أحد أبرز المشكلات التي يمكن أن تواجه جهات التحري، وتبدأ هذه المشكلة بشكل عام في سائر مجالات التخزين والمعالجة الآلية للبيانات، حيث تنتفي غالبا قدرة ممثلي الجهات المتخصصة ومكاتب التدقيق والمراجعة، كمكاتب المحاسبة وجهات التحقيق على أن يتولوا بطريقة مباشرة، فحص واختبار المشتبه فيها.

[1]– هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994، ص17.

وتزداد حدّتها بوجه خاص في حالات التلاعب في برامج الحاسبات نظرا لتطلب الفحص الكامل للبرنامج واكتشاف التعليمات والروتينيات غير المشروعة المخفية داخله قدرا كبيرا من الوقت والعمل غالبا ما لا يكون له من الوجهة الاقتصادية مبررا[1].

2- افتقاد أكثر الآثار التقليدية حيث قد يتم في بعض العمليات إدخال البيانات مباشرة في نظام الحاسب دون تطلب وجود وثائق مساندة (وثائق خاصة بالإدخال) كما هو الحال في بعض نظم العمليات المباشرة التي تقوم على إبدال الإذن الكتابي لإدخال البيانات (مثل الموافقة على الطلبات) بإجراءات أخرى تعتمد على ضوابط للإذن متضمنة في برنامج الحاسب (مثل المصادقة على الحد الأقصى للائتمان)، وفي العمليات المالية، قد يجري الحاسب بعض العمليات المحاسبية بغير حاجة إلى إدخال، كما هو الحال في احتساب الفائدة على الإبداعات البنكية، وقيدها آليا بأرصدة حسابات العملاء على أساس الشروط المتفق عليها مسبقا والموجودة في برنامج الحاسب وفي نوعي العمليات يكون من السهل ارتكاب بعض أنواع من الجرائم، كاختلاس المال والتزوير[2] بإدخال بيانات غير معتمدة في نظام الحاسب أو تعديل برامجه أو البيانات المخزنة داخله دون أن يتخلّف ما يشير إلى حدوث هذا الإدخال أو التعديل[3].

وعلى المحقق إزاء صعوبة الاهتداء إلى مرتكبي الجرائم الواقعة في سياق مثل هذه العمليات، و عدم ترك التغيرات في البرامج والبيانات آثارا كتلك التي يخلفها التزوير المادي في المحررات التقليدية، أن يسعى لتحديد دائرة الاشخاص القائمين أو المتصلين بعمليات إدخال البيانات ومعالجتها، مع الاستفادة

---

[1]- هشام محمد فريد رستم، المرجع السابق، ص19.

[2]- خصص المشرع الجزائري الفصل السابع لكافة جرائم التزوير من المادة 179 إلى المادة 241 من ق.ع.ج، وتجدر الإشارة إلى أنّه رغم وفرة النصوص القانونية في قانون العقوبات حول جريمة التزوير إلا أن المشرع الجزائري إلى حد الآن لم يجرم عملية التزوير التي تقع على دعائم معنوية كالمستندات الرقمية أو المعلوماتية " Document numérique ou informatiques" مثلا معطيات معلوماتية (Données) مستندات معلوماتية (Documents)، برامج معلوماتية (Programmes)، كما أنّه لم يعرف بصفة عامة جريمة التزوير، إلا أن تعريفها نصت عليه المادة 441-1 من ق.ع.ف و التي تنص على ما يلي: " يشكل مزوّر كل تغيير أو تحريف للحقيقة من طبيعته أن يسبب ضرر والذي يتم بأي طريقة كانت على محرر أو على دعامة أخرى للتعبير عن الفكرة الذي من خلال موضوعه أو أثره قد ينشئ الدليل عن حق أو واقعة لها نتائج قانونية..."، و ما يمكن ملاحظته من هذه المادة أنّها جمعت بين جريمة التزوير التقليدية (على دعامة ماديّة) وجريمة التزوير المعلوماتية (على دعامة معنوية كالمستندات المنطقية أو المعلوماتية).

[3]- هشام محمد فريد رستم، المرجع السابق، ص20.

من الضوابط الرقابية التي تباشر في النظام المعلوماتي على الإدخال والمعالجة، إضافة إلى تتبع الأموال المختلسة إن وجدت باعتبارها ثمرة الجريمة التي ستؤول في نهاية المطاف الى الجناة.

3-إعاقة الوصول إلى الدليل بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها[1] لإعاقة المحاولات الرامية إلى الوصول إليها و الإطلاع عليها أو استنساخها[2].

4- سهولة محو الدليل أو تدميره في زمن قصير جدا، فالجاني يمكنه أن يمحي الأدلة التي تكون قائمة ضدها أو تدميرها في زمن قصير جدا، بحيث لا تتمكن السلطات من كشف الجريمة إذا ما علمت بها، وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده، وبالتالي تنصله من مسؤولية هذا الفعل و إرجاعه إلـــى خطأ في نظام الحاسبة الإلكترونية أو الشبكة أو في الأجهزة[3].

ومن الأمثلة الواقعية التي أحبط فيها مسعى الجاني لتدمير الأدلة على إدانته بطريقه آلية متطورة حالة شهدتها النمسا تتلخص وقائعها في قيام أحد مهربي الأسلحة بإدخال تعديلات علـى الأوامر العادية لنظام تشغيل حاسب صغير، يستخدمه في تخزين عناوين عملائه والمتعاملين معه، بحيث يترتب على إدخال أمـر إلى الحاسب، من خلال لوحة مفاتيحه بالنسخ أو الطبع محو وتدمير البيانات كلها.

---

[1]- نظام التشفير يجعل إقامة الدليل على ارتكاب الجريمة أمرا مستحيلا، والدليل على ذلك ما حدث في قضيه السيدfaurisson، حيث نشرت رسائل عنصريه ومضادة لليهوديةRévisionnisteتحمل اسم ROBERT Faurisson، و تم اكتشافها على أحد المواقع بعنوانAAARGH، والذي تم إيواؤه في أمريكا، إلا أن المحكمة لم تستطيع إقامة الدليل على أن هذا المتهم هو صاحب الرسالة المجرمة، وأضافت المحكمة أن وجود اسم المتهم في نهاية المقال لا يعني أنه قد صدر عنه، على أساس أن هذا الاسم يمكن لأي شخص أن يكتبه إمعانا في التمويه، الأمر الذي يقتضي إلزام متعهد الوصول بتحديد شخصية المشترك و عدم توصيل الأسماء المجهولة بشبكة الأنترنيت. أنظر: جميل عبد القاضي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية، القاهرة، 2002، ص16- 17.

[2]- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 25. وأنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 80.

[3]- علي عدنان الفيل، اجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع نفسه، ص 80.

و مع أن تعديل برمجة نظام تشغيل الحاسب، كان قد أجري خصيصا من قبل الفاعل للحيلولة دون نجاح أجهزة الملاحقة في إجراءاتها المتوقعة للبحث عن الأدلة و ضبطها،إلاّ أنه لم يفلح في تحقيق هذا الهدف نتيجة شعور أو حدس راود المتخصصين في معالجة البيانات بالجهاز المركزي لمكافحة الغش بالنمسا بأنّ شيئا ما في نظام تشغيل حاسب الفاعل قد جرى تغييره، وقيامه بناء على ذلك باستنساخ الأقراص الممغنطة المضبوطة عن طريق أنظمة حاسباتهم[1].

5-الضخامة البالغة لكم البيانات المتعين فحصها أين يشكل الكم الهائل للبيانات التي يجري في الأنظمة المعلوماتية تداولها أحد مصادر الصعوبات التي تعيق تحقيق الجرائم التي تقع عليها أو بواسطتها، حيث طباعة كل ما يوجد الدعامات الممغنطة لمركز حاسب متوسط الأهمية يتطلب مئات الآلاف من الصفحات التي لا تثبت كلها تقريبا شيئا على الاطلاق[2].

وفي مواجهته لهذه الصعوبة، يسلك المحقق غير المدرب أحد سبيلين إما حجز البيانات الإلكترونية بقدر يفوق القدرة البشرية على مراجعتها، أو التغاضي عن هذه البيانات بأمل الحصول على اعتراف بالجريمة من المتهم.

والواقع أنه بالإمكان تقليص حدتها وتيسير مواجهتها بسبيلين آخرين هما:

- السبيل الأول : الإستعانة بالخبرة الفنية لتحديد ما يجب دون سواه، البحث عنه وللاطلاع عليه وضبطه.
- السبيل الثاني : الإستعانة بما تتيحه نظام المعالجة الآلية للبيانات من أساليب للتدقيق والفحص المنظم أو المنهجي ونظم وسائل الاختبار والمراجعة، بالإضافة إلى أساليب الفحص المنصب بوجه خاص على الحالة أو الواقعة.

ثانيا : عوائق تتعلق بالجهات المتضررة

إلى جانب العوائق المتعلقة بالجريمة الإلكترونية، هناك عوائق أخرى تتعلق بالجهات المتضررة وهي:

---

[1]- هشام محمد فريد رستم، المرجع السابق، ص23.

[2]- هشام فريد رستم، المرجع السابق، ص24. أنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص81.

1- عدم إدراك خطورة الجرائم الإلكترونية من قبل المسؤولين بالمؤسسات تعد إحدى معوقات التحقيق[1].

2- إغفال الجانب التوعوي لإرشاد المستخدمين إلى خطورة الجرائم المتعلقة بالأنترنيت، حيث نجد أن هناك بعض المؤسسات أسست نظم معلوماتها على تطبيقات خاصة من التقنية على أساس أنها تقدم لعملائها خدمات أسرع بدون عوائق ويكون ذلك على حساب الأمن[2].

3- تسابق الشركات في تبسيط الإجراءات وتسهيل استخدام البرامج والأجهزة وملحقاتها، وزيادة المنتجات واقتصار تركيزها على تقديم الخدمة وعدم التركيز على الجانب الأمني، على سبيل المثال مستخدمي شبكة الأنترنيت عبر مزودي الخدمة أو بطاقات الأنترنيت المدفوعة ليسوا مطالبين بتحديد هويتهم (عملية ربط رقم المستخدم مع هويته) عند الاشتراك في خدمة الأنترنيت، أي أن مزود الخدمة لا يعرف هوية مستخدم الخدمة[3].

4- إلى جانب اعتبار الإحجام عن الإبلاغ خاصية من خصائص الجريمة الإلكترونية، يعد كذلك معوقا من معوقات التحقيق، والسؤال المطروح في هذا الصدد: لماذا يحجم الضحايا عن الابلاغ؟

يمكن القول في هذا الصدد أن الإحجام عن الإبلاغ يعتبر من أهم وأخطر المشكلات التي تتعلق بعملية الإبلاغ عن الجرائم الإلكترونية حيث يحجم البعض عن إبلاغ السلطات المختصة عن الجرائم التي ارتكبت بحقهم وخاصة المؤسسات والشركات التجارية حتى في الدول المتقدمة من الناحية التقنية والتي ترتفع فيها معدلات هذا النوع من الجرائم، ففي دراسة للمعهد الوطني للعدالة التابع لوزارة العدل الأمريكية شملت 127 من العاملين في مجال التحقيق في جرائم الحاسبة الإلكترونية والأنترنيت التي يتم اكتشافها لا يبلغ عنها للشرطة، كما توصلت دراسة أخرى أجراها معهد أمن الحاسبة الإلكترونية (CSI) بالاشتراك مع مكتب التحقيق الفيدرالي في الولايات المتحدة الأمريكية إلى أن حوالي 70 %

---

[1]- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص 523. وأنظر أيضا: علي عدنان الفيل، اجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق،ص 81.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص67.

[3]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 81 – 82. وأنظر أيضا: خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص76.

من الجرائم التي يتم اكتشافها لا يتم البلاغ عنها[1] ويكون الإحجام عن التبليغ لعدة أسباب تتعلق أساسا بعدم إدراك الأفراد أو مدراء الأنظمة الحاسوبية ومسؤولي الشركات أن مثل هذه الافعال والهجمات يعتبر جرائم يمكن معاقبة مرتكبيها بموجب التشريعات والأنظمة المطبقة ضمن إقليم الدولة أو المطبقة دوليا.

و كذا خوف الجهات التي وقعت عليها الجرائم ،خاصة المؤسسات والشركات المالية من أن يؤثر انتشار الخبر على سمعتها ومصداقيتها وظهورها بمظهر مشين أمام الآخرين، لأن تلك الجرائم ارتكبت ضدها، مما قد يترك انطباعا بإهمالها أو قلة خبرتها أو عدم وعيها الأمني ولم تتخذ الاحتياطات الأمنية اللازمة لحماية معلوماتها، الأمر الذي ينعكس سلبا على أرباحها وقيمة أسهمها[2].

إضافة إلـــى ذلك خوف المؤسسات والشركات التجارية من أن تؤدي أعمال التحقيق إلى احتجاز حاسباتها أو تعطيل شبكاتها فترة طويلة، مما قد يتسبب في زيادة خسائرها المالية جراء التحقيق، عطفا على ما قد تتسبب الجريمة خسارتها أصلا.

وبما أن بعض هذه الجرائم محدودة الأثر، هذا ما يدفع بعدم الإبلاغ عنها، فقد يكون مخترق ما للنظام بإظهار رسالة تفيد قيامه بهذه العملية، أو يقوم مجرم آخر بإرسال فيروس حاسبة إلكترونية إلى جهاز المستفيد ويكون هذا الفيروس محدود الأثر،أو تقوم برامج الحماية من الفيروسات بالقضاء عليه.

وقد يكون الإفصاح عن التعرض لجريمة إلكترونية من شأنه حـرمان شخص من خدمات معينة على الأنترنيت أو قد يحرم من خدمات الأنترنيت عموما حين يتعرض لجريمة إلكترونية ناتجة عن الاختراق أو زيارته لأماكن غير مأمونة أو غير مسموح بزيارتها[3].

أما الصعيد الدولي فإن من أسباب الإحجام عن الإبلاغ هو صعوبة الإبلاغ ذاته بالنسبة لهذا النوع من الجرائم، لعدم وجود جهات دولية تتولى تلقي البلاغات على مستوى العالم، وكذلك عدم وجود

---

[1]– علي عدنان الفيل ، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 82.

[2]– أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، الطبعة الأولى، دار النهضة العربية، القاهرة، 2010، ص171. وأنظر أيضا: سرحان حسن المهيني، المرجع السابق، ص33.

[3]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص78– 79 .

شبكة دولية لتبادل المعلومات الأمنية كما هو الحال بالنسبة للشبكة أنترنيت التي تمثل إتحاد شركات عالمية تعمل بمعزل عما تواجهه شبكة الأنترنيت من مشكلات ثغرات[1].

فالجريمة في صورتها التقليدية تصل إلى علم سلطات الضبط عن طريق الشكوى أو البلاغ التي يجب على ضباط الشرطة القضائية بقولها متى وردت في شأن جريمة ويحرر بها محضرا، والشكوى كالبلاغ، إلا أنها توجه ضد شخص معين، وتقدم من المجني عليه أو المضرور من الجريمة، بينما البلاغ يقدم من غيرهما أو يخلوا من تعيين اسم من تنسب إليه الجريمة، كذلك قد يصل علم الجريمة إلى الضبطية القضائية، متى ضبط الجريمة متلبسا بوقوعها، إذ أن هناك إجراءات وجوبية وجب اتخاذها في حالات التلبس وهي: مشاهدة الجريمة حال ارتكابها، مشاهدة الجريمة عقب ارتكابها ببرهة يسيرة، تتبع الجاني أثر وقوع الجريمة ومشاهدة الجاني بعد وقوع الجريمة في وقت قريب حاملا أشياء أو به آثار يستدل منها على أنه فاعل الجريمة أو شريك فيها.

بينما الجريمة الإلكترونية تصل أخبارها إلى السلطات الضبط بإحدى الطرق التالية:

– تلقي سلطات الضبط أو جهات التحقيق معلومات عن أشخاص معروفين أو غير معروفين يمارسون أنشطة تندرج تحت تعريف الجريمة الإلكترونية، وذلك في مكان معروف وعلى أجهزة محددة، ووفق لغات برمجية معلومة.

– ضبط شخص معين وبحوزته أموال مشبوهة أو بطاقات مزورة أو بطاقات تعريف مشبوهة (حاله التلبس).

– بلاغ إلى سلطات الضبط والتحقيق من أحد المجني عليهم يفيد تلاعب أو ممارسات خاطئة في حقه أو حقوق الآخرين سواء تمثل ذلك في صورة عجز مالي في حسابات عجز مالي في حسابات مؤسسة مالية أو ضياع حقوق أو تغييرات في الودائع، وذلك دون بيان ما إن كانت هذه جريمة إلكترونية من عدمه، لأن عمليه تكييف السلوك الإجرامي هي مسألة أخرى لا دخل للمبلغ بها.

[1]– عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والأنترنيت، دار الفكر الجامعي، الإسكندرية، 2006، ص117.

– توافر معلومات عن نشر فيروسات تخريبية عبر شبكة الأنترنيت، لاسيما وأن تطبيق القانون في مجال مكافحة الفيروسات المعلوماتية، تواجه عده صعوبات وموانع كثيرة هي[1]:

1. عدم معرفة المجني عليه بالمخرج الذي صمم الفيروس الذي هاجمه.
2. عدم رغبة المجني عليه في الإبلاغ عن وجود فيروس بنظامه المعلوماتي، حفاظا على الثقة بينه وبين الذين يستخدمون هذا النظام.
3. عدم دراية المجني عليه بإصابة نظامه بفيروس معلوماتي لفترة غير محدودة من الزمن، وبالتالي يصعب تحديد وقت الإصابة.
4. عدم القدرة على قياس الخسائر التي يحدثها هذا الفيروس.
5. توافر معلومات عن وقوع عمليات اعتراض أو قرصنة للمعلومات، ذلك أنّ الظاهرة الاختراقية للمعلومات تتجاوز حدود الجغرافيا، وقد جعلت شبكة الأنترنيت هذا النوع من الجرائم ساحة للمعارك بين الدول، وصارت الحركة التجارية والتعاملات المصرفية هدفا لهذه الاختراقات الإلكترونية.

ومن أجل تفعيل عملية الإبلاغ عن الجريمة الإلكترونية، ومن تم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، ما يطالب البعض به في الولايات المتحدة الأمريكية وذلك بأن تتضمن القوانين المتعلقة بجرائم الحاسب والمعلومات، نصوصا تلزم موظفي الجهة المجني عليها، بضرورة الإبلاغ عما يصل إلى عملهم من جرائم تتعلق بهذا المجال، وتقرير خبراء على الإخلال بذلك الالتزام[2].

إلاّ أنّه ولدى عرض هذا الاقتراح على(لجنة خبراء مجلس أوروبا) قوبل بالرفض لسبب قانوني مؤداه أنّ المجني عليه وهو الشركة التي ارتكبت في حقّها جريمة إلكترونية سوف تصبح متهمة أو جانية بعد أن كانت مجني عليها ولذلك وردت اقتراحات بديلة قد تكون مقبولة منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصّة لتبادل المعلومات، وكذلك إصدار شهادة

[1]– علي عدنان الفيل، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص71 – 72.

[2]– هشام محمد فريد رستم، المرجع السابق، ص26.

"أمن خاصة" تمنح بعد عمل مراجعة وتدقيق من قبل هيئة خاصّة من المراجعين، ويتعين على هذه الهيئة إبلاغ الشرطة بما يكشفه من جرائم[1].

ثالثا: عوائق تتعلق بجهات التحقيق

و إلى جانب المعوقات السالفة الذكر هناك عوائق تتعلق بجهات التحقيق نذكر منها:

1- معوقات ترجع إلى شخصية المحقق:

تتمثل هذه المعوقات في التهيّب من استخدام الحاسب الإلكتروني والتهيّب من استخدام الأنترنيت، بالإضافة إلى عدم الاهتمام بمتابعة المستجدات في مجال الجرائم الإلكترونية[2].

2- معوقات تتعلق بالنواحي الفنية:

تتمثل هذه المعوقات في نقص المهارة الفنيّة المطلوبة للتحقيق في هذا النوع من الجرائم و نقص المهارة في استخدام الكمبيوتر والأنترنيت، وعدم توافر المعرفة بأساليب ارتكاب جرائم الحاسب الآلي والأنترنيت، وقلّة الخبرة في مجال التحقيق في جرائم الحاسب الآلي والأنترنيت والمعرفة باللّغة الإنجليزية[3].

لاسيما وإنّ للعاملين في مجال الحاسب الآلي مصطلحات علمية خاصّة أصبحت تشكل الطابع المميّز لمحادثاتهم وأساليب التفاهم معهم، وليس هذا فحسب بل اختصر العاملون في هذا المجال تلك المصطلحات والعبارات بالحروف اللاتينية الأولى لتكون لديهم لغة غريبة تعرف بلغة المختصرات وهي لغة متطورة ومتجدّدة.

---

[1]- هشام محمد فريد رستم، المرجع نفسه، ص27. وأنظر أيضا: عبد الفتاح بيومي حجازي، مبادئ الاجراءات الجنائية في جرائم الكمبيوتر والأنترنيت، المرجع السابق، ص116. وأنظر أيضا: علي عدنان الفيل، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص 75- 76.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 69. وأنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 84.

[3]- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص 525.

كل هذا دفع بمعتادي الإجرام المعلوماتي أن يطلقوا على أنفسهم صفة النخبة، وفي ذات الوقت يطلقون على رجال انفاذ القانون صفة الضعفاء أو القاصرين[1].

لأجل ذلك بدأت بعض الأجهزة الأمنية والقضائية في استيعاب المتخصصين في الحاسب الآلي ضمن كوادرها، كما جرى تدريب رجال الشرطة والقانون على استخدام الحاسب الآلي، وعلى الرغم من ذلك فقد تكون تلك الأجهزة غير قادرة على مواكبة التطور السريع في الحاسب الآلي لعدّة أسباب:

أ- إن الميزانيات المالية المرصودة للكادر البشري في الأجهزة الحكومية لا تفي لاستقطاب النخبة المتميزة في مجال الحاسب الآلي والذي تستقطبهم عادة الشركات ومؤسسات القطاع الخاص.

ب-أجهزة الشرطة و النيابة أمامها مجالات متنوعة ينبغي تغطيتها بالدعم والعناية وهي ليست متفرغة لجرائم الحاسب الآلي وحدها.

ت- حداثة تجربة أجهزة الشرطة والنيابة لجرائم الحاسب الآلي وقلّة الجرائم المكتشفة لم تسمح لتلك الأجهزة من اكتساب الخبرة الكافية للعمل في هذا المجال.

ث-إنشاء الحاسب الآلي على نطاق واسع وتنوع أنظمته و برامجه يجعل من الصعب حصر أساليب الجريمة وصورها وأنماطها، وبالتالـــي يتعذر تدريب المحققين على مواجهة حالات محددة.

إزاء ذلك يرى البعض أن توكل مهمة التحقيق في الجرائم الإلكترونية لجهات الخبرة المتخصّصة في هذا المجال، خاصة وقد تكونت شركات عالمية حققت النجاح في كثير من الحالات، بينما هناك من يرى الخطورة في تخلي أجهزة العدالة الجنائية الحكومية عند دورها في هذا النوع من الجرائم، إذ أنها تضع حقوق المجتمع تحت رحمة أفراد أو شركات همها تحقيق الكسب المالي، وهي غير مكلفة قانونا بتحقيق العدالة الناجزة ، كما أن هناك جرائم تتصل بأمن الدولة والمصالح العليا، وتلك من تصميم مسؤوليات الأجهزة الحكومية دون غيرها[2].

---

[1]- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنيت من 1 - 3 ماي هي 2000، المجلد الثالث، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، 2004، ص 1071.

[2]- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص 1072.

فمتطلبات العدالة الجنائية تقتضي تحمل الأجهزة الأمنية الحكومية كامل المسؤولية اتجاه اكتشاف كافة الجرائم ومن بينها الجرائم الإلكترونية[1]، وفي هذا الصدد ألزمت الاتفاقية الأوروبية لجرائم تقنيه المعلومات الدول الأطراف بضرورة تبني الإجراءات التشريعية أو أية إجراءات أخرى ترى أنها ضرورية وفقا لقانونها الداخلي من أجل إنشاء وتأسيس سلطات مختصة في مجال التنقيبات و الإجراءات الجنائية النوعية في مجال الجريمة الإلكترونية[2].

وقد بادرت مختلف الدول في إنشاء وحدات متخصّصة في مجال البحث والتحري عن الجريمة الإلكترونية داخل الأجهزة الحكومية (الضبطية القضائية) ففي فرنسا مثلا قامت بإنشاء عدة وحدات متخصّصة وغير متخصصة ضمن جهازي الشرطة والدرك لمكافحة هذا الإجرام المستحدث بجميع صوره ومن ذلك المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات[3](OCLTIC)، والذي من بين أهم مهامه تقديم المساعدة التقنية لجهات التحقيق وتنسيق الأعمال التحضيرية اللازمة على المستوى الوطني، ويشارك في نشاطات المنظمات الدولية ويحافظ على الروابط العملية بين المصالح المتخصصة في البلدان الأخرى التي تسهر على مكافحة جرائم تقنية المعلومات، بالإضافة إلى قسم الأنترنيت التابع للمصلحة التقنية للبحوث القانونية والوثائقية المعروف اختصارا بـ (STRTD) و القسم الإلكتروني التابع لمعهد البحوث الجزائية التابع للدرك الوطني المعروف اختصارا بـــ (IRCGN) وكذا وحدات أقسام الاستعلامات و التحقيقات القضائية المعروف اختصارا بـــ(BDRIJ) .

أما في الجزائر تم إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام تحت وصاية القيادة العامة للدرك الوطني، وذلك بموجب المرسوم الرئاسي رقم 183/04 والمؤرخ في 2004/06/27، حيث تنص المادة الثانية منه على" أنه يكلف هذا المعهد بإجراء الخبرات والفحوصات العلمية في إطار

---

[1]– محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص1072 – 1073. وأنظر أيضا: حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص 527.

[2]– مشار إلى هذا الموضوع في المؤتمر الدولي بعنوان الشرطة و الأنترنيت المنعقد بجامعة السربون باريس في 14/ 01/ 2005 وكذا المؤتمر الدولي السادس بشأن الجرائم المعلوماتية المنعقد بالقاهرة في الفترة من 13 إلـــى 2005/04/15.

[3]– تم إنشاء المكتب المركزي لمكافحة الإجرام المرتبط بتكنولوجيا المعلومات والاتصالات بموجب مرسوم وزاري مشترك رقم 2000/ 405،الـــمؤرخ في2000/05/15 على مستوى المديرية المركزية للشرطة القضائية بـــوزارة الداخلية.

التحريات الأولية والتحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعّرف على مرتكبي الجنايات والجنح ، وذلك بناءا على طلب من القضاة والمحققين أو السلطات المؤهلة ، كما تم إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته"[1].

ومن أجل إيجاد أسلوب خاص للتحقيق في الجرائم الإلكترونية يجمع بين الخبرة الفنية و الكفاءة المهنية لابد من إتباع الخطوات التالية:

أ- تبادل المعلومات بين المحقق وخبير الحاسب الآلي وذلك قبل البدء في التحقيق وأخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهمين، بحيث يشرح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم، ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنية والنقاط التي ينبغي استجلائها من الأشخاص، وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معينهاليتم الاستفادة منها عند الضرورة.

ب – يتم حصر النقاط المطلوب استجلائها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب تلك النقاط.

ج – يتـــم أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي يتم الاتفاق عليها مسبقا قبل بدء التحقيق.

د – التنسيق بين المحقق والخبير في الحصول على البيانات المخزّنة في الحاسب الآلي و ملحقاته الخاصة بالشاهد أو المتهم الذي تم التحقيق معه، مع مراعاة أن هذا الأخير لا يجـــوز إجباره على تقديم دليل يدينه[2].

ولضمان نجاح التحقيق في الجرائم الإلكترونية هناك بعض القواعد التي ينبغي مراعاتها أهمـــها:

1. تفادي ضياع الوقت في التحقيق حول جرائم لا يمكن اكتشافها أو أن الأدلة اللازمة لاكتشافها واثبات التهمة قد قضي عليها.

[1]- المـــادة 13 مـــن القانون 04/09، السالف الذكر.

[2]- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص 1073- 1074.

2. ضرورة مراعاة وجود نوع من التعامل بين المحققين وخبراء الحاسب الآلي العاملين في المؤسسة المجني عليها.
3. مراعاة القوانين السارية بشأن الحقوق الفردية و سرّية البريد الإلكتروني وغيرها من الحقوق.
4. العناية بإصدار الأوامر القضائية الخاصة بالتفتيش وضبط[1] أجهزة الحاسب الآلي وملحقاتها وبرامجها.
5. مراعاة حفظ الأدلة الجنائية بالطرق المناسبة، كل حالة على حدى وذلك حتى يتم تقديمها للمحكمة وهي على حالتها التي ضبطت عليها.
6. الإستعانة بالتقنيات المتطورة في المجال المعلوماتي في مواجهة الجريمة الإلكترونية، لاسيما أن هذه التقنيات أثبتت جدارتها ونجاحها في جمع الأدلة الجنائية وصناعة البنية الاتهامية وتحليل القرائن واستنتاج الحقائق[2].

الفرع الثاني : الحصول على الدليل الالكتروني

إن من دواعي التحقيق في الجريمة الإلكترونية، الحصول على الدليل الإلكتروني، والذي غالبا ما يكشف بمحض الصدفة، حيث أن الجرائم الإلكترونية يتم ارتكابها في بيئة معالجة البيانات المخزنة في الوثيقة الإلكترونية في صفحات الفضاء الإلكتروني.

فثورة تقنية المعلومات وإن كانت قد أثرت على نوعية الجرائم التي صاحبتها فإنها في المقابل قد أثرت كذلك على الإثبات إذ أصبحت الأدلة التقليدية غير قادرة على إثبات هذا النوع من الجرائم، فهذه الثورة قد أمدّت الجناة بوسائل متطورة تمكنهم من إخفاء أفعالهم غير المشروعة كاستخدام كلمات السّر والتشفير والتلاعب في المعلومات المخزّنة والعبث بها بل ومحوها عن طريق نبضات إلكترونية و رقمية لا ترى في الوقت الذي يرونه مناسبا وفي وقت قياسي قد يكون جزء من الثانية، كل ذلك في

---

[1]– سيتم التطرق إلى التفتيش والضبط في الجريمة الإلكترونية عند الحديث عن الإجراءات التقليدية في تحقيق الجرائم الإلكترونية.

[2]– حسين بن سعيد الـــغافري، السياسة الجنائية في مواجهة جرائم الأنترنيت، المرجع السابق، ص528 – 529. وأنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 85 – 86، وأنظر أيضا: خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 73.

إطار بيئة غير مادية غبر نظام الحاسب الآلي أو شبكة المعلومات الدولية، وهو ما يضعف بكثير من قوة الأدلة التقليدية المعروفة من حيث كفايتها في إقامه بنيان الإدانة في هذه الجرائم التي تتم في العالم الافتراضي كإعتراف الفاعل بارتكابه للجريمة أو الحصول على أداة الجريمة... وغيرها.

وعليه فعملية الإثبات الجزائي للجريمة الإلكترونية ترتكز على الدليل الإلكتروني باعتباره الوسيلة الأفضل لإثبات هذه الجريمة ضف إلى ذلك أنّ الإقرار بصعوبة الدليل الإلكتروني ليست منبثقة من كيفية الحصول عليه فقط، بل تمكن الصعوبة كذلك في مدى اقتناع القاضي الجزائي به وما مدى حجية كذلك في الإثبات .

أولا: تعريف الدليل الإلكتروني وخصائصه

إن التطور المستمر للبيئة التي يرتبط بها الدليل الالكتروني حال دون وضع تعريف موحد لهذا الأخير، خشية حصر نطاقه داخل إطار تجريمي محدد قد يضرُّ به خاصة في ظل التطور المستمر للتقنية الإلكترونية، لكنه لم يمنع الفقه الجنائي من تحديد الخصائص والسّمات التي يتميز بها الدليل الإلكتروني عن غيره من الأدلة التقليدية.

1- تعريف الدليل الإلكتروني:

لم يتفق الفقه الجنائي حول تعريف موّحد للدليل الإلكتروني، وذلك راجع إلى التطور المستمر واللامتناهي الذي يطرأ على البيئة التقنية التي ينشأ فيها، فقد عرفه البعض بأنه: "الدليل الذي يجد له أساسا في العالم الافتراضي ويقود على الجريمة"، فهو ذلك الجزء المؤسسّ على الاستعانة بتقنية المعالجة التقنية للمعلومات، والذي يؤدي إلى اقتناع قاضي الموضوع بثبوت ارتكاب شخص ما لجريمة عبر الأنترنيت، فكلّما كان هناك مزج في موضوع الدليل بالمعالجة الآلية للمعلومات، فإنه يعد هنا دليلا تقنيا[1].

وعرفه البعض الآخر بأنه: " ذلك الدليل المأخوذ من أجهزة الحاسب الآلي، ويكون في شكل ذبذبات رقمية ونبضات مغناطيسية أو كهربائية يمكن تجميعها أو تحليلها باستخدام برامج وتطبيقات وتقنية

[1]- منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2013، ص162.

خاصة، وهي مكون رقمي لتقديم بيانات ومعلومات في أشكال متنوعة كالنصوص المكتوبة أو الصور أو الأشكال والأصوات والرسوم وذلك من أجل الاستناد إليه واعتماده أمام القاضي المختص"[1].

ومن التعريفات التي قدمت كدلك للدليل الإلكتروني أنه: " معلومات يقبلها المنطق والعقل ويصدقها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزّنة في أجهزة النظم المعلوماتية وملحقاتها وشبكات الإتصال ويمكن استخدامها في أية مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بالجريمة"[2].

وهناك من يعرفه على أنه :" كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي، بحيث تمكن الحاسوب من إنجاز مهمة ما"[3].

وعرفه آخرون بأنه: " الدليل الكامن في العالم الافتراضي، وهو العالم الذي خلقه تطور تكنلوجيا المعلومات، وما يرتكب فيه من جرائم محكومة بالقاعدة الموضوعية في قانون عقوبات الأنترنيت"[4].

كما عرّف الدليل الإلكتروني أيضا بأنه " الدليل المشتق من أو بواسطة النظم البرمجية المعلوماتية الحاسوبية وأجهزة ومعدات وأدوات الحاسب الآلي أو شبكات الاتصال من خلال إجراءات قانونية وفنية لتقديمها للقضاء بعد تحليلها علميا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة لتقرير البراءة أو الادانة فيها"[5].

---

[1]– أسامة بن غانم العبيدي، الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية، مجلة جامعة الملك سعود، الحقوق والعلوم السياسية(1)، المجلد الخامس والعشرون، الرياض ، المملكة العربية السعودية، 2013، ص57–58.

[2]– محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الأنترنيت، بحث مقدم في الحلقة العلمية بعنوان " الأنترنيت والإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، دبي، في الفترة الممتدة ما بين 15 إلى 2008/11/19، ص25.

[3]– رشيدة بوبكر، المرجع السابق، ص382–383. وأنظر أيضا: منى فتحي أحمد عبد الكريم، المرجع السابق، ص162.

[4]– أحمد سعد محمد الحسيني، المرجع السابق، ص151.

[5]– طارق فوزي الفقي، المرجع السابق، ص81.

أما التعريف المقترح للدليل الإلكتروني من قبل المنظمة الدولية لأدلة الحاسوب (IOCE)، (International Organisation Of Computer Evidence)، بأنه: " المعلومات المخزنة أو المتنقلة في شكل ثنائي ويمكن أن يعتمد عليها في المحكمة"[1].

استرشادا بما سبق عرضه من تعريفات للدليل الإلكتروني يمكننا تعريفه بأنه: " كل معلومات مخزّنة في نظم المعالجة الآلية وملحقاتها من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالطابعات والفاكس أو متنقلة عبرها بواسطة شبكة الاتصالات، والتي يتم تجميعها وتحليلها باستخدام برامج تطبيقات تكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها".

2- خصائص الدليل الإلكتروني:

إن البيئة الرقمية التي يعيش فيها الدليل الإلكتروني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكون دليلا للإدانة أو البراءة، وقد انعكس هذا العالم الرقمي على طبيعة هذا الدليل، مما جعله يتصف بعدة خصائص ميّزته عن الدليل الجنائي التقليدي وهي كالتالي:

أ- الدليل الإلكتروني دليل علمي:

الدليل الإلكتروني هو دليل يحتاج إلى بيئة التقنية التي يتكوّن فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فإن ما ينطبق على الدليل العلمي ينطبق على الدليل الإلكتروني، الدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القضاء المقارن هي قاعدة أن القانون مسعاه العدالة أو العلم فمسعاه الحقيقة: Science Seeks Truth،Law Seeks Justice ، وإذا كان الدليل العلمي له منطقته الذي يجب ألا يخرج عليه من حيث أنه يجب عدم تعارضه مع

[1]- وهو تقريبا نفس التعريف المتبنى من قبل الفريق العلمي العامل على مستوى الأدلّة الرقمية (SWGDE) (Standard Working Group On Digital Evidence) ، باعتبار هذا الأخير أنشأ من أجل توحيد الجهود التي تقوم بها المنظمة الدولية للأدلة الحاسوب (IOCE) وتطوير مختلف التخصصات والمبادئ التوجيهية من أجل استراد والمحافظة ودراسة الأدلة الإلكترونية بما فيها الصوتية والمصورة.

القاعدة العلمية السليمة، فإن الدليل الإلكتروني له ذات الطبيعة إذ يجب ألا يخرج الدليل العلمي عما توصل إليه العلم الرقمي وإلا فقد معناه[1].

ب- **الدليل الإلكتروني من طبيعة تقنية:**

فهو مستوح من البيئة التي يعيش فيها و هي البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الإلكترونية في العالم الافتراضي، وهذا العالم كامن في أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها، فالأدلة الرقمية ليست مثل الدليل المادي[2]، فلا تنتج التقنية سكينا يتم به اكتشاف القاتل أو اعترافا مكتوبا أو بصمة أصبع...، وإنما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان والمكان[3].

ونتيجة الطبيعة التقنية للدليل الإلكتروني فإنه سوف يتميز عن الدليل المادي المأخوذ عن مسرح الجريمة المعتاد بما يلي:

ب.1 طريقة نسخ الدليل من أجهزة الكمبيوتر تقلل أو تعدم تقريبا مخاطر إتلاف الدليل الأصلي، حيث تتطابق طريقة النسخ مع طريقة الإنشاء.

ب.2 باستخدام التطبيقات والبرامج الصحيحة، يكون من السهولة تحديد ما إذا كان الدليل الإلكتروني، قد تم العبث به أو تعديله وذلك لإمكانية مقارنته بالأصل.

ب.3 نشاط الجاني لمحو الدليل، يسجل كدليل أيضا، حيث أن نسخة من هذا الفعل يتم تسجيلها في الكمبيوتر، و يمكن استخلاصها لاحقا لاستخدامها كدليل إدانة ضده [4].

---

[1]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009، ص179-180.

[2]- هناك الفرق بين الدليل المادي والمتعلق بالجريمة التقليدية والدليل الإلكتروني المرتبط أساسا بالجريمة الإلكترونية، فالدليل المادي هو كل ما يتركه الجاني في مكان الجريمة أو في الأماكن المحيطة أو المجاورة لارتكاب الجريمة والذي يمكن من خلاله الاستدلال على مرتكب الجريمة وربطه بها.

[3]- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الاثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010، ص62.

[4]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص182.

ب.4 إمكانية احتواء الدليل على سعة تخزينية عالية، فديسك أو فلاش صغير يمكنه تخزين آلاف الصفحات والصور الرقمية[1].

ج- الدليل الإلكتروني متنوع و متطور:

يشمل الدليل الرقمي كافة أشكال وأنواع البيانات الرقمية الممكن تداولها رقميان بحيث يكون بينها وبين الجريمة رابطة من نوع ما، وتتصل بالضحية على النحو الذي يحقق هذه الرابطة بينها وبين الجاني[2].

و يترتب على طبيعة الدليل الإلكتروني من حيث التعدد والتنوّع نتيجة هامة وهي صعوبة الوصول إليه، وذلك نتيجة قيام كبرى المواقع العالمية على الأنترنيت بإحاطة البيانات المخزنة على صفحاتها بسياج من الحماية الفنية لمنع التسلل للوصول غير المشروع إليها لتدميرها أو تبديلها أو الإطلاع عليها أو نسخها، هذا من جهة، ومن جهة أخرى يمكن للمجرم زيادة صعوبة عملية ضبط أي دليل يدينه، وذلك من خلال استخدامه كلمات مرور بعد تخريب الموقع مثلا، أو استخدامه تقنيات التشفير.

د- الدليل الإلكتروني صعب التخلص منه:

تعد هذه الخاصية من أهم خصائص الدليل الإلكتروني بل يمكن اعتبارها ميزة يتمتع بها الدليل الرقمي عن غيره من الأدلة التقليدية، حيث يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلّة إذا حملت في ذاتها إقـــرار بارتكاب شخص لجرائم وذلك بتمزيقها وحرقها، كما يمكن التخلص أيضا من بصمات الأصابع بمسحها من موضعها، كما أنه في بعض الدول الغربية يتم التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة[3].

وإذا كان الأمر كذلك بالنسبة للأدلّة التقليدية فإن الحال غير ذلك بالنسبة للأدلة الإلكترونية، ذلك أن موضوع التخلص من الدليل الإلكتروني باستخدام التخلص من الملفات في الحاسب الآلي أو الأنترنيت كخاصية Delete،Remove، Erase، لا تعد من العوائق التي تحيل دون استرجاع

---

[1]- أسامة بن غانم العبيدي، المرجع السابق، ص58.

[2]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص182-183.

[3]- عائشة بن قارة مصطفى، المرجع السابق، ص62-63.

الملفات المذكورة، إذ تتوافر برمجيات من ذات الطبيعة الرقمية يمكن بمقتضاها استرداد كافة الملفات التي تم إلغائها أو إزالتها من الكمبيوتر[1].

ويترتب على هذه الخاصية مسائل هامة في القانون أبرزها مسألة التخلص من الدليل، فإذا أثبت الخبير التقني مثلا أن مرتكب الجريمة استخدم برمجيات للتخلص من الأدلة، فإنه يمكن إدانته بالنصوص القانونية التي تجرم مثل هذه الأفعال، وهنا ينبغي تقوية عناصر النصوص القانونية التي تجرم التخلص من الأدلة بتخصيص منطق فيها يجعل التشديد وجوبا فيها حال وجود علاقة بين التخلص من الأدلّة وبين العالم الرقمي.

ذ- الدليل الإلكتروني ذو طبيعة رقمية ثنائية (1-0):

ليس للدليل الإلكتروني هيئة واحدة، وإنما له خصيصة الالتصاق بمفهوم تكنولوجيا المعلومات من حيث تكوينه، إذ يتكون من تعداد غير محدود لأرقام ثنائية موحدة في الواحد (1) والصفر(0) والتي تتميز بعدم تشابهها فيما بينها على الرغم من وحدة الرقم الثنائي الذي تتكوّن منه، فالكتابة مثلا في العالم الرقمي ليس لها الوجود المادي الذي نعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فأي شيء في العالم الرقمي يتكون من الصفر والواحد، وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، وأما تكوين معطياته فإنّها تختلف من حيث الحجم والموضوع، إذ كمية (1-0) في ملف يمكن أن تختلف عن الحجم في ملفات أخرى[2].

هذه الخصائص السالف ذكرها أكست الدليل الإلكتروني طابع متميّز، وجعلت منه الدليل الأفضل لإثبات الجريمة الإلكترونية، لأنه من طبيعة الوسط الذي ارتكبت فيه.

ثانيا: أشكال وأنواع الدليل الإلكتروني

يقسم الدليل الإلكتروني إلى قسمين الدليل الإلكتروني الأصلي والدليل الإلكتروني المتكرر وسيتم التفصيل فيه على النحو التالي:

---

[1]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص185.

[2]- رشيدة بوكر، المرجع السابق، ص390.

1- **الـــــدليل الإلكتروني الأصلـــــي:** وهو البنود العينية أو الحسية، وكذلك المستمسكات البيانية التي تتعلق بهذه البنود عند الإمساك بها وحجزها.

2- **الـــــدليل الإلكتروني المـــــكرر:** وهو استنساخ رقمي دقيق لجميع المستمسكات البيانية التي يحتويها البند العيني الأصلي، أما المحرر الإلكتروني فهو بيانات يدخلها المزود ويرسلها عن طريق وسيط إلكتروني فيترجمها الوسيط وفق برنامج معين ويمررها إلى المتلقي الذي يمكنه استخراجها بالاستعانة بوسيط إلكتروني آخر ويمكنه قراءتها بذات البرنامج وإظهارها على صورة الإدخال، وأما الصورة المأخوذة عن الدليل الإلكتروني فهي صورة وطبق الأصل للمعلومات الواردة في الوثائق البيانية والمستقلة عن البنود العينية الأصلية.

وفي كلا التقسيمين بمعنى سواءا كان الدليل الإلكتروني أصليا أو مكررا فهو من حيث هيأته له عدة أشكال تتمثل عموما فيما يلي:

1. **الصورة الرقمية:** وهي عبارة عن تجسيد الحقائق المرئية حول الجريمة، وفي العادة تقدم الصورة إمّا في شكل ورقي أو في شكل مرئي باستخدام الشاشة المرئية، والواقع أن الصورة الرقمية تمثل تكنلوجيا بديلة للصورة الفوتوغرافية التقليدية وهي قد تبدوا أكثر تطورا ولكنها ليست بالصورة الأفضل من الصورة التقليدية.
2. **التسجيلات الصوتية:** وهي التسجيلات التي يتم ضبطها وتخزينها بواسطة الآلية الرقمّية، وتشمل المحادثات الصوتية على الأنترنيت والهاتف.
3. **النصوص المكتوبة:** وتشمل النصوص التي يتم كتابتها بواسطة الجهاز الرقمي، ومنها عبر البريد الإلكتروني (EMAIL)، ورسائل الهاتف المحمول النصيّة (SMS)، و البيانات المسجلة بأجهزة الصرف الآلي[1].

[1]- رشيدة كابوية، حجية الدليل الرقمي في الإثبات الجنائي، ملتقى دولي حول أدلة الإثبات الجنائية الحديثة في التشريعات المقارنة، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، يومي 26/25 أبريل 2018، ص7.

ثالثا: أنواع الدليل الإلكتروني

المقصود بالتنوع في الدليل[1] الإلكتروني أنه ليست هناك وسيلة واحدة للحصول عليه، وإنما تتعدد وسائل التوصل إليه، وفي كل الأحوال يضل الدليل المستمد منه إلكترونيا حتى وإن اتخذ هيئة أخرى.

و يرجع التنوع في مصادر الدليل الإلكتروني إلى أن الأنترنيت يتكون من حاسب آلي به معلومات، تلك المعلومات تنتقل بين الأجهزة المختلفة في دول العالم عن طريق شبكة الأنترنيت وإذا تم فحص تلك المعلومات المتنوعة فإنها بالتالي تعطينا أدلة تقنية متنوعة.

1. **أدلة مرتبطة بوظائف الجهاز الرقمي:** وهذا النوع من الأدلة يمكن إجمالها فيما يلـــي:

أ. البيانات التي أنشأت بواسطة الجهاز الرقمي بشكل تلقائي، حيث تعتبر هذه البيانات من مخرجات الجهاز الرقمي التي لم يساهم الإنسان في إنشائها مباشرة مثل: ملفات الدخول التي يتم حفظ جميع التغيرات التي تحصل في قاعدة البيانات (Log Files)، وسجلات الهاتف (Phone Record) وفواتير أجهزة الحاسب الآلي.

ب. البيانات المحفوظة بالإدخال داخل الجهاز الرقمي: وهي البيانات المكتوبة، والتي يساهم الإنسان بإدخالها قبل أن يقوم بحفظها داخل الجهاز الإلكتروني، مثل البريد الإلكتروني (E-Mail)، ورسائل غرفة المحادثة علـــى الأنترنيت (Charring Room)[2].

ت. البيانات التي يتم حفظ جزء منها بالإدخال ويتم إنشاء جزء آخر منها بواسطة الجهاز الإلكتروني، مثل أوراق العمل المالية في برنامج (Excel) والتي تكتسب محتواها بالإدخال قبل أن تتم

---

[1]- هناك فرق بين الدليل وإجراءات الحصول عليه، فالدليل: يشمل كل واقعة مادية أو معنوية، تؤدي إلى إثبات وقوع الجريمة، أو تحديد شخصية مرتكبها، أو إثبات ارتكابه لها سواء تم ذلك مباشرة، أو عن طريق غير مباشر، وهو الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة، بالاعتماد على الدليل الذي يمثل أثرا منطبعا في نفس أو في شيء، أو متجسّما في شيء ينم عن ارتكاب جريمة وقعت في الماضي، أو تقع في الحاضر، وعلى كل شخص معين تنتمي هذه الجريمة إلى سلوكه.

أما إجراءات الحصول على الدليل فلا تعد أدلّة، وإنما هي المصدر الذي يتم عن طريقة الحصول على الدليل مثل المعاينة والتفتيش والخبرة وما إلى ذلك من إجراءات. أنظر: ناصر بن محمد البقمي، أهمية الأدلة الرقمية في الإثبات الجنائي- دراسة وفق الأنظمة السعودية-، الفكر الشرطي، المجلد 20، العدد4، رقم 79، الشارقة، الامارات العربية المتحدة، 2011، ص28- 29.

[2]- رشيدة كابوية، المرجع السابق، ص6.

معالجتها تلقائيا بأدوات البرنامج ذاته وإعطاء محتوى جديدا من خلال إجراء عمليات حسابية على المدخلات.

ث. الورق ومخرجات الطابعات[1]: غالبا ما تترك الجرائم الواقعة على الأموال أو على الأشخاص آثارا من الأوراق بالغة الأهمية التي يتم حفظها في الحاسب الآلي فالكثير ممّن يقومون بطباعة المعلومات، بهدف المراجعة أو التأكيد من الشكل العام أو صحة المستند موضوع الجريمة، فالطابعات وأجهزة الحاسب الآلي ذات السرعة الفائقة تطبع الكثير من الأوراق في وقت يسير لذلك يعد الورق من الأدلة الرقمية التي يتم من خلالها بحث وتفتيش مسرح الجريمة، وللورق أربعة أنواع وهي[2]:

- المسودة التي يتم إعدادها بخط اليد مثل تصور للعملية يتم برمجتها.
- أوراق تالفة والتي يتم طباعتها للتأكد من برمجة العملية ومن ثم إلقائها في سلة المهملات.
- الأوراق التي تتم طباعتها والإحتفاظ بها لأغراض تفيد الجريمة.
- الأوراق الأساسية والمحفوظة في الملفات العادية أو دفاتر الحسابات وخاصة التي يتم تزويدها من أجل تنفيذ الجريمة.

2. **أدلة لم تعد لتكون وسيلة إثبات:** وهي الأدلة التي تنشأ دون إرادة الشخص، أي أثر يتركه الجاني دون أن يكون راغبا في وجوده، وسمّي هذا النوع من الأدلة بالبصمة الرقمية أو الآثار المعلوماتية الرقمية، وهي تتجسد في الآثار التي يتركها مستخدم النظام المعلوماتي وشبكة الإتصالات، والواقع أن هذا النوع من الأدلّة لم يعد أساسا للحفظ من طرف من صدر عنه، غير أن الوسائل التقنية الخاصّة تمكن من ضبط هذه الأدلّة ولو بعد فترة زمنية من نشوئها، فالاتصالات التي عبر المنظومة

---

[1]– الطابعات: عبارة عن جهاز يقوم بإنتاج نسخ مطبوعة من البيانات، مثل التقارير والشيكات، وقوائم البيانات والبرامج التي يحتاج إليها المستخدمون، وتنوع الطابعات الملحقة بجهاز الكمبيوتر لإنتاج المخرجات الورقية من حيث طريقة= =تشغيلهاوسرعةالتشغيل والتطبيق المستهدف وخصائص المخرجات الورقية إلى: طابعات تصادمية تعمل مثل الآلات الكاتبة بمعنى أن الكتابة تتم بعد اصطدام شكل الحرف مع الورقة والشريط المبلل بالحبر، وطابعات غير تصادمية تستخدم المواد الكيمياوية أو أشعة الليزر أو الحرارة. أنظر: هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة ، 2008، ص16.

[2]– رشيدة كابوية، المرجع السابق، ص6.

المعلوماتية المرتبطة بشبكة الاتصالات وكذا المراسلات الصادر عن الشخص أو التي يتلقاها يمكن ضبطها بواسطة تقنية خاصة بذلك[1].

وتبدوا أهمية التمييز في نوعي الدليل الإلكتروني فيما يلي:

أ. سهولة الحصول على النوع الأول من الأدلة الإلكترونية، لكونها دليلا على الوقائع التي يضمنها، في حين يتم إتباع تقنية خاصة لا تخلوا من الصعوبة للحصول على النوع الثاني من الأدلة الإلكترونية.

ب. النوع الثاني من الأدلة الإلكترونية أهم من النوع الأول، لما يتضمنه في العادة من معلومات ترتبط بين الجريمة الإلكترونية ومرتكبيها.

ج. نسبة ضياع النوع الأول من الأدلة الإلكترونية قليلة لكونه جاهز بطبيعته كوسيلة إثبات لبعض الوقائع والحالات، الأمر الذي يؤدي إلى حفظه لوقت أطول من إمكانية الرجوع إليه في حالات الاحتجاج به، بينما النوع الثاني فيفقد أو يندثر لكونه غير معّد للحفظ أساسا، وهو معرض للضياع لأبسط الأسباب كفصل التيار الكهربائي عن الحاسب الآلي[2].

رابعا: مدى اقتناع القاضي الجنائي بالدليل الإلكتروني

الأصل أنّ القاضي في المواد الجزائية يبني حكمه على أساس اقتناعه الشخصي القائم على حريته في تقدير الأدلة المعروضة عليه في الدعوى[3]، دون أن يخضع في ذلك لرقابة المحكمة العليا.

---

[1]– نعيم سعيداني، المرجع السابق، ص129.

[2]– رشيدة كابوية، المرجع السابق، ص7.

[3]– إذا كان مبدأ الاقتناع الشخصي عام النطاق لدى كافة أنواع المحاكم الجزائية سواءا كانت محاكم الجنايات أم الجنح أم المخالفات، إلا أن قواعد تقدير القاضي للدليل تختلف حسب اختلاف وصف الفعل المجرّم، فإذا كان الفعل الإجرامي يحمل وصف جناية فإن محكمة الجنايات تتمتع بسلطة تقديرية مطلقة في مواجهة الأدلة المعروضة أمامها وتصدر أحكامها وفقا لمحض قناعتها دون أن يكون قضاتها مطالبين بتسبيب أو تعليل أحكامهم، مع العلم أن التعديل الأخير لقانون إ.ج.ج بموجب القانون رقم(6/17) ألزم المشرع الجزائري في المادة 309 قضاة المحاكم الجنائية الابتدائية منها والاستئنافية بتسبيب جميع أحكامهم القاضية بالإدانة أو البراءة أو حتى الإعفاء من المسؤولية.
أمّا إذا أخذ الفعل المجرم وصف جنحة، فإن القاضي في هذه الحالة مطالبا ببيان تقديره للدليل المعروض عليه من خلال تسبيب حكمه، والذي يكون محل رقابة من قبل جهات الطعن، أي أنّ قاضي الموضوع في مواد الجنح مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسيلة من وسائل الإثبات بما فيها وسائل الإثبات الإلكترونية.

غير أنه لا يجب أن يفهم من ذلك أن حرية القاضي في تكوين عقيدته، هي حرية تحكمية، بحيث يمكنه أن يحل محل وسيلة الإثبات تخميناته وآراء الشخصية، أو أن يقضي وفق مزاجه وأهوائه، فذلك يعني التحكم والتعسف، فحرية التقدير شيء والتحكم شيء آخر.

و يعتبر مبدأ الاقتناع الشخصي للقاضي الجزائي من أهم وأرقى المبادئ القانونية التي عرفتها التشريعات الإجرائية الجنائية، وقد عرفه الدكتور إبراهيم الغماز بأنه عبارة عن: " حالة ذهنية ذاتية تستنتج من الوقائع المعروضة على بساط البحث احتمالات ذات درجة ثقة عالية من التأكيد الذي نصل إليه نتيجة استبعاد لأسباب الشك بطريقة قاطعة"[1].

وفي تقدير الدكتور فاضل زيدان محمد أنّ اقتناع القاضي هو : "عملية عقلية منطقية لتحليل الدليل، والتعرف على فحواه ومضمونه، وما يترتب عليه من نتائج، أن يصل القاضي إلى تقدير القيمة الفعلية للدليل المعروض عليه"[2].

وعليه يجوز للقاضي الجزائي الاعتماد على الوسائل المقدّمة إليه بما فيها الدليل الإلكتروني، حيث نص المشرع الجزائري في المادة 212 من قانون.إ .ج.ج[3] علـــى ما يلي: " يجوز إثبات الجرائم بأي طريق من طرق الاثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص".

وهنا يبدو جليّا أن المشرع الجزائري كرس مبدأ الاقتناع الشخصي للقاضي الجزائي، وأفسح له المجال في حرية الاستعانة بأي دليل أو وسيلة للإثبات[4].

---

[1]– إبراهيم إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980، ص627.

[2]– فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان، 2006، ص109.

[3]– يقابلها نص المادة 427 من ق.إ ج.ج.

[4]– بالرغم من أن القاضي حرّا في تكوين عقيدته والاستعانة بما شاء من أدلة، ويطرح ما يراه غير مناسب وفقا لسلطته التقديرية، كما له حريّة في تكييف الواقعة المعروضة عليه تكييفا قانونيا سليما، وأيضا له سلطة تقدير العقوبة أو تدبير الأمن الذي يراه مناسبا إلا أنه مقيد في هذا كله بضوابط وقيود وجدت أساسا حتى يبقى هذا المبدأ في إطاره الصحيح، وهو الوصول إلـــى الحقيقة وتحقيق العدالة، ومن بين القيود الواردة على منح للقاضي الجزائي من حرية في الاقتناع وسلطة في التقدير نجد قاعدة مشروعية الدليل الجنائي وقرينة البراءة الأصلية.

كما نصت المادة 34 من قانون.إ .ج.ج على أنه: " يجوز للجهة القضائية إمّا من تلقاء نفسها أو بناءا على طلب النيابة أو المدعي المدني أو المتهم أن تأمر بإجراءات الانتقال اللاّزمة لإظهار الحقيقة"، وأيضا نصت المادة 286 من نفس القانون على أنه: " ضبط حسن سير الجلسة وفرض الاحترام الكامل لهيئة المحكمة واتخاذ أي إجراء يراه مناسبا لإظهار الحقيقة".

من المادتين يتضح أيضا أن المشرع أطلق للقاضي الحريّة في الاستعانة بكل وسائل الاثبات، كما أن له أيضا أن يتخذ أي إجراء من الاجراءات التي يراها مناسبة لإظهار الحقيقة.

كما كرّس المشرع حرية القاضي الجنائي في الاقتناع في المادة 307 من قانون إ.ج.ج بقولها: " إنّ القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت وتدبر وأن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتهم وأوجه الدفاع عنها، ولم يضع لها القانون سوى هذا السؤال الذي يتضمن كل نطاق واجباتهم: هل لديكم اقتناع شخصي؟".

ومجرد وجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكف للتعويل عليه، إذ يلزم أن تكون لهذه الأدلة قيمة قانونية، وقيمة الدليل الجنائي تتوقف على مشروعية هذا الأخير.

ويقصد بالمشروعية[1]: " التوافق والتقيد بأحكام القانون في إطاره ومضمونه العام، فهي تهدف إلى تقرير ضمانة أساسية وجديّة للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة ومن

[1]– هناك اختلاف واضح بين المشروعية والشرعية حيث تعد المشروعية الوعاء الأكبر الذي يشمل كل أنواع المصطلحات القانونية المتفرغة عنها ومنها الشرعية الجنائية المعبر عنها بقاعدة "لا جريمة ولا عقوبة ولا تدبير أمر بغير قانون" أما الشرعية الإجرائية وهي مشروعية الدليل الجنائي، أي وجوب الحصول عليه بطرق ووسائل مشروعة قانونا، كما أن المشروعية تسند على أسس عامة هي التوافق المستمر بين أفراد المجتمع والقواعد القانونية المقررة منهم في مواجهتهم، حيث لا تقتصر هذه القواعد باعتبارها مصادر المشروعية على النصوص الصادرة من المشرّع وحدها بل أيضا قواعد الدستور وما استقر عليه العمل القضائي من مبادئ مستمدة من الأحكام القضائية، ثم العرف، ومبادئ العدالة والقانون الطبيعي وقواعد النظام العام والآداب، ثم المواثيق والمعاهدات الدولية.
أمّا أساس الشرعية فهو أحد هذه المصادر العامة مستعملا في الاطار العام ومصدرها وهو القانون المستمدة منه كقانون العقوبات بالنسبة للشرعية الجنائية وقانون الإجراءات بالنسبة للشرعية الإجرائية، أي أن الشرعية جزء من كل

التطاول عليها في غير الحالات التي رخصّ فيها القانون بذلك من أجل حماية النظام الاجتماعي وبنفس القدر تحقيق حماية مماثلة للفرد ذاته"[1].

لذلك لابّد لصحة الإجراءات التي تقوم بها جهات التحقيق أن تغلق بمبدأ المشروعية[2]، مما يثمر عن دليل صحيح وسليم يعوّل عليه القضاء في أحكامه، فالعبرة إذن ليست بتوافر الأدلة وحشدها لكن بنزاهة وشرعية تحصيلها.

ولو نتفحص قانون الإجراءات الجزائية الجزائري والتعديلات الواردة عليه، نجد أن ظهور الدليل الإلكتروني لم يغير شيئا في مبدأ الاقتناع الشخصي للقاضي الجزائي، وإنما هو مجرد دليل لا تزيد قيمته ولا حجيته عن غيره ويخضع كذلك لقناعة القاضي الشخصية، وعليه يصح للقاضي أن يعتمده كدليل ويؤسس حكمه عليه وهذا بطبيعة الحال إذا اطمئن إليه، أمّا في حالة ما إذا توغل عليه الشك بشأنه جاز له طرحه وعدم الأخذ به.

عام شامل هو المشروعية، التي تعمل في إطاره. أنظر: إسماعيل طواهري، الاقتناع الشخصي للقاضي في المواد الجنائية، أطروحة دكتوراه، كلية الحقوق، فرع القانون العام، جامعة الجزائر 1، 2014/2013، ص374.

[1]– خاد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص129.

[2]– في هذا الصدد نصت المادة 15 من اتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001، على مجموعة من الشروط والضمانات التي يجب على الدول الأطراف مراعاتها لضمان مشروعية الإجراءات الجزائية المتبعة في التحري والتحقيق عن الجرائم الإلكترونية حيث:

أ– يجب على كل طرف أن يحرص على تأسيس، وتنفيذ، وتطبيق السلطات والإجراءات المنصوص عليها في القسم الحالي والتي تخضع للشروط والاحتياجات المقررة في قانونه الداخلي، والذي يجب أن يضمن حماية كافية لحقوق الانسان وحرياته، وعلى الأخص الحقوق الناشئة عن الالتزامات التي تعهد بها في ظل اتفاقية المجلس الأوروبي عام 1950 لحماية حقوق الانسان وحرياته الأساسية، والاتفاقية الدولية للحقوق المدنية والسياسية للأمم المتحدة لعام 1966، والاتفاقية العالمية الأخرى المطبقة والخاصة بحقوق الانسان، والتي يجب أن تتكامل مع مبدأ التناسب.

ب– وهذه الشروط والاحتياطات يجب أن تشمل على نحو يتناسب مع طبيعة السلطة والاجراء المعني بشأنه، على إشراف قضائي، أو أيّة أشكال أخرى للإشراف المستقل، البواعث المبررة للتطبيق، تحديد نظام التطبيق، والمدة الزمنية للسلطة أو الاجراء.

ج– وفي النطاق الذي يتسق فيه ذلك مع المصلحة العامة، وبالأخص حسن تطبيق العدالة، يجب على كل طرف أن يفحص أثر السلطات أو الإجراءات الواردة في هذا القسم على الحقوق والمسؤوليات والمصالح القانونية للطرف الثالث. أنظر: هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003، ص176–177.

ومن الشروط الواجب توافـــرها في الدليل حتى يعتمده القاضي في إصدار حكمه القضائي ما يلي:

1- أن الدليل الإلكتروني ذي علاقة بموضوع الجريمة الإلكترونية:

وهذا الشرط يشار إليه في قانون الإثبات الفيدرالي الأمريكي بمبدأ العلاقة الكاشفة The Principal Relevance، حيث يتطلب القانون الأمريكي ضرورة أن يكون هناك علاقة من نوع ما بين الدليل وبين الواقعة محل لدعوى.

وشرط ثبوت العلاقة الكاشفة في الدليل الإلكتروني المستخرج من الكمبيوتر للأصل الموجود بداخله، بحيث لا يكون هناك ثمّة إدعاء أو دفع بأنّ البيانات غير صحيحة بسبب عدم دقة عمل الكمبيوتر، وهو ما اشترطه القانون الانجليزي بشأن الشرطة وإثبات الأدلة الجنائية لسنة 1984[1].

2- يتعيّن مناقشة الأدلة الإلكترونية تطبيقا لمبدأ شفوية المرافعة:

إذا كانت مخرجات الوسائل الإلكترونية تعد أدلة إثبات قائمة في أوراق الدعوى التي ينظرها القاضي، فإنه يجب عليه مناقشتها أمام الخصوم، سواء كانت هذه المخرجات مطبوعة أم بيانات معروضة على شاشة الحاسب، أم كانت بيانات مدرجة في حاملات، أم اتخذت شكل أشرطة وأقراص ممغنطة أو ضوئية أو مصغرات فلمية، تكون محلا للمناقشة عند الاعتماد عليها كأدلة أمام المحكمة[2].

بمعنى آخر يجب أن يستمد القاضي اقتناعه من أدلة طرحت بالجلسة، وخضعت لمناقشة الخصوم، واستناد القاضي على أدلة لم تطرح للمناقشة موجب للبطلان هذا ما تناوله المشرع الجزائري في المادة 212 من قانون إ.ج.ج السالفة الذكر، والمشرع الفرنسي في المادة 2/427 من قانون.إ.ج.ف بقولها: " لا يجوز للقاضي أن يؤسس حكمه إلا على أدلة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الأطراف" والمشرع المصري في المادة 302 من قانون.إ.ج.م بقولها: " لا يجوز للقاضي أن يبني حكمه على أي دليل لم يطرح أمامه في الجلسة.

ومن تم فإن الدليل الذي تبنى عليه المحكمة حكمها لابد من أن يكون له أصل ثابت في ملف الدعوى، وأن يكون قد طرح للمناقشة دون تفرقة فيما إذا كان دليل إدانة أو دليل براءة، والأصل في كل

---

[1]- خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص188.

[2]- خالد ممدوح إبراهيم، المرجع نفسه، ص188- 189.

هذا هو تمكين الخصوم من الإطلاع عليه وإبداء رأيهم فيه وعدم مفاجأتهم بأدلة أو وسائل إثبات استعملت كدليل ولا علم لهم بها، وعليه فأي دليل لم يقدم للخصوم قصد مناقشته، لا يجوز الاستناد عليه أو جعله أساسا للحكم.

خلاصة القول أنّ ضرورة عرض الأدلة في الجلسة للمناقشة جعلها القانون الجزائري أمرا جوازيا لا إلزاميا بل خاضعا لحرية القاضي وتقديره، وإن لم يتمسك به الدفاع، وفي حالة ما إذا تمسّك به هذا الأخير، يصبح مفروضا على القاضي عرضها وتقديمها.

3- يجب أن تكون الأدلة الإلكترونية يقينية[1]:

يشترط في الأدلة الإلكترونية أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ولا يمكن دحض قرينة البراءة وافتراض عكسها إلا عندما يصل القاضي الجزائي لحد الجزم واليقين.

و يصل القاضي إلى يقينية مخرجات الكمبيوتر عن طريق نوعين من المعرفة، أولهما المعرفة الحسية التي تدركها الحواس من خلال معاينة هذه الأدلة وتفحصها، وثانيهما المعرفة العقلية التي يقوم بها القاضي عن طريق التحليل والاستنتاج من خلال الربط بين هذه المخرجات والملابسات التي أحاطت بها، فإذا لم ينتهي القاضي إلى الجزم بنسبة الفعل أو الجريمة الإلكترونية إلى المتهم الإلكتروني كان من المتعين عليه أن يقضي بالبراءة، فالشك يجب أن يستفيد منه المتهم المعلوماتي[2].

والمحقق أو القاضي الذي يعاين جسم الجريمة سواء كانت جريمة تقليدية أم كانت جريمة إلكترونية عن طريق حواسه، لا يمكنه معاينة الفعل الجنائي لحظة وقوعه وإنما يعاين فقط النتائج التي ترتبت عليه، وعن طريق التحليل والاستنتاج يمكنه التوصل إلى الكيفية التي تمت بها الجريمة والأداة التي استخدمت والآثار التي تدل على شخصية مرتكبها ومراحل تنفيذها من قبل فاعليها كما حدثت على أرض الواقع.

---

[1]- يعرف اليقين القانوني بأنه: تلك الحالة الناتجة عن القيمة التي يضفيها القانون على الأدلّة ويفرضها على القاضي، فهو نوع من اليقين يتلقاه القاضي من إرادة المشرع.

[2]- طارق فوزي الفقي، المرجع السابق، ص219. وأنظر أيضا: خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص188.

واليقين ذو خاصية شخصية أو نفسية تختلف من قاضي إلى آخر، ومن ثم فإن القناعة التي يمكن أن يتوصل إليها قاضي في قضيه معينه، قد لا يتوصل إليها قاض في قضية مماثلة، ويترتب على ذلك احتمال حدوث أخطاء أثناء ممارسة هذا المبدأ، لذلك يجب أن يتسّم هذا المبدأ بالثبات أو ما يمكن تسميته باليقين الثابت، وهو اليقين المشترك بين جميع القضاة بخصوص إدانة أو براءة شخص معين[1].

وهكذا يستطيع القاضي من خلال ما يعرض عليه من مخرجات كمبيوترية سواء كانت مخرجات ورقيه تنتجها الطابعة Printers أو الراسم Plotte ، أم كانت مخرجات لا ورقية أو إلكترونية كالأشرطة المغناطيسية Magnetic Tape، والأقراص المغناطيسية Magnetic Disks، والمصغرات الفيلمية Computer Output Microfilm، وغيرها من الأشكال الإلكترونية التي تتوافر عن طريق الوصول المباشر، أم كانت مجرد عرض لهذه المخرجات المعالجة بواسطة الكمبيوتر على الشاشة الخاصة به Monitor أو على الطرفيات Terminals، وما ينطبع في ذهنه من تصورات واحتمالات بالنسبة لها، أن يحدد قوتها الإستدلالية على صدق نسبة الجريمة الإلكترونية إلى شخص معين من عدمه.

خامسا: حجيّة الدليل الإلكتروني في الإثبات

يقصد بالحجيّة الاستدلال على صدق الدعوى أو كذبها وهي تعني البيّنة وحجية المخرجات الكمبيوترية هي قوتها الإستدلالية على صدق نسبة الفعل الإجرامي إلى شخص معين أو كذبه، ويقصد بها كذلك قيمة ما يتمتع به الدليل الإلكتروني بأنواعه المختلفة سواء كانت ورقية أم إلكترونية أم مصغرات فيلمية من قوة استدلالية على نسبه الفعل الإجرامي إلى شخص معين أو كذبه[2].

فحجيّة الدليل الإلكتروني في الإثبات تعترضه العديد من المشكلات، ترتب على ذلك وجود خلاف فقهي حول حجية الدليل الإلكتروني بحسب الفقه المقارن فيما إذا كان لاتينيا أو أنجلوسكونيا أو مختلطا.

---

[1]– هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص81.

[2]– مروك نصر الله، محاضرات في الإثبات الجنائي، الجزء الثاني، دار هومة، الجزائر، 2004، ص461.

1- حجية الدليل الإلكتروني في النظام اللاتيني:

تشمل القوانين ذات الصياغة اللاّتينية القانون الفرنسي والقوانين الأخرى التي تأثرت به كالقانون الايطالي والاسباني وقوانين أمريكا اللاتينية، وتشمل أيضا القانون الألماني، ذلك إنّ القانون الألماني وإن لم يكن لاتيني النزعة إلا أن صياغته تتشابه مع القانون الفرنسي، وكذلك القوانين المتأثرة بالنزعة الاشتراكية الحديثة كالقانون الصيني وأخيرا القانون الجزائري والمصري، فهذه القوانين تتشابه في الصياغة، حيث تكون مصادرها واحدة، و أصولها العامة متحدة، وتقسيماتها متماثلة والإصلاحات القانونية فيها متشابهة[1].

والإثبات في هذه القوانين (اللاّتينية)، يتبع نظام الاثبات الحر[2]، حيث أصبح هذا الأخير القانون العام في الإجراءات الجزائية لهذه التشريعات.

و بمقتضاه يحكم القاضي في الدعوى حسب العقيدة التي تكونت لديه بكامل حريته، وتتمثل خصائص هذا النظام في عدم تحديد الأدلّة، بمعنى أن الخصوم لهم الحرية في الالتجاء إلى أي دليل يمكنّهم من إثبات إدعائهم، كما أن هذا النظام يخول القاضي سلطة تقييم الأدلة دون أن يفرض عليه قيدا أو شرطا، فالقاضي حر في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة، وهو حر في وزن وتقدير كل دليل، وفي التنسيق بين الأدلة التي تتمثل في الحكم بالإدانة أو البراءة [3].

و نتيجة لذلك يحظر على المشرع إضفاء قوة معينة لأي دليل من شأنه أن يقيد سلطة القاضي في تكوين قناعته، أو يسبغ على بعضها شكا أو عدم ثقة كي يستبعدها القاضي من تقديره الحر.

ومبدأ حرية القاضي في الاقتناع يبدو أكثر شمولا في القانون الفرنسي، حيث نصت عليه المادة 310 من ق.إ.ج.ف[4]، والتي بموجبها أسندت للقاضي سلطة تفويضية تسمح له في اللجوء إلى كل الإجراءات المفيدة لإظهار الحقيقة، ولا قيد عليه سوى شرفه وضميره.

---

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص56.

[2]- أقـــر المشرع الفرنسي مبدأ حريّة الإثبات الجنائي صراحة في المادة 427 من ق.إ.ج.ف، والمشرع الجزائري في المادة 212 من ق.إج.ج، والمشرع المصري في المادة 291 من ق.إ.ج. م.

[3]- عائشة بن قارة مصطفى, المرجع السابق, ص183.

[4]- Art 310 (Loi n° 72 – 1226 du 29 décembre 1972) :

إذن نظام الإثبات الحر يمنح للقاضي الجزائي سلطه تقديرية كبيرة في قبول الأدلة وموازنتها وتقدير قيمتها التدليلية، محتكما إلى ضميره و معتمدا على ثقافته وخبرته القانونية، فله أن يأخذ بأدلة ويستبعد أخرى، كما له أن ينسق بين الأدلة المطروحة أمامه و إزالة التعارض بينهما واستكمال نقصها، ومن تم تكوين حكمه على أساس القناعة التي توصل إليها من مناقشة هذه الأدلة.

والدليل الإلكتروني شأنه شأن الأدلة الأخرى مقبول مبدئيا في الإثبات الجنائي بصفه عامة، والإثبات في الجرائم الإلكترونية بصفة خاصة، إذا ما تم الاحترام فيه على ضابط المشروعية، ذلك لأنّ الحرية هنا لا يقصد بها إمكان اللجوء إلى وسائل غير مقبولة قانونا، فحرية الأطراف في مجال الإثبات يجب أن تمارس في إطار ما تفرضه عليه ضوابط المشروعية من قيود يستحيل مخالفتها وإلاّ ترتب على ذلك عدم مشروعيته ذلك الدليل، ومن تم عدم قبوله بل بطلانه.

وتشترط بعض الدول كألمانيا، تركيا، لوكسمبورغ، اليونان والبرازيل، أن يكون الدليل الإلكتروني مقروءا سواء كان مطبوعا بعد خروجه من الجهاز أم كان مقروءا من خلال شاشة الجهاز نفسه، ومن التطبيقات القضائية على ذلك ما قضت به محكمة النقض الفرنسية في أن" أشرطة التسجيل الممغنطة التي يكون لها قيمة دلائل الإثبات يمكن أن تكون صالحة للتقديم أمام القضاء الجنائي"[1].

Le président est investi d'un pouvoir discrétionnaire en vertu du quel il peut, en son honneur et en ca conscience, prendre toutes mesures qu'il croit utiles pour découvrir la vérité. Il peut, s'il l'estime opportun, saisir la cour qui statue dans les conditions prévues à l'article 316.
= Il peut au cours des débats appeler, au besoin par mandat d'amener et entendre toute personnes ou se faire apporter toutes nouvelles pièces qui lui paraissent, d'après les développements donnés à l'audience, utiles à la manifestation de la vérité.
Les témoins ainsi appelés ne prêtent pas serment et leurs déclarations ne sont considérées que comme renseignement.

[1]– هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص43.

2- حجية الدليل الإلكتروني في النظام الأنجلوسكسوني:

في هذا النظام يحدد المشرّع أدلة الإثبات ويقدر قيمتها الإقناعيّة، ومقتضى ذلك أن يتقيد القاضي في حكمه بالإدانة أو بالبراءة بأنواع معينة من الأدلة، أو بعدد منها طبقا لما يرسمه التشريع المطبق، دون أن يأبه في ذلك بمدى إقتناع القاضي بصحة ثبوت الواقعة أو عدم ثبوتها[1].

معنى ذلك أن المشرع يحدد أدلة الاثبات، ويلزم القاضي بالتقيد بها، فيكون دوره آليّا لا يتعدى مراقبة مشروعيتها، وليس له أن يطلب استكمالها إذا كانت ناقصة.

و نظام الإثبات المقيد يقوم على مجموعة من الخصائص أهمها أنّ دور القاضي الجزائي سلبي، ذلك أن الإثبات الجنائي في هذا النظام يخضع لقواعد شكلية تتضح في سلطة القاضي المقيدّة في تقدير عناصر الإثبات التي يستمد منها اقتناعه وتقدير قيمة الأدلة المعروضة عليه، كما يتميز أيضا هذا النظام بالدور الإيجابي للمشرع في عمليه الإثبات من حيث أنه هو الذي ينظم قبول الأدّلة سواء عن طريق تعيين الأدلة المقبولة للحكم بالإدانة، أو باستبعاد أدلة أخرى، أو بإخضاع كل دليل لشروط معينة، و أنه هو الذي يحدد القيمة الاقناعية لكل دليل بأن يعطي لبعض الأدلة الحجيّة الأقوى دون الأدلة الأخرى[2].

ويعاب على هذا النظام أنه أخرج القاضي من وظيفته التي تتمثل في فحصه للدليل وتقديره، ومن تم تكوين اقتناعه الشخصي، فمثلا لا يستطيع أن يحكم بالإدانة ، بل يحكم باستبعاد الدليل حتى ولو يقتنع بأن المتهم مدان، بمعنى أنه لا يستطيع أن يتحرى الحقيقة بطرق أخرى، بموجب اقتناعه بذلك الدليل باعتباره حجة، ما لم ينص عليه القانون، وأقحم المشرع في وظيفة القاضي وإملاء أدلة الإدانة عليه على سبيل الحصر.

ومن الدول التي تأخذ بهذا النظام بريطانيا، كندا، أستراليا وجنوب إفريقيا، حيث تتطلب هذه الدول شروطا خاصة في الأدلة بوجه عام حتى يتم الأخذ بها[3].

---

[1]- هلالي عبد الاله أحمد، المرجع نفسه، ص49. أنظر أيضا: مريم قسول، مبدأ مشروعية الأدلة العلمية في المواد الجنائية، رسالة دكتوراه، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة جيلالي اليابس، سيدي بلعباس، 2015-2016، ص 304- 305.

[2]- نعيم سعيداني، المرجع السابق، ص244.

[3]- شيماء عبد الغني محمد عطا الله، المرجع السابق، ص479.

ففي كندا مثلا نصت المادة 29 من قانون الاثبات الكندي على عدد من الشروط التي يجب توافرها قبل عمل صورة (COPY) من السجل الذي يضاف إلى الأدلة، ومن هذه الشروط أن تكون الصورة حقيقية من المدخل الأصلي[1] .

كما نصت قواعد الإثبات الفدرالية الأمريكية علـــى أن: الشرط الأساسي للتوثيق أو التحقق من صحة أو صدق الدليل كشرط مسبق لقبوله، هو أن يفي بأمارة أو بينة كافية لأن تدعم اكتشاف أو الوصول إلى الأمور التي تتصل بالموضوع بما يؤيد الادعاءات أو المطالب المدعى بها[2].

3- **حجية الدليل الإلكتروني في النظام المختلط:**

في القوانين ذات الاتجاه المختلط يتم الجمع بين النظامين اللاّتيني والأنجلوسكسوني، فيعتمد النظام المختلط على أن يحدد القانون أدلة معينة لإثبات بعض الوقائع دون بعضها الآخر، أو يشترط في الدليل شروطا في بعض الأحوال أو يغطي القاضي الحريّة في تقدير الأدلة القانونية، مثل القانون الإجرائي الياباني، وقد حصر المشرع الياباني طرق الإثبات المقبولة بمـــا يأتي: أقـــوال المتهم، وأقوال الشهود، والقرائن والخبرة.

أما بالنسبة للأدلة الحاسوب والأنترنيت، فيقـــرر الفقه الياباني أن السجلات الإلكترومغناطيسية تكون غير مرئية في حد ذاتها، ولذلك لا يمكن أن تستخدم كدليل في المحكمة، إلا إذا تم تحويلها إلـــى صورة مرئية و مقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات، وفي مثل هذه الحالة يتم قبول هذه الأدلة الناتجة عن الحاسوب والأنترنيت، سواء كانت هي الأصل أم كانت نسخة من هذا الأصل[3].

ويرى الفقه الشيلـــي، أنّ الدليل الناتج عن الحاسوب والأنترنيت، يمكن أن يكون مقبولا في المحكمة كدليل كتابي أو مستندي، مثله مثل النظم الحديثة الأخرى لجمع وتسجيل المعلومات، ومنها التصوير الفوتوغرافي، و التصوير بالأقمار الصناعية، فهذه الوسائل العلمية يمكن اعتبارها مستندات بالمعنى الواسع، ذلك أنّ التقدم الفني قد تجاوز المفهوم التقليدي للمستند الذي يعرفه أنه مجرد ورقة مكتوبة.

---

[1]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص55.

[2]- فهد عبد الله العبيد العازمي، المرجع السابق، ص389- 390.

[3]- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، المرجع السابق، ص62.

خلاصة لما سبق ذكره حول مدى قبول حجية الدليل الإلكتروني في الإثبات الجنائي، يتضح بأن الإثبات الجنائي بالوسائل العلمية الحديثة ومنها الوسائل الإلكترونية الحديثة، أصبح ضرورة في عصر تكنولوجيا المعلومات، هذا العصر الذي استخدم فيه الحاسب الآلي ونظم الشبكات لتبادل المعلومات والبيانات ومعالجتها، وغير ذلك من مجالات الحياة المختلفة التي تسيرها أجهزة الحاسوب، ونظم الشبكات والبرامج والبيانات.

وعليه لابد أن يلاقي الدليل الإلكتروني قبولا لدى جهات العدالة الجنائية، وفقا للشروط التي تخضع لها سائر الأدلة، ومن تلك الشروط عدم الحصول على الدليل بالإكراه، أو بأية طريقة غير مشروعة، وأصبح لزاما على التشريعات المختلفة مواكبة التطور الحاصل في مجال التكنولوجيا الرقمية من خلال النصّ على إجراءات تتناسب و التعامل مع تلك الأدلة، وإعطاء القاضي صلاحيات تقديرية للتعامل معها، فليس هناك ما يمنع هذا الأخير من قبول الدليل الإلكتروني كدليل يدخل تقدير قيمته الإثباتية في دائرة اقتناعه، مادام أنه يتوافر على شروط المشروعية والسلامة من العبث والخطأ.

وبالرغم من الخلاف حول حجية الدليل الإلكتروني في الإثبات، فإن إتجاها دوليا ذهب نحو الاعتراف بالمراسلات الإلكترونية بمختلف أنواعها، والإعتراف كذلك بحجية الملفات المخزنة بالنظم ومستخرجات الحاسوب، وحجية الملفات ذات المدلول التقني وكذا حجية التوقيع الإلكتروني[1]، والتخلي شيئا فشيئا عن أية قيود تحد من الإثبات في البيئة الالكترونية.

---

[1]– يعتبر التوقيع الإلكتروني من بين الأدلة الإلكترونية ويتم استعماله في الاثبات الإلكتروني ولقد عرفه المشرع الجزائري في المادة 1/2 من القانون رقم 04/15، المؤرخ في 1 فبراير 2015 المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية العدد 6، الصادرة في 2015/12/10 علـــى أنه: " بيانات إلكترونية في شكل إلكتروني مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق كما عرفت المادة 7 من نفس القانون التوقيع الإلكتروني الموصوف بأنـــه: التوقيع الذي تتوفر فيه المتطلبات الأتية:

– أن ينشأ على أساس شهادة تصديق إلكتروني موصوفة.

– أن يرتبط بالموقع دون سواه.

– أن يمكن من تحديد هوية الموقع.

– أن يكون مصمما بواسطة آلية مؤمنة خاصة بإنشاء التوقيع الإلكتروني.

– أن يكون منشأ بواسطة وسائل تكون تحت التحكم الحصري للموقع.

– أن يكون مرتبطا بالبيانات الخاصة به بحيث يمكن الكشف عن التغيرات اللاّحقة لهذه البيانات فإذا توافرت الشروط في التوقيع الإلكتروني يعتد به في مجال الإثبات لأنه يؤدي نفس وظائف التوقيع التقليدي، وحتى عمليا فإنه أفضل من التوقيع التقليدي خاصة إذا توافر فيه شرط الأمان والتوثيق من الجهات المختصة.

الباب الثاني

الأحكام الإجرائية للتحقيق الجنائي في الجرائم الإلكترونية

يشهد العالم في الوقت الراهن تقدما هائلا تتجلى أبرز مظاهره في التكنولوجيا الجديدة للمعلومات والإتصالات و تطوير أجيال من الحاسبات الآلية، ولا شك في أن هذه التكنولوجيا الحديثة تقدم للدول و أجهزتها الأمنية الكثير من التسهيلات والإمكانيات التي تسهم في رفع كفاءتها و تطوير قدرتها على التصدي للجريمة إلا أن هذا التطور التكنولوجي أدى و يؤدي في الوقت نفسه إلى تطوير وتحديث الجريمة من حيث الأساليب و المضامين و بخاصة في ظل اتجاه العناصر الإجرامية إلـــى توظيف بعض مخرجات التكنولوجيا كالمعلوماتية في أنشطتها و ممارستها الإجرامية.

هذا ما أدى بالدول إلى البحث عن سياسة جزائية قادرة على مجابهة هذه الظاهرة الإجرامية الحديثة، واعتماد أساليب إجرائية خاصة و تطوير تلك الموجود سابقا فلطالما تصدت التشريعات الجزائية الإجرائية لكل مستحدث و ذلك لحسن سير العدالة و عدم إفلات الجناة من العقاب، بشكل يكفل التطبيق السليم والفعال للقواعد الجزائية الموضوعية، وإذا كان البحث في مسألة قدرة القواعد الإجرائية التقليدية في ضبط جريمة إلكترونية صعبا، هذا ما جعل مسألة ملائمة الإجراءات الجنائية أو البحث والتحري والتحقيق مع خصوصية هذا النوع من الجرائم تستأثر اهتمام المشرعين، حيث نال الشق الإجرائي النصيب الأكبر من ناحية التعديل والتحيين.

نظرا لخصوصية هذه الجريمة التي استطاع مرتكبوها التوغل في كل أنحاء العالم دون أن تشكل الحدود و بعد المسافات أي عائق لها في زيادة انتشارها بين الدول والقارات.

فالجريمة الإلكترونية و ما يعتريها من إشكاليات ومعوقات تمثل خطرا يهدد الاستقـــرار الدولي والأمن الداخلي هذا ما جعل الدول في حاجة ماسة إلى تفعيل التعاون الدولي في جميع مجالاته، من خلال الحرص على إسناد التحقيق لجهات متخصصة بالطابع الخاص للجريمة الإلكترونية **(فصل الأول)** و اعتماد قواعد إجرائية تقليدية في زيّ يتلاءم و طبيعة الجريمة الإلكترونية و أخرى مستحدثة على الصعيدين الوطني و الدولي بموجب أساليب تحقيق وطنية و دولية في الجريمة الإلكترونية **(الفصل الثاني)**.

الفصل الأول: إسناد التحقيق في الجرائم الإلكترونية للأجهزة الوطنية و الدولية

يعود اختصاص التحقيق في الجريمة الإلكترونية في معظم الدول إلى القضاء العادي في جانبه الجزائي ما جعل اكتشاف هذا النوع من الجرائم أمرا صعبا مع نقص الدراية لأجهزة التحقيق ونقص خبرتهم الفنية في مجال الكمبيوتر والأنترنت، في مواجهة مجرمين من نوع خاص لهم من المهارة العالية في مجال الالكترونيات والمعلوماتية من الكفاءة ما يجعل أمر اكتشافهم أمرا عسيرا من قبل جهات التحقيق المختصة.

لذا كان من الضروري أن يتولى التحقيق الجنائي في الجريمة الإلكترونية جهات مختصة تعتمد أساسا على الكفاءة في مجال تكنولوجيا الاعلام والاتصال على الصعيدين الوطني و الدولي، لأنه لا يمكن لأي دولة وحدها أن تتصدى لهذا النوع المستحدث من الجرائم بل لابد من تعزيز التعاون في المجال الإجرائي، وذلك خصوصا للسمات التي تتميز بها هذه الجرائم ولما تثيره تقنية المعلومات من مشكلات في مجال جمع الأدلة والإثبات ومشروعية الإجراءات التي تقوم بها تلك الجهات، كما أنه كان لابد من تخصيص جهات مختصة بالتحقيق في الجريمة الإلكترونية تختص بأساليب البحث والتحقيق عن الأدلة في مجال الرقمية والتعايش مع التطور الحاصل في مجال الجريمة الإلكترونية تحت رعاية كفاءات متخصصة عمدت الكثير من الدول إلى توفيرها وتدريبها فنيا في مجال الإعلام والاتصال لأنه لا مجال للحديث عن القدرات البدنية بقدر ما هم بحاجة إلى الكفاءة التقنية والفنية الإلكترونية.

ومع تزايد حجم الجريمة الإلكترونية باعتبارها سلوكا غير مشروع يمس بأنظمة المعلومات، فإنها قلبت موازين التحقيق حيث أصبح لزوما على المحقق الجنائي أن يكون ماهرا في المجال المعلوماتي ومتقنا له، فمن دون تلك المعرفة لا يمكنه كشف خبايا وخيوط ارتكاب الجريمة الإلكترونية والتعرف على مرتكبيها، ففي ظل هذا التزايد سارعت العديد من الدول إلى إنشاء أجهزة مختصة تستطيع التعامل مع الجريمة الإلكترونية منح لها القانون هذا الاخصاص وتم تعزيزها بإمكانيات مادية وبشرية تساعدها على كشف لغز الجرائم الإلكترونية، وذلك لارتكابها في فضاء إلكتروني، فقد ترتكب هذه الأخيرة في أكثر من نطاق اختصاص على إقليم الدولة الواحدة، وقد ترتكب في أكثر من دولة مما يثير تنازع الاختصاص القضائي داخليا وخارجيا.

لما سبق ذكره سنتناول الاختصاص القضائي لجهات التحقيق في الجريمة الالكترونية في **(المبحث الأول)** من هذا الفصل،و تفعيل دور أجهزة التحقيق في الجرائم الالكترونية في **(المبحث الثاني)**.

المبحث الأول: الاختصاص القضائي لجهات التحقيق في الجرائم الإلكترونية

يعرف الاختصاص القضائي على أنه :"مباشرة ولاية القضاء في نظر الدعوى في الحدود التي رسمها القانون" فهو بمثابة الاختصاص الولائي الذي مناطه هو ضرورة أن يكون النظر في الدعوى الجزائية:

- داخلا على الصعيد الدولي ولاية القضاء الوطني عموما.
- أن يكون داخلا على الصعيد الوطني ضمن ولاية القضاء الجنائي عموما.
- أن يكون داخلا في اختصاص المحكمة التي رفعت إليها الدعوى[1].

كما يعرف أيضا بأنه:" السلطة السيادية للدولة التي تمكنها من تطبيق قوانينها الداخلية داخل إقليمها."

وإذا كان الاختصاص في الجرائم الداخلية يؤول إلى قضاء دولة واحدة، فإن الاختصاص القضائي في الجريمة الإلكترونية يثير العديد من الإشكالات، كتحديد القانون الواجب التطبيق والقضاء المختص بنظر تلك الجرائم سواء على الصعيد الداخلي أو الخارجي، وذلك راجع إلى صفتها الممتدة في أكثر من إقليم دولة، إما من حيث ارتكاب هذه الجريمة أو من حيث الآثار المترتبة عليها.

وعليه ينبغي على السلطات القضائية أن تتثبت قبل كل شيء من مدى دخول النظر في الدعوى ومن ضمنها التحقيق فيها على الصعيد الدولي ضمن ولايتها كقضاء وطني، فإذا ظهر لها عدم ولايتها من الناحية الدولية فلا يجوز لها النظر في الدعوى ولا التحقيق فيها، ومثل هذا الأمر وارد كثيرا في مجال التحقيق في الجرائم الإلكترونية باعتبارها من الجرائم العابرة للدول والقارات، كما وله آثاره السلبية على التحقيق في مثل هذه الجرائم فيما إذا لم تتمكن جهات التحقيق من التحقيق فيها بالنظر لعدم اختصاصها بذلك دوليا كقضاء وطني.

ولم تكن الجريمة داخلة ضمن الاختصاص القضائي الوطني لأيّة جهة من جهات التحقيق في الدول الأخرى فهذا سيؤدي لا محالة إلى إفلات المجرم الإلكتروني بجريمته من العقاب[2]، وموضوع

---

[1]– رشاد خالد عمر، المرجع السابق، ص96.

[2]– رشاد خالد عمر، المرجع نفسه، ص96– 97.

الاختصاص القضائي يتطلب التطرق إلى معايير تحديد الاختصاص لجهات التحقيق في الجريمة الإلكترونية (المطلب أول)، و كذا التعريف بمشكلة الاختصاص لجهات التحقيق في الجريمة الإلكترونية (المطلب ثاني).

المطلب الأول: معايير تحديد الاختصاص لجهات التحقيق في الجريمة الإلكترونية

إن التقدم السريع الذي يعيشه العالم اليوم نتيجة تطور وسائل الاتصال وتعقد أساليب الحياة في كافة جوانبها الاجتماعية والاقتصادية والسياسية، أدى إلى اتساع دائرة الإجرام واختراقه للحدود الدولية وتنوع أساليبه، هذا الأمر أوجب ضرورة التفكير في صيغة جديدة ووسيلة كفيلة بإيجاد الحلول المناسبة للحد من الاجرام بكافة أشكاله ومتابعة المجرمين وإيقافهم مهما كانت البلاد التي يتواجدون على ترابها[1]، وبالتالي لا تستطيع أي دولة بمفردها القضاء على الجريمة أو الحد منها، كما هو الحال في الجريمة الإلكترونية باعتبارها عابرة للحدود.

فحالة الاستمرار كذلك التي تتميز بها الجريمة الإلكترونية، وتجاوزها لحدود الدولة الواحدة، من شأنه أن يخلق ما يسمى بحالة تنازع القوانين، حيث تتزاحم التشريعات الجزائية للدول للنظر في هذه الجريمة عندما يرتكب في كل دولة منها سلوك من السلوكيات المكونة لهذه الجريمة[2].

ولحل مشكلة تنازع الاختصاص القضائي بين الدول، بغية الوقوف على الدولة صاحبة الاختصاص القضائي، أقر فقه القانون المقارن مجموعة من المبادئ نصت عليها القوانين الجزائية منها: مبدأ إقليمية القانون الجزائي(الفرع الأول)، مبدأ عينية القانون الجزائي(الفرع الثاني)، ومبدأ شخصية القانون الجزائي (الفرع الثالث) و مبدأ عالمية القانون الجزائي(الفرع الرابع).

الفرع الأول: مبدأ إقليمية القانون الجزائي

يعد مبدأ إقليمية القانون الجزائي من أكثر المبادئ القانونية شيوعا، ويقصد به تطبيق القانون الوطني على كافة الجرائم المرتكبة على إقليم الدولة بغض النظر عن جنسية الجاني أو المجني عليه، حيث يستوي أن يكون وطنيا أو أجنبيا، وبغض النظر عن المصلحة التي أهدرتها الجريمة، ولو كانت

---

[1]– قد يتمكن الجنات الافلات من العقاب، إذا كان ارتكاب الجريمة خارج إقليم الدولة هذا ما دفع الدول في إقرار أحكام تسمح بامتداد اختصاص القضاء الوطني بالنظر في جرائم وقعت خارج حدود الدولة، نظرا للخطورة التي أضحت تشكلها الجرائم بصفة عامة والجريمة الإلكترونية بصفة خاصة.

[2]– حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة دكتوراه في العلوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2017/2016، ص 230.

مصلحة تتعلق بدولة أجنبية[1]، على أساس أن كل ما يرتكب في إقليم الدولة من جرائم يعد مساسا بسيادتها، وبالتالي فإن هذا الاختصاص لا يمكن التنازل عنه لأي دولة من الدول لتعلقه بالنظام العام[2]، كما أنه يعبر عن استقلالها وتمتعها بالشخصية المعنوية داخل المجتمع الدولي[3]، إذن يقتضي تطبيق مبدأ الإقليمية سريان القانون الجزائي في حدود إقليم الدولة[4].

ولكن ينقصنا هنا تحديد المقصود بإقليم الدولة، حيث يشمل هذا الأخير وفقا لقواعد القانون الدولي العام أجـــزاءا ثلاثة هي: الإقليم الأرضي: وهو المنطقة من الكرة الأرضية التي تعين استنادا إلى الحدود السياسية للدولة بكل طبقاتها، والإقليم المائي: وهو مساحات الماء التي تقع داخل حدود الدولة كالبحار والأنهار والوديان، والإقليم الجوي: الذي يشمل طبقات الهواء التي تعلوا الإقليم الأرضي والمائي[5]، وامتداد الإقليم حيث تعد السفن والطائرات والسفارات امتدادا لإقليم الدول[6].

ولمبدأ إقليمية القانون الجزائي شقين: الشق الإيجابي: وهو أن القانون تعبير عن سيادة الدولة على أراضيها فينطبق على جميع الأشخاص المقيمين بإقليم الدولة من المواطنين أو الأجانب، وينشئ من هذا المبدأ [7] قانون الأحوال الشخصية، والقوانين الدستورية والسياسية، أما الشق السلبي يتمثل في عدم تطبيق القانون الجزائي على أية جريمة ترتكب خارج حدود الدولة وذلك لاعتبارين أولهما وجود الشخص داخل سيادة دولة أخرى يخضع لقوانينها، وثانيهما: صعوبة تطبيق وتنفيذ قوانينها خارج حدودها[8].

---

[1]– رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء قواعد القانون الجنائي الداخلي والدولي، الطبعة الأولى، دار الجامعة الجديدة، مصر، 2007، ص13.

[2]– عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام)، الجزء الأول: الجريمة، الطبعة السادسة، ديوان المطبوعات الجامعية، الجزائر، 2005، ص101– 102.

[3]– منصور رحماني، الوجيز في القانون الجنائي العام، فقه وقضايا، دار العلوم للنشر، الجزائر، 2006، ص 108 .

[4]– FREDERIC Deboue، FRANÇOIS Falletti et EMANUAL Dupic،Précis de droit pénal et de procédure pénal، PUF، Paris، France، 5éme édit mise a jour، 2013، p73.

[5]– محمود نجيب حسني، شرح قانون العقوبات(القسم العام)، المجلد الأول، الطبعة الثالثة، (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، لبنان، بدون سنة نشر، ص 182.

[6]– أحمد سعد محمد الحسيني، المرجع السابق، ص229.

[7]– محمد صغير بعلي، مدخل للعلوم القانونية، دار العلوم، عنابة،2006، ص79.

[8]– محمد صغير بعلي، المرجع نفسه، ص81. وأنظر أيضا: محمد طارق عبد الرؤوف الحن، المرجع السابق، ص211.

ويستند هذا المبدأ إلى عدة مبررات، منها فكرة سيادة الدولة على إقليمها إذ أن تطبيق القانون الجزائي إقليميا هو من أهم مظاهر السيادة على الإقليم[1]، فالقانون الجزائي هو الذي يضمن حماية الحقوق الدستورية والقانونية، أضف إلى ذلك أن محكمة مكان ارتكاب الجريمة أقدر على جمع الأدلة والإحاطة بجميع ظروفها وشهودها وفعالها، كما أن محاكمة الجاني في مكان ارتكاب الجريمة يحقق الردع العام، ويقضي على الاضطراب الاجتماعي الذي أحدثته الجريمة بالمجتمع[2].

ونظرا لخصوصية الجريمة الإلكترونية، أشارت المادة 30 من الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لعام 2010 على المبادئ التي يجب على الدول الأطراف اعتمادها لتحديد الاختصاص القضائي فيما يتعلق بالجرائم المنصوص عليها في هذا الفصل الثاني من هذه الاتفاقية منها مبدأ الإقليمية، حيث نصت المادة 1/30 على أنه:" تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمدة اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية، وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت:

أ- في إقليم الدولة الطرف.

ب- على متن سفينة تحمل علم الدولة الطرف[3].

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

كما نصت المادة 1/22 من اتفاقية بودابست لمكافحة جريمة المعلوماتية لعام 2001 على أنه:" يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنّها ضرورية من أجل تقرير اختصاصه بالنسبة لكل جريمة جنائية محددة وفقا للمواد من 2 إلـــى 11 من هذه الاتفاقية وفقا لما يلي:

---

[1]- يرتبط مبدأ الإقليمية ارتباطا وثيقا بمفهوم السيادة حيث نصت المادة 12 من الدستور على أنه:" تمارس الدولة سيادتها على مجالها البري، ومجالها الجوي، وعلى مياهها.

كما تمارس الدولة حقها السيد الذي يقره القانون الدولي على كل منطقة من مختلف مناطق المجال البحري التي ترجع إليها "

[2]- محمود نجيب حسني، شرح قانون العقوبات اللبناني، المجلد الأول، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، 1988، ص180.

[3]- محمد طارق عبد الرؤوف الخن، المرجع السابق، ص211.

أ- مبدأ الإقليمية :

نصت على هذا المبدأ في المادة 1/22 البند "أ" من نفس الإتفاقية ، حيث جاء هذا البند بطلب من كل دولة طرفا في هذه الاتفاقية أن تعاقب على الجرائم المنصوص عليها، إذا ارتكبت الجريمة ضمن النطاق الإقليمي للدولة.

وعلى سبيل المثال يعّد هذا الاختصاص منعقدا إذا كان نظام الحاسوب العائد للمعتدي ضمن الإطار الاقليمي، ولو كان المعتدي مقيما خارج الدولة، أو إذا كان نظام الحاسوب العائد للضحية ضمن الإطار الاقليمي للدولة ، كما يعد الاختصاص الإقليمي متوفرا وفق هذا البند، إذا كان مصدر الإرسال أو جهة الوصول داخل إقليم الدولة[1].

ب- مبدأ نسبية الاختصاص المكاني(الإقليم الاعتباري):

جاء هذا المبدأ بالبند "**ب**" و "**ج**" من المادة 1/22 من ذات الذي ينص على أن" يقيم كل طرف اختصاصه بالنسبة للجرائم المرتكبة على متن السفن التي ترفع علم الدولة الخاص به أو الطائرات المسجلة وفقا لنظمه وقوانينه، على أساس أنّ هذه السفن أو الطائرات بمثابة امتداد لإقليم الدولة.

كما نصت المادة 15 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة[2]على أنه:" يتعين على كل دولة طرف أن تعتمد ما يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقررة في الحالات الآتية:

-حينما ترتكب الجريمة في إقليم تلك الدولة.

-حينما ترتكب الجريمة ضد أحد مواطني تلك الدولة.

- حينما ترتكب الجريمة من طرف أحد مواطني تلك الدولة أو من طرف شخص عديم الجنسية اتخذ مكان إقامته المعتاد في إقليمها ".

[1]- محمد طارق عبد الرؤوف الخن، المرجع السابق، ص200.

[2]- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25، الدورة 55، المؤرخة في تشرين الثاني، نوفمبر 2000، وثيقة رقم: A/RES/55/25.

وفي هذا السياق نصت المادة 1/39 مطة (أ) من الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية[1] على ما يلي:"..... تتخذ الدول الأطراف ما يلزم من تبريرات لتقرير اختصاص سلطاتها وأجهزتها القضائية بملاحقة وبالنظر في الجرائم المشمولة لهذه الاتفاقية في عدة حالات خاصة عندما تقع الجريمة كلّها أو أحد عناصرها في إقليم الدولة، أو حينما يتم الإعداد أو التخطيط أو الشروع في الجريمة أو تحقق إحدى صور المساهمة فيها في هذا الإقليم أو حينما تمتد آثار الجريمة إليه."

كما نصت الدول كذلك من خلال تشريعاتها الداخلية على هذا المبدأ[2] كما يلي:

أولا: بالنسبة للتشريع الفرنسي

اعتمد المشرع الفرنسي مبدأ إقليمية النص الجزائي في المادة 2/113 ق.ع.ف التي نصت على ما يلي:" يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية وتعتبر الجريمة قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقع على هذا الإقليم."

ثانيا: بالنسبة لدولة الإمارات العربية المتحدة:

طبّق قضاء إمارة دبي مبدأ الإقليمية على واقعة قذف عبر الإنترنيت ارتكبتها إحدى الصحف الإلكترونية التي مقرّها لندن، حيث كانت المجني عليها عند قراءة ألفاظ القدح موجودة في دبي، وقد اعتبرت المحكمة أنه طالما أن نتيجة الفعل تحققت في دبي، فإن الجريمة تعد قد وقعت في إقليم الدولة وتخضع لأحكام قانون العقوبات الإماراتي[3].

---

[1]– الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة، بتاريخ 21 ديسمبر 2010، وثيقة متاحة على موقع الشبكة القانونية العربية، إدارة الشؤون القانونية التابعة للأمانة العامة لجامعة الدول العربية، متوفر على الموقع الإلكتروني: (www.arablegalnet.org)

[2]– من التشريعات المقارنة التي تتجه إلى التوسع في مفهوم الإقليمية التشريع الأمريكي الذي يعطي الاختصاص للمحاكمة الجنائية بمجرد حدوث آثار الجريمة على إقليمها. حيث قضي في أمريكا بأنه تم إدخال بيانات من مكان معين وكانت تتضمن ما يشكل جريمة إلكترونية وكانت هذه البيانات مقروءة في مكان آخر، فإن الاختصاص ينعقد لمحاكم الدولة التي يمكن الاطلاع على تلك البيانات في إقليمها، فإذا كان الجاني قد وضع صور مؤتمنة على جهاز الخادم المتواجد في إيطاليا وكانت هذه الصور متاح الاطلاع عليها في الولايات المتحدة الأمريكية فإن القضاء الأمريكي يحكم اختصاصه، أنظر: نعيم سعيداني، المرجع السابق، ص100.

[3]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص209.

ثالثا: بالنسبة للتشريع اليمني:

نصّ القانون اليمني على مبدأ الإقليمية من خلال نص المادة 3 من ق.ع.ي على أنه:" يسري هذا القانون على كافة الجرائم التي تقع على إقليم الدولة، أيا كانت جنسية مرتكبها، وتعد الجريمة مقترفة في إقليم الدولة إذا وقع فيه عمل من الأعمال المكونة لها، ومتى وقعت الجريمة كلها أو بعضها في إقليم الدولة يسري هذا القانون على من ساهم فيها ولو وقعت مساهمته في الخارج."

يفهم من هذا النص أنّ القانون اليمني اشترط أن تكون الجريمة أو أحد الأفعال المكونة لها قد تم ارتكابها في نطاق الإقليم الوطني للدولة.

رابعا: بالنسبة للتشريع المصري:

نصت المادة الأولى ق.ع.م على أن:" تسري أحكام هذا القانون على كل من يرتكب في القطر المصري جريمة من الجرائم المنصوص عليها فيه"، وبالتالي يأخذ المشرع المصري بمبدأ الإقليمية، ويطبق قانون العقوبات على أية جريمة ترتكب داخل القطر بغض النظر عن جنسية المتهم أو المجني عليه في هذه الجريمة.

كما نصت المادة الثانية منه في فقرتها الأولى على أن: " تسري أحكام هذا القانون أيضا على الأشخاص الآتي ذكرهم: كل من ارتكب في خارج القطر فعلا يجعله فاعلا أو شريكا في جريمة وقعت كلها أو بعضها في القطر المصري."

والمشرع هنا أراد أن يشمل بالعقاب الشريك الذي يرتكب فعلا بالاشتراك مع آخرين في جريمة وقعت عناصرها ونتيجتها في القطر المصري حتى لا يفلت الشريك من العقاب، و هذا النص قد يكون معالجا أيضا لجرائم قد يتمكن أصحابها من ارتكابها وهم في خارج القطر المصري مثل الجرائم الإلكترونية، حيث يمكن عن طريق شبكة الأنترنيت أن ترتكب الجريمة والفاعل أو الشريك خارج القطر المتحقق فيه النتيجة[1].

خامسا: بالنسبة للتشريع الجزائري

اعتنق المشرع الجزائري على غرار باقي المشرعين مبدأ إقليمية القانون الجزائي، حيث نص في المادة 3 من ق.ع.ج على أن:" يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في اختصاص المحاكم

[1]– أحمد سعد محمد الحسيني، المرجع السابق، ص229.

الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية "، وبالتالّي يسري هذا المبدأ على كافة الجرائم التي ترتكب في الإقليم الجزائري سواءا الإقليم البري أو البحري أو الجوي.

كما اعتبر المشرع أن الجريمة واقعة في الإقليم الجزائري في حالة ارتكاب عمل من الأعمال المميزة لأحد أركانها المكونة لها في الجزائر وهذا ما نصت عليه المادة 586 من ق.إ.ج.ج[1]، وحسن ما فعل المشرع الجزائري حيث أن هذا الحكم يضمن خضوع الجريمة الالكترونية إلى القضاء الجزائري لمجرد أن إحدى عناصرها وقعت بالجزائر، خاصة وأن هذه الجريمة تتوزع في أكثر من إقليم دولة واحدة ما جعل منها جريمة عابرة للحدود.

كما أخضع المشرع الجزائري لاختصاص القضاء الوطني، كل من كان شريكا في جناية أو جنحة مرتكبة في الخارج، في حالة تواجده داخل إقليم الجمهورية، وكانت الواقعة معاقبا عليها في كلا القانونين الأجنبي والجزائري، شريطة أن تكون تلك الواقعة المساهم فيها والموصوفة بأنها جناية أو جنحة قد ثبت ارتكابها بقرار نهائي صادر من الجهة القضائية الاجنبية[2].

أضف إلى ذلك أن اختصاص قانون العقوبات قد يمتد إلى خارج الإقليم الجزائري[3]، وذلك في حالة إذا كان عنصر من عناصر الجريمة الإلكترونية وقع على ظهر سفينة تحمل العلم الجزائري في عرض البحر[4]، أو وقع على متن طائرة وذلك في حالتين: الحالة الأولى إذا كانت الطائرة جزائرية بغض النظر عن جنسية مرتكب الجريمة، والحالة الثانية إذا كانت الطائرة أجنبية ولكن بشرط هبوط الطائرة بالجزائر بعد وقوع الجناية أو الجنحة[5].

مع إمكانية تطبيق مبدأ إقليمية النص الجزائي على الجرائم الإلكترونية وبالخصوص المرتكبة منها عن طريق الأنترنيت، إلا أن ذلك يثير بعض المشكلات منها: مشكلة تنازع الاختصاص القضائي لأكثر من دولة،

---

[1]– تنص المادة 586 ق.إ.ج.ج علـــــى أنه:" تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميز لأحد أركانها المكونة لها قد تم في الجزائر "

[2]– أنظر المادة 585 من القانون نفسه.

[3]– يترتب على أعمال مبدأ إقليمية القانون الجزائي أن القانون الجزائي لدولة معينة، لا يمتد إلى خارج إقليمها أيا كانت صفة مرتكب الجريمة أو جنسيته، مع ذلك يمكن أن يمتد القانون الجزائي الوطني في حالة ما إذا كانت هذه الجرائم قد ارتكبت في ظروف معينة، وبالتالي تكون من اختصاص الجهات القضائية الوطنية.

[4]– هذا ما نصت عليه المادة 590 من ق.إ.ج.ج.

[5]– أنظر المادة 591 من ق.إ.ج.ج.

حيث أن معظم هذه الجرائم يتم السلوك فيها في بلد معين إلا أن النتيجة تتم في كل من دول العالم حيث أنها متاحة لكل متصفحي الأنترنيت، الأمر الذي يعطي الاختصاص لكل دولة وقعت على إقليمها تلك الجرائم.

كما أنّ عدم فاعلية المحاكم عن الجرائم الإلكترونية التي تقع في الخارج تعد كذلك من مشكلات الاختصاص القضائي حيث أنّ تدويل الجرائم المرتكبة عن طريق الأنترنيت، يجعل منعها والعقاب عليها أمرا احتماليا في ظل الوضع الراهن للأنظمة القانونية، فمن السهل على خدمة ما صدر حكم قضائي بمنعها أن تغير اسمها وتعود بسرعة لبث المعلومات غير المشروعة، وهذه العملية يمكن أن تتم في وقت أقصر من الوقت اللازم لاتخاذ الاجراءات القضائية المستعجلة[1].

ومن المشكلات التي تعيق تطبيق الاختصاص القضائي القائم على مبدأ الاقليمية في مجال الجرائم الإلكترونية، تتمثل في حالة أن يكون مزور الأنترنيت تابع لمزود آخر موجود في دولة أخرى، أو يكون مزود الأنترنيت الأساسي موجود في دولة بينما المزودات الفرعية في أكثر من دولة، فأي من قضاء تلك الدول يكون مختصا؟ وأي من القوانين يكون واجب التطبيق؟[2] .

وبالرغم من أن هناك بعض القوانين تعالج مسألة الاختصاص القضائي وفقا لمبدأ إقليمية النص الجزائي بصورة مغايرة لما هو معمول به في أغلب التشريعات، حيث يرتبط تطبيق النص الاقليمي على الجريمة بشرط أن تكون مجرّمة أيضا في البلد الآخر، وأن تكون ثابتة بموجب حكم قضائي في البلد الأجنبي، وهو ما أشارت إليه المادة 5/113 ق.ع.ف، حيث تضمنت هذه الأخيرة تطبيق قانون العقوبات الفرنسي على كل من ارتكب فعل في إقليم الجمهورية يجعله شريكا في جناية أو جنحة وقعت في الخارج، إذا كانت الجناية أو الجنحة معاقبا عليهما في القانون الفرنسي و القانون الأجنبي، وثابتة بموجب حكم قضائي من البلد الأجنبي"[3]، غير أن المشكلة في هذه الحالة تتمثل في صعوبة تحديد مكان ارتكاب الجريمة الأصلية، لكوني تجريم الفعل الأصلي في الخارج هو شرط أولي لعقد

---

[1]– جميل عبد الباقي الصغير، الجوانب الاجرائية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية، القاهرة، 2002، ص59.

[2]– فايز محمد راجح غلاب، المرجع السابق، ص383.

[3]– Article 113_5 de C.P.F: « La loi pénal française est applicable quiconque s'est rendu coupable sur le territoire de la république comme complice، d'un crime ou d'un délit commis à l'étranger si le crime، ou le délit est puni à la fois، par la loi française et par la loi étrangère et s'il a été constaté par une décision définitive de la juridiction étrangère. »

الاختصاص القضائي للقضاء الفرنسي، وعليه فإن عدم معرفة الدولة التي تبث منها المعلومات المجرمة يحول دون محاكمة الشريك في فرنسا، لأن تحديد مكان ارتكاب الفعل الأصلي يترتب عليه معرفة ما إذا كان هذا الفعل معاقب عليه في بلد الارتكاب من عدمه[1].

ولتفادي المشكلات المتعلقة بالاختصاص القضائي القائم على مبدأ إقليمية النّص الجنائي في الجرائم الإلكترونية لابد من وجود تعاون دولي عن طريق اتفاقية تسليم المجرمين[2]، وتبادل الإنابة القضائية الدولية، نظرا لاستحالة اتفاق جميع الدول على اختصاص قضائي دولي لهذه الجرائم.

الفرع الثاني: مبدأ عينية القانون الجزائي

يقصد بمبدأ عينية القانون الجزائي: تطبيق القانون الجنائي للدولة على الجرائم الواقعة خارج إقليمها فيما إذا كانت مضرّة بإحدى المصالح الأساسية أو الجوهرية للدولة، وبغض النظر عن جنسية مرتكبيها وصفتهم، وبغض النظر عما إذا كانت الجريمة معاقبا عليها بمقتضى قانون البلد الذي وقعت فيه أم لا، والمصالح الأساسية للدولة بدورها تختلف من بلد لآخر ولا يمكن تحديدها و لا حصرها إلا من قبل الدولة نفسها[3].

وهذا المبدأ تم تقريره كمبدأ مكمل لمبدأ العينية[4]، حيث يفرضه حرص الدولة على حماية مصالحها الأساسية.

وهذا المبدأ يمكن تطبيقه على الجرائم الإلكترونية إذا كانت تمّس بالسيادة الوطنية ووحدة الدولة أو تعمل على المساس بالمصالح الحيوية و لو ارتكبت من قبل أجانب خارج إقليم الدولة[5].

ولقد أشارت المادة 1/30 البند (هـ) من الاتفاقية العربية لمكافحة المعلوماتية لعام 2010 على أنه:" تلتزم كل دولة بتبني الإجراءات الضرورية لمدة اختصاصها على أي من الجرائم المنصوص عليها في

---

[1]– جميل عبد الباقي الصغير، المرجع السابق، ص51.

[2]– تسليم المجرمين هو أحد مظاهر التعاون الدولي لمكافحة الجريمة، وهو عباره عن إجراء قانوني مؤسس على معاهدة، أو معاملة بالمثل، أو قانون وطني، توافق بموجبه دولة تسمى الدولة المطلوب إليها، على أن تسلم إلى دولة أخرى تسمى الدولة الطالبة شخصا يتواجد على إقليمها، وذلك كي تتيح للدولة الطالبة أن تحاكم الشخص المطلوب تسليمه، أو تنفذ عليه العقوبة إذا كانت قد تمت محاكمته من قبل، أنظر: نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017، ص20.

[3]– رشاد خالد عمر، المرجع السابق، ص107.

[4]- CLAUDE Soyer، Droit Pénal et Procédure Pénale، L.G.D.J، Paris، France، 12 éme édit، 1996، p73.

[5]– لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، مقال منشور ضمن مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، 2013، مشار إليه في الموقع الإلكتروني:revenue_univ_ourgla.dz يوم 2017/06/22.

الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت وكانت تمس أحد المصالح العليا للدولة"

كـما نصت الدول من خلال تشريعاتها الداخلية على مبدأ عينية القانون الجزائي من خلال ما يلي:

أولا: التشريع الأمريكي

أخذ المشرع الأمريكي بمبدأ العينية حينما قرر امتداد القانون الأمريكي إلى الجرائم التي تقع في الخارج والتي من شأنها المساس بالمصالح الأمريكية و المنصوص عليها في قانون العلاقات الخارجية، حيث أنه جعل الاختصاص الأمريكي قائما طالما هناك سلوك ذو تأثير على الإقليم الأمريكي ولو كان السلوك الخطر هنا واقعا بأكمله خارج الولايات المتحدة الأمريكية، وأيضا يمتد الاختصاص الأمريكي بنظر الجرائم الواقعة خارج الإقليم الأمريكي والتي يقرر النائب العام إحالتها متى كانت الواقعة تشكل عملا إرهابيا يمس المصالح الأمريكية وفقا لما قرره قانون مكافحة الإرهاب عام1986 [1].

ثانيا: التشريع الفرنسي

اعتمد المشرع الفرنسي مبدأ عينية القانون الجزائي في المادة 113/ 10 من ق.ع.ف والتي تنص على ما يلي: " يطبق القانون الفرنسي على الجنايات والجنح التي ترتكب في الخارج، والتي تشكل اعتداء على المصالح الأساسية للأمّة، المنصوص عليها في الباب الأول من الكتاب الرابع، وكذلك جرائم تقليد و تزوير أختام الدولة، وتزييف العملة المعدنية أو الورقية أو السندات العامة والمعاقب عليها بالمواد 1/242 ، 1/243، وعلى أيّة جناية أو جنحة ترتكب ضد أعضاء أو أماكن البعثات الدبلوماسية والقنصلية الفرنسية في الخارج".

ثالثا: التشريع المصري

أخذ المشرع المصري بمبدأ العينية فنصت المادة الثانية من ق.ع.م على سريان أحكام هذا القانون على كل من ارتكب في خارج القطر جريمة من الجرائم الآتية:

أ – جناية مخلّة بأمن الحكومة مما نص عليه في البابين الأول والثاني من الكتاب الثاني من هذا القانون.

ب – جناية التزوير مما نص عليه في المادة 206 من هذا القانون.

[1]– طارق فوزي الفقي، المرجع السابق، ص241.

ج- جناية تقليد أو تزييف عملة ورقية أو معدنية مما نصّ عليه في المادة 202 أو جناية إدخال تلك العملة الورقية، أو المعدنية المقلّدة، أو المزيفة، أو المزورة إلى مصر، أو إخراجها منها، أو ترويجها، أو حيازتها بقصد الترويج، أو التعامل بها مما نصّ عليه في المادة 203 بشرط أن تكون العملة متداولة قانونا في مصر."

يفهم من نص المادة السالفة الذكر أن قانون العقوبات المصري يطبق على الجرائم التي تم الإشارة إليها والتي ترتكب في الخارج دون تطلب قيد أو شرط بجنسية مرتكبها، أو تكون الجريمة معاقبا عليها في قانون الدولة المرتكبة فيها، أو عودة الجاني إلى مصر، فكل ما اشترطه النص هو أن تكون الجريمة من نوع الجرائم التي ذكرت على سبيل الحصر.

رابعا: التشريع اليمني

نص القانون اليمني على هذا المبدأ من خلال نص المادة 247 ق.ع.ي على أن:" تختص المحاكم اليمنية بمحاكمة كل من ارتكب خارج إقليم الدولة جريمة مخلة بأمن الدولة مما نص عليه في الباب الأول من الكتاب الثاني من قانون العقوبات[1] أو جريمة تقليد أو تزييف أختام الدولة أو إحدى الهيئات العامة أو تزوير عملة وطنية متداولة قانونا أو إخراجها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها."

خامسا: التشريع الجزائري

أخذ المشرع الجزائري بمبدأ العينية في تحديد الاختصاص القضائي للجهات الوطنية للنظر في بعض الجرائم المرتكبة في الخارج ، وهذا ما نصت عليه المادة 588 ق.إ.ج.ج بقولها:[2]" تجوز متابعة و محاكمة كل أجنبي وفقا لأحكام القانون الجزائري، ارتكب خارج الإقليم الجزائري بصفة الفاعل أصلي أو شريك في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية أو المحلات الدبلوماسية والقنصلية الجزائرية أو أعوانها، أو تزييفا لنقود أو أوراق مصرفية وطنية متداولة قانونا في

---

[1]- نشير في هذا الصدد أن قانون العقوبات اليمني يتضمن في الباب الثاني منه الجرائم الماسة بالأمن القومي للدولة من خلال المواد من 125 إلـــى 136، منها: المساس باستقلال الجمهورية أو وحدتها أو سلامة أراضيها، وأي فعل يهدف إلى اضعاف القوات المسلحة، أو التخابر لدى دولة أجنبية، بالإضافة إلى الجرائم الماسة بالأمن الداخلي للدولة.

[2] -يقابلها نص المادة 113-7 من ق.ع.ف و التـــي تقضي بأنه " يطبق على كل جناية و على كل جنحة معاقب عنها بالحبس ترتكب من طرف فرنسي أو أجنبي خارج تراب الجمهورية عندما تكون الضحية من جنسية فرنسية وقت ارتكاب الجريمة."

الجزائر أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري"، وبالتالي إذا كان هناك اعتداء على المصالح الجوهرية للجزائر من طرف أجنبي في بلد أجنبي فإن قانون العقوبات الجزائري هو المختص بمعاقبة مقترفيه.

كما نصّت على هذا المبدأ المادة 15 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث ورد النص كالتالي:" زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الاعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني".

تمّيز المشرع الجزائري عن غيره في النص على تمديد الاختصاص القضائي عندما يتعلق الأمر بالجرائم المتصلة بتكنولوجيا الاعلام والاتصال عندما تستهدف تلك الجرائم مؤسسات الدولة الجزائرية أو الدفاع الوطني، أو المصالح الإستراتيجية للاقتصاد الوطني، و تلك الجرائم يمكن ارتكابها بواسطة الأنترنيت: منها إفشاء أسرار الدفاع أو جريمة التجسس كاختراق النظام المعلوماتي لوزارة الدفاع الجزائرية عبر الأنترنيت من أجل الحصول على معلومات سرية وغيرها من الجرائم الماسة بالأمن القومي للدولة[1]، غير أن تطبيق مبدأ العينية يواجهه العديد من المشكلات منها:

1- مشكلة تعارض الاختصاص وفقا لمبدأ العينية مع الاختصاص وفقا لمبدأ الاقليمية في حالة أن تكون الجريمة المرتكبة وفقا لمبدأ العينية مُجرمة في قانون الدولة الأخرى التي اقترفت فيها، فهنا تثار مسألة تنازع الاختصاص ما بين الدولة المقترفة فيها الجريمة وفقا لمبدأ الاقليمية والدولة الأخرى التي تعد تلك الجريمة من الجرائم التي ينظر فيها وفقا لمبدأ العينية، وبالتالي فقد يحاكم الشخص على فعله مرتين[2].

2- تطبيق مبدأ العينية من طرف الدولة التي تم الاعتداء على مصالحها، يجعل هذا التصرف أنانيا حيث أن هذه الأخيرة سوف تدافع عن مصالحها دون أي اعتبار للدولة التي وقعت الجريمة على

[1]- هذه الجرائم المنصوص عليها في المواد من 61 إلى 83 ق.ع.ج.

[2]- فايز محمد راجح غلاب، المرجع السابق، ص391.

أراضيها، فامتداد الاختصاص القضائي إلى الجرائم التي ترتكب على اقليم دولة أخرى، ينطوي بلا شك على اعتداء على سيادة الدولة التي ارتكبت الجريمة على اقليمها.

3- كذلك من المشكلات المتعلقة بالاختصاص القضائي هو أن اختصاص القضاء ينظر جرائم الكمبيوتر والقانون المتعين تطبيقه على الفعل لا يحظى دائما بالوضوح أو القبول أمام حقيقة أن غالبية الأفعال ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، وهو ما يبرز أهمية قواعد الاختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة تطال هذه الجرائم أم أنه يتعين إفراد قواعد خاصة بها في ضوء خصوصيتها وما تثيره من مشكلات تتعلق بالاختصاص القضائي[1].

4- أيضا مبدأ العينية يتوقف نفاده إذا كان الفعل المرتكب على مصالح الدولة الجزائرية في الخارج غير مجرما في الدولة الأجنبية، ومن أمثلة ذلك ما حدث سنة 2000 في قضية الدودة الحاسوبية **لوف باغ (LOVE BUG)** التي أعدت في الفلبين، وقيل أنها عطلت ملايين الحواسيب الآلية في جميع أنحاء العالم، ما أدى إلى إعاقة التحقيقات القضائية على اعتبار أن ذلك العمل المؤدي والضار لم يكن مجرما بشكل كاف[2]، وهذا ما يعيق الدولة في حماية مصالحها إذا كان المعتدي مقيما بدولة أجنبية لا تجرم مثل هذه الأفعال.

الفرع الثالث: مبدأ شخصية القانون الجزائي

مقتضى مبدأ شخصية القانون الجزائي هو سريان القانون الجزائي للدولة على الجرائم المرتكبة فيما إذا كان أحد طرفي الجريمة (الجاني أو المجني عليه) من حاملي جنسيتها[3] ، وهذا يعني أن لهذا المبدأ وجهان أحدهما إيجابي ويتمثل في تطبيق النص الجزائي على كل من يحمل جنسية الدولة و لو ارتكب جريمة خارجها، والثاني سلبي يعني تطبيق النص على كل جريمة يكون المجني عليه منتميا إلى جنسية الدولة ولو كان مرتكبها أجنبيا وارتكبها خارج الدولة[4].

---

[1]- فايز محمد راجح غلاب، المرجع السابق، ص391-392.

[2]- يوسف صغير، الجريمة المرتكبة عبر الأنترنيت، مذكرة لنيل شهادة الماجستير في القانون، قسم الحقوق، جامعة مولود معمري، تيزي وزو 2013/03/06، ص135.

[3]- رشاد خالد عمر، المرجع السابق، ص100.

[4]- محمود نجيب حسني، شرح قانون العقوبات اللبناني، المرجع السابق، ص100. وأنظر أيضا: رشاد خاد عمر، المرجع السابق، ص100-101. وأنظر أيضا: جميل عبد الباقي صغير، المرجع السابق، ص55.

وتطبيق مبدأ الشخصية بالطريقة الإيجابية، يؤدي إلى تجنب فرار المجرم الذي يسيء إلى سمعة وطنه عندما يرتكب جريمته خارج إقليم دولته ثم يفر إليها، إذ أن دولته لا تستطيع تسليمه إلى الدولة التي ارتكب الجُرم على أرضها، لأنه من رعاياها كما هو سائد في معظم التشريعات الجزائية، أما تطبيق مبدأ الشخصية بالطريقة السلبية، فهو يؤمن حماية رعايا الدولة من الاعتداءات الجرمية عليهم[1].

والحكمة من تقرير هذا المبدأ هو ضمان أن لا تكون الدولة معقلا للمجرمين، وحتى لا تكون الدول فيما بينها ملجأ يحمي هؤلاء المجرمين الذين يرتكبون جرائم في الخارج ثم يعودون إلى وطنهم[2].

ولقد نصت اتفاقية بودابست على هذا المبدأ في المادة 1/22 بند (د) وهو يفترض أن رعايا الدولة يتصرفون وفقا للقانون الداخلي إذا تواجدوا خارج النطاق الاقليمي لدولهم، وعليه إذا ارتكب أحد الرعايا جريمة إلكترونية على إقليم دولة أخرى، فإن دولته تقوم بالتنقيبات والتحقيقات اللاّزمة إذا كانت هذه الجريمة معاقب عليها بمقتضى قانون الدولة التي ارتكبت عليها.

أما فيما يخص الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لسنة 2010، فقد نصت على مبدأ الشخصية في المادة 1/30 بند (د) حيث تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمدة اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية، وذلك إذا ارتكبت الجريمة كليا أو جزئيا أو تحققت من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

كما أكدت اتفاقية الأمم المتحدة على ضرورة مراعاة مبدأ الشخصية بشقيه الإيجابي والسلبي، عندما ترتكب الجريمة ضد أحد مواطني الدولة أو عندما ترتكب من أحد مواطني الدولة، وهذا نصت عليه المادة 2/15 من الاتفاقية.

كما نصت الدول كذلك من خلال تشريعاتها الداخلية على هذا المبدأ على النحو التالي:

---

[1]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص222.

[2]– حبيب عباسي، المرجع السابق، ص232.

أولا: بالنسبة للتشريع الفرنسي

إن القانون الفرنسي يأخذ بهذا المبدأ في جانبه الإيجابي والسلبي، فالجانب الإيجابي نصّت عليه المادة 6/113 ق.ع.ف على أن:" يطبق القانون الفرنسي على كل جناية يرتكبها فرنسي خارج إقليم الجمهورية، إذا كانت الوقائع المكونة لها معاقب عليها في قانون الدولة التي ارتكبت فيها، كما يسري هذا التطبيق حتى ولو كان المتهم قد اكتسب الجنسية الفرنسية بعد ارتكاب الواقعة المنسوبة إليه".

وعليه فإن المادة 6/113 ق.ع.ف يمكن أن تطبق على موقع دعارة الأطفال الذي ينشئه فرنسي في بلد أجنبي، شريطة أن يكون هذا معاقبا عليه هناك، كذلك لا ينعقد الاختصاص للقانون الفرنسي بالنسبة للمعلومات أو العبور غير المشروعة التي تبث من الخارج، إذا كانت هذه المعلومات مشروعة في بلد المنشأ[1].

أما فيما يخص الجانب السلبي فقد أخذ به المشرع الفرنسي في المادة 7/113 من ق.ع.ف على أن: " يطبق القانون الفرنسي على أية جناية، وكذلك على أي جنحة يعاقب عليها بالحبس يرتكبها فرنسي أو أجنبي في الخارج، إذا كان المجني عليه فرنسيا لحظة ارتكاب الجريمة".

فمعيار اختصاص القانون الفرنسي وفقا للمادة 7/113 من ق.ع.ف، هو أن يكون المجني عليه فرنسيا، من أجل حماية هذا الأخير ضد الجرائم التي تقع عليه في الخارج، ويترتب على ذلك أن فاعل الجريمة التي ترتكب بواسطة الأنترنيت على إقليم دولة أجنبية ضد مواطن فرنسي يحاكم في فرنسا، حتى ولو كان هذا الفعل غير معاقب عليه في البلد الأجنبي.

وعليه فإن تطبيق المادة 7/113 من ق.ع .ف، على جرائم دعارة الأطفال التي ترتكب على أحد مواقع شبكة الأنترنيت في الخارج، يقتضي إقامة الدليل على أنّ الشخص الذي تم عرض صوره على هذه الشبكة، وهو يمارس دعارة الأطفال، يحمل الجنسية الفرنسية[2].

ثانيا: بالنسبة للتشريع اليمني

أخذ المشرع اليمني بمبدأ الشخصية من خلال المادة 246 من ق.إ.ج.ي، والتي نصت على ما يلي:" تختص المحاكم اليمنية بمحاكمة كل يمني ارتكب خارج اقليم الدولة فعلا يعد بمقتضى القانون جريمة، إذا عاد إلى الجمهورية، وكان الفعل معاقبا عليه بمقتضى قانون الدولة الذي ارتكبت فيه".

---

[1]– جميل عبد الباقي الصغير، المرجع السابق، ص56–57.

[2]– جميل عبد الباقي الصغير، المرجع نفسه، ص58.

وعليه يطبق القانون الجزائي اليمني على كل من يحمل الجنسية اليمنية شريطة أن يكون الفعل المجرم في القانون اليمني مجرما أيضا في قانون البلد الذي أقترف فيه، وأن يعود هذا المتهم إلى اليمن في حالة ما إذا كان يمنيا وأن يكون النظر في الجريمة المرتكبة من قبل المحكمة المختصة بموجب طلب من النيابة العامة بعد إخطارها من الشخص المضرور، أو ببلاغ من سلطات القطر الذي ارتكبت فيه الجريمة[1].

ثالثا: التشريع المصري

ورد النص على مبدأ شخصية القانون الجزائي طبقا للتشريع المصري في المادة 3 من ق.ع .م والتي نصّت على أنه: " كــل مصري ارتكب وهو خارج القطر فعلا يعتبر جناية، أو جنحة في هذا القانون يعاقب بمقتضى أحكامه إذا عاد إلى القطر وكان الفعل معاقبا عليه بمقتضى البلد الذي ارتكب فيه".

وعليه فإن المشرع المصري أخذ بهذا المبدأ في شقه الإيجابي، ولا يعرف هذا المبدأ في شقه السلبي[2]، فجنسية المجني عليه لا تعتبر معيارا يحدد نطاق تطبيق النص الجزائي من حيث المكان.

وطبقا للمادة 4 من ق.ع.م " لا تقام الدعوى الجنائية على مرتكب جريمة أو فعل في الخارج إلا من النيابة العامة ولا تجوز إقامتها على من يثبت أن المحاكم الجنائية قد برأته مما أسند إليه وأنها حكمت عليه نهائيا واستوفى عقوبته".

فالاختصاص لا ينعقد للمحاكم المصرية تلقائيا بالنسبة للجرائم التي تقع في الخارج فيجب تحريكها إذن بمعرفة النيابة العامة، كما لا يجوز محاكمة الشخص عن فعله مرتين وهو ما نصّت عليه أيضا المادة 8/113 من ق.ع. ف[3].

---

[1]– فايز محمد راجح غلاب، المرجع السابق، ص386–387.

[2]– Art 113-8 de C.P.F : » Dans les cas prévus aux articles 113-6 et 113-7، la poursuite des délits ne peut être exercée qu'à la requête du ministère public. Elle doit être précédée d'une plainte de la victime ou de ses ayants droit ou d'une dénonciation officielle par l'autorité du pays ou e fait a été commis ».

[3]– كذلك هو الحال بالنسبة للمشرع الأمريكي أين أخذ بهذا المبدأ في شقه الإيجابي في المادة (3271) من قانون الجرائم والإجراءات الجنائية الأمريكي والمشرع العراقي في المادتين 10 و12 ق.ع.ع، وعدم الأخذ بهذا لمبدأ الشخصية في شقه السلبي من طرف كلا المشرعين يعد بمثابة ثغرة تشريعية يمكن من خلاله للمجرم الإلكتروني الإفلات من العقاب، فيما إذا لم تكن الجريمة معاقب عليها في قانون البلد الذي وقعت فيه أو فيما إذا تغاضت الدولة التي وقعت

رابـــعا: التشريـــــع الـــجزائري

اعتنق المشرع الجزائري مبدأ شخصية النص الجزائي، حيث جعل كل واقعة موصوفة بأنها جناية معاقب عليها في القانون الجزائري، ارتكبتها جزائري في خارج إقليم الجمهورية، يجوز أن تتابع ويحكم فيها في الجزائر.

غير أنه لا يجوز أن تجري المتابعة أو المحاكمة إلا إذا عاد الجاني إلى الجزائر، ولم يثبت أنه حكم عليه نهائيا في الخارج، وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة أو سقطت عليه بالتقادم، أو حصل العفو عنها، وهو ما نصت عليه المادة **582** ق.إ.ج.ج، فعنصر الجنسية هـو المحدد لسريان القانون الجزائري على الجرائم المرتكبة بالخارج استنادا إلى جنسية مرتكب الجريمة.

كما نصت المادة 583 ق.إ.ج .ج على أن:" كل واقعة موصوفة بأنها جنحة سواءا في نظر القانون الجزائري أم في تشريع الُقطر الذي ارتكبت فيه، يجوز المتابعة من أجلها والحكم فيها إذا كان مرتكبها جزائريا.

ولا يجوز أن تجري المحاكمة أو يصدر الحكم إلا بالشروط المنصوص عليها في الفقرة الثانية من المادة 582.

وعلاوة على ذلك فلا يجوز أن تجري المتابعة في حالة ما إذا كانت الجنحة مرتكبة ضد أحد الأفراد إلّا بناءا على طلب النيابة العامة بعد إخطارها من الشخص المضرور، أو ببلاغ من سلطات القطر الذي ارتكبت فيه الجريمة".

يفهم من ذلك أن المشرع الجزائري أخذ بمبدأ الشخصية في شقه الإيجابي، حيث يطبق النص الجزائي على كل جزائري يحمل الجنسية الجزائرية إذا توافرت الشروط التالية:

- وقوع جريمة موصوفة بأنها جناية معاقب عليها في القانون الجزائري.
- ارتكاب الجريمة خارج الإقليم الجزائري.
- أن يكون الفاعل يحمل الجنسية الجزائرية، حتى ولو اكتسبها بعد اقتراف الفعل.
- أن يعود الجاني إلى الجزائر بعد ارتكاب الجريمة.

فيها الجريمة عن ملاحقة الجاني ومعاقبته، مما يعني عدم إمكان اتخاذ أية إجراءات تحقيقيه في مواجهته. أنظر رشاد خالد عمر، المرجع السابق، ص102.

- أن لا يكون قد حكم عليه بحكم نهائي في الخارج، و أن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة، أو سقطت عنه بالتقادم، أو حصل العفو عنها.

كذلك هو الحال إذا كان الفعل يوصف بأنه جنحة شريطة تقديم شكوى من الطرف المضرور أو بلاغ من سلطات القطر الذي ارتكبت فيه الجريمة.

كما أخذ المشرع الجزائري بمبدأ الشخصية في شقه السلبي، حين أجاز متابعة ومحاكمة كل أجنبي وفقا لأحكام القانون الجزائري، ارتكب خارج الإقليم الجزائري بصفته فاعل أصلي أو شريك جناية أو جنحة إضرارا بمواطن جزائري، وهو ما نصت عليه المادة 588 ق.إ.ج.ج.

كـــذلك يتطلب مبدأ شخصية القانون الجزائري في حالة الجنايات أو الجنح التي ترتكب على متن طائرة أجنبية، إذا كان الجاني جزائري الجنسية، بغض النظر عـن مكان هبوط الطائرة، وبالتالي ينعقد الاختصاص لقانون العقوبات الجزائري طبقا للنص المادة 591 ق.إ.ج.ج.

والاختصاص القضائي وفقا لمبدأ الشخصية يثير العديد من المشكلات منها:

- عدم اختصاص قضاء الدولة في الجريمة المرتكبة في الخارج ممن يحمل جنسيتها، إذا لم تعتبر جريمة في الدولة المرتكبة فيها، فالاختصاص لا ينعقد بالنسبة للمعلومات، والصور التي تبث من الخارج، إذا كانت غير مجرّمة في بلد المنشأ حيث تم البث، مع أنها جريمة في الدول التي يصلها البث، وفي مثل هذه المسألة حينما لا يكون القانون الوطني مختصا في نظر الواقعة، تثار المشكلة بالنسبة لمن أصابه الضرر من الجريمة المرتكبة، حيث يجب عليه أن ينتقل إلى الدولة التي ارتكبت فيها الجريمة لرفع دعواه، وتثار المشكلة بصورة أكبر كـون الفعل غير معاقب عليه في هذه الدولة[1].
- كذلك العقاب على فعل وقع في الخارج يكون غير فعال، لأن تنفيذ العقوبة سوف يصطدم بعقبات كثيرة، ولا يمكن القول حينها بوجود اتفاقية تسليم المجرمين، لأن عدد الدول التي وقعت على هذه الاتفاقية بسيط مقارنة بعدد الدول المرتبطة بالأنترنيت.

[1]– فايز محمد راجح غلاب، المرجع السابق، ص388.

كما أن اتفاقية التسليم تقابلها عقبات، سواء بالنسبة لعدم تسليم المواطنين، أو بالنسبة لمبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرّة، لذلك يجب أن يكون هناك قانون جنائي دولي على غرار القانون الدولي الخاص ليطبق على الجرائم التي ترتكب على الأنترنيت أو بواسطتها[1].

الـــفرع الرابع: مبدأ عالمية القانون الجزائي

مقتضى هذا المبدأ هو سريان القانون الجزائي للدولة على بعض الجرائم المحددة في القانون فيما إذا تواجد مرتكبها على اقليمها، وبغض النظر عن جنسية المجني عليه أو صفة أو جنسية مرتكبيها وبغض النظر عن مكان ارتكابها[2].

ويمتاز هذا المبدأ بأنه يقرر للنص الجزائي نطاقا متسعا قد يشمل العالم كله، إذ لا يتقيد بمكان ارتكاب الجريمة، أو بجنسية مرتكبها، ولا يشترط سوى أن يقبض على الجاني في إقليم الدولة التي تريد أن تطبق عليه النص الجزائي الخاص بها[3].

وقد اختلف الفقهاء حول ما إذا كان الأخذ بهذا المبدأ واجبا على الدول أم حقا لها أم أنه الإثنان معا، وذلك نتيجة اختلاف اتجاه التشريعات الجزائية للدول بهذا الصدد[4].

ومما لا شك فيه أن مبدأ العالمية يكتسي أهمية بالغة مستمدة بالدرجة الأولى من خطورة ما وصل إليه حال الإجرام المعاصر، في ظل التطور التكنولوجي أين أتيحت الفرصة للمجرمين من جنسيات مختلفة بارتكاب جرائم مستحدثة، يمتد نشاطها إلى أقاليم دول عديدة، الأمر الذي يتطلب ضرورة أن

---

[1]– جميل عبد الباقي الصغير، المرجع السابق، ص60.

[2]– رشاد خالد عمر، المرجع السابق، ص103.

[3]– محمد حسن الكندري، المسؤولية الجنائية عن التلوث البيئي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005، ص331.

[4]– هذا الاختلاف هو نتيجة منطقية متأتية من حقيقة أن مبدأ العالمية له وجهان أحدهما إلزامي والآخر جوازي، فالوجه الإلزامي لهذا المبدأ يظهر في حقيقة أن الدولة يقع على عاتقها التزام بالنص في قانونها الجزائي فيما إذا تواجد مرتكبها أو أحد مرتكبيها في اقليمها بغض النظر عن جنسية الجاني والمجني عليه وبغض النظر عن مكان وقوع الجريمة، وذلك تطبيقا لاتفاقيات دولية صادقت هي عليها أو كانت طرفا فيها، أما الوجه الجوازي ومقتضاه أن لكل دولة الحق في أن تخضع بعض الجرائم المرتكبة في الخارج إلى قانونها الجزائي، باعتبارها جرائم خطيرة في نظرها، وذلك في حال تواجد مرتكبها في إقليمها وبغض النظر عن جنسية هذا الأخير وصفته أو جنسية المجني عليه، على أن لا يكون هناك طلب مسبق أو قبول مسبق بتسليمه من أو إلى الدولة التي وقعت فيها الجريمة. أنظر: رشاد خالد عمر، المرجع السابق، ص103 و105.

تتولى كل دولة متابعة ومعاقبة المجرم الذي يضبط في اقليمها، بوصفها نائبة عن المجتمع الدولي، دون إكتراث بالجنسية التي يحملها ولا بمكان وقوع الجريمة[1].

وما ينبغي تأكيده أيضا هو أن مبدأ العالمية، وإن كانت له أهمية كبيرة في إيضاح الكثير من المشاكل القانونية، في حالة ثبوت عدم كفاية المبادئ التقليدية في مجابهة أنواع معينة من الجرائم، إلا أن مباشرته تعتريها عدة صعوبات قانونية إجرائية، أهمها عدم توافر الأدلة الكافية والالتزامات التي تقع على عاتق الدولة الناظرة في الدعوى العمومية، التي تستدعي حماية خاصة للمجني عليه والشهود، وهو ما لا يتحقق إذا وقعت الجريمة خارج اقليمها[2].

ولقد نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلوماتية على هذا المبدأ في المادة 30/ 2 أين " تلتزم كل دولة طرف بتبني الاجراءات الضرورية لهذا الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة 1/31 من الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضرا في اقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

كما نصت اتفاقية الأمم المتحدة على هذا المبدأ في حالات معيّنة وذلك بموجب المادة 3/15 والتي تقتضي ضرورة أن "... تعتمد كل دولة طرف ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المشمولة بهذه الاتفاقية، عندما يكون الجاني المزعوم موجودا في اقليمها ولا تقوم بتسليم ذلك الشخص بحجة وحيدة هي كونه أحد رعاياها..."، كما أضافت الماد 4/15 من الاتفاقية أن تتخذ نفس التدابير " ... عندما يكون الجاني المزعوم موجودا في إقليمها ولا تقوم بتسليمه".

كما أضافت المادة 4 من نفس الاتفاقية على أن " تؤدي الدول الأطراف التزامها بمقتضى هذه الاتفاقية على نحو يتفق مع مبدأ المساواة في السيادة والسلامة الإقليمية للدول، ومع مبدأ عدم التدخل في الشؤون الداخلية للدول الأخرى.

ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في اقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصرا بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي".

مما يفهم أنه بالرغم من الأخذ بمبدأ العالمية كأساس لتحديد الولاية القضائية إلا أنه ليس هو الأصل.

---

[1]– حبيب عباسي، المرجع السابق، ص365.

[2]– حبيب عباسي، المرجع نفسه، ص367.

ومن التشريعات التي أخذت بمبدأ عالمية القانون الجزائي القانون الفرنسي في المادة 1/8/113 ق.ع. ف والتي تقضي بسريان قانون العقوبات الفرنسي على الجريمة المرتكبة في الخارج من قبل أجنبي، في حالة رفض فرنسا تسليم المتهم بناءا على طلب مقدم لها، شريطة أن توصف الجريمة بأنها جناية أو جنحة معاقب عليها بالحبس لمدة لا تقل عن خمس سنوات على أن يكون قد تم رفض طلب تسليمه من قبل السلطات الفرنسية بالنظر لخضوع الجريمة في الدولة الطالبة للتسليم إلى عقوبة أو تدبير احترازي يتعارض مع السياسات العامة الفرنسية أو يكون الجاني قد تمت محاكمته مسبقا في تلك الدولة أمام محكمة لا تحترم لا الضمانات الاجرائية الجوهرية ولا حقوق الدفاع أو بالنظر لكون الجريمة ذات طابع سياسي.

ولم يأخذ أي من المشرع المصري ولا الكويتي ولا الجزائري بمبدأ عالمية النص الجزائي بالرغم من أهميته مكتفين بمبدأ الشخصية والعينية كمبدأين مكملين لمبدأ الاقليمية.

وفي الأخير ينبغي أن نشير إلى أنه من الصعوبة إضفاء الصفة العالمية على كافة الجرائم الإلكترونية، لأنّ هذه الجرائم كثيرة ومتنوعة ومتجددة باستمرار بشكل لا يمكن معه السيطرة عليها وحصرها في جرائم محددة.

وبغية تحقيق هذا الأمر ينبغي على الدول أن تتكاثف فيما بينها وأن تلجأ إلى إبرام اتفاقيات دولية فيما بينها في سبيل تحديد الجرائم الإلكترونية التي تشكل تهديدا وخطرا على مصالحها المشتركة، ومن تم إلزام نفسها بإخضاع تلك الجرائم لقانونها الجزائي وفقا لمبدأ عالمية النص الجزائي هذا من جهة.

المطلب الثاني: التعريف بمشكلة الاختصاص لجهات التحقيق في الجريمة الإلكترونية

إن قواعد القانون الجنائي (بشقيه الموضوعي والإجرائي) تعد مظهرا من مظاهر سيادة الدولة، وبالتالي فإن تطبيقها من حيث المكان يخضع لمبدأ مستقر ألا وهو مبدأ الاقليمية[1].

ومع ما تتسم به الجرائم الإلكترونية من سمات وخصائص، وكونها جرائم عابرة لحدود الدول، وذات طبيعة عالمية التأثير والتدبير، فإنها تعد من أكثر الجرائم التي تثار بشأنها مشكلة الاختصاص القضائي بين الدول[2].

---

[1]– لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجية المعلوماتية، بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، بدون بلد النشر، 2017، ص61.

[2]– عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015، ص59.

فقد يقع تنازع[1] الاختصاص القضائي بين جهتين قضائيتين تابعتين لدولتين أين يوصف هذ التنازع بأنه خارجي، ذلك إما بسبب اختلاف التشريعات الجزائية في تحديد المقصود بمبدأ اقليمية القوانين، أو بسبب اعتناق المبادئ التي تسمح بتمديد الاختصاص للنظر في الجرائم الواقعة خارج إقليم الدولة، كما قد يقع بسبب الاختلاف في تحديد المقصود بالأفعال التنفيذية، ومكان وقوعها في الجرائم المستمرة والمتتابعة[2].

والأصل أن عناصر الركن المادي[3] للجريمة تكتمل في مكان واحد أي في نطاق إقليم دولة واحدة، حيث يقع السلوك الاجرامي وتترتب آثاره في إقليم دولة واحدة، وعلى ضوء ذلك يتحدد القانون الواجب التطبيق وبالتبعية للمحكمة المختصة بنظر الدعوى، بيد أن بعض الجرائم منها الجريمة الالكترونية يتجاوز مداها أحيانا حدود الدولة، حينما يتجزأ ركنها المادي أو يتوزع على أكثر من مكان بحيث يمكن وقوع السلوك في مكان، بينما تتحقق النتيجة الإجرامية الضارة في نطاق إقليم دولة أخرى[4]، مما يقودنا إلى التساؤل عن مكان وقوع الجريمة في هذه الحالة فهل هو مكان وقوع السلوك الإجرامي أم المكان الذي تحققت فيه النتيجة؟.

حاول الفقه الإجابة عن هذا التساؤل من أجل حل مشكلة تنازع القوانين من حيث المكان وأنقسم إلـــى ثلاثة اتجاهات كـــــالآتي:

---

[1]– التنازع قد يكون إيجابيا، بأن تدعي دولتان أو أكثر باختصاص كل منهما في الجرائم المرتكبة ولا تتنازل أية منهما عن اختصاصها للدولة الأخرى وقد يكون تنازعا سلبيا عندما تنكر كلا منهما ولاية قضائها بالجريمة، فهي لا ترغب في أن تتدخل سلطاتها القضائية في الجريمة المرتكبة. أنظر: فاطمة محمد العطوي، الإشكاليات التي يثيرها التعاون الدولي في المواد الجنائية، دار النهضة العربية، القاهرة، 2013، ص245.

[2]– حبيب عباسي، المرجع السابق، ص362، 363.

[3]– لا تقوم الجريمة كما نص عليها القانون، ولا يترتب عليها عقاب إلا إذا توافر ركنيها المادي و المعنوي، بالإضافة إلى ركنها الشرعي، والسلوك المادي في الجريمة الإلكترونية يتطلب وجود بيئة رقمية وجهاز كمبيوتر وإيصال بشبكة الأنترنيت، ويتطلب أيضا معرفة بداية هذا النشاط والشروع فيه ونتيجته، كما أن السلوك الإجرامي في الجرائم الإلكترونية يختلف حسب نوع الجريمة فأحيانا يكون نشاطا واحدا في الجرائم البسيطة، وأحيانا يكون سلوكا إجراميا متعددا ينطلق من الدخول إلى نظام الحاسب الآلي أو إلى موقع ما على شبكة الأنترنيت بوجه غير شرعي ثم القيام بالتلاعب بإحدى محتوياته، هذا التلاعب ينطوي على عدة أنشطة =إجرامية كمحو أو تدمير لمحتويات النظام، أنظر: معتوق عبد اللطيف، المرجع سابق، ص23. وأنظر أيضا: خالد ممدوح إبراهيم، الجرائم المعلوماتية، المرجع السابق، ص98 وما بعدها.

[4]– في هذه الحالة تثار مشكلة الاختصاص، لأن تحديد الجهة القضائية المختصة للتحقيق في مثل هذه الجريمة وكذا القانون الواجب التطبيق يتوقف على تحديد مكان وقوع الجريمة.

الفرع الأول: مذهب السلوك أو النشاط الإجرامي

وفقا لهذا المعيار، ينعقد الاختصاص للمحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه، بدعوى أن اتخاذ آثار الفعل كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات، يمكن إجمالها في أنه معيار مرن وفضفاض، فضلا عن أن معيار حصول النشاط أدى إلى تسيير عملية الإثبات وجمع الأدلة، وأن المحكمة التي لها ولاية النظر في الدعوى تكون قريبة من مسرح الجريمة، ناهيك أن الحكم الذي يصدر في الواقعة يكون أكثر فعالية ويسهل معه ملاحقة الجناة[1].

كما يضيف المؤيدون لهذا الاتجاه حججا أخرى، منها أن حدوث الضرر في مكان معين مرده في الغالب إلى أسباب، لا دخل لإدارة مقترف السلوك فيها، وأن من شأن تطبيق قانون الدولة التي تحقق في نطاقها الضرر لا يتفق واعتبارات العدالة نظرا لجهل الجاني بهذا القانون الذي يتم إعماله بحقه، وفي الغالب ليس ممكنا العلم به، إذ حينما أقدم على ارتكاب الفعل، يعتقد بمشروعيته وفقا لقانون البلد الذي وقع فيه السلوك، وإذا به غير ذلك من منظور قانون البلد الذي تحقق فيه الضرر[2].

ومن التشريعات التي تبنت هذا الاتجاه التشريع النمساوي الصادر سنة 1979 وكذا التشريع المجري الصادر في نفس السنة.

الـــــفرع الثاني: مذهب مكان تحقق النتيجة الإجرامية

على الرغم من الحجج التي ساقها مؤيدوا المذهب الأول، فإن هذا الاتجاه تعرض لجملة من الانتقادات من جانب آخر من الفقه، وقد انصبت هذه الانتقادات على أن هذا المذهب لا يعير اهتماما للمكان الذي تحقق فيه الضرر أو أثر النشاط الإجرامي الذي كان الجاني يسعى إلى تحقيقه فيه، فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، في حين أن مكان وقوع السلوك لا يعدو أن يكون مصدر الضرر ليس إلا، كما أن تمام الجريمة لا يكون إلا في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها.

---

[1]– أحمد عبد الكريم سلامة، قانون حماية البيئة، دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، السعودية، 1997، ص535.

[2]– كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، تخصص علوم قانونية ، كلية الحقوق والعلوم السياسية، فرع العلوم الجنائية، جامعة جيلالي اليابس، سيدي بلعباس، 2014–2015، ص334.

ضف إلى ذلك أن تقادم الجريمة يتم احتسابه من الوقت الذي تحققت فيه النتيجة، كما يؤخذ في الحسبان جسامة الضرر كأساس لتقدير التعويض ولا عبرة بخطورة الفعل أو درجة الخطأ، كذلك يعد حصول الضرر شرطا لقيام المسؤولية المدنية، فتنتفي هذه المسؤولية متى انتفى الضرر، ومن تم لا مصلحة للمدعي في الدعوى، ما يجعلها بالتالي غير مقبولة.

ومن المبررات التي سيقت لتعزيز هذا الاتجاه، أن الاخذ به يحقق وحدة الجريمة وعدم الفصل بين عناصرها، كذلك يمتاز هذا الاتجاه بأنه الأكثر واقعية على اعتبار أن الضرر له مظهر خارجي ملموس خلافا لنشاط الذي قد لا يكون كذلك إذا اتخذ صورة الامتناع أو السلوك السلبي[1].

ولقي هذا الاتجاه ترحيبا من بعض التشريعات المقارنة، منها القانون الألماني الصادر سنة 1975، والقانون الدولي الخاص التركي الصادر سنة 1982.

ومع ذلك لم يسلم هذا الاتجاه من النقد، حيث أن الأخذ به يفضي في نهاية المطاف إلى عدم تجريم الشروع إذا لم تتحقق النتيجة، وكذلك عدم العقاب على ما يعرف بالسلوك المجرد (جرائم السلوك المجرد).

الفرع الثالث: المذهب المختلط

أمام الانتقادات التي تعرض لها كلا من الاتجاهين السابقين، ظهر اتجاه ثالث مفاده أن الجريمة تعد واقعة في مكان حصول النشاط (العمل التنفيذي)، وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه، وهذا الاتجاه حظي بمباركة أغلب الفقه ويجد مبرّره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر، وهي الفعل أي النشاط، والنتيجة والعلاقة السببية، ما يعني أن الجريمة تعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي، أي في مكان النشاط ومكان النتيجة على حد سواء.

وهذا الاتجاه أخذت به بعض التشريعات المقارنة منها المشرع النرويجي، المشرع الإيطالي، لسنة 1930 والمشرع الدانماركي، كما تبنته محاكم بعض الدول كفرنسا، حيث ذهبت إلى أن اختصاصها

[1]– كمال حطاب، المرجع السابق، ص335.

يتسع ليشمل كل الأمكنة التي كانت مسرحا للجريمة عند وقوعها مقابل الوفاء فيها يخص صنّكا كان محررا خارج فرنسا ومسحوبا على أحد البنوك فيها[1].

ويتم تغليب قانون تحقق النتيجة إذا كانت الجريمة تامة، ومن قبيل ذلك جرائم السلوك والنتيجة، في حين يفضل مكان النشاط أو السلوك إذا كانت الجريمة قد وقفت عند حد الشروع أو كانت من قبيل جرائم السلوك المجرد[2].

وبالوقوف على المبررات التي استند إليها كل اتجاه مما تقدم وما يكتنفه من قصور، يرى كثير من الفقه أن الاتجاه الأخير يفضل على غيره، لكونه تجاوز المآخذ التي اعترت المذهبين الآخرين، وفي الوقت ذاته استجمع مميّزات كل منهما، فهو يوسع من نطاق الحماية الجزائية، ويتيح مرونة أكثر في مد نطاق الاختصاص، لا سيما وأن بعض الأفعال مجرمة في ذاتها، ولا ينجم عنها أي ضرر مادي، ومن هنا تمتد آثاره الضارة لدولة أو دول أخرى غير التي وقع فيها النشاط الأمر الذي يهدد مصالحا الحيوية، وربما يكون أكثر انسجاما مع الطبيعة المميزة للجرائم الإلكترونية وبما يكفل حل مشكلة تنازع الاختصاص، إذن مشكلة الاختصاص في الجرائم الإلكترونية أصبحت الحاجة فيها ملحة إلى إبرام اتفاقيات دولية ثنائية أو جماعية، يتم فيها توجيه وجهات النظر فيما يتعلق بقواعد الاختصاص القضائي، بالإضافة إلى تحديث القوانين الجنائية الموضوعية منها والإجرامية بما يتناسب والتطور الكبير التي تشهده تكنلوجيا المعلومات والاتصال[3].

ومشكلة الاختصاص القضائي تثار على المستوى الوطني أو الدولي، وتعني مشكلة الاختصاص المحلي (الوطني) في الجرائم الإلكترونية تنازع الاختصاص بين أكثر من جهة قضائية داخل إقليم الدولة، أما مشكلة الاختصاص الدولي فتعني تنازع الاختصاص بين أكثر من دولة.

أولا: مشكلة الاختصاص لجهات التحقيق عـــلى المستوى الـــــداخلي

تثار مشكلة الاختصاص القضائي المحلي بالنسبة للجرائم الإلكترونية، في حالة أن تكون الجريمة مرتكبة فـــي أكثر من نطاق اختصاص محلي داخل الاقليم الوطني للدولة.

---

[1]– موسى مسعود أرحومة، الاشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا طرابلس، ليبيا خلال الفترة 28-2009/10/29، ص18.

[2]– كمال حطاب، المرجع السابق، ص336.

[3]– عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، المرجع السابق، ص355.

وتثار أيضا حـــالة أن تكون الجريمة المرتكبة كلها على إقليم الدولة، بحيث لا يوجد قضاء أو قـانون لدولة أخرى ينازع قوانين تلك الدولة، أو اختصاصها القضائي.

فـــالمشكلة إذن تتعلق بالاختصاص القضائي المحلي في حالة أن تكون الجريمة قد ارتكبت بكاملها في نطاق الاقليم الوطني، إلا أنها في أكثر من نطاق اختصاص قضائي داخل الدولة، بسبب طبيعة الجريمة وبشبكة المعلوماتية.

فـــالجريمة وفقا لهذه الفرضية تكون قد ارتكبت بكامل أركانها في نطاق اختصاص المحاكم الوطنية، وهذه المشكلة يمكن القضاء عليها في حال أن يتم تمديد الاختصاص القضائي داخل إقليم الدولة بما يتناسب وطبيعة الجريمة المرتكبة، حيث يكون بإمكان أي دولة وضع أو تعديل النصوص القانونية الإجرائية التي تنظم الاختصاص القضائي فيها بما يتناسب مع كشف وضبط تلك الجرائم وملاحقة مرتكبيها[1].

ويطلق على الاختصاص الداخلي بالاختصاص الاقليمي باعتبار أن القضاء الوطني هو المختص في الفصل في الدعوى الجزائية، ويقوم على تحديد إطار جغرافي أو دائرة اختصاص مكاني تتحدد بمنطقة معينة من إقليم الدولة.

وبالتالي فإن فكرة الاختصاص الاقليمي أو المكاني تقوم على تقسيم إقليم الدولة إلى مناطق تم توزيعها بين المحاكم التي تنتمي إلى ذات النوع والدرجة، وأساس ذلك هو اتساع رقعة الاقليم واستحالة أن تختص به محكمة واحدة[2].

وقد حدد الاختصاص الإقليمي للمحاكم الجزائية[3]، استنادا إلى معايير ثلاثة هي: مكان وقوع الجريمة أو محل إقامة المجرم، أو محل القبض عليه[1].

---

[1]– فايز محمد راجح غلاب، المرجع السابق، ص375–376.

[2]– كامل سعيد، شرح قانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005، ص678.

[3]– وبالرجوع إلى قانون الإجراءات الجزائية الجزائري حدد الاختصاص المكاني للمحاكم بنص المادة 1/37 منه والتي تنص على ما يلي: "يتحدد الاختصاص المحلي لوكيل الجمهورية بمكان وقوع الجريمة، وبمحل إقامة أحد الأشخاص المشتبه في مساهمتهم فيها، أو بالمكان الذي تم في دائرته القبض على أحد هؤلاء الأشخاص حتى ولو حصل هذا القبض لسبب آخر".

كما أخـذ به المشرع الفرنسي في م 43 و52 ق.إ.ج.ف، والـــمشرع المصري في المادة 217 ق.إ.ج.م أما المشرع اليمني فأخذ به في نص المادة 234 ق.إ.ج.ي.

1- محكمة مكان وقوع الجريمة:

يعد معيار مكان وقوع الجريمة من أهم المعايير المعتمدة في تحديد الاختصاص المكاني للمحاكم الجزائية، فهو المعيار الأصل في تحديد الاختصاص المكاني، وذلك بالنظر لسهولة إجراء التحقيق وجمع الأدلة في مكان وقوع الجريمة[2] بمعنى آخر مكان وقوع الأفعال التنفيذية المكونة للجريمة أو جزء منها، وإذا وقعت هذه الأفعال في دائرة أكثر من محكمة، فإن الاختصاص يؤول لكل محكمة وقع فيها جزء من أعمال التنفيذ المعاقب عليها، كما هو الحال في الجرائم المستمرة التي يعتبر مكان وقوعها كل محل تقوم فيه حالة الاستمرار وكذلك الجرائم المتتابعة التي يعد مكانا لها كل محل يقع فيه أحد الأفعال الداخلة فيها[3].

فاختصاص مكان ارتكاب الجريمة هو الاختصاص الطبيعي لها، ففيه اختل الأمن واضطربت المراكز القانونية التي كانت مستقرة وأهدرت حقوق يحميها القانون[4].

2- محكمة محل إقامة المتهم:

يتحدد الاختصاص الاقليمي في القضاء الجزائي أيضا استنادا إلى محل إقامة المتهم أو المشتبه به، أو المشتبه فيهم في حالة تعددهم الذين يحول حولهم الشك في ارتكابهم لجريمة معينة.

وبمقتضى هذا المعيار فإن المحكمة التي يتواجد فيها مكان إقامة المتهم ضمن منطقة اختصاصها هي التي تختص بالتحقيق في الجريمة الواقعة[5].

ويلاحظ أن العبرة هنا ليس بالموطن[6] الذي هو في الأصل محل السكن الرئيسي، وإنما بمحل الاقامة أي بمسكنه المعتاد، وبشكل أدق محل الاقامة وقت ارتكاب الجريمة وليس وقت المحاكمة[7].

---

[1]– غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل شهادة دكتوراه في القانون، الجامعة الاسلامية، كلية الحقوق، لبنان، 2004، ص518.

[2]– رشاد خالد عمر، المرجع السابق، ص113.

[3]– حبيب عباسي، المرجع السابق، ص389. وأنظر أيضا: محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2008، ص44.

[4]– كامل سعيد، المرجع السابق، ص680.

[5]– رشاد خالد عمر، المرجع السابق، ص143-144.

[6]– للموطن عنصران: العنصر المادي: يتمثل في الإقامة الفعلية في مكان معين، والعنصر المعنوي: يرتبط بنية الاستقرار في ذلك المكان ويقوم محل الاقامة العادي محل الموطن.

[7]– حبيب عباسي، المرجع السابق، ص370.

وتبرز أهمية هذا الاختصاص حينما يكون مكان ارتكاب الجريمة أو المكان الذي قبض على المتهم فيه مجهولين أو كانا غير محددين، ومن المحتمل أن يغير المتهم موطنه بعد ارتكاب الجريمة، ففي هذه الحالة يبقى الاختصاص للمحكمة التي باشرت إجراءات القضية في دائرتها، وليس المحكمة التي انتقل إلى دائرتها[1]، ومثل هذا الأمر ممكن الوقوع في مجال الجرائم الإلكترونية في ظل صعوبة اكتشاف المكان الأصلي لوقوع هذه الجرائم في كثير من الأحوال، خصوصا فيما يتعلق بجريمة غسيل الأموال عبر شبكة الأنترنيت[2].

3- محكمة محل القبض على المتهم:

ومقتضى هذا المعيار أن المحكمة التي يتم إلقاء القبض على المتهم في منطقة اختصاصها هي التي تختص بالتحقيق في الجريمة التي ارتكابها هذا الأخير.

وتكمن أهمية هذا المعيار في إمكان الاعتماد عليه لتحديد الاختصاص المكاني في حال إذا لم يكن بالإمكان إعمال أي من المعيارين السابقين كأن يكون مكان وقوع الجريمة مجهولا، أو من دون أن يكون للجاني محل إقامة معروف، ومثل هذا الأمر متوقع في مجال الجرائم الإلكترونية بالنظر إلى الصعوبات والعوائق التي تعترض سبيل اكتشاف هذه الجرائم، واكتشاف مكان وقوعها وكذلك مكان إقامة الجاني بالنظر لتباعد مكان وقوع الفعل الإجرامي فيها عن مكان تحقق نتيجتها الجرمية اللذان قد تفصل بينهما آلاف الأميال في أغلب الأحوال.

كما وتكمن أهمية هذا المعيار أيضا في أنه يساعد في الحفاظ على الأدلة التي يعثر عليها بحوزة المتهم ويحقق أكبر قدر ممكن من الحماية لها، خصوصا فيما لو كان يتخوف عليها من التعرض للإتلاف أو الضياع في حالة نقلها، والأدلة الإلكترونية كغيرها من الأدلة التي يتخوف عليها من المحو والإتلاف نتيجة نقلها[3].

---

[1]– كامل سعيد، المرجع السابق، ص683.

[2]– غسيل الأموال عبر شبكة الأنترنيت جريمة ناتجة عن أعمال وأنشطة إجرامية حققت عوائد مالية ضخمة من الأموال القذرة الناتجة عن أعمال غير شرعية يعاد ضخها في الاقتصاد العالمي عبر شبكة الأنترنيت باستخدام النقود الإلكترونية أو بطاقات= =السحب التي تحمل أرقاما سرية بالشراء عبر الأنترنيت، أو تداول الأسهم وغيرها، من الأنشطة التجارية والمالية التي تتم عبر شبكة المعلومات الدولية.

[3]– رشاد خالد عمر، المرجع السابق، ص115.

ومن خلال ما سبق ذكره يتضح بأن الاختصاص القضائي المكاني يتطلب توافر حالة من الحالات الثلاثة التالية[1] :

أ- أن تكون الجريمة قد اقترفت بكاملها، أو أحد عناصر الركن المادي لها، أو تحقق صورة من صور الاستمرار بالنسبة للجريمة المستمرة، أو أي فعل من أفعال الاعتياد أو التتابع بالنسبة للجريمة المركبة، أو أي عمل من أعمال البدء في التنفيذ بالنسبة للشروع في دائرة الاختصاص المكاني لعضو النيابة العامة أو قاضي التحقيق.

ب- أن تكون إقامة المتهم أو المشتبه به، أو إقامة أحد المشتبه بهم في دائرة اختصاص عضو النيابة العامة أو قاضي التحقيق، و يتحدد مكان الإقامة بوقت إتيان الجريمة.

جـ- أن يكون قد ألقي القبض على أحد المتهمين أو المشتبه بهم في نطاق تلك الدائرة[2] .

وعليه يسري الاختصاص القضائي وفقا للقواعد التقليدية على الجرائم الإلكترونية إذ يمكن تطبيق أي معيار من المعايير السالفة الذكر عليها سواءا تمثلت بمكان وقوع الجريمة أو بمحل إقامة المتهم أو المشتبه به ، أو بمكان القبض عليه.

من هنا يظهر جليّا بأن المشرع الجزائري على غرار باقي المشرعين، قد عمد إلى توسيع الأسس التي ينبني عليها تحديد الاختصاص الإقليمي للجهات القضائية الجزائية في النظر في الدعاوى العمومية [3]، غير أن ذلك لم يكن كافيا لضمان مكافحة ناجعة لبعض الجرائم وهو ما دفعه إلى تمديد الاختصاص بشأن بعض الجرائم منها الجريمة الإلكترونية [4].

---

[1]- فايز محمد راجح غلاب، المرجع السابق، ص375.

[2]- في هذا الصدد نصت المادة 1/329 من القانون رقم(04-14) المؤرخ في 10 نوفمبر 2004 الجريدة الرسمية العدد71، ص6، المعدل والمتمم لـــ ق.إ.ج.ج أنه : " تختص محليا بالنظر في الجنحة محكمة محل الجريمة، أو محل إقامة أحد المتهمين، أو شركائهم، أو محل القبض عليهم، ولو كان هذا القبض قد وقع لسبب آخر".

[3]- يمكن تعريف الدعوى العمومية: بأنها ذلك الطلب الموجه من الدولة مثلة في جهاز النيابة العامة إلى المحكمة بغرض توقيع العقاب على المتهم الذي ارتكب جريمة في حق المجتمع، أنظر: عبد الرحمن خلفي، المرجع السابق، ص89.

[4]- حبيب عباسي، المرجع السابق، ص370.

هـذا التمديد أملته حالات وضرورات قانونية وعملية استلزمت أن يخرج فيها المشرع عن القواعد العامة في الاختصاص أين يتحدد هذا الاختصاص الإقليمي في القضاء الجزائي استنادا إلى المعايير الثلاث، وذلك بتقرير امتداد إحدى المحاكم الجزائية بالنظر في قضايا لم تكن أصلا من اختصاصها[1].

فبموجب التعديل الذي أجري على قانون الإجراءات الجزائية بالقانون رقم 14/04 المؤرخ في 10 نـوفمبر 2004 فـي المـادة 2/40 منـه[2]، قـام المشـرع الجزائـري بتوسـيع الاختصـاص المحلـي لـبعض المحـاكم ووكـلاء الجمهوريـة وقضـاء التحقيق بـالنظر فـي بعض الجـرائم التـي تـدخل فـي الأصـل فـي الاختصـاص الإقليمـي لمحـاكم أخـرى، وهـذه الجـرائم حـددها المشـرع علـى سـبيل الحصـر منهـا الجـرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بالإضافة إلى جرائم الفساد بموجب المادة 24 مكرر من قانون الوقاية من الفساد ومكافحته[3] إثر تعديله سنة 2010 بالأمر 05/10.

إن هذه التعديلات الواردة بقانون الإجراءات الجزائية والمتعلقة بتوسيع اختصاص جهات المتبعة والتحقيق وبالتالي الحكم كلما تعلق الأمر بجرائم المساس بنظام المعالجة الآلية للمعطيات كانت بهدف وضع إطار إجرائي متماسك بإمكانه التحري والفصل في هذا النوع من القضايا بكل مهنية لإنجاز هذا الغرض يفترض أن تكون هذه الجهات معززة بقضاء متخصصين في جميع المجالات[4].

وعلى هذا الأساس يواجه قطاع العدالة عدة صعوبات في مجال مكافحة الإجرام المعلوماتي تتمثل في قلّة خبرة السلطات الأمنية وأجهزة العدالة نظرا إلى ندرة التطبيقات القضائية في هذا الشأن هذا من جهة، ومن جهة أخرى صعوبة إقامة الدليل على ارتكاب هذه الجرائم، وفي حالة الحصول على الدليل يصعب القبض على المجرمين نظرا إلى كون الفعل يرتكب في بلد والنتيجة تتحقق في بلد آخر [5].

---

[1]– حبيب عباسي، المرجع السابق، ص370. وأنظر أيضا: كامل سعيد، المرجع السابق، ص687.

[2]– تنص المادة 2/40 من ق.إ.ج.ج، علـــى ما يلي: " يتحدد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص، عن طريق التنظيم في جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف".

[3]– القانون رقم 01/06 المؤرخ في 20 فبراير 2006، المتعلق بالوقاية من الفساد ومكافحته، جريدة رسمية للجمهورية الجزائرية، العدد 14، بتاريخ 18 مارس 2006، المعدل والمتمم.

[4]– نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017، ص216.

[5]– نجاة بن مكي، المرجع نفسه، ص216.

ولقد جاء المرسوم التنفيذي رقم 06-348[1] ليحدد المحاكم المعنية بالتمديد والنطاق المكاني الذي أصبح يدخل ضمن اختصاصها، عندما يتعلق الأمر ببعض المحاكم التي على أساسها تم التمديد.

من خلال استقرار أحكام هذا المرسوم التنفيذي، يتضح بأن الاختصاص المحلي لبعض المحاكم يكون على النحو التالي:

أ- **محكمة سيدس أمحمد:** يمتد الاختصاص المحلي لمحكمة سيدي أمحمد ليشمل اختصاص محاكم المجالس القضائية للجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة وعين الدفلى[2].

ب- **محكمة قسنطينة** : يمتد الاختصاص المحلي لمحكمة قسنطينة ليشمل اختصاص محاكم المجالس القضائية لقسنطينة ، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس وميلة[3].

جـ- **محكمة ورقلة:** يمتد الاختصاص المحلي لمحكمة ورقلة ليشمل اختصاص محاكم المجالس القضائية لورقلة، أدرار، تمنراست، إليزي، تندوف وغرداية[4].

د- **محكمة وهران** : يمتد اختصاص المحلي لمحكمة وهران ليشمل اختصاص محاكم المجالس القضائية لوهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيض، تسمسيلت، النعامة، عين تموشنت وغليزان[5].

كما يختص رئيس المجلس القضائي الذي تقع في دائرة اختصاصه المحكمة التي تم تمديد اختصاصها بالفصل بموجب أمر لا يقبل أي طعن في الإشكالات التي قد تثيرها تطبيق أحكام التمديد وهو ما نص عليه المادة 6 من المرسوم 348/06.

---

[1]- المرسوم التنفيذي رقم 348/06 مؤرخ في 12 رمضان 1427 الموافق لـ 5 أكتوبر 2006، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، جريدة رسمية للجمهورية الجزائرية، العدد63 بتاريخ 8 أكتوبر 2006.

[2]- أنظر المادة 2 من المرسوم التنفيذي 348/06.

[3]- أنظر المادة 3 من المرسوم نفسه.

[4]- أنظر المادة 4 من المرسوم نفسه.

[5]- أنظر المادة 5 من المرسوم نفسه.

كما اشترط المشرع الجزائري ضرورة مراعاة أحكام معينة من أجل اتساع العمل بين مختلف الجهات القضائية ولضمان عدم التنازع بين المحكمة المختصة أصالة، استنادا إلى القواعد العامة والمحكمة التي أصبحت مختصة نتيجة تمديد اختصاصها المحلي، تتجلى هذه الأحكام فيما يلي[1]:

- قيام ضباط الشرطة القضائية بالإخبار الفوري لوكيل الجمهورية لدى المحكمة الكائن بها مكان الجريمة، ويبلغونه بأصل ونسختين من إجراءات التحقيق، يرسل هذا الأخير فورا النسخة الثانية إلى النائب العام لدى المجلس القضائي التابعة له المحكمة المختصة[2].
- يطالب النائب العام فورا باتخاذ الإجراءات، وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص المحكمة الممدد اختصاصها، التعليمات مباشرة من وكيل الجمهورية لدى هذه المحكمة[3].
- طلب النائب العام لمباشرة الإجراءات يكون في جميع مراحل الدعوى[4] ، أما في حالة فتح تحقيق قضائي، فإن قاضي التحقيق التابع للمحكمة المختصة في الأصل يصدر أمرا بالتخلي عن الإجراءات لفائدة قاضي التحقيق لدى المحكمة المختصة.

---

[1]– حبيب عباسي، المرجع السابق، ص372.

[2]– أنظر المادة 40 مكرر/ 1 من ق.إ.ج.ج.

[3]– أنظر المادة 40 مكرر/ 2 من ق.إ.ج.ج.

[4]– يمكن إيجاز مراحل الدعوى على النحو التالي:

أ– مرحلة الاتهام: وهي المرحلة الأولى من مراحل الدعوى العمومية وبها تتحرك هذه الأخيرة وتقوم بها النيابة العامة باعتبارها سلطة إتهام، ويتم هذا الإجراء بالطرق التالية:

- إما عن طريق التكليف بالحضور للجلسة خاصة في المخالفات والجنح البسيطة.
- إما بإجراءات التلبس.
- إما عن طريق طلب افتتاحي لإجراء تحقيق أمام قاضي التحقيق.

ب – مرحلة التحقيق الابتدائي: تهدف هذه المرحلة إلى جمع أكبر قدر ممكن من الأدلة عن الجريمة، يتولى هذه المرحلة قاضي التحقيق باعتباره السلطة المختصة بالتحقيق، وما تجدر الإشارة إليه أن التحقيق وجوبي في الجنايات واختياري في الجنح طبقا لنص المادة 66 ق.إ.ج.ج.

جـ– مرحلة المحاكمة: ويطلق عليها مرحلة الفصل في الدعوى، وتكون بيد قاضي الحكم، وتشمل جميع الإجراءات التي تباشر أمام قضاء الحكم منذ دخول الدعوى في حوزة المحكمة إلـــى غاية صدور الحكم النهائي والبات فيها.

وتدخل ضمن هذه المرحلة الدعوى المقامة أمام محكمة أول درجة أو المنظور فيها على مستوى ثاني درجة بالمجلس القضائي، أو على مستوى المحكمة العليا.

وتتصل المحكمة بالدعوى بطرق مختلفة:

وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة التعليمات مباشرة من قاضي التحقيق بهذه الجهة القضائية[1]، مع إمكانية الأمر باتخاذ كل إجراء تحفظي أو تدبير أمن زيادة على حجر الأموال المتحصل عليها من الجريمة أو التي استعملت في ارتكابها، سواءا من تلقاء نفسه أو بناءا على طلب النيابة العامة[2].

إذا صدر ضد المتهم أمر بالقبض أو أمر بالحبس المؤقت، فإن هذا الأمر يحتفظ بقوته التنفيذية إلى أن تفصل فيه المحكمة المختصة، أصبحت مختصة نتيجة تمديد اختصاصها[3].

وتمديد الاختصاص الإقليمي لم يقتصر على الجهات المذكورة سابقا بل مسّ كذلك ضباط الشرطة القضائية[4] إذا تعلق الأمر ببعض الجرائم الخطيرة، حيث نص القانون الجزائري على أن اختصاص ضباط الشرطة القضائية كاستثناء يمتد إلى كامل الإقليم الوطني إذا تعلق الأمر بالبحث والتحري عن جرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية

- إما بتكليف المتهم بالحضور أمامها عن طريق النيابة العامة.
- إما بإحالته من طرف النيابة العامة بإجراءات التلبس.
- إما بتكليف المتهم بالحضور أمامها بإجراء التكليف المباشر بالحضور من طرف الضحية.
- أو بإحالة الدعوى إليها من طرف قاضي التحقيق أو غرفة الاتهام.

والمحكمة أثناء نظر الدعوى تجري تحقيقا يطلق عليه التحقيق النهائي، أنظر: عبد الرحمن خلفي، المرجع السابق، ص91-92.

[1]- أنظر المادة 40 مـــكرر/3 ق.إ.ج.ج.

[2]- أنظر المادة 40 مـــكرر/5 ق.إ.ج.ج.

[3]- أنظر المادة 40 مـــكرر /4 ق.إ.ج.ج.

[4]- من مهام ضباط الشرطة القضائية تلقي البلاغات والشكاوي طبقا للمادة 17 من ق.إ.ج.ج ، غير أنه نتيجة التطور التكنولوجي ظهرت هناك صور جديدة للتبليغ مثل التبليغ عن طريق البريد الإلكتروني والتبليغ من خلال مواقع مخصصّة لذلك: مثل مركز الشكاوى الخاص الأنترنيت **(IC3)** هو كناية عن نظام التبليغ وإحالة لشكاوى الناس في الولايات المتحدة الأمريكية، ومثاله أيضا الجهاز التابع للشرطة الدولية – الأنتربول- المسمى SCOCI (Service De Coordination De La Lutte Contre La Criminalité Sur Internet=) و بالتالي نرى بأن هناك تأخر في الجزائر بخصوص تطوير وسائل تلقي البلاغات لاسيما فيما يتعلق بالجرائم الإلكترونية، أما الشكوى قد تكون كذلك أمام قضاة النيابة العامة طبقا لنص المادة 36 من ق.إ.ج.ج، كما قد تكون في شكل شكوى مصحوبة بادعاء مدني أمام قضاة التحقيق المادة 72 ق.إ.ج.ج.

للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف إلى كامل الإقليم الوطني[1].

كما أجاز القانون لضباط الشرطة القضائية وتحت سلطتهم أعوان الشرطة القضائية أن يمتدوا عبر كامل الإقليم الوطني، عمليات مراقبة الأشخاص الذين يوجد ضدهم مبرر مقبول أو أكثر يحمل على الاشتباه في ارتكابهم الجرائم المذكورة أعلاه ما لم يعترض على ذلك وكيل الجمهورية المختص بعد إخباره[2].

أما فيما يخص تمديد الاختصاص لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عندما يتعلق الأمر بالجرائم السالفة الذكر فنصت عليه المادة 2/37 من ق.إ.ج.ج، و كذلك هو الأمر بالنسبة لقاضي التحقيق، ولو كان القبض على المتهم حصل لسبب آخر وهو ما نصت عليه المادة 40 من ق.إ.ج.ج.

وعليه يمكن القول بأن المشرع الجزائري ساير التطور الحاصل في التشريعات الجزائية بخصوص تمديد الاختصاص الإقليمي للأجهزة المكلفة بالاستدلال والتحقيق في الجريمة الإلكترونية، لأن متابعة وكشف هذه الجرائم تحتاج إلى السرعة قبل أن يقوم الجاني بمحو أو تعديل أو التلاعب بالبيانات.

كما أن المشرع الجزائري لم يقتصر على تمديد الاختصاص القضائي بمفهومه التقليدي بل أجاز تمديد الاختصاص والقيام ببعض الإجراءات عن بعد في حال تطلب الأمر تفتيش المنظومة المعلوماتية عن بعد وكذلك حجز المعطيات[3]، وهو ما نصت عليه المادة 5 من القانون 04/09 [4].

---

[1]– أنظر المادة 16 من ق.إ.ج.ج.

[2]– أنظر المادة 16 مكرر من القانون نفسه.

[3]– فايز راحج محمد غلاب، المرجع السابق، ص378.

[4]– تنص المادة 5 من القانون رقم: 04/09 السابق الذكر على أنه : " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش، ولو عن بعد إلـــــى:

أ– منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب– منظومة تخزين معلوماتية.

في الحالة المنصوص عليها في الفقرة "أ"من هذه المادة، إذا كانت هناك أسباب تدعوا للاقتصاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى، وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة ، أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك...".

كما يمكن اللجوء إلى المراقبة الإلكترونية للوقاية من الأفعال الموصوفة لجرائم الإرهاب أو لتخريب أو الجرائم الماسة بأمن الدولة، حيث يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية المنتمين للهيئة المنصوص عليها في المادة 13 أدناه[1]، إذن (رخصة) لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[2].

وتظل مشكلة الاختصاص القضائي الوطني قائمة على مستوى الإقليم الوطني بالنسبة للجرائم المعلوماتية قائمة بالنسبة لبعض التشريعات منها التشريع اليمني، حيث لم يرد نص قانوني يتضمن تمديد الاختصاص القضائي إلى كافة الإقليم في حالة إن يتطلب الأمر ذلك، وبالتالي على المشرع تضمين نصوصه ما يوسع من امتداد الاختصاص القضائي لكافة الإقليم الوطني بالنسبة للإجراءات المتخذة بخصوص الجرائم الإلكترونية أسوة بالتشريع الجزائري، وذلك أثناء قيامه بوضع نصوص قانونية لمواجهة هذه الجريمة المستحدثة موضوعيا وإجرائيا[3].

ثانيا: مشكلة الاختصاص لجهات التحقيق على المستوى الدولي

تثار مشكلة الاختصاص القضائي الدولي بالنسبة للجرائم الإلكترونية بصورة أكبر مما هي عليه على مستوى إقليم الدولة الواحدة، حيث يكون بإمكان الدولة وضع حل للمشكلة على المستوى الوطني أو المحلي من خلال النصوص القانونية التي يمكن إقرارها بهذا البلد أو ذلك لأن الجريمة محصورة في النطاق الإقليمي للدولة، ومعالجتها يرتبط بكل دولة على انفراد، بخلاف مشكلة الاختصاص القضائي على المستوى الدولي، لأن الجريمة في هذه الحالة لا ترتبط بحدود إقليمية لدولة ما ، بل العكس من ذلك فهي جريمة عابرة للحدود، بالإضافة إلى اختلاف التشريعات والنظم القانونية من دولة إلى أخرى في مواجهة تلك الجرائم[4].

---

[1]– تنص المادة 13 من القانون 04/09 على ما يلي: " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحته، تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

[2]– أنظر المادة 04 من القانون نفسه.

[3]– فايز محمد راجح علاب، المرجع السابق، ص378.

[4]– فايز محمد راجح علاب، المرجع نفسه، ص379.

أما عن الاختصاص القضائي الدولي فيقصد به: " سلطة محاكم كل دولة في أن تنظر دعاوى معينة"[1].

ويقصد به أيضا: " بيان الحدود التي تباشر فيها الدولة سلطاتها القضائية بالمقابلة مع الحدود التي تباشر فيها الدول الأخرى سلطاتها القضائية، ولما كانت الدولة تباشر سلطاتها القضائية بواسطة محاكمها، كان معنى الاختصاص القضائي الدولي بيان الحدود التي تباشر فيها محاكم دولة معينة وظيفة القضاء بالمقابلة مع الحدود التي تباشر فيها محاكم الدول الأجنبية هذه الوظيفة[2].

فقد يحدث أن ترتكب جريمة في إقليم دولة معينة ويكون مرتكب الجريمة أجنبيا، فتخضع هذه الجريمة للاختصاص الجنائي للدولة الأولى استنادا إلى مبدأ العينية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن وسلامة دولة أخرى فتخضع عندئذ لاختصاصها استنادا لمبدأ العينية[3].

المبحث الثاني: تفعيل دور أجهزة التحقيق في الجريمة الإلكترونية

كسرت الجريمة الإلكترونية الحواجز الجغرافية وتغلبت على القواعد التي تحكم مفهوم المكانية للجريمة، يرتكبها شخص ذا دوافع مختلفة بين الانتقام والاحتيال والسرقة والفضول والتحدي والإرهاب وغيرها، والمؤكد أنه شخص متميز ذكاءا ذا دراية بأحدث ما توصلت إليه التقنية الرقمية من تقدم لن يكتشف أمره إلا شخص لابد أن يعادله خبرة ومهارة وفنا، لهذا فالدول أعدت العدّة وجهزت الوسائل وعززت التعاون بينها كل ذلك لتخصيص إطارات وكفاءات تعمل على البحث والتحري والتحقيق ومكافحة الجريمة الإلكترونية عامة.

كما تختلف الجريمة الإلكترونية عن العادية من حيث تكوينها وارتكابها وآثارها ونطاقها فلابد أن يكون الاستعداد لمكافحتها متناسبا مع طبيعتها، فتم إنشاء أجهزة متخصصة بهذه الجرائم تعمل بها أطر بشرية تم تكوينها وتدريبها لتفعيل دور تلك الأجهزة في سبيل مكافحة الجريمة الإلكترونية، ورغبة من المشرعين من موازنة المعادلة التي يعتبر أحد أطرافها قراصنة محتالون يواكبون كل تطور في

---

[1]– عادل عبد العادل إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع سابق، ص59.

[2]– عز الدين عبد الله، القانون الدولي الخاص، الجزء الثاني (تنازع القوانين وتنازع الاختصاص القضائي الدوليين، الطبعة الثامنة، دار النهضة العربية، القاهرة، 1977، ص605.

[3]– جميل عبد الباقي الصغير، المرجع السابق، ص73.

مجال التقنية الرقمية وطرفها الثاني رجال تحقيق مع نقص خبرة وقدرة على البحث والتحري في بيئة رقمية افتراضية.

لهذا سيتم تقسيم هذا المبحث إلى مطلبين: المطلب الأول (إعتماد نظام التكوين لتفعيل التحقيق الجنائي) والمطلب الثاني(إعتماد نظام التدريب لتفعيل التحقيق في الجريمة الإلكترونية.)

المطلب الأول: إعتماد نظام التكوين لتفعيل التحقيق الجنائي

تعتبر الكفاءة والعناية والتكوين من المستلزمات الأولية للممارسة السليمة للمهمة القضائية، فأمام تطور إستعمال التكنلوجيا الحديثة وظهور الجريمة الإلكترونية، تم استحداث جهات قضائية للنظر في هذه الجريمة أمام التزايد الكبير لها ومساسها بالحياة الشخصية للأفـراد.

فعمليات التكوين يستفيد منها جميع القضاة، حيث تهدف إلى تمكين المستفيدين منها من اكتساب وتطوير معارفهم ومهارتهم وخبراتهم العلمية بغرض الرفع من مردوديتهم المهنية وتحسين مسارهم المهني طبقا للحاجات المستجدة، إلى جانب دعم القدرات المهنية للقضاة في ميدان تتبع هذه النوعية من الجرائم والبحث والتحقيق والحكم فيها وفي ميدان التعامل مع الأدلة الإلكترونية.

لهذا عمدت الدول على تكوين أطر يعملون ضمن جهات متخصصة بين الوطنية والدولية وذلك لتفعيل التحقيق في الجريمة الإلكترونية لما لهذه الأخيرة من سمات تجعل من أفراد التحقيق غير قادرين على التحكم في التحقيق فيها دون إدراك للتقنية المعلوماتية.

وتختلف هذه الأجهزة عن الأجهزة المختصة بضبط الجرائم التقليدية من حيث طريقة التكوين فهي لا تعتمد على التدريبات الجسدية وإنما تعتمد على البناء العلمي والتكنلوجي، كما لا يقتصر دورها على المستوى الوطني(الفرع الأول) ، بل هناك أيضا أجهزة متخصصة على المستوى الدولي في الجرائم الإلكترونية(الفرع الثاني).

الفرع الأول: الأجهزة الوطنية المختصة بالتحقيق في الجريمة الإلكترونية

ظهرت العديد من الأجهزة المختصة في مجال الجريمة الإلكترونية على المستوى الوطني سواءا على صعيد الدول الأجنبية أم على صعيد الدول العربية لمكافحة هذه الجريمة والتحقيق فيها نظرا لما تمتاز به هذه الجريمة من خاصية تختلف عن الجريمة التقليدية.

أولا: الأجهزة المختصة في الدول الأجنبية

كانت الدول المتقدمة سباقة بإحداث هذه الأجهزة، إذ أن مكافحة الجرائم الإلكترونية يرتبط بمدى تقدم الدول من الناحية التقنية، وبمدى توفر الإمكانيات المادية اللازمة لإنشاء هذه الأجهزة[1].

1- **الولايات المتحدة الأمريكية** : قامت الولايات المتحدة الأمريكية بإنشاء عدّة أجهزة لمكافحة الجرائم الإلكترونية منها:

أ- **شرطة الوب:** وهي نقطة مراقبة على الأنترنيت، إضافة إلى أنها تتلقى الشكاوى من مستخدمي الشبكة، وملاحقة الجناة والقراصنة، والبحث عن الأدلة ضدهم وتقديمهم إلى المحاكمة[2].

ب- مركز تلقي شكاوى جرائم الأنترنيت "**IC_3**"[3]: تم إنشاؤه من قبل مكتب التحقيقات الفيدرالي **F.B.I** في سنة 2000، وفي سنة 2003 تم دمج مركز شكاوى الاحتيال عبر الأنترنيت المعروف بـ **IFCC**[4] مع هذا المركز، ويعمل مركز IC_3 بصورة تشاركية مع مكتب التحقيقات الفيدرالي والمركز الوطني لجرائم الياقات البيضاء NW_3C[5]، ويقوم هذا المركز بتلقي الشكاوى عبر موقعه على الأنترنيت، حيث يقوم الشاكي بملأ استمارة إلكترونية، ثم يقوم المختصون في هذا المركز بتحليل الشكاوى وربطها بالشكاوى الأخرى المسلّمة من قبل ثم يتم إحالة المعلومات الناتجة عن عملية التحليل إلى الجهات المسؤولة عن تطبيق القوانين الأمريكية.

جـ- قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية: يختص بالتعريف بهذه الجرائم والكشف عنها وملاحقة مرتكبيها[6].

د- نيابة جرائم الحاسوب والاتصالات CTC[7] : تتألف من مجموعة من قضاة النيابة العامة الذين تلقوا تدريبات مكثفة على نظم المعالجة الآلية للبيانات، وتم منحهم صلاحيات واسعة في مجال

---

[1]- محمد طارق عبد الرؤوف الخن، المرجع السابق، ص232.

[2]- محمد طارق عبد الرؤوف الحن، المرجع نفسه، ص 232.

[3]- "IC_3" : اختصار لـــــ: Internet Crime Complaint Center.

[4]- IFCC : اختصار لـــــ: Internet Fraude Complaint Center .

[5]- NW_3C : اختصار لـــــ: National White Coliart Center.

[6]- سعيداني نعيم، المرجع السابق، ص105.

[7]- CTC اختصار لـــــ: Computer And Télécommunication Coordinat.

الاستعانة بغيرهم من خبراء لا سيما قسم جرائم الحاسوب والعدوان على حقوق الملكية الفكرية، وهم مرتبطون بنظام تأهيلي وتدريبي مستمر [1].

هـ- المركز الوطني لحماية البنية التحتية: التابع للمباحث الفيدرالية الأمريكية، وقد حدد هذا المركز البنى التحتية التي تعتبر هدفا للهجومات والاعتداءات عبر الأنترنيت وعلى رأسها شبكات الإتصالات والمصارف وغيرها.

بالإضافة إلى هذه الأجهزة يوجد في الولايات المتحدة الأمريكية، وحدة متخصصة بمكافحة الإجرام المعلوماتي تابعة لقسم العدالة الأمريكي تتكون من خبراء في نظم الحوسبة و الأنترنيت، ومن مستشارين قانونيين.

2- **فرنسا:** تعتبر فرنسا من الدول التي اهتمت بتطوير قوانينها الجنائية للتوافق مع المستجدات الإجرامية لمكافحة الجريمة الإلكترونية، حيث قامت الحكومة الفرنسية بإنشاء عدة أجهزة لمكافحة الجرائم الإلكترونية، نذكر منها:

أ- الهيئة الوطنية لمكافحة الجرائم المتصلة بتكنلوجيا الإعلام والاتصال LOCLCTIC[2]:

تم إنشاء الشرطة الوطنية[3] في 15 ماي 2000، وهي مصلحة دولية تتكون من رجال الشرطة والدرك الوطني، مهامها متابعة الجرائم المرتكبة مباشرة بالأنترنيت، والجرائم التي تكون الأنترنيت وسيلة لارتكابها، وتعمل الشرطة الوطنية على التحقيق في: الاحتيال الهاتفي، تزوير بطاقة الائتمان، الاحتيالات المتعلقة بالتجارة الإلكترونية، توزيع المحتويات غير المشروعة على الأنترنيت، انتهاكات قانون الصحافة، انتهاكات قانون حماية البيانات وغيرها.

وتعمل هذه الشرطة الوطنية أيضا على الحفظ السريع للبيانات المعلوماتية، المخزنة لضمان عدم ضياعها، خاصة وأن طلبات المساعدة القضائية الفرنسية أو الأجنبية في هذا المجال، تتطلب في بعض الأحيان وقت طويل للوصول، كما أن مقدمي خدمة الأنترنيت لا يحتفظون بالبيانات المتعلقة بهوية المشتركين أكثر من سنة، وعليه فالشرطة الوطنية هي التي تضمن بطريقة فعالة حماية هذه

---

[1]- محمد طارق عبد الرؤوف الخن، المرجع السابق، ص233.

[2]- LOCLCTIC اختصار لـــــ L'office Central De La Lutte Contre La Criminalité Liée Aux Technologies De L'information Et De La Communication.

[3]- تتكون هذه الشرطة الوطنية من أربع أقسام: قسم العمليات، قسم التقني، قسم مراقبة التكنلوجيا، قسم التكوين والتدريب.

البيانات، بالنظر إلى المبادلات بين الدول والاتفاقيات[1]، وتعد هذه الهيئة الأساس في مكافحة الجرائم الإلكترونية في فرنسا[2].

ب- الهيئة المركزية لردع العنف ضد الأشخاص OCRVP[3] تختص هذه الهيئة بـ:

- مكافحة الانتهاكات العنيفة ضد الأشخاص مثل: القتل العمدي، الشروع في القتل، السرقة، الاعتداءات الجنسية أو الشروع فيها، تسيير واستغلال المكالمات الهاتفية والبريد الإلكتروني.
- إكتشاف الجثث المجهولة.
- محاربة المجرم المعلوماتي الباث والمالك للصور الإباحية ضد القصر[4].

ج- فرقة التحقيق في الإحتيالات عبر تكنولوجيا الإعلام BEFTI[5] : هي عبارة عن وحدة للشرطة الوطنية تابعة لمديرية الشرطة القضائية لشرطة محافظة باريس حيث أن ثلث عمالها يعمل على توفير مساعدة تقنية ومادية للمصالح التابعة لشرطة محافظة باريس والقضاة، أما الثلثين الآخرين فيتمثل في محققين في الجريمة الإلكترونية.

د- فرقة حماية القصر لباريس BPM[6]: تعتبر هذه الفرقة السادسة من الفرق المركزية لمديرية الشرطة القضائية لمحافظة باريس، وهي فرقة خاصة للتحقيق في جرائم الأنترنيت تقوم بالتحريات في الأفعال الإباحية التي تمارس على القصر عبر الأنترنيت منذ سنة 1998.

كما تقوم بالتحقيقات المتعلقة بالانتهاكات ضد القصر كالاعتداءات الجنسية، أفعال إباحية تمارس على القصر، صور إباحية لقصر على الأنترنيت... وغيرها، كما يمكن لفريق الأنترنيت القيام بالمراقبات والتحريات التقنية للشبكات والأقراص الصلبة، وأيضا الأمر بالقبض واستجواب الأشخاص المشتبه فيهم[7].

---

[1] -QUEMENER Myriam، YVES Charpenel، Cyber criminalité، Droit Pénal Appliqué،Economica، Paris، 2010، P178.

[2]- فهد عبد الله العبيد العازمي، المرجع السابق، ص684.

[3]- OCRVP اختصار لـــ L'office Central De Répression Des Violences Aux Personnes .

[4] -QUEMENER Myriam، YVES Charpenel،OPCIT، P 198-199.

[5]- BEFTI اختصار لـــ La Brigade D'enquête Sur Les Fraudes Aux Technologies De L'information.

[6]- BPM اختصار لـــ La Brigade De Protection Des Mineurs De Paris.-

[7] -QUEMENER Myriam، YVES Charpenel،OPCIT، P 202.

هـ- مركز البحوث الإجرامية للدرك الوطني IRCGN[1] : أنشأ هذا المركز سنة 1992 وله أربع مهام:

- القيام بناءا على طلب وحدات الدرك الوطني أو القضاء بالفحوصات العلمية والخبرات الضرورية لسير التحقيقات القضائية.
- توفير لوحدات التحقيق المساعدة الضرورية لسير الحسن للمعاينات.
- المشاركة في تكوين التقنيين في مجال الاجرام وتكوين المحققين.
- متابعة البحوث الضرورية من أجل تطوير أدوات وتقنيات التحريات الإجرامية.

هذا المركز مجهز بمخبر كامل، من أجل استرجاع المعلومات المخزنة على دعائم التخزين المضبوطة، أقراص صلبة، هواتف نقالة...إلخ، والهدف من ذلك هو عمل نسخة على قرص، يقدم للدرك الوطني، من أجل إستغلالها في إطار التحقيق[2].

و- الجمارك: أنشأت خلية الجريمة الإلكترونية للجمارك في فبراير 2009، تابعة للمديرية الوطنية للاستعلام والتحقيقات، ففي إطار مكافحة الاحتيال عبر الأنترنيت، تقوم مصلحة الجريمة الإلكترونية بأبحاث لمصلحتها، تهدف إلى التعرف على الأشخاص الطبيعيين والمعنويين بفرنسا الذين يستعملون الأنترنيت لارتكاب عمليات احتيالية وتتركز الأبحاث على الأشخاص البائعين عبر الأنترنيت أو الشاهرين لإعلانات على منتوجات ممنوعة أو عالية الرسوم[3].

4- **بريطانيا:** قامت السلطات البريطانية بتخصيص وحدة تضم نخبة من رجال الشرطة متخصصين في البحث والتنقيب عن الجرائم الإلكترونية، كالجرائم الجنسية الواقعة على الأحداث، والقرصنة ونشر الفيروسات، تضم هذه الوحدة 80 عنصرا على درجة عالية من الكفاءة في المجال التقني، وقد بدأت هذه الوحدة نشاطها سنة 2001 ومركزها لندن[4].

ثانيا: الأجهزة المختصة في الدول العربية

لم تقف الدول العربية مكتوفة الأيدي أمام الخطر المتزايد للجرائم الإلكترونية، حيث قامت بعض الدول بإنشاء أجهزة متخصصة لمكافحة هذه الجرائم، ومن بين هذه الدول.

---

[1]- IRCGN اختصار لـــl'institut De Recherche Criminelle De La Gendarmerie Nationale.

[2] -QUEMENER Myriam، YVES Charpenel،OPCIT، P 202.

وانظر أيضا: فهد عبد الله العبيد العازمي ،المرجع السابق، ص 688.

[3] -QUEMENER Myriam، YVES Charpenel،OPCIT، P 204.

[4]- محمد طارق عبد الرؤوف الخن، المرجع السابق، ص234.

1- الأردن: ففي عام 1988، أنشأت الأردن قسما خاصا بجرائم الحاسوب تابع لمديرية الأمن، ويتعامل هذا القسم مع مختلف جرائم الحاسوب والأنترنيت منذ ذلك العام.

وفي عام 2006، تم تأسيس جمعية خاصة باسم " الجمعية الأردنية للحد من جرائم المعلوماتية والأنترنيت " مركزها عمان، وتهدف إلى تقديم الدعم العلمي للمؤسسات والأفراد، وتنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الأنترنيت[1].

2- دولة الامارات العربية المتحدة :طبقت ما يعرف بنظام الرقيب Proxy وهو الذي يقوم بمراجعة الخدمات المقدمة عبر شبكة الأنترنيت، فعندما يطلب المشترك موقعا ما يقوم الرقيب بعرض الموقع على قائمة من المواقع الممنوعة، فإذا تبين للرقيب أن الموقع المطلوب من ضمن هذه القائمة الممنوعة والمحظورة، لا يستطيع المشترك الحصول على هذا الموقع، وتظهر رسالة على الشاشة تقول تم منع هذا الموقع بواسطة رقيب انترنيت الإمارات.

وصدر القانون الاتحادي رقم 2 لسنة 2006 لمكافحة جرائم تقنية المعلومات، حدد فيه المشرع الإماراتي الأفعال التي يعد ارتكابها جريمة من جرائم المعلومات، كما حدد العقوبات الملائمة لها تبعا لخطورتها، وقد شمل القانون أغلب الجرائم الإلكترونية منها: التوصل بغير وجه حق إلى موقع أو نظام معلوماتي بدخول الموقع أو النظام، أو يتجاوز مدخل مصرح به، والتعدي على البيانات الشخصية، وإلغاء بيانات أو معلومات أو حذفها أو تدميرها، أو تغييرها، أو إعادة نشرها...إلخ، وهو أول قانون في الدول العربية يصدر بشكل مستقل لمواجهة الجرائم المعلوماتية[2].

3- قطر: صدر القانون 25 لسنة 1995 بشأن حماية المصنفات الفكرية وحقوق المؤلف، والذي تضمن نصا لحماية برامج الحاسب الآلي بوصفها من المصنفات[3].

4- المملكة العربية السعودية:

تعد المملكة العربية السعودية الدولة العربية الثالثة التي أصدرت نظاما لمكافحة الجرائم الإلكترونية، فقد صدر نظام مكافحة الجرائم الإلكترونية بالمرسوم الملكي رقم 17، الذي يهدف إلى مواجهة جرائم الحاسب الآلي والأنترنيت، من خلال وضع آلية نظامية للحد من وقوع هذا النوع من الجرائم، وذلك بتحديد الجرائم المستهدفة بالنظام والعقوبات المقدرة لكل جريمة، وحدد النظام السعودي

---

[1]- محمد طارق عبد الرؤوف الخن، المرجع نفسه، ص237.

[2]- فهد عبد الله العبيد العازمي، المرجع السابق، ص 698-699.

[3]- فهد عبد الله العبيد العازمي، المرجع نفسه، ص 700.

أغلب الجرائم الإلكترونية والأفعال التي تشكل خطرا على المعلومات، إضافة إلى الأحكام الخاصة بالمساهمة الجنائية، وتشديد العقوبة، والشروع فيها، والإعفاء من العقاب، والعقوبة التكميلية، وتحديد جهة الاختصاص بمتابعتها وتطبيق العقوبات، بما يؤدي إلى تحقيق الأمن المعلوماتي، وزيادة استخدامات الحاسب وشبكاته[1].

كما أصدرت المملكة العربية السعودية لمكافحة الجريمة الإلكترونية تنظيما للتعاملات الإلكترونية وضبطها بعض الأنظمة واللوائح والتعليمات والقرارات لمواجهة الاعتداءات الإلكترونية والإرهاب الإلكتروني، ونصت تلك الأنظمة على عقوبات في حال المخالفة لهذه الأنظمة والتعليمات واللوائح، كقرار مجلس الوزراء رقم 163 سنة 1417هـ الذي ينص على إصدار الضوابط المنظمة لاستخدام شبكة الأنترنيت والاشتراك فيها، ومن ذلك:

- الامتناع عن الوصول أو محاولة الوصول إلى أي من أنظمة الحاسبات الآلية الموصولة بشبكة الأنترنيت، أو إلى أي معلومات خاصة، أو مصادر معلومات دون الحصول على موافقة المالكين، أو من يتمتعون بحقوق الملكية لتلك الأنظمة والمعلومات.
- الإمتناع عن إرسال أو استقبال معلومات مشفرة إلا بعد الحصول على التراخيص اللازمة من إدارة الشبكة المعنية.
- الإمتناع عن الدخول إلى حسابات الآخرين، أو محاولة إستخدامها بدون تصريح.
- الإلتزام باحترام الأنظمة الداخلية للشبكات المحلية والدولية عند النفاذ إليها.
- الإمتناع عن تعريض الشبكة الداخلية للخطر، وذلك عن طريق فتح ثغرات أمنية عليها.

5- مـصر: قامت وزارة الداخلية في مصر بإنشاء عدة أجهزة أوكلت لها مهمة ضبط ما يتبع من جرائم من خلال الشبكة المعلوماتية نذكر منها:

أ- **إدارة مكافحة جرائم الحاسبات وشبكات المعلومات:** أنشأت هذه الإدارة بموجب قرار وزاري وهي تابعة للإدارة العامة للمعلومات والتوثيق[2] وتخضع للإشراف المباشر لمدير الإدارة العامة وتشرف عليها

---

[1]- فهد عبد الله العبيد العازمي، المرجع نفسه، ص 704.

[2]- تعتبر الإدارة للمعلومات والتوثيق من أكثر الإدارات تعاملا مع الجرائم الإلكترونية حيث أنها تختص بعمليات المتابعة الفنية لكثير من الجرائم ويبدأ الإدارة من خلال:

أ- المتابعة الفنية والتحري عن الجرائم التي تبلغ إلى الإدارة من الإدارات الأخرى وذلك من خلال استخدام شبكة الأنترنيت وتحديد شخص المتهم.

فنيا مصلحة الأمن العام التابعة لوزارة الداخلية، وتضم ثلاثة أقسام رئيسية: قسم العمليات، قسم التأمين وقسم البحوث و المساعدات الفنية.

وتعتبر هذه الإدارة من أكبر الإدارات تعاملا مع الجرائم الإلكترونية، فهي تتكون من ضباط متخصصين في مجال الحسابات والشبكات وتختص بمكافحة جرائم الأنترنيت على مختلف أنواعها[1].

ب- قسم مكافحة جرائم الحاسبات وشبكات المعلومات: وقد أنشئ هذا القسم بالإدارة العامة للبحث الجنائي بمديرية أمن القاهرة، ويتبع إدارة المعلومات والحاسب الآلي ويخضع من حيث الإشراف الفني لإدارة مكافحة الحاسبات وشبكات المعلومات، ويختص بعمليات تأمين ورقابة نظم وشبكات المعلومات لمنع وقوع أية جرائم عليها باستخدام الأساليب والتقنيات العلمية الحديثة، ورصد ومكافحة وضبط الجرائم التي تقع باستخدام الحاسب على نظم وشبكات المعلومات وقواعد البيانات[2].

إلى جانب هذه الأجهزة، تم تأسيس " الجمعية المصرية لمكافحة جرائم المعلوماتية والأنترنيت " وهي منظمة غير حكومية خاضعة للقانون المصري ومشهرة تحت رقم 2176 لسنة 2005، وتهدف إلى تقديم الدعم العلمي للمؤسسات والأفراد، وتنمية الكوادر البشرية في مجال مكافحة الإجرام عبر الأنترنيت [3].

6- الجزائر: تعتبر من الدول التي عملت على إنشاء أجهزة متخصصّة لمكافحة الجريمة الإلكترونية نظرا للخصوصية التي تتميز بها، كما تعد الجزائر كذلك من الدول الرائدة في مجال المؤسسات الأمنية ذات الطابع المدني، فكثيرا ما تستعين الدول بالتجربة الجزائرية نظرا لخبرة هذه المؤسسات ودورها السباق والجلي في مواجهة التحديات الإجرامية من هذه المؤسسات جهاز الشرطة[4].

ب- تقوم كذلك الإدارة بتحديد شخص المتهم من خلال عملية تتبع له عند اكتشافهم لجريمة ترتكب باستخدام شبكة الأنترنيت. أنظر: أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص456.

[1]- نعيم سعيداني، المرجع السابق، ص106.

[2]- نعيم سعيداني، المرجع نفسه، ص106.

[3]- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والأنترنيت (الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص94 وما بعدها.

[4]- تصنف المؤسسات التابعة لجهاز الشرطة إلى نوعين، النوع الأول: يتعلق بتجسيد وتنفيد التعاون الأمني الدولي، يتمثل في المكاتب التابعة للشرطة الجنائية الدولية والنوع الثاني: يرتبط بالمتطلبات الوطنية لتحقيق الأمن والاستقرار الداخلي و يتمثل، في المديرية العامة للأمن الوطني. أنظر: حبيب عباسي، المرجع السابق، ص435.

في هذا الصدد أنشأت هذه الجهات المتخصصة على مستوى المديرية العامة للأمن الوطني، والمديرية العامة للدرك الوطني بالإضافة إلى إنشاء هيئة وطنية مختصة في الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال.

أ- **المديرية العامة للأمن الوطني**[1]: تعد هذه المديرية الجهاز الأمني صاحب الاختصاص الأصيل في مجال الوقاية وهي تقوم بقيادة جهاز الشرطة في الجزائر، تحت رعاية وزارة الداخلية من مهامها حفظ الأمن والنظام العام بالمدن الجزائرية الكبرى والمناطق الحضرية، بالإضافة إلى حماية الأشخاص والممتلكات وكذا التحقيق في الجرائم وإلقاء القبض على الجناة و ومراقبة الحدود[2].

وفي إطار التخصص في مجال الشرطة القضائية، قامت المديرية العامة للأمن الوطني بإدخال تعديلات تمس الهياكل التنظيمية الخاصة بمصالح الشرطة القضائية، وذلك من أجل جعل المصالح المكلفة بمكافحة الجريمة أكثر تقاسما مع الواقع وأكثر استعدادا لما تشير إليه التنبؤات المستقبلية[3].

ففي مجال الجريمة الإلكترونية، أصبح من الضروري وضع آليات عملياتية على مستوى مصالح الشرطة القضائية كفيلة بالتصدي ومعالجة هذا النوع من الإجرام الذي لم يسبق التعامل معه من قبل، فتتم بذلك إنشاء مصالح متخصصة في مكافحة هذه الجرائم[4]:

- على مستوى مخابر الشرطة العلمية: في سنة 2007، تم تدعيم مخابر الشرطة العلمية المتواجدة في كل من العاصمة، وهران وقسنطينة بأقسام مختصة في الأدلة الإلكترونية، مهمتها استخراج المعطيات المخزنة بداخل الأجهزة الإلكترونية[5] بعد استغلالها والتي قد تساعد المحقق في التحقيق.

---

[1]- جميع المهام المسندة للأمن الوطني محددة في المرسوم التنفيذي رقم 10-322، المؤرخ في 22 ديسمبر 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، جريدة رسمية للجمهورية الجزائرية، العدد78، بتاريخ 26 ديسمبر 2010.

[2]- حبيب عباسي، المرجع السابق، ص439.

[3]- كريم راشد، بحث إستراتيجية المديرية العامة للأمن الوطني في مكافحة الجريمة المعلوماتية مقدم لليوم الدراسي حول مخاطر الأنترنيت وجرائم الإعلام من تنظيم مخبر الدراسات القانونية ومسؤولية المهنيين المنعقد بتاريخ 14 فبراير 1019، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، ص09.

[4]- فهد عبد الله العبيد العازمي، المرجع السابق، ص 70. وأنظر أيضا: كريم راشد، المرجع السابق، ص09.

[5]- ومن الأجهزة التي تتكفل هذه الأقسام باستغلالها: أجهزة الكمبيوتر ولواحقها، أدوات التخزين الرقمية كالأقراص المضغوطة، أقراص صلبة، أجهزة الهواتف النقالة وغيرها.

- المصالح الولائية للشرطة القضائية: في شهر جانفي من سنة 2010، تم تنصيب على مستوى مديرية الشرطة القضائية 25 خلية مركزية لمكافحة الجرائم المتصلة بتكنلوجيا الإعلام والإتصال موزعة كالتالي: عشر خلايا (10) على مستوى ولايات الوسط، ثمانية(8) خلايا على مستوى ولايات الشرق، ستة (6) خلايا على مستوى ولايات الغرب، خلية واحدة (1) على مستوى ولايات الجنوب.

أما في سنة 2013، تم تنصيب 48 خلية لمكافحة الجريمة الإلكترونية على مستوى المصالح الولائية للشرطة القضائية التابعة للأمن الولايات، وفي سنة 2015 تم تحويل الخلايا 48 على مستوى المصالح الولائية للشرطة القضائية إلى فرقة لمكافحة الجريمة الإلكترونية، من بين أهم مهام هذه الفرقة:

- إنجاز التحقيقات القضائية ذات الصلة بمكافحة الجريمة الإلكترونية.
- تنسيق تحريات الشرطة القضائية في ميدان الوقاية من الجريمة الإلكترونية.
- تنفيذ الإنابات القضائية والدولية ذات الصلة بمكافحة الجريمة الإلكترونية.
- القيام بوضع منظومة للرصد على شبكة الأنترنيت، تمثل في تنظيم عمليات لتحصيل ومراقبة وتحليل المعلومات التي يتم جمعها على شبكات حول المضامين المخالفة للقانون أو تلك التي تشكل تهديدا للأمن والنظام العام[1].

ومن القضايا المعالجة من طرف فرقة مكافحة الجريمة الإلكترونية بأمن ولاية بشار :

- قضايا المساس بحرمة الحياة الخاصة عن طريق نشر صور الغير عبر مواقع التواصل الإجتماعي.
- قضايا النصب والاحتيال الموجه للجمهور عبر الأنترنيت.
- قضايا الدخول والبقاء عن طريق الغش في جزء من منظومة معلوماتية (القرصنة).
- قضايا السّب والقذف عبر مواقع التواصل الاجتماعي.
- قضايا التحريض والمساس بالنظام العام عبر الأنترنيت.
- قضايا التهديد بالاعتداء عبر مواقع التواصل الاجتماعي.
- قضايا انتحال الهوية وصفة الغير عبر الأنترنيت[1].

[1]– كريم راشد، المرجع السابق، ص14.

- مثال تطبيقي في معالجة قضية على مستوى فرقة مكافحة الجريمة الإلكترونية بأمن ولاية بشار.

بالنسبة للجانب الإجرامي يتم: استقبال الضحية، معاينة الجرم أو الجريمة من طرف محقق متخصص في الجرائم المعلوماتية، سماع أقوال الضحية على محضر رسمي، إخطار السيد وكيل الجمهورية المختص إقليميا بكافة الوقائع، فتح تحقيق في القضية مع مباشرة التحريات التقنية.

أما في الجانب التقني فيتم: استغلال الوسائل التقنية مدعمة بالتقنيات المعلوماتية من أجل تحديد هوية المشتبه فيه، استرجاع وتحديد عنوان البرتوكول الأنترنيت (IP) المشتبه فيه، تعريف وتحديد بدقة الهوية الحقيقية للمشتبه فيه صاحب برتوكول الأنترنيت (IP)، توقيف المشتبه فيه مع حجز الوسيلة الإلكترونية المستعملة في الجرم، سماع المشتبه فيه مع استغلال الوسيلة الإلكترونية المستعملة في الجرم لاستخراج منها كل ما يفيد التحقيق وأخيرا انجاز الملف القضائي ضد الفاعل وتقديمه أمام الجهة القضائية المختصة[2].

وحتى في مجال التعاون الدولي كان لمديرية الأمن الوطني دور فعال حيث تتوفر هذه الأخيرة على مديرية مكلفة بالتعاون الدولي وهي الهيئة المخول لها الإتصال الدولي في كل جوانب التعاملات الدولية للمديرية العامة للأمن الوطني وعلاقاتها الخارجية، وكمعظم دول العالم تتمتع أجهزة الأمن الجزائرية بأطر تنظيمية خاصة وقنوات دولية مماثلة للمكاتب المركزية الوطنية للشرطة الجنائية لباقي دول العالم بحيث أن لمديرية الشرطة القضائية للمديرية العامة للأمن الوطني، مكتب وطني يلعب دورا محوريا في تعاون مصالح الشرطة القضائية مع المصالح الدولية الأخرى الشقيقة والأجنبية[3].

ب- الدرك الوطني: يعرف الدرك الوطني[4] على أنه قوة عمومية ذات طابع عسكري، له علاقة بالخدمات الوطيدة مع أجهزة الأمن الأخرى ومع الأجهزة الوطنية، ويتولى الدرك الوطني مهام الشرطة

---

[1]- كريم راشد، المرجع نفسه، ص15.

[2]- كريم راشد، المرجع السابق، ص17.

[3]- عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة، دار الجامعة الجديدة، الإسكندرية، 2013، ص198.

[4]- بالنسبة للمهام المنوطة لجهاز الدرك الوطني منصوص عليها في المرسوم الرئاسي رقم 143/09، المؤرخ في 27 أفريل 2009، يتضمن مهام الدرك الوطني وتنظيمه، جريدة رسمية للجمهورية الجزائرية، العدد 26، بتاريخ 03 ماي 2009..

القضائية والإدارية والعسكرية، بالإضافة إلى مهمته الرئيسية والمتمثلة في الدفاع الوطني طبقا للخطط المقررة من قبل وزير الدفاع الوطني[1].

ويتألف الدرك الوطني من عدة أجهزة نظرا لحجم المهام الملقاة على عاتقه نصت عليها المادة 12 من المرسوم الرئاسي 09-143 كالآتي:

- قيادة الدرك الوطني.
- الوحدات الإقليمية.
- الوحدات المشكلة.
- الوحدات المتخصصة.
- وحدات الإسناد.
- هياكل التكوين.
- المعهد الوطني للأدلة الجنائية وعلم الإجرام.
- المصالح والمراكز العلمية والتقنية.
- المصلحة المركزية للتحريات الجنائية.
- المفرزة الخاصة للتدخل.
- ولقد تمكن الدرك الوطني في الجزائر من أخذ مكانه في قاطرة الأجهزة الأمنية المكلفة بمكافحة الجريمة، وهذا بفضل إرادة وتفاني وحماس القوات التابعة له إزاء المهام المنوطة بها والنتائج الكبيرة والإيجابية المحققة لا سيما في مجال المحافظة على أمن وراحة المواطنين[2].

كما تعود أيضا هذه المكانة التي حظي بها الدرك الوطني أيضا إلى تنوع المهام الموكلة إليه وتعدد الأجهزة أو الهياكل المكونة له، بالإضافة إلى كل من الوسائل البشرية والمادية الكفيلة بتحقيق الأهداف المنشودة من ورائه[3].

وفي مجال مكافحة الجريمة الإلكترونية على مستوى الدرك الوطني تم إنشاء مركز للوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها إلى جانب المعهد الوطني للأدلة الجنائية وعلم الإجرام.

---

[1]- الدرك الوطني الجزائري، مقال منشور على موقع ويكيبيديا، الموسوعة الحرة، على الرابط الإلكتروني: الدرك-الوطني-الجزائري /http :ar.wikipediaorg/wiki ، تاريخ الزيارة: 16 ماي 2018 ، سا: 10:00.

[2]- حبيب عباسي، المرجع السابق، ص447.

[3]- حبيب عباسي، المرجع نفسه، نفس الصفحة.

ب1- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها :

بدأت قيادة الدرك الوطني تطبيق برنامجها من خلال مباشرة مهامها إبتداءا من سنة 2004، أي بعد إدراج فقرة متعلقة بمكافحة الإجرام المعلوماتي ضمن قانون العقوبات والتي حددت أنماط المساس بأنظمة المعالجة الآتية للمعطيات وعقوبتها، من ثمة كثفت قيادة الدرك الوطني عملها الرامي إلى مكافحة الجريمة الإلكترونية وكافة الأشكال الجديدة للجريمة الافتراضية التي لها صلة وطيدة باستخدام الأنترنيت، حيث تم إنشاء مركز للوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها من أجل القضاء أو الحد من هذه الآفة[1]، وذلك من خـــلال:

- مساعدة وحدات الدرك الوطني الممارسة لمهام الشرطة القضائية في البحث والتوصل إلى مرتكبي المخالفات المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات وكذا المخالفات المتعلقة باستخدام الأنظمة المعلوماتية لتكنلوجيا الإعلام والاتصال.

- من أجل تطبيق ذلك يحوز الأفراد الذين يطاردون الجريمة الإلكترونية أحدث الأنظمة والأجهزة والبرمجيات المتطورة من أجل استخدامها في عمليات الوقاية من الإجرام المعلوماتي ومكافحته.

- في إطار ممارسة مهامه، يقوم المركز بالتعاون والتنسيق مع المصالح الأمنية والوطنية وعدد من متعاملي الخدمات الهاتفية من أجل الإستفادة للطلبات التي تأتي من مختلف وحدات الدرك الوطني والمتعلقة بتشخيص والتعرف على العناوين الإلكترونية أو أرقام المرسلين محل التحقيق، كما أن المركز يتعاون مع مختلف السلطات القانونية والتشريعية في مجال طلبات التعامل مع الهيئات القانونية الدولية[2].

أما فيما يخص آفاق الـــمركز فيمكن القول بأن الـــمركز يسعى إلـــى:

- تعميم واستكمال نشر فرق المحققين في الجريمة المعلوماتية وتعميم نظام لليقظة على المستوى الوطني عبر كافة الوحدات التابعة للدرك الوطني.

- تكوين مجموعة مختصة في مهام أمن الأنظمة المعلوماتية وحمايتها.

- تكوين المكونين في المجال وإعداد برامج المواد المتعلقة بالتكنلوجيا الجديدة ومكافحة الجريمة الإلكترونية على صعيد كافة مستويات التكوين.

---

[1]- رجم جمال، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ، مجلة الجيش، مجلة شهرية للجيش الشعبي الوطني، عدد 599، تصدر عن مؤسسة المنشورات العسكرية، جوان، 2013، ص14.

[2]- رجم جمال، المرجع نفسه، نفس الصفحة.

ويوجد داخل المركز مكتب اليقظة والتحسيس الذي يتكفل بمهام اليقظة المعلوماتية[1]، حيث تتمثل مهمة المسؤولين عن مهام اليقظة في مطاردة وتتبع ورصد كل أشكال وصور المخالفات والجرائم التي ترتكب بواسطة الشبكة العالمية للمعلومات، على غرار تقليد صناعة المنتوجات الذم، الشتم والتحقير، التهديد و الابتزاز، القرصنة المعلوماتية، وغيرها من الجرائم، وبالتالي يتم على مستوى مكتب اليقظة متابعة كل ما ينشر عبر الأنترنيت قصد تتبع آثار الجريمة وملاحقة المجرم الإلكتروني ومعاقبتهم من خلال إعتماد ستة أنواع من اليقظة وهـــي:

– اليقظة الأمنية: يمكن بفصلها متابعة مدى تطور الإجرام وأساليبه بصفة عامة والخطط العملية التي ينتهجها المجرمون بغرض تحضير وتجنيد أفضل للأفراد والوسائل للتصدي لهذا النوع من الجرائم.

– اليقظة التكنولوجية والعلمية: تتمثل في جمع المعلومات والمعطيات التي تسمح بمتابعة الإبتكارات والتطورات الحاصلة في المجال التكنلوجي والعلمي في مختلف المجالات التي تهم الدرك الوطني.

– اليقظة الاجتماعية: وتعنى بمتابعة التحاليل ومختلف الدراسات التي تهتم بالمجتمع وتطوراته والمعايير التي تتحكم فيه وعلاقتها بالأمن العام.

– اليقظة القانونية: تهتم بمتابعة التطورات الحاصلة في المجال القانوني والنصوص التشريعية المتعلقة بمختلف المهام والنشاطات التي لها صلة بمهام الدرك الوطني لا سيما الحفاظ على الأمن العام.

– اليقظة الاقتصادية: تهتم بالجوانب الاقتصادية وتطورات السوق الوطنية والأجنبية، وتهدف إلى حماية المصالح في إطار توقيع العقود أو معاهدات الشراكة الاقتصادية[2] الحديثة التي توصل إليها التقدم العلمي[3].

---

[1]– تعد اليقظة المعلوماتية اليوم من أهم الطرق المستخدمة في مسار إعداد، تكييف وتطوير آليات جديدة للإنذار، تسمح باتخاذ القرارات الملائمة في مجال المحافظة على الأمن العام، بالإضافة إلى تعدد وتنوع مصادر المعلومات التي تتزايد وتتضاعف من يوم إلى آخر بل من دقيقة إلى أخرى، وهذا ما يزيد من صعوبة كشف وتحديد التهديدات والمخاطر أو التنبؤ بها.

[2]– رجم جمال، المرجع السابق، ص15.

[3]– حبيب عباسي، المرجع السابق، ص448.

ب2- المعهد الوطني للأدلة الجنائية وعلم الإجرام:

استحدث المشرع الجزائري هيئة تابعة للدرك الوطني سميت (المعهد الوطني للأدلة الجنائية وعلم الإجرام)[1] في مجال الوقاية من الجريمة الإلكترونية ومكافحتها.

والمعهد عبارة عن مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي، موضوعة تحت وصاية وزير الدفاع الوطني، ويخضع إلى جميع الأحكام التشريعية والتنظيمية المطبقة على المؤسسات العسكرية[2].

وتتمثل المهام الملقاة على عاتقه فيما يلي:

- إجراء بناء على طلب من القضاة والمحققين أو السلطات المؤهلة، الخبرات والفحوص العملية التي تخضع لاختصاص كل طرف في إطار التحريات الأولية والتحقيقات القضائية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح.
- تقديم مساعدة علمية أثناء القيام بالتحريات المعقدة باستخدام مناهج الشرطة العلمية والتقنية الرامية إلى تجميع وتحليل الأشياء والآثار والوثائق المأخوذة من مسرح الجريمة.
- المشاركة في الدراسات والتحاليل المتعلقة بالوقاية والتقليل من كل أشكال الجريمة.
- تصميم بنوك معطيات وإنجازها طبقا للقانون، بما في ذلك تلك الخاصة بالبصمات الجينية، التي ستكون في متناول المحققين بغرض وضع المقاربات واستخلاص الروابط المحتملة بين المجرمين وأساليب النشاط الإجرامي.
- المشاركة بصفته هيئة تضمن الفحوص والخبرات في مجال علم الإجرام، وفي إطار الرقي والرفع من كفاءة الأداء الصادر عن القوات التابعة للدرك الوطني، تم إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني وهي عبارة عن مؤسسة عمومية ذات طابع إداري، تتمتع بالشخصية المعنوية

[1]- هذا ما نصت عليه المادة 1 من المرسوم الرئاسي 183/04، مؤرخ في 26 جوان 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، جريدة رسمية للجمهورية الجزائرية، العدد41، بتاريخ 27 جوان 2004.

[2]- أنظر المادة 2 من المرسوم نفسه.

والاستقلال المالي، وهي موضوعة تحت وصاية وزير الدفاع الوطني[1]، أنشأت هذه المؤسسة لضمان التكوين المتخصص في صفوف الدرك الوطني[2].

تتمثل مهام هذه المدرسة في الآتي:

– ضمان تكوين متخصص لضباط صف الدرك الوطني أو التابعين لهياكل أخرى لوزارة الدفاع الوطني والمترشحين للحصول على صفة ضابط شرطة قضائية.

– ضمان تكوين متواصل ومتخصص في مجال الشرطة القضائية لضباط وضباط صف الدرك الوطني، وعند الاقتضاء، لمستخدمين آخرين معنيين تابعين لوزارة الدفاع الوطني.

– ضمان تكوين التأهيل الموجه للمستخدمين الضباط وضباط صف المدعوين لتولي قيادة وحدات وهياكل مكلفة لمهمة الشرطة القضائية.

– المساهمة في إطار سياسة التكوين لوزارة الدفاع الوطني، عندما تسمح قدرات الاستقبال في تكوين إطارات تابعين لدوائر وزارية أخرى أو متربصين أجانب في إطار التعاون.

– المشاركة في إعداد الدراسات والأبحاث حول نشاط الشرطة القضائية"[3].

وبهذا يكون الدرك الوطني قد حقق قفزة نوعية في مجال محاربة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة من خلال إنشاء هذه المدرسة التي تساهم بشكل كبير في مد عناصر الدرك بالتكوين اللازم وبالتقنيات تحديد سياسة جنائية مثلى لمكافحة الإجرام.

– المبادرة بالبحوث المتعلقة بالإجرام وإجرائها باللجوء إلى التكنولوجيا الدقيقة.

– العمل على ترقية البحث التطبيقي وأساليب التحريات التي ثبتت فعاليتها في ميادين علم الإجرام والأدلة الجنائية على الصعيدين الوطني والدولي.

– المشاركة في كل الملتقيات والمحاضرات أو الندوات على الصعيدين الوطني والدولي الضرورية في تطوير مستخدمي المعهد.

– المشاركة في تنظيم دورات تحسين المستوى والتكوين ما بعد التدرج في تخصصات العلوم الجنائية.

---

[1]– أنظر المادة 2 من المرسوم الرئاسي رقم 151/08، المؤرخ في 26 ماي 2008، يتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، جريدة رسمية للجمهورية الجزائرية، العدد 27، بتاريخ 28 ماي 2008.

[2]– أنظر المادة 1 من المرسوم نفسه.

[3]– أنظر المادة 3 من المرسوم نفسه.

– تصور الأبحاث المخولة إلى الغير وضمان متابعتها و تقديرها [1].

ويوجد على مستوى المعهد عدة دوائر منها: دائرة البحث وتطوير المعطيات، دائرة البصمات، دائرة البيئة، دائرة الحرائق، دائرة الجريمة الإقتصادية والمالية، دائرة الجريمة المنظمة، دائرة الجرائم المتصلة بالتكنولوجيا الحديثة و من مهامها:

– القيام بدراسات وأبحاث لها علاقة بالجرائم المتصلة بالتكنولوجيات الحديثة، تطورها، آثارها وتأثيرها على المجتمع.

– المشاركة ودعم التحقيقات المعقدة في مجال الجرائم المتصلة بالتكنولوجيات الحديثة.

– المشاركة في تكوين ضباط الشرطة القضائية للدرك الوطني.

– المشاركة في إنجاز السياسة الجنائية فيما يتعلق بالجرائم المتصلة بالتكنولوجيات الحديثة.

ويوجد على مستوى دائرة الجرائم المتصلة بالتكنولوجيات الحديثة ثلاثة مخابر هي:

مخبر جرائم الأنترنيت، مخبر الجرائم المتصلة بالتكنولوجيات الحديثة، مخبر جموح الإعلام الآلي.

أما في مجال التحقيق فغالبا ما يشرع فيه بناءا على شكوى مودعة عند وحدة من وحدات الدرك الوطني، لذلك وفي إطار التحسيس ، يحث الدرك الوطني المواطنين على عدم التردد في التوجه إلى وحداتها المنتشرة عبر كامل التراب الوطني من أجل إيداع الشكاوى في حالة تعرضهم إلى أعمال نصب أو قرصنة أو تلقي رسائل مجهولة عبر البريد الإلكتروني.

و انطلاقا من هنا، يباشر المختصون في الكشف والتحري حول هذا النوع من الجرائم من أجل تشخيص وتحديد العلاقة بين مصدر الرسائل المجهولة مثلا قبل التوصل إلى تحديد هوية مجرمي الشبكة العنكبوتية، خاصة مع إعتبار الأدلة الإلكترونية أدلة قانونية، حيث أنها تجمع بين مجمل العناصر المادية بنسختها الرقمية (مثل المعطيات المخزنة بالأقراص الصلبة للشخص المشبوه أو الضحية أثناء عمليات التحري)، كل هذا أصبح ضروريا خلال القيام بالتحقيقات لفائدة العدالة[2].

وتجري التحقيقات بالتنسيق مع المخابر على مستوى المعهد الوطني لعلم الإجرام والأدلة الجنائية التي تقوم بعمل تقني محض مثل تحليل قرص مرن، إذ رغم اللجوء إلى حذف الأدلة يمكن للمختص

[1]– أنظر المادة 4 من المرسوم الرئاسي رقم 183/04، السابق الذكر.

[2]– رجم جمال، المرجع السابق ص17.

في التحريات[1] أن يتتبع خيوط الجريمة وتقفي آثار الرسائل المرسلة من الجهاز أو مختلف الروابط أو الموقع التي تم تصفحها إعتمادا على تقنيات تحليل نظام التشغيل.

ولا تقف مهمة المحققين عند هذا الحد، بل تمتد إلى الدوريات الإلكترونية عبر صفحات الواب التي قد تكشف عن وجود صلة ترابط القضايا فيما بينها وهو ما من شأنه المساعدة على فك اللغز، وبالتالي الإسراع في عملية التحقيق.

من خلال ما سبق ذكره يتضح مدى أهمية المهام الملقاة على عاتق المعهد الوطني للأدلة الجنائية وعلم الإجرام في كشف خيوط الجريمة وإعداد الإستراتيجية الكفيلة بضمان الوقاية من الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة ومكافحتها إستنادا إلى المعايير المتطلبة في البحث العلمي، وهو بدون شك سيساهم مساهمة كبيرة في خضوع المجرم الإلكتروني لسلطان القانون، الذي استطاع الإفلات من زمام المتابعة الجزائية بفصل تحكمه الكبير في التكنلوجيا[2]، إذ نحن أمام مجرم يتمتع بالذكاء الفائق والخبرة الكبيرة في مجال الحاسب الآلي مما يجعل ملاحقته غاية في الصعوبة.

ب3- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال:

بدوره المشرع الجزائري وتصديا للجريمة الإلكترونية، أصدر قوانين عقابية لكل السلوكات الماسة بالأشخاص والأموال والتي ترتكب عن طريق أنظمة معلوماتية وفي فضاء افتراضي من بين هذه القوانين القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحتها، حيث نصت المادة 13 منه: " تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال، تحدد تشكيلة الهيئة وتنظيمها وكيفيات سيرها عن طريق التنظيم".

كما نصت المادة 14 من ذات القانون على أنه: " تتولى الهيئة المذكورة في المادة 13 أعلاه، خصوصا المهام التالية:

---

[1]- يستطيع المحقق التوصل إلى الوثائق الشخصية للأشخاص المشبوهين أو الضحايا لغرض التحري وجمع الأدلة والتعرف على حيثيات القضية من خلال الإعتماد على أساليب التحقيق الإلكتروني المتطورة من بينها:

أ- جمع وحفظ الأدلة الإلكترونية على المستوى المركزي أو على مستوى المخابر التقنية.

ب- البحث عن أساليب حذف وثيقة أو ملف ما أو رسالة معينة وكيفية استخراجها و استرجاعها.

جـ- إعادة تحليل وتتبع لأرشيف الإيجار عبر الأنترنيت أو استخدام جهاز الحاسوب.

د- تتبع مسار البريد الإلكتروني وتحديد مصدر الهجمات بالفيروسات أو الاختراق غير القانوني للوثائق الشخصية.

هـ- توفير الأدلة حول سرقة المعطيات والمعلومات أو في حالة تزوير الوثائق و استعمالها.

[2]- حبيب عباسي، المرجع السابق، ص450-451.

1- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال ومكافحته.

2- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنلوجيا الإعلام والاتصال بما في ذلك من تجميع المعلومات وإنجاز الخبرات القضائية.

3- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وتحديد مكان تواجدهم.

تم تنظيم هذه الهيئة وفقا لعدة مراسيم بداية بالمرسوم الرئاسي 15-261 المؤرخ في 8 أكتوبر 2015[1]، الذي عرف الهيئة بموجب المادة 2 على أنها: " سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضح لدى الوزير المكلف بالعدل"، ثم جاء المرسوم الرئاسي 19-172، المؤرخ في 6 يونيو 2019[2] ، وأعاد تعريف الهيئة بموجب المادة 2 منه على أنها : "مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية وهي خاضعة لوزارة الدفاع الوطني"، وأعيد تنظيم الهيئة من جديد بموجب المرسوم الرئاسي 20-183 المؤرخ في 13 يوليو 2020،[3] حيث عرفت الهيئة بأنها:" سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلالية المالية توضع تحت سلطة رئيس الجمهورية.

وما يلاحظ في هذا الصدد أنه تم تعديل الجهة الوصية حيث أصبحت الهيئة توضع تحت سلطة رئيس الجمهورية، بعدما كانت خاضعة لوزارة العدل بموجب المرسوم الرئاسي 261/15 المتعلق بتشكيل الهيئة وخاضعة لوزارة الدفاع الوطني بموجب المرسوم الرئاسي 172/19 السالف الذكر، كما غير هذا المرسوم المصطلح من سلطة إدارية مستقلة إلى مؤسسة عمومية ذات طابع إداري، وحسن ما فعل المشرع بتعديل مصطلح في المرسوم الأخير لسنة 2020، باعتبار الهيئة في ميدان الضبط

---

[1]- المرسوم الرئاسي 15-261، المؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة بتاريخ 8 أكتوبر 2015، ص 16.

[2]- المرسوم الرئاسي رقم 172/19 المؤرخ في 6 يونيو 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات يسرها، جريدة رسمية للجمهورية الجزائرية، العدد 37، مؤرخة في 09 يونيو 2019، ص05 .

[3]- المرسوم الرئاسي رقم 20-183، المؤرخ في 13 يوليو 2020،يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 40، الصادرة بتاريخ 18 جويلية 2020، ص 05.

الإداري أين استعمل مصطلح السلطة أو هيئة مستقلة، وتتمتع هذه الأخيرة بالشخصية المعنوية والاستقلال المالي، أما فيما يخص وضع الهيئة تحت سلطة رئيس الجمهورية لأنها امتداد للسلطة التنفيذية وباعتبار رئيس الجمهورية هو رئيس السلطة التنفيذية وبالتالي فهو متحكم في هذه الهيئات. ويحدد مقر الهيئة بالجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني طبقا للمرسوم الرئاسية لسنة 2020.

أما فيما يخص مهام الهيئة فقد أبقى المرسوم الرئاسي لسنة 2020 على مهام الهيئة تحت رقابة السلطة القضائية، وفيما يتعلق بتنظيم الهيئة وضع هذا المرسوم كل من مجلس التوجيه ومديرية عامة[1]، تحت السلطة المباشرة لرئيس الجمهورية، ويقدمان له عرضا عن نشاطاتهما[2].

كما أعيدت صياغة اسماء المديريات والمصالح التابعين للمديرية العامة، حيث تضم الهيئة[3]:

- **مديرية للمراقبة الوقائية واليقظة الإلكترونية:** حيث اضافت المادة 15 صلاحية اليقظة الالكترونية في مجال جرائم المتصلة بتكنولوجيا الاعلام والاتصال وهو سبب تغيير المصطلح الذي كان في المرسوم الرئاسي لسنة 2019 "مديرية تقنية".
- **مديرية للإدارة والوسائل:** لم يتغير محتوى المادة في المرسوم الجديد.
- **مصلحة الدراسات والتلخيص:** حيث اضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 19 منه.
- **مصلحة التعاون واليقظة الالكترونية:** حيث اضاف المرسوم الرئاسي الجديد صلاحيات هذه المصلحة بموجب المادة 20 منه.

أما فيما يخص المديرية العامة للهيئة، فتتولى السهر على حسن سيرها، إعداد مشروع ميزانيتها، إعداد وتنفيذ برنامج عملها، كما تعمل على تبادل المعلومات مع مثيلاتها الأجنبية بغرض تجميع كل

---

[1]– فيما يخص مجلس التوجيه أبقى المرسوم الرئاسي الجديد على نفس الصلاحيات الممنوحة له بموجب المرسوم الرئاسي لسنة 2019، غير أنه عدل التشكيلة برئاسة رئيس الجمهورية ويمكنه أن يفوض ممثله، حيث يتشكل مجلس التوجيه من الوزير الأول المكلف بالعدل، الوزير المكلف بالداخلية، الوزير المكلف بالمواصلات السلكية واللاسلكية وقام المرسوم بإضافة كل من المدير العام للأمن الداخلي وقائد الدلاك الوطني والمدير العام للأمن الوطني وممثل رئاسة الجمهورية وممثل عن وزارة الدفاع، ويعين رئيس الجمهورية ممثلي رئاسة الجمهورية ووزارة الدفاع الوطني، أما فيما يخص المديرية العامة فيديرها مدير عام تعيينه وإنهاء مهامه يكون بموجب مرسوم رئاسي.

[2]– أنظر المادتين 4 و5 من المرسوم الرئاسي رقم 20– 183، السالف الذكر، ص 5–6.

[3]-أنظر المادة 11 من المرسوم نفسه، ص 7.

المعطيات المتعلقة بتحديد مكان مرتكبي الجرائم المتصلة بتكنلوجيا الإعلام والاتصال والتعرف عليهم[1].

ب4. السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي:

قام المشرع الجزائري بموجب القانون 07/18 و المتعلق بحماية الأشخاص الطبيعيين ذات الطابع الشخصي[2]، باستحداث سلطة قضائية تسهر على مطابقة معالجة المعطيات ذات الطابع الشخصي، وهي عبارة عن سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي .[3]

تتكون هذه السلطة من (16) عضو يعينون بمرسوم رئاسي لعهدة مدتها (05) سنوات قابلة للتجديد منهم:03 أعضاء بما فيهم الرئيس يعينهم رئيس الجمهورية من ذوي الإختصاص و 03 قضاة يقترحهم المجلس الأعلى للقضاء و عضو عن كل غرفة من البرلمان و ممثل واحد عن كل من: المجلس الوطني لحقوق الإنسان، وزير الدفاع الوطني، وزير الشؤون الخارجية و الداخلية، وزير العدل، وزير البريد و الموصلات، وزير الصحة، وزير الضمان الاجتماعي، وللسلطة الحق في الإستعانة بأي شخص مؤهل من شأنه مساعدتها في أشغالها.[4]

ومن المهام المسندة للسلطة حسب ما حددته المادة (25) من نفس القانون ضمان عدم إنطواء استعمال تكنولوجيات الإعلام و الإتصال على أي أخطار تجاه حقوق الأشخاص و الحريات العامة و الخاصة، منح تراخيص و تقديم أللاستشارات للأشخاص و الكيانات التي تلجأ إلى معالجة المعطيات ذات الطابع الشخصي

---

[1]– نصت المادة 16 من القانون 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنلوجيا الإعلام والاتصال على أنه:" في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني...".

إضافة المادة 17 من نفس القانون والتي قضت على أنه: " تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو إتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة، والاتفاقيات الثنائية ومبدأ المعاملة بالمثل".

[2]– القانون 18– 07 المؤرخ في 10 جوان سنة 2018 و المتعلق بحماية الأشخاص الطبيعيين ذات الطابع الشخصي ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ،العدد 34.

[3]– أنظر المـــادة 1،2/22 من القانون نفسه.

[4]–انظر المادة 23 من القانون 18– 07، السالف الذكر.

و الترخيص بنقل المعلومات إلى الخارج في حال إذا كانت هذه الدولة تضمن مستوى حماية كافة للحياة الخاصة و الحريات و الحقوق الأساسية للأشخاص إزاء معالجة المعطيات.

كما يلزم رئيس السلطة و أعضائها حسب المادة (26) من نفس القانون بالمحافظة على الطابع السري للمعلومات و المحافظة على المعلومات التي اطلعوا عليها خاصة بعد انتهاء مهامهم و بالمقابل يستفيدون من حماية الدولة ضد أي تهديد أو إهانات أو اعتداءات من أي طبيعة كانت بمناسبة أو أثناء تأديتهم لمهامهم.

هذا و نص القانون على تزويد السلطة الوطنية بأمانة تنفيذية يسيرها أمين تنفيذي و يساعده مستخدمون بعد تأديتهم لليمين و المكور في المادة 27 منه أمام مجلس قضاء الجزائر على أن يحدد التنظيم شروط و كيفيات إستحداث هذه الأمانة[1] .

كما تكلف السلطة الوطنية بتأمين الإرسال عن طريق التشفير متى استدعت نوعية و أهمية المعطيات خاصة إذا كانت ترسل عن طريق الشبكة، ويمكن لها إصدار أنظمة تحدد فيها الشروط والضمانات للشخص المعني متى تعلق الأمر بحرية التعبير و الصحة و الشغل و البحث التاريخي والإحصائي العلمي والمراقبة عن بعد و استعمال تكنولوجيا الإعلام والإتصال، و ذلك عن طريق التنسيق مع القطاعات المعنية[2]

ب.5 المنظومة الوطنية لأمن الأنظمة المعلوماتية:

وفقا لنص المادة 02 من المرسوم الرئاسي 20-05 فإن المنظومة الوطنية لأمن المعلوماتية[3] هي أداة الدولة في المجال أمن المعلوماتية و هي تشكل الإطار التنظيمي لأعداد الإستراتجية الوطنية لأمن الأنظمة المعلوماتية و تشمل مجلسا وطنيا مكلف بإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية و الموافقة عليها و توجيهها ووكالة لأمن الأنظمة المعلوماتية مكلف بتنسيق تنفيذ الإستراتيجية التي أعدها المجلس.

يعتبر المجلس إضافة إلى الوكالة و هياكل مختصة لوزارة الدفاع الوطني هيكل المنظومة الوطنية التي يعتبر من جملة أهدفها مكافحة الجريمة المعلوماتية، فأصبح الآن إلى جانب رجال التحقيق جهات

---

[1]- انظر المواد من 25 إلى 40 من القانون السابق.

[2]- أنظر المادة 29 من القانون نفسه.

[3]-المنظومة الوطنية لأمن الانظمة المعلوماتية موضوعة لدى وزارة الدفاع الوطني.

تعزز مهامهم و تساعدهم فيها تتمثل أساسا في المجلس الوطني لأمن الأنظمة المعلوماتية و الوكالة الوطنية لأمن الأنظمة المعلوماتية .

أ- دور المجلس الوطني لأمن الانظمة المعلوماتية في مكافحة الجريمة الالكترونية :

يتولى المجلس الوطني[1] لأمن الأنظمة المعلوماتية في إطار إعداد الإستراتيجية الوطنية مجال أمن الأنظمة المعلوماتية جملة من المهام منها ما يتعلق بالموافقة على اتفاقيات التعاون و الاعتراف المتبادل مع الهيئات الاجنبية في مجال امن الأنظمة المعلوماتية، إضافة إلى أنه للمجلس أن يبدي رأيا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الانظمة المعلوماتية هما المهمتين اللتان تساهمان في مكافحة الجريمة الإلكترونية.[2]

ب-وكالة أمن الأنظمة المعلوماتية:

تعتبر وكالة أمن الانظمة المعلوماتية مؤسسة عمومية ذات طابع اداري تتمتع بالشخصية المعنوية و الاستقلال المالي[3] ،يقع مقررها في الجزائر العاصمة ،تدير الوكالة لجنة توجيه و تزود بلجنة علمية [4]، تكلف الوكالة بعدة مهام في مجال أمن الأنظمة المعلوماتية، و في اطار مكافحة الجريمة الإلكترونية فإن الوكالة تقوم بإجراء تحقيقات رقمية في حالة الهجمات أو الحوادث التي تستهدف المؤسسات الوطنية.[5]

كما تسهر الوكالة على جمع و تحليل و تقيم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية، إضافة إلى متابعة التدقيق لأمن الأنظمة المعلوماتية[6].

---

[1]- حددت المادة 5 من المرسوم الرئاسي 20-05، الصادر في 2020/01/20، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ، الجريدة الرسمية العدد 04، الصادرة في 2020/01/21 .تشكيلة المجلس، بينما تنظيمه عالجته المادة 9.8.7 ، إضافة إلى المواد 16.10التي حددت طريقة سير عمل المجلس.

-أنظر المادة 4 من المرسوم نفسه.

[3]- أنظر المادة 17 من المرسوم نفسه.

[4]- حددت المادة 22 من المرسوم نفسه تشكيلة لجنة التوجيه.

- أنظر المادة 4/18 من المرسوم نفسه.

[6]- أنظر المادة 5،6/18 من المرسوم الرئاسي 20-05، السالف الذكر.

كما يمكن للوكالة اقتراح مشاريع نصوص تشريعية أو تنظيمية في مجال أمن الأنظمة المعلوماتية بعد الرأي المطابق للمجلس.[1]

الفرع الثاني: الأجهزة الدولية المختصة بالتحقيق في الجرائم الإلكترونية

أدى التطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الأنترنيت والإنتشار الواسع لها و السريع إلى ظهور أنماط جديدة من الجرائم هي الجرائم الإلكترونية، هذه الجرائم التي باتت تشكل خطراً على سرية النظم الحاسوبية أو سلامتها أو توافرها، بل إلى أمن البنى الأساسية الحرجة.[2]

فكون الجرائم الإلكترونية عالمية لأنها عابرة للحدود، فإن مكافحتها لا تتحقق إلا بوجود تعاون دولي، يسمح بالإتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك عن طريق إنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي هذه الجرائم، ومن أبرز الأجهزة الدولية المتخصصة في مكافحة هذه الجرائم الإلكترونية: المنظمة الدولية للشرطة الجنائية، الأوروبول، الأفربول، الأورجست وشنجن، وسنتعرض لدور كل جهاز من هذه الأجهزة كالآتي:

أولاً: المنظمة الدولية للشرطة الجنائية (الإنتربول/INTERPOL)

تعد المنظمة الدولية للشرطة الجنائية إحدى الأجهزة الدولية التي تم إنشائها لمكافحة الإجرام بصفة عامة، لتهتم بعد ذلك بالجريمة الإلكترونية بصفة خاصة نظراً لخطورتها أين دعت الحاجة لوجود كيان دولي يتمتع بامتيازات وحصانات موسعة ومتميزة تكفل التعاون الدولي ضد الجريمة والمجرم، فكان ظهورها لازماً بإعتبارها المنظمة العالمية الوحيدة المتخصصة أصلاً في مجال مكافحة الجريمة.[3]

والإنتربول هي أكبر منظمة شرطية دولية، أنشأت سنة 1923 ومقرها الرئيس في مدينة ليون بفرنسا،[4] تحت اسم اللجنة الدولية للشرطة الجنائية،[1] تتألف من 177 دولة عضواً ، لها مكاتب وطنية وطنية في كل دولة من الدول الأعضاء.[2] وتستخدم هذه المنظمة وسيلتين لتحقيق أهدافها:

---

[1]– أنظر المادة 12/18 من المرسوم السابق.

[2]– حسين بن سعيد الغافري، المرجع السابق، ص 636.

[3]– نادية دردار، المرجع السابق، ص 128.

[4]– عادل عبد العال إبراهيم خراشي، دور الضبطية الإدارية والقضائية، في مكافحة جرائم بطاقات الائتمان الإلكترونية و التعاون الأمني الدولي حيالها، دار الجامعة الجديدة، الإسكندرية، 2015، ص 126.

- الوسيلة الأولى: القيام بتجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم، عن طريق المكاتب المركزية الوطنية للشرطة الجنائية الدولية المتواجدة في أقاليم الدول الأعضاء.
- الوسيلة الثانية: تتمثل في التعاون في ضبط وملاحقه المجرمين الفارين، وتسليمهم إلى الدولة التي تطلب تسليمهم وهي بذلك متخصصة بمكافحة الجرائم ذات الطابع الدولي كما تختص بمكافحة الإجرام المنظم العابر للحدود بجميع صوره بما في ذلك الجريمة الإلكترونية.[3]

تتألف المنظمة الدولية من عدة أجهزه رئيسية تعمل في إطار تجسيد الأهداف المبتغاة من وراء إنشاء هذه المنظمة تتمثل فيما يلي:

1- الجمعية العامة: هي أعلى سلطه تشريعيه في المنظمة تتكون من كل مندوبي الدول يختارون من طرف حكومات بلدانهم وفقا لما نصت عليه المادة 6 من دستور المنظمة، تعين الدولة وفدها من المتخصصين في إدارة الشرطة وغالبا ما يضم الوفد رئيس المكتب المركزي الوطني للشرطة الجنائية الدولية،[4] يترأس اجتماعات الجمعية العامة رئيس المنظمة ويدير جلساته العامة، وذلك بمشاركة نوابه ويكون لكل منهم رئاسة في هذه الجلسات تفتح أعمال الجمعية بحضور رئيس الدولة التي تعقد الجمعية العامة بها، وفي الدول ذات الأنظمة البرلمانية يقوم رئيس مجلس الوزراء بافتتاح أعمال الجمعية العامة وبحضور وزير داخليتها.[5]

أما بالنسبة لاختصاصات الجمعية العامة فتتمثل في تحديد السياسة العامة للمنظمة ووضع السياسة المالية لها بالإضافة إلى إصدار التوصيات والقرارات لأعضائها و دراسة و إقرار الاتفاقيات التي تعقدها المنظمة مع الهيئات الأخرى.

---

[1]- منتصر سعيد حمودة، المنظمة الدولية للشرطة الجنائية الانتربول، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008، ص 11.

[2]-كوركيس يوسف داوود، الجريمة المنظمة، الطبعة الأولى ، الدار العلمية الدولية للثقافة والنشر والتوزيع، عمان، الأردن، 2001، ص110.

[3]- محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، بدون بلد نشر، 2016، ص 184.

[4]- سراج الدين الروبي، آلية الإنتربول في التعاون الدولي الشرطي، الطبعة الثانية ، الدار المصرية اللبنانية للطباعة والنشر، 2001 ، ص 7.

[5]- سراج الدين الروبي، المرجع نفسه، ص 7-8.

تقوم الجمعية العامة بجميع هذه الأعمال بهدف تأكيد وتشجيع المعونة المتبادلة بين أجهزه الشرطة وإقامة النظم التي تسهم بشكل فعال في مكافحه ومنع الجريمة[1].

من اختصاصات الجمعية العامة كذلك، الموافقة على انضمام الدول لعضوية المنظمة، وانتخاب رئيس المنظمة ومساعديه والأمين العام وأعضاء اللجنة التنفيذية إضافة إلى وجوب موافقتها على تعيين المستشارين في المنظمة وهي التي تنحي المستشار عن وظيفته بقرار يصدر عنها، وتختص كذلك بوضع أسس المساهمة المالية للدول الأعضاء في مالية المنظمة، وتختص بالموافقة على العلاقات التي تربط منظمة الانتربول مع الهيئات الأخرى وتختص كذلك بالنظر فيما ترفعه إليها الدولة العضو المخلة بالتزاماتها المالية والتي قررت اللجنة التنفيذية حرمانها مؤقتا من حق التصويت في الجمعية العامة والاستفادة من خدمات المنظمة.

2- اللجنة التنفيذية: هي جهاز تابع لمنظمة الانتربول ويضم البعض من الدول الأعضاء في المنظمة، وتتكون وفق لنص المادة 15 من قانونها الأساسي من 13 عضوا هم رئيس منظمة الأنتربول ونوابه الثلاثة تنتخبهم الجمعية العامة من بين مندوبي الدول الأعضاء، ويجب الحصول على أغلبيه ثلثي أصوات أعضاء الجمعية العامة مدة ولاية الرئيس أربع سنوات، أما بالنسبة للنواب الثلاث يتم انتخابهم لمده 3 سنوات ولا يجوز إعادة انتخابهم لشغل نفس الوظائف أو لعضوية اللجنة التنفيذية، ويجب أن يكون الرئيس والنواب من بلاد مختلفة.[2]

أما بالنسبة للأعضاء التسعة الآخرين تنتخبهم الجمعية العامة من بين أعضائها لمدة 9 سنوات دون إعادة انتخابهم لنفس الوظائف إعطاء الفرصة لمندوبي الدول الأخرى مراعاة لمبدأ التمثيل الجغرافي العادل.[3]

يعمل رئيس منظمة الانتربول على رئاسة جلسات اللجنة التنفيذية وإدارة المناقشات فيها، وتجتمع هذه اللجنة مرتين في السنة بناءاً على دعوة رئيس المنظمة[4]، وفيما يخص اختصاصات ومهام اللجنة التنفيذية فقد حددتها المادة 22 من قانونها الأساسي والمتمثلة فيما يلي:

- الإشراف على تنفيذ قرارات الجمعية العامة.

---

[1]- نادية دردار، المرجع السابق، ص 137.

[2]- نادية دردار، المرجع نفسه، ص 137.

[3]- عكروم عادل، المرجع السابق، ص 151.

[4]- نادية دردار، المرجع السابق، ص 138.

- إعداد جدول أعمال الجمعية العامة.
- الإشراف على عمل وإدارة الأمين العام للمنظمة.
- مباشرة كافة الاختصاصات التي تفوضها لها الجمعية.
- تعيين أماكن انعقاد دورات جمعيه العامة، إن رأت أن المكان المعين من الجمعية العامة غير ملائم.
- فحص ميزانية الأمانة العامة والإذن لها بقبول التبرعات و الجوائز الممنوحة للمنظمة.
- متابعة نشر مجلة الشرطة الدولية، وفحص طلبات المنح التدريبية للضباط العاملين بها.
- تختص اللجنة التنفيذية بمراجعه الميزانية وفحصها في أي وقت تشاء وإن كان للسكرتير العام للمنظمة مسؤولية إدارة ميزانية المنظمة.
- تحدد المبادئ التي تسير عليها المكاتب المركزية الوطنية في عملها اليومي، وتحديد قنوات الاتصال مع الأمانة العامة.
- تجتمع اللجنة التنفيذية العامة مرتين على الأقل كل عام، لمدة تتناسب مع انتهاء مناقشة برنامج العمل الذي تعده الأمانة العامة في مقر المنظمة، أما المرات الثالثة و الرابعة كما جرت العادة ففي الدولة المضيفة لاجتماعات الجمعية العامة.[1]

3- الأمـــــــانة العامـة: يجب أن يكون للمنظمة الدولية جهاز إداري يتولى تصريف الأعمال اليومية للمنظمة ويتكون من موظفين إداريين وفنيين يباشرون أعمالهم من مقر المنظمة وهذا الجهاز موجود بصفة مستمرة يطلق عليه تسميه الأمانة العامة.[2]

يرأس الأمين العام الأمانة العامة في مقّرها بمدينه ليون بفرنسا ويقيم إقامة كاملة في هذا المقر ويشرف إشرافا عاما عليها، من خلال إشرافه المباشر على مكتبه التنفيذي والمراقب المالي بالإضافة إلى الأمين تقوم المنظمة الدولية للشرطة الجنائية على أربعة أقسام أو إدارات[3] وهـــــي:

قسم الإدارة العامة، قسم التنسيق الشرطي، قسم البحوث والدراسات ،القسم الخاص بالمجلة الدولية للشرطة الجنائية.

4-المستشارين:

---

[1]- منتصر سعيد حمودة، المرجع السابق، ص 43-47

[2]- عكروم عادل، المرجع السابق، ص 153.

[3]- سراج الدين الروبي، المرجع السابق، ص 193.

تختص اللجنة التنفيذية بتعيين المستشارين في المنظمة لمدة ثلاث سنوات ويكون المستشارين من بين ذوي الخبرة والدراية في المسائل العلمية التي تهم المنظمة، لأنه في مجال مكافحة الجريمة قد يثور أمام المنظمة بعض الأمور العلمية ذات الصلة بمكافحة الجريمة، وبالتالي فهي تلجأ لهؤلاء المستشارين بهدف الاستئناس برأيهم في تلك الأمور العلمية ولهؤلاء المستشارين حق حضور دورات انعقاد الجمعية العامة للإنتربول –كمراقبين– بناءا على دعوة رئيس المنظمة [1].

5–اللجنة الدائمة لتكنولوجيا المعلومات:

تتكون هذه اللجنة من رؤساء المحطات الإقليمية ومن ممثلي عدد من المكاتب الوطنية المركزية وهي تجتمع مرتين في السنة وتقدم المشورة الفنية للجنة التنفيذية عندما تعتزم المنظمة استخدام وسائل تكنولوجية جديدة[2].

6– المكاتب المركزية الوطنية:

وهي الجهاز المساعد المنظمة الدولية للشرطة الجنائية من أجل بلوغ أهدافها التي تحتاج إلى تعاون دائم وتنشيط من الأعضاء الذين يتوجب عليهم بذل كافه الجهود المنسجمة مع قوانين بلدانهم للمشاركة بمهمة في نشاطات هذه المنظمة [3]، تحقيقا لفعالية التعاون الدولي خاصة بعد أن أثبتت التجارب أن التعاون الدولي تعترضه ثلاثة عقبات كبيرة وهي:

- اختلاف البنية التنظيمية الشرطية للدول مما يجعل التعاون فيما بينها جد صعب.
- اختلاف اللغات.
- الاختلاف في التشريعات القانونية بين الدول.

كل هذا استوجب على كل دولة عضو في المنظمة الدولية للشرطة الجنائية إنشاء مكتب مركزي وطني له يكون هذا المكتب حلقه الاتصال ومن اختصاصاته:

- تحقيق الاتصال الشرطي بين الدولة التي ينتمي إليها وبين الأمانة العامة للمنظمة الدولية للشرطة الجنائية.

---

[1]– نادية دردار، المرجع السابق، ص 144.

[2]– نادية دردار، المرجع نفسه ، نفس الصفحة.

[3]– حبيب عباسي، المرجع السابق، ص 552

- تحقيق الاتصال بين السلطات المحلية وبين المكاتب المركزية الوطنية للشرطة الدولية في الدول الأخرى[1].

ومن أجل مكافحة هذا النوع المستحدث من الإجرام قامت منظمة الانتربول بوضع استراتيجيات محكمة بالتعاون مع المجموعة الثامنة(**G8**) وذلك من خلال:

- إنشاء مركز اتصالات أمني عبر الشبكة يعمل 24 ساعة على 24 ساعة و 7 أيام على 7 أيام على مستوى مصالح البوليس في الدول الأطراف.
- استخدام وسائل حديثة في مكافحة هذه الجرائم حيث استحدثت المنظمة عدد من فرق العمل تضم خبراء من أنحاء دول العالم متخصصين في مختلف الجرائم منها الجرائم الإلكترونية.[2]

إضافة إلى ذلك تقوم المنظمة بتزويد شرطة الدول الأطراف بكتيبات إرشادية حول الجرائم الإلكترونية وكيفية التدريب على مكافحتها والتحقيق فيها مثل ذلك الذي قدمته الشرطة الأوروبية والذي تم مناقشته في اجتماع Poitiers والمسمى "بدليل جرائم الحاسب الآلي"[3]

وهكذا يتولى الانتربول[4] إقامة العلاقات بين الدول وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بالجرائم المتشعبة في عدة دول كالجرائم الإلكترونية.

ثانيا: مركز شرطه الأوروبية أو الأوروبول (EUROPOL)

الأوروبول هو أحد الأجهزة المتواجدة على المستوى الأوروبي والتي تتخذ من لاهاي بهولندا مقرا لها، وقد تم إنشاء الأوروبول من قبل المجلس الأوروبي في لكسمبورغ سنه 1991، وهي منظمة عن

---

[1]– عكروم عادل، المرجع السابق، ص 159

[2]– محمد عبد الله ابراهيم ، المرجع السابق، ص 158

[3]– محمد عبد الله ابراهيم، المرجع نفسه، نفس الصفحة.

[4]– إلى جانب الأنتربول، توجد منظمات أخرى لها دور فعال في معالجة إشكالية مواجهة هذه الأنواع من الجرائم على المستوى الدولي، كمنظمة التعاون الاقتصادي والتنمية (O E C D) ومجموعة الثمانية الاقتصادية، التي قامت بإعداد ملتقى دولي مع منظمات دولية أخرى وبعض الدول (مصر، الصين) في نهاية نوفمبر 2000 في طوكيو لتكوين قوة دولية تسمـــىTHE DIGITAL OPPORTUNITY تتمثل مهامها في تحقيق أمن تكنولوجيا المعلومات.

طريق الاتفاقية الأوروبية الموقعة في 1995/7/26 والتي تحدد مهامها و المسماة باتفاقيه ماستريخت[1] واتفاقيه الاتحاد الأوروبي[2].

وتجدر الإشارة في هذا السبب أن فكره إنشاء هذا الجهاز الأوروبي للشرطة ترجع إلى اقتراح تقدّم به المستشار الألماني **HELMUT Kohl** في1991/6/23 بحيث يكون هذا الجهاز على نموذج الشرطة الفيدرالية الألمانية أي بمثابة **FBI** مكتب فيدرالي أوروبي للتحقيقات وهي مكلفة بمكافحة الإجرام عن طريق معالجة المعلومات المرتبطة بالأنشطة الإجرامية على مستوى الإتحاد الأوروبي، ودعم وتشجيع سلطات التحقيق، وذلك بتكميل وسائلهم وتحديثها من أجل مكافحة جميع أنواع الإجرام الخطير، وكذا بتسهيل تبادل تلك المعلومات عن طريق تزويد المحققين بتحاليل عملية و إستراتيجية، ويدعمهم بخبراته ومدهم بمساعداته التقنية.[3]

وللأوروبول دور فعال في مكافحة جرائم الانترنت، حيث نجده يقوم بتسهيل التحقيقات المرتبطة بوقائع بث او بامتلاك المواقع الإباحية ونشرها عبر الانترنت في الدول الأوروبية.

وتجدر الإشارة إلى أن ملفات التحليل الثريّة بالمعلومات المبلغة من قبل سلطات التحقيق التابعة للدول الأطراف في الإتحاد الأوروبي ، تمثل وسيلة هامة في عمل المحققين وفي مكافحتهم للشبكات الإجرامية مثل ملف تحليل الدعارة عبر الانترنت.[4]

ثالثاً: جهاز الأفريبول AFRIPOL

خطت آلية التعاون الشرطي الأفريقي أفريبول أولى خطواتها العملية من خلال تدشين الذي احتضن هذا المشروع الإفريقي والكائن بـــ: بن عكنون بالجزائر العاصمة ، تم افتتاحه في ديسمبر ويتكون من

---

[1]– أبرمت اتفاقية ماستريخت في 7 من فبراير1992 والتي دخلت حيز التنفيذ سنة 1993، بّينت هذه الاتفاقية أن الانفتاح بين دول الإتحاد الأوروبي يستفيد منه المجرمون مثلما يستفيد منه المواطنون العاديون وهو ما يتطلب توثيق صلة التعاون القضائي والأمني بما فيها إنشاء جهاز إقليمي بين دول الإتحاد. أنظر:
MICHEL Quille, Ouropol, La Criminalité Organisée , Sous La Direction De Marcel , LECLERC, Paris, 1996, P264 et 265.

[2]– محمد عبد الله ابراهيم ، المرجع السابق، ص 185–186.

[3]– محمد عبد الله ابراهيم، المرجع نفسه، ص 186.

[4]– محمد طارق عبد الرؤوف الخن ، المرجع السابق، ص 240.

ثمانية مكاتب وقاعتين للمحاضرات، الذي سيشكل أداة للتعاون الشرطي الدولي، تضمن ردا مشتركا أمام التهديدات المستحدثة الماسة بالسلم و الأمن، وستضمن أفريبول نشاطاً يتماشى ومبادئ الديمقراطية و إحترام حقوق الإنسان وسيادة القانون .

وأكد وزير الداخلية والجماعات المحلية نورالدين بدوي لدى إشرافه على افتتاح أشغال اجتماع المديرين والمفتشين العامين للشرطة الأفارقة حول الأفريبول، عزم الجزائر المتواصل على دعم هذه الألية الإفريقية للتعاون الشرطي، والسعي مع جميع الأطراف للرقي بعملها وأدائها، ورفع مستوى التنسيق والتعاون فيما بين دول القارة ومع باقي الشركاء في مكافحة الجريمة العابرة للحدود[1].

وأوضح اللواء عبد الغني هامل المدير العام للأمن الوطني آنذاك، أن الغاية الأولى للأفريبول تتمثل في تعزيز مجالات التكوين وتبادل الخبرات وكذا الممارسات الأمنية الصحيحة فيما يخص مكافحة الجريمة ونشاطاتها، مشيراً إلى أن الهيئة الجديدة تسعى إلى تأهيل بعض أجهزة الشرطة الإفريقية في مجال التكوين وتحديث الوسائل والتجهيزات، مضيفاً بضرورة تنظيم دورات تكوينية لصالح أعوان الشرطة وأخرى للطلبة الضباط، تكثيف تبادل التجارب المميزة على المستوى الإقليمي والدولي تجلت من خلال تطبيق عدة برامج في مجالات هامة كالتكوين التخصصي، ورفع جودة التدريب واستعمال تكنولوجيا الإعلام و الإتصال.[2]

كما أكد اللواء عبد الغني هامل أن أفريبول تشكل أداة تعاون دولي لا يمكن الاستغناء عنها في مجال الشرطة لمواجهة المخاطر الجديدة التي تهدد السلم والأمن، وتعتبر كذلك الحلقة القوية في سياق التحالف الاستراتيجي.

رابعاً: الأورجست EURJUST

يتواجد الأورجست على المستوى الأوروبي، كجهاز يساعد على التعاون القضائي والشرطي في مواجهة ومكافحة جميع أنواع الجرائم الخطيرة، تم إنشاؤه سنة 2002، من قبل مجلس الإتحاد الأوروبي، ولقد تم إنشاؤها بهدف تقوية مكافحة جميع أنواع الإجرام الخطير، وتنعقد اختصاصاته عندما يمس ذلك الإجرام دولتين على الأقل من أعضاء الإتحاد الأوروبي أو دولة عضو مع دولة من

[1]– راجع الموقع الرسمي للأفريبول : www.el-mass.com/dz ، تاريخ الزيارة 2017/05/16 على الساعة 10:00 .

[2]– الموقع الرسمي للأفريبول، المرجع السابق.

دول العالم الثالث أو دولة عضو مع الرابطة الأوروبية، وهي في ذلك غير مقتصرة على الأشخاص بل تشمل كذلك المؤسسات.[1]

وتجدر الإشارة أن الأورجست يمثل دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية، وخصوصا فيما يتعلق بالأنشطة المرتبطة بجرائم الأنترنيت، حيث تعتبر جرائم الأنترنيت من الجرائم التي تختص المنظمة بمكافحتها، ومن أهم نشاطات الأورجست ما يلي:

- تحسين التنسيق والتعاون بين السلطات القضائية المختصة لدول الأطراف.
- تبادل المعطيات بين دول أعضاء الإتحاد الأوروبي وكذا التحفظ عنها.
- كما يمكنه أن يطلب من الوكلاء العامين ذوي الإختصاص الوطني إجراء تحقيقات أو إجراء ملاحقات أو التبليغ عن الجرائم إلى السلطات المختصة للدول الأطراف.[2]

خامساً: شنجن SCHENGEN

تم إنشاء فضاء جماعي لا حدود له، أطلق عليه اسم شنجن وذلك من خلال التوقيع على معاهدة شنجن في 1985/06/14 وعلى اتفاقية تطبيق تلك المعاهدة في 1990/06/19، وقد استحدثت هذه الإتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوروبي لمواجهة التحديات الأمنية، منها الجرائم الإلكترونية، وهاتان الوسيلتان هما: مراقبة المشتبه بهم عبر الحدود، وملاحقة المجرمين.[3]

المطلب الثاني: إعتماد نظام التدريب لتفعيل التحقيق في الجريمة الإلكترونية

التدريب[4] يعد جزءاً من عملية التنمية الإدارية وهو يهتم بالدرجة الأولى بالكفاءة والفعالية في إنجاز العمل، بإعتباره أحد الأدوات الأساسية لرفع مستوى الأداء وزيادة الكفاية الإنتاجية وإعداد العاملين على إختلاف مستوياتهم للقيام بواجبات أعمالهم والأعمال الموكلة لهم على خير وجه، لهذا

---

[1]– طارق عبد الرؤوف الحن ، المرجع السابق، ص 240

[2]– محمد عبد الله ابراهيم ، المرجع السابق، ص 187.

[3]– محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 240–241.

[4]– يعرف التدريب بأنه: نشاط مستمر ومخطط يهدف إلى سد الفجوة بين الأداء الحالي والأداء المتوقع لشاغل الوظيفة فهو يقوم على أساس تحديد المهارات والقدرات الواجب توافرها في شاغل الوظيفة، ومن تم إحداث التغيرات في السلوك وقدرات الفرد أو الجماعة المسؤولة عن أداء هذه الوظيفة، ويعرف أيضاً بأنه: " عملية منظمة ومستمرة، تهدف إلى إحداث تغيرات التي تعرضها الإحتياجات التدريبية في عقلية الأفراد وقيمهم وسلوكياتهم، من اجل رفع مستوى أداء المنظمات أو معالجة إشكاليتها أو تمكينها من = مواجهة تحديات مستقبلية محتملة." أنظر: عامر خضير حميد الكبيسي، التدريب الأمني العربي، واقع وآفاق تطويره، جامعة نايف للعلوم الأمنية، الرياض، 2007، ص13.

أصبح ينظر إلى التدريب على أنه وسيلة للاستثمار الذي تلجأ إليه المنظمات الإدارية لتحقيق أهدافها بإعتباره عنصرا حيويا لابد منه لبناء الخبرات والمهارات المتجددة.[1]

والتدريب المقصود ليس التدريب التقليدي فحسب، فلا يكفي أن تتوافر لدى رجال العدالة الجزائرية الخلفية القانونية أو أركان العمل الشرطي و إنما لابد من اكتسابهم خبرة فنية في مجال الجريمة الإلكترونية، وهذه الخبرة الفنية لا تتأتى دون تدريب تخصصي يراعى فيه العناصر الشخصية للمتدرب من حيث توافر الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب.[2]

وتبدو أهمية وضرورة التدريب في أنه من جهة يعد الوسيلة الفعلية والتطبيقية الناجحة التي تضمن الإستفادة من مهارات وتجارب الآخرين من خلال أشخاص أكفاء مؤهلين وقادرين على نقل هذه التجارب وتلك المهارات بطرق سهلة وميسرة، كما أنه يعد من ناحية أخرى الوسيلة الملائمة والفعالة لوضع المعارف العلمية موضع التطبيق الفعلي والتعرف على الأخطاء والسلبيات التي يمكن أن يكتشف التطبيق العملي للقوانين والأنظمة، وضع الحلول الكفيلة بتجنبها، وتزداد أهمية التدريب نظراً للتطور التكنولوجي الكبير الذي يشهده العالم اليوم[3].

لهذا سنتناول المتدرب ومنهج التدريب (الفرع الأول) أما صفة وأسلوب التدريب (الفرع الثاني) ، ثم نتطرق في الفرع الثالث إلـــــى المحاكاة الحاسوبية كإحدى الوسائل التدريبية الحديثة.

الفرع الأول: المتدرب ومنهج التدريب

تتطلب عملية التحقيق في الجرائم الإلكترونية، وضع سياسة جنائية رشيدة، تستند على تدريب أجهزة العدالة الجنائية لمكافحة هذه الجريمة، ويمتد هذا التدريب إلى العاملين بأجهزة الضبطية القضائية، ولعملية التدريب الناجحة في هذا المجال عناصر يمكن إجمالها فيما يلـــي:

أولا: المتدرب

[1]– يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى، المصدر القومي للإصدارات القانونية، القاهرة، مصر، 2011، ص 176.

[2]– حسين بن سعيد الغافري، المرجع السابق، ص 679.

[3]– حسين بن سعيد الغافري، المرجع نفسه، نفس الصفحة. وأنظر أيضا: محمد سيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005، ص2.

حتى يأتي التدريب بثماره يجب أن تتوافر لدى المتدرب الصلاحية العلمية والقدرات الذهنية والنفسية لتلقي التدريب، وفيما يتعلق بالتدريب على التحقيق في الجرائم الإلكترونية، يلاحظ أنه من الأسهل تدريب متخصص في معالجة البيانات عن تدريب القائمين على تنفيذ القانون كرجال الشرطة وممثلي الإدعاء العام[1].

كما يجب أن تتوافر لدى المتخصص في معالجة البيانات الذي يتلقى التدريب خبرة لا تقل عن خمس سنوات في المجالات التالية المرتبطة بمعالجة البيانات: عمليات الحاسب، البرمجة، تصميم، النظم وتحليلها، إدارة المشروعات والخبرة في مختلف أنواع نظم الحاسوب ليست متطلبة وإن كان توافرها لدى المتدرب مرغوبا فيه.[2]

ثانياً: منهج التدريب (منهج الدورة التدريبية)

من العناصر الأساسية في دورة التدريب على التحقيق في الجرائم الإلكترونية تضمينها سائر المجالات الحيوية للمعرفة إضافة إلى محاضرات ودراسة حالات ونقل خبرات علمية في مختلف جوانب عمليات الحاسب، ويجب أن يتضمن منهج هذه الدورة الموضوعات التالية:

- المخاطر والتهديدات وأماكن الاختراق لشبكة المعلومات وأجهزة الحاسب والتي يمكن تعرضه لها.
- مفاهيم معالجة البيانات، سواءاً ما تعلّق منها بالبرامج أو الأجهزة.
- أنماط الجريمة الإلكترونية.
- أسلوب أو منهج التحقيق من حيث: إجراءات التحقيق، خطة التحقيق، كيفية تجميع المعلومات وعرضها (الاستدلالات)، المواجهة والاستجواب، النظم الفنية للبيانات، طريقة عمل المختبر الجنائي، أسلوب عرض ودراسة حالة[3].

يضاف إلى ذلك موضوعات أخرى مثل التفتيش والضبط، واستخدام الحاسب كوسيلة في الحصول على أدلة الإتهام، والتعاون الدولي المشترك في ملاحقة هذه الجرائم.

ومن الاتفاقيات الدولية التي أعطت أهمية للمنظومة التدريبية، اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية والتي نصت في المادة 1/29 من الإتفاقية على أنه: " تعمل كل دولة

---

[1]– هشام محمد فريد رستم ، المرجع السابق، ص41.

[2]– هشام محمد فريد رستم، المرجع نفسه ، ص 42.

[3]– عبد الفتاح بيومي حجازي ، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص 89-90.

طرف، قدر الضرورة، على إنشاء أو تطوير أو تحسين برنامج تدريب خاص للعاملين في أجهزتها المعنية القانون، ومنهم أعضاء النيابة العامة، وقضاة التحقيق وموظفو الجمارك، وغيرهم من العاملين المكلفين بمنع وكشف ومكافحة الجرائم المشمولة بهذه الاتفاقية ".

و من الأمثلة على أنماط التدريب والاهتمام به على المستوى العالمي:

1- تجربة الإتحاد الأوروبي في مجال التدريب على مكافحة الجريمة الإلكترونية:

كان للاتحاد الأوروبي تجربة في مجال التدريب على مكافحة الجرائم الإلكترونية، حيث يعتبر هذا الأخير من أهم الجهات التي قامت بالمشروعات والبرامج التدريبية الهادفة لمكافحة الجرائم عالية التقنية من خلال أحد مؤسساتها وهو مركز التدريب الوطني عن الجرائم التقنية NSLEC، قد أعد هذا المركز العديد من المشروعات والبرامج التي تتعامل مع مكافحة هذه الجرائم، ولعل أهمها مشروع فالكون 2001 وأيضاً برنامج أجيس 2004/2003[1].

أ- مشروع فالكون 2001 للتدريب على مكافحة الجريمة الإلكترونية:

ينظم هذا المشروع العديد من الدورات التدريبية في إطار الإتحاد الأوروبي تختص بمواجهه الجرائم الإلكترونية، من أهم توصياته:

- الاتفاق على أن المنهج الأوروبي للتدريب مطلوب في سائر أنحاء الإتحاد الأوروبي.
- يـــــلزم على مؤسسات الأكاديمية أن تعتمد هذا تدريب.
- ينصح بالتعاون بين المؤسسات الأكاديمية وأجهزه انفاد القانون في كل دولة من دول الاتحاد الأوروبي.
- الحاجة إلـــــى عقد دورات تخضع لمراقبة وإدارة جهاز مركزي.

كــما ينظم المشروع الدورات التدريبية التالية:

- الدورة الأساسية في تحقيقات الحاسوب والانترنت
- الدورة المتوسطة (دبلوم) في تحقيقات الحاسوب والانترنت والشبكات، ويمكن التنويع في المواد الخاصة التي يتلقاها المشارك بحيث توفي بمتطلباته في مجال محدد.

[1]- رامي متولي القاضي ،مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية ، الطبعة الأولى، دار النهضة العربية، القاهرة 2011، ص 167.

- الدورة المتقدمة في تحقيقات الحاسوب والأنترنيت ويمكن توزيع المواد التي يتلقاها المشارك بحيث توفي بمتطلباته في مجال محدد.[1]

ب-مشروع أجيس 2004/2003[2] للتدريب على مكافحه الجريمة الإلكترونية:

يهدف مشروع أجيس إلى ما يلي:

- توفير برنامج تدريبي أوروبي نموذجي معتمد يمكن أجهزه تنفيذ القانون من مكافحة الجريمة الإلكترونية.
- تدعيم المتطلبات المنصوص عليها في المادة (35) من اتفاقية المجلس الأوروبي حول الجريمة الإلكترونية والتي نصت على إلزامية أن تتكفل كل دولة من الدول الأطراف بتوفير الأفراد المدربين والمجهزين، لتسهيل عمل الشبكات ومن خطط هذا المشروع ما يـــــلي:
- تطوير وتقديم برنامج تدريبي تعاوني حول الجريمة الإلكترونية للعاملين في أجهزه تنفيذ القانون في الدول الأوروبية.
- توفير إطار ابتكاري ومستديم في دول الإتحاد الأوروبي والدول المرشحة للانضمام إليه.
- توفير المواد التدريبية التي يتم تطويرها بموجب هذا المشروع إلى دول الإتحاد الأوروبي والدول الطالبة للتدريب بغرض تشجيع الممارسات المثلى وكفالة اتساق معايير التدريب.
- توزيع الدروس المستفادة من هذا المشروع على دول الإتحاد الأوروبي والدول طالبة التدريب، من أجل تشجيع التعاون الوثيق بين الدول.
- اشتراك المعاهد الأكاديمية بهدف خلق إطار معتمد وموثق للتدريب يدعم تطوير المستويين الثاني والثالث من العملية التدريبية وفقاً للنمو الموصف في مشروع فالكون[3].

2- تجربة الولايات المتحدة الأمريكية في مكافحة الجريمة الإلكترونية:

[1]- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة،2013، ص 409.

[2] - شارك في هذا المشروع كل من النمسا وبلغاريا و الدانمارك وفرنسا وألمانيا والمجر وايرلندا لكسمبورغ والبرتغال واسبانيا والمملكة المتحدة والمفوضية الأوروبية والشرطة الأوروبية و الانتربول.

[3]- سليمان أحمد فضل، المرجع السابق، ص410.

تعد الولايات المتحدة الأمريكية من الدول المتقدمة تكنولوجيا والمتطورة تقنيا في مجال مكافحة الجرائم الإلكترونية، وعلى الرغم من ذلك فهي تعلم أنه ما من دولة وإن كانت متقدمة يمكنها التصدي لأخطار هذه الأنماط المستحدثة من الجرائم، لهذا نجدها تحرص على مكافحة الجريمة المعلوماتية من خلال توفير المساعدة التقنية والتدريب لرفع قدرات العدالة الجزائية لدى الحكومات الأخرى، ومساعدة ما لديها من أجهزة الشرطة والقضاة ليصبحوا أكثر فعالية في مكافحة الجريمة، فمثل هذه المساعدة لا تؤدي إلى تيسير بناء إطار الدولي في مجال تطبيق القانون وحسب، ولكنها تعزز أيضاً قدرة الحكومات الأجنبية المعنية على ضبط مشاكل الجريمة الإلكترونية لديها قبل أن يمتد يتجاوز حدود بلدانها.[1]

فمكتب المساعدة والتدريب على تطوير أجهزه الإدعاء العام في الخارج، التابع لوزارة العدل الأمريكية مكلف تحديدا بتوفير المساعدة اللازمة لتعزيز مؤسسات العدالة الجزائية في دول أخرى وتعزيز إدارة القضاء في الخارج.

كما أن البرنامج الدولي للمساعدة و التدريب على التحقيق الجزائي (ICITAP) الذي كثيرا ما يعمل مع مكتب المساعدة والتدريب على تطوير أجهزه الإدعاء العام في الخارج، والذي يعمل على توفير مساعدات لأجهزة الشرطة في البلدان النامية في مختلف أنحاء العالم، وتهدف المساعدة التي يقدمها هذا البرنامج الأخير إلى تعزيز القدرات التحقيقية لدى أجهزه الشرطة في البلدان الناشئة.

وفي الوقت الحالي، تقدم وزاره العدل الأمريكية مساعدات لتطوير القطاع القضائي في عدد من البلدان في إفريقيا ، آسيا ، أوروبا الشرقية والوسطى ، أمريكا اللاتينية والدول المستقلة حديثاً كروسيا والشرق الأوسط، مستعينة في ذلك بخبرة الوحدات المتخصصة التابعة لها، كوحدة مكافحة استغلال الأطفال وأعمال الفحش التابعة للقسم الجزائي بها والتي قامت بدور أساسي في صياغة قانون نموذجي يهدف إلى مكافحة استغلال الناس عن طريق الاتجار بالبشر.[2]

كما أنّ أجهزة تطبيق القانون الأمريكية توفر أيضا تدريبا لنظيراتها من الأجهزة في البلدان الأخرى داخل الولايات المتحدة الأمريكية أو خارجها عن طريق إنشاء معاهدة خاصة بتدريب العاملين في أجهزة تطبيق القانون كما هو الحال في كل من المجر، وبوتسوانا كوستاريكا و تايلندا، وفي هذه

[1]– حسين بن سعيد الغافري، المرجع السابق، ص 687–688.

[2]– حسين بن سعيد الغافري، المرجع نفسه ، ص 688.

المعاهدة يقوم خبراء أمريكيون في عمل أجهزة تطبيق القانون بإطلاع المتدربين على أساليب وسبل مبتكرة للتحقيق، كما يشجعون على تبادل الآراء مع نظرائهم في مختلف أنحاء العالم.[1]

الفرع الثاني: صفة وأسلوب التدريب

إن اعتماد نظام التدريب لتفعيل التحقيق في الجريمة الإلكترونية يتطلب أيضا التطرق إلى:

أولاً: صفة التدريب

إن التدريب على التحقيق في الجرائم الإلكترونية، يمكن أن يكون رسمي أو غير رسمي، والنمطان متكاملان، فلا يغني أحدهما عن الآخر.

فبالنسبة للتدريب الرسمي، فيمكن أن يتم من خلال حلقات دراسية وحلقات نقاش أو ما يسمى بورش العمل، تعقد حول جرائم الحاسب أو إساءة استخدامه أو كلاهما وكذلك حول أمن الحاسب، وحلقات النقاش التي يمكن أن تثمر أفضل تدريب رسمي هي تلك التي تكفل تفاعل المشاركين وتتضمن تحليلاً لحالات دراسية، واكتساب خبرة علمية في الحاسب، ومحاضرات تتعلق بذلك، ومن اللازم حتى يتحقق لهذا التدريب فعاليته ويحقق أهدافه، أن يكون مستمراً، وأن يتضمن دروات في المحاسبة ومعالجة البيانات والمراجعة المحاسبية في نظم المعالجة الآلية للبيانات والتحقيق وأمن المعلومات.

أمّا التدريب غير الرسمي يكمن أن يتلقاه الفرد عن طريق تكليفه بالعمل مع شخص لديه خبرة في تحقيق الجرائم الناشئة عن الحاسب، ومن الوسائل الأخرى لتقديمه " تناوب العمل" الذي لا يزيد عن تكليف المتدرب بأن يقضي فترة من الوقت في كل قسم من الأقسام المختلفة لمعالجة البيانات والعمل كذلك مع أفراد أمن الحاسبات[2].

ثانياً: أسلوب التدريب

أكثر أساليب تدريب محققي الجرائم الإلكترونية ملائمة لطبيعة هذه الجرائم وخصائص بيئة تكنولوجيا المعلومات هو ذلك الموسوم بأسلوب الفريق، والذي تقوم فلسفته على تدريب الفريق أو مجموعة متخصصة في الجرائم الإلكترونية مرة واحدة.

---

[1]– يوسف حسن يوسف، المرجع السابق، ص 184.

[2]– هشام محمد فريد رستم ، المرجع السابق، ص44 –45. وأنظر أيضاً : خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، بدون بلد نشر، 2012، ص 89.

بحيث يكون لكل فريق من الفرق [1] مهمه محددة، فضلاً عن إلمامه بمهام زملائه الآخرين فطبقاً لهذا الأسلوب يتم التركيز على تدريب مجموعة من المتخصصين في مجالات معينة، بحيث يلزم كل منهم بتخصص الآخرين ويزداد في نفس الوقت فهما لتخصصه الأصلي.[2]

يتعين هنا على الفريق أن يخوض تجارب عملية بحيث تعرض عليه عينة من الجرائم الإلكترونية التي تم التحقيق فيها، على أن يراعي في هذه العينة التنويع لكي تؤدي دورها في اكتساب المشاركين في البرنامج التدريبي الخبرة المطلوبة[3].

تحقيق نتائج جيدة في عملية التدريب، والعملية التدريبية لابد وأن تكون تماثل فلسفة تدريب هؤلاء الفرق فلسفة الدرجات العلمية في مجال إدارة الأعمال، والتي تتضمن موضوعين رئيسيين هما[4]:

- تعليم متخصصون في مختلف فروع العلم ليصلوا إلى درجة مشتركة من البراعة و الاحتراف، ومن الوجهة الواقعية، فإن المحاسب في فريق التحقيق يتعلم المزيد من الرياضيات، ويتعلم خروج العلوم أو الهندسة، ويتعلم خريج الحقوق كل من المحاسبة والرياضيات.
- ببلوغ مستوى المشترك للبراعة أو الاحتراف، تبدأ المرحلة الثانية من التعليم، وتتضمن استخدام دراسات حالة متزايدة التعقيد ومن المفترض أن تمكن هذه المرحلة أعضاء الفريق من معرفة كيفية معالجة الأعضاء الآخرون في الفريق للمشكلة المشتركة كل من زاوية خلفيته وتخصصه، ومع التناوب الملائم للأعضاء في الفرق المختلفة، سيتأقلم كل متخصص على العمل مع مجموعة متنوعة من المتخصصين الآخرين بأسلوب الفريق.

و الحالات الدراسية للجرائم الإلكترونية المتعين في هذه المرحلة عرضها وتحليلها، يجب أن تكون مفصلة، معبرة عن تنوع هذه الجرائم والمجالات المحتملة لارتكابها، وأن تدعم بمستندات أو تقارير أو أشرطة وأقراص ممغنطة أو غيرها من وسائط و أوعية بما يكفي لإضفاء الواقعية على الحالة الدراسية.

---

[1]– يتم تقسيم الفريق إلى ثلاثة مجموعات رئيسة هـــي:

أ– المجموعة الأولـــى: مهمتها تنفيذ القانون (رجال الضبط و التحقيق).

ب– المجموعة الثانية: متخصصون في التدقيق والمراجعة الحسابية.

جـ– المجموعة الثالثة : متخصصون في معالجة البيانات إلكترونياً.

[2]– يوسف حسن يوسف ، المرجع السابق، ص 178–179. وأنظر أيضاً: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص 91.

[3]– خيرت علي محرز، المرجع السابق، ص 90.

[4]– هشام محمد فريد رستم ، المرجع السابق، ص46.

كما ينبغي أن تشمل هذه الحالات على الأنماط الثلاثة التالية:

1) الحالة المركبة المبين فيها كل الوقائع مع وجود الحل بموضع ما داخلها بحيث يمكن التوصل إليه عن طريق التحليل المنظم للوقائع.
2) الحالة غير المرتبة التي تعرض فيها الوقائع، ولكنها تحتاج إلى إعادة تنظيم، مع تضمنها للحل بموضع ما بداخلها.
3) الحالة غير المرتبة التي قد تعرض فيها كل الوقائع أو لا تعرض، والتي قد يعرض فيها الاحتيال الذي تتضمنه أو لا يعرض[1].

في الأخير يمكن القول إن نجاح عملية التدريب تتطلب إسناده إلى جهات متخصصة تُعنى بإختيار المدربين ممن تتوافر لديهم الصلاحية العلمية والصفات الشخصية ليتولوا التدريب، والذي من شأنه تحقيق نتائج جيدة في عملية التدريب ، والعملية التدريبية[2] لابد وأن تكون مستمرة ولا تتوقف عند حد معين، خاصة وأن الجرائم الإلكترونية في تطور مستمر وبشكل سريع.

ليس هذا فحسب، بل لا بد وأن تسعى الجهة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ليكون ضمن كوادرها والاستفادة منهم، فغرس الثقافة الحاسوبية وسط رجال القانون والشرطة وربطها بالثقافة القانونية والشرطية يكفل للأجهزة الأمنية ولسلطات التحقيق النجاح في مواجهة الجرائم الإلكترونية.

وعن أهمية التدريب التخصصي في الرفع من كفاءة قوات الأمن أكد اللواء هامل عبد الغني المدير العام للأمن الوطني الجزائري سابقا أثناء ترأسه لفعاليات اليوم الدراسي حول التكوين في جهاز الأمن الوطني تحت عنوان "تطوير العمل التدريبي للارتقاء بجودة أداء منتسبي جهاز الشرطة" بولاية عنابة بتاريخ 15 سبتمبر 2014، أين اعتبر أن التكوين له فعالية في مواجهة التحديات والمستجدات الأمنية المستقبلية وأن اللجوء إلى التدريب و التأهيل التخصصي من شأنه أن يحقق نتائج ايجابية في

---

[1]– هشام محمد فريد رستم ، المرجع السابق، ص47.

[2]– اللواء هامل عبد الغني، المدير العام للأمن الوطني الجزائري سابقا: السنوات القادمة ستكون سنوات التدريب التخصصي، للمديرية العامة للأمن الوطني، مشار إليه على الموقع الإلكتروني:
www.algeriepolice.dz تاريخ الزيارة 6 جوان 2017 سا 11:0.

مجال صقل المهارات وتسليح الأفراد بالعلم والمعرفة ليكونوا قادرين على أداء مهامهم بكل قوة وعزم إلى درجة اعتبار أن السنوات القادمة ستكون سنوات التدريب التخصصي[1].

الفرع الثالث: المحاكاة الحاسوبية كإحدى الوسائل التدريبية الحديثة

تعتبر المحاكاة الحاسوبية من أحد الوسائل التدريبية والتعليمية الحديثة، وكذلك كأسلوب لكشف الجرائم فيما يعرف باسم إعادة تمثيل مسرح الجريمة، حيث يستفاد منها كأحد التطبيقات المعاصرة للكمبيوتر وفي كيفية إعداد نماذجها في عمليه التحقيق الجزائي.

وتعرف المحاكاة الحاسوبية بأنها: " عبارة عن التقليد المحكم الذي يطابق ويماثل الأصل تماما بحيث يتم التعايش مع ظروف وملابسات واحتمالات الواقع الفعلي للمواقف والأحداث بصورة تزيد من القدرة على التعامل مع مثل هذه المواقف في الحياة العملية" [2] ، كما تعرف أيضا بأنها: " قيام المحلل ببناء نموذج لما يريد دراسته يكون تمثيلا صادقاً للواقع الموجود في النظام وتجريداً لما فيه من مكونات وتفاصيل ثم يقوم بعدها بالتعامل مع النموذج بدلاً من النظام" [3].

من خلال التعريفين السابقين يتضح أن المحاكاة الحاسوبية تعني:

- التقليد المحكم أي نقل صورة الواقع بكافة أشكاله وصوره دون حذف أو إضافة.
- هي حالة افتراضيه غير واقعية يتم إعدادها لغرض توفير المناخ الطبيعي وظروفه وملابساته بنموذج المحاكاة.
- إمكانية إيجاد أكثر من نموذج وفقاً للمعلومات والبيانات المتاحة وخبرة وقدرة وإمكانات معد النموذج على الإستفادة منها في إعداد نموذج المحاكاة.
- قيام نماذج المحاكاة على أحدث المستجدات في مجال الحقيقة الافتراضية، يعني قيام جهاز الحاسوب ومن خلال مجموعة من الخبراء والتقنيين بإعداد عالم خيالي ثلاثي الأبعاد.

---

[1]– تعرف العملية التدريبية بأنها: " جموع الأنشطة أو العمليات الفرعية التي توجه لعدد من المتدربين لتحقيق أهداف معينة في برنامج تدريب معين وتحدث الأثر أو الآثار المطلوبة فيه.

[2]– محمد محمد درويش، التطلعات المستقبلية نحو استخدام أسلوب المحاكاة في مجال التدريب الأمني بأكاديمية الشرطة، مقال منشور بمجلة الأمن العام المصرية، العدد 46، ص51،

[3]– حسام محمد رمضان ،تطبيقات المحاكاة الحاسوبية في التخطيط والتدريب على إدارة الكوارث، مقال منشور بمجلة البحوث الأمنية ،أكاديمية الملك فهد، المجلد 11، العدد 22، أكتوبر 2002، ص204.

- وجود عدة مستويات للتعامل مع العالم الإفتراضي لنموذج المحاكاة، منها ما يسمى بالانغماس الكلي، والآخر يطلق عليه الانغماس الجزئي وفي الحالة الأولى ينغمس المتدرب كليّة مع الوقائع التي يتفاعل معها في العالم المفترض ثلاثي الأبعاد [1].

و يتطلب إعداد نموذج المحاكاة الحاسوبية فريق عمل متكامل لا يقتصر على خبراء الحاسب الآلي، بل كل من لهم دراية بكافة التفاصيل الدقيقة الخاصة بالموضوع الجاري إعداد النموذج من أجله، وهؤلاء الأشخاص يجب أن يكونوا من بيئة العمل ذاتها حتى يستطيعوا نقل كافة جزئياتها وبياناتها التي تمكن في نهاية الأمر من تطابق النموذج الحاسوبي المعد مع الواقع، كما يجب أن يتضمن هذا الفريق، كاتب سيناريو جيّد يستطيع صياغة الأفكار والحقائق والتفصيلات بالصورة المطلوبة ، وحتى يتم التطابق اللازم مع الواقع لابد من وجود خبراء للمؤثرات الصوتية و الضوئية مع فريق العمل القائم بإعداد النموذج[2].

و لإعداد نموذج المحاكاة الحاسوبية يستلزم الأمر تتبع الخطوات التالية:

- بيان أو تحديد المشكلة أو الحالة أو الواقعة المطلوب محاكاتها والهدف المراد تحقيقه من ذلك، وعما إذا كان ذلك سيحقق فائدة، وما مدى ملائمة أسلوب المحاكاة لتحقيق هذا الأمر.
- إعداد ما يسمى بالتصميم الأولي والذي يشمل الأركان الأساسية للموضوع وأحداثه الجوهرية والمتوقع من المتغيرات، ويمكن الإستعانة في إعداد هذا التصميم ببعض البرامج التي تقوم بتخزين المعلومات الخاصة بالجرائم وتساعد في إعداد قوائم المعلومات وكيفية توظيفها مع الاستعانة بأساليب تحليل المعلومات التي تمكن من التعرف على العلاقات والمؤثرات التي تربط بين العصابات والمنظمات الإجرامية، و أنواع الجرائم المرتكبة للوصول إلى المعلومات الجديدة التي تساهم في مواجهه الجريمة[3].
- بعد ذلك تأتي مرحلة جمع البيانات وتحليلها باعتبارها إحدى المراحل الهامة في إعداد نماذج المحاكاة الحاسوبية ويمكن الاستفادة مثلا في هذا المجال عند الحديث عن مجال التحقيق الجنائي من مادة تطبيقات الكمبيوتر في مجال تحليل الجرائم لأنها تساعد القائمين على هذا

---

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص151.

[2]– ممدوح عبد الحميد عبد المطلب، المرجع نفسه، ص152.

[3]– حسني درويش عبد الحميد، البحث الجنائي المعاصر، مقال منشور بمجلة البحوث الأمنية، كلية الملك فهد، المجلد 10، العدد 1522، نوفمبر 2001 ص152.

الأمر في كيفية القيام بعمليات جمع المعلومات والقيام بتحليلها وأساليب استخدام نتائج تحليل المعلومات في تغذية النموذج المراد إعداده بكافة المعلومات عن الجرائم المراد محاكاتها.

- تحويل التصميم المبدئي إلى برنامج حاسوبي، وهذا الأمر يعني تحويل السيناريو النظري الذي تم تجهيزه في ضوء البيانات والمعلومات التي تم تجميعها وتحليلها إلى نموذج حاسوبي، ثم اختيار لغة البرمجة المناسبة لهذا الغرض.
- ويلي مرحلة التصميم المبدئي إلى برنامج حاسوبي خطوات تهدف إلى التحقق من صحة النموذج وصلاحيته للتأكد من توفيره لبيئة المحاكاة التي يقصد بها البرنامج الحاسوبي المتكامل، الذي يوفر للمبرمج واجهة رسومية وتسهيلات برمجية عديدة تمكنه من تطوير برنامج المحاكاة المطلوب بسهولة ويسر[1].

و تبرز أهمية الاستفادة من المحاكاة الحاسوبية في مجال البحث والتحقيق الجنائي بإعتباره أحد أهم الأدوات التي يتم استخدامها حاليا في الكثير من المجالات، وتتمثل هذه الأهمية في الآتـــــي:

- إنّ الأجهزة الشرطية العاملة في مجال البحث والتحقيق الجنائي يجب عليها الاستفادة من الوسائل العلمية والحديثة عند إعدادها لبرامج التدريب، بحيث يتم الاعتماد على استخدام أجهزة الحاسب، والطرق المعتمدة على استخدام الذكاء الاصطناعي والنص المدمج والتدريب عن طريق الأنترنت وباستخدام نماذج المحاكاة الحاسوبية.
- إن نماذج المحاكاة الحاسوبية يتم تصميمها لعرض مواقف وبيئات مختلفة لمشكلات أو عوائق تصادف في الحياة، ويمكن الإستفادة في هذا الأمر، في تصميم نماذج للبيئات والمواقف الأمنية المختلفة في مجال البحث والتحقيق في الجريمة حيث يتم إعداد هذه النماذج بصورة متدرجة تصاعديا بهدف تنمية مهارات الباحث والمحقق الجنائي في عمليات البحث والتحقيق والارتفاع بمستوى أدائه [2].

---

[1]– محمد نور الدين عبد الحكيم، دور نظم المعلومات في المجال الشرطي، مقال منشور بمجلة الفكر الشرطي ،المجلد العاشر، يناير 2002 ، ص113.

[2]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص169.

- إن الوقاية من الجريمة ومكافحتها سواء في الشق المنعي أو الشق التعاقبي للجناة بعد تنفيذ جرائمهم، تستلزم ضرورة الاستفادة مما حققه التطور العلمي والتقدم التكنولوجي، وبصفة خاصة أجهزة الحاسب الآلي المتعلقة بنماذج المحاكاة الحاسوبية وفي مجال تحليل المعلومات الجنائية [1].
- إن ظهور أنماط مستحدثة خاصة الجرائم الإلكترونية يستلزم للوقاية من أخطارها ومواجهتها إمكانيات مادية وتكنولوجية عالية المستوى، وبالتالي يستلزم إعداد نماذج لأساليب ارتكاب هذه الجرائم ذات سيناريوهات زمانية ومكانية مختلفة مع محاكاة هذه النماذج الحاسوبية، بهدف التعلم والتدريب الأمني واكتساب الخبرات على كيفيه التعامل معها ومواجهتها.
- تتيح نماذج المحاكاة الحاسوبية استخدام المنهجية في مجال البحث والتحقيق الجنائي، حيث يتم الاعتماد على التسلسل والترتيب والمنطق في إبـــراز جوانب المشكلة مع تنقيتها من الشوائب والجوانب غير المؤثرة وغير المطلوبة والتي قد يتم استخدامها كغطاء الجوهر الحقيقي في القضية، مما يساعد على الربط بين الأحداث الحقيقية وغير المفتعلة والتوصل إلى الجاني ودافعه الحقيقي لارتكاب الجريمة[2].
- إن نماذج المحاكاة الحاسوبية تسهم في معاونة الباحث والمحقق الجنائي إذ يمكن تضمينها فرضيات متعددة لأحد المواقف أو الأحداث في ضوء الوقائع والظروف والملابسات والآثار و الأدلة المادية ومحتويات مسرح الجريمة، وتصور ارتكاب الجريمة و الأسلوب الإجرامي المتبع من الجاني والأداة المستخدمة منه في ارتكاب الجريمة، وهذه الفرضية يمكن شمولها بالتعديل والتصويب حتى يتم التوصل إلى الفرضية التي تتفق والمنطق والتسلسل الطبيعي للأحداث، مما يساهم في تضييق دائرة البحث وقصرها على أكثر الاحتمالات بما يتيح التعامل المنهجي مع الحدث الإجرامي والتوصل إلى نتائج إيجابية بشأنه.
- إن نماذج المحاكاة الحاسوبية تسمح وتساعد في الحفاظ على درجه استعداد العاملين في مجال التحقيق الجنائي، إذ تسمح عمليات التدريب التقنية على نماذج المحاكاة الحاسوبية والمعايشة مع الافتراضات المتعددة التي تطرحها في الإعداد الذهني الجيد دون انتظار لوقوع الجريمة للبدء في

[1]– حسني درويش عبد الحميد، المرجع السابق، ص 139.

[2]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص170.

التحرك والتعامل معها، فهذه النماذج تسمح بالتعايش والتدريب المستمر مع التعديل والتطوير في النماذج الحاسوبية المعدة بالصورة التي تحقق متطلبات وأهداف البحث الجنائي.

- إن كبر حجم التحديات التي تواجه العمل الشرطي في المرحلة الحالية والتي يتمثل البعض منها في زيادة معدلات الجريمة ووجود أنماط مستحدثة منها وتميّز أساليب ارتكابها بالذكاء والقدرة على التخفي باستخدام وسائل احتيالية، و امتداد نشاطها عبر الكثير من الدول، يتطلب جهد كبيراً من أجهزة الشرطة لمواجهة هذه التحديات بالإضافة إلى الحاجة لمخصصات مالية كبيرة لأغراض التدريب واقتناء التجهيزات التقنية الحديثة التي تمكن الشرطة من مواكبة التقدم التقني للوسائل الإجرامية.

ولا شك أن الاستعانة بأسلوب المحاكاة الحاسوبية لتدريب جهات التحقيق سيؤدي إلى توفير نفقة مالية كثيرة كان سيتم تخصيصها لتوفير متطلبات التدريب الميداني بالإضافة إلى أن هذه النوعية من التدريب أصبحت لا تفي بمتطلبات العملية التدريبية في ضوء التقدم التقني للجريمة و أساليب ارتكابها[1].

- إن الاعتماد على نماذج المحاكاة الحاسوبية في مجال التدريب لجهات التحقيق سيؤدي إلى اكتسابهم قدراً أكبر من الخبرة والدراية في مواجهة الصور المختلفة للجرائم خاصة الجريمة الإلكترونية، وكيفية التعامل معها وكشف أسرارها من خلال التعرف على أساليب الانتقال وجمع المعلومات وإدارة عمليات البحث بطريقة صحيحة.

مما سبق ذكره يتضح أنه بالرغم، من أهمية المحاكاة الحاسوبية إلا أن هناك الكثير من الصعوبات التي تواجه عملية إعدادها حتى يتسنى الاستعانة بها في تدريب الجهات المختصة والقائمين على الوقاية من الجريمة ومكافحتها، إلا أن ذلك لا يمنع من الاستعانة بها في مجال الوقاية من الجريمة بجميع صورها، ويتطلب الأمر العمل على توفير المتطلبات المادية والفنية و التقنية والخبرات العلمية اللازمة لإعداد النماذج المطلوبة، وكذلك أيضا إعداد السيناريوهات الأمنية التي سيتم الاستعانة بها في إعداد هذه النماذج لتحقيق الاستفادة المطلوبة للجهات القضائية المختصة في التحقيق.

[1]– ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص172.

الفصل الثاني: أساليب التحقيق في الجريمة الإلكترونية

إنّ التطور العلمي له تأثيره البالغ على القانون وعلى الواقع الذي يطبق عليه هذا القانون، ولكي تتحقق الفائدة المرجوّة من هذا التقدم، فإنّ القانون يجب ألا ينفصل عن الواقع الذي يفرزه ويطبق عليه، بل يجب أن يكون متجاوبا معه ومتطورا بتطوره.

فالتطور الحاصل في أنواع الجرائم وأسلوب ارتكابها، والوسائل المستخدمة في تنفيذها، جعل القائمين على مكافحة الجريمة في سباق مستمّر مع الزّمن لمواكبة هذا التطور، وقد أدى هذا السياق إلى تطور في وسائل مكافحة الجريمة ووسائل إثباتها.

وقد يشمل هذا التطور أساليب التحقيق التي تتخذ في جمع الأدلّة، فلم يعد جمع الأدلّة قاصرا على البصمات والوسائل المستخدمة في ارتكاب الجريمة من أسلحة وغيره من وسائل تقليدية، بل تطورت تلك الأساليب لتواكب التطور في هذا المجال، مثل كيفية التعامل مع الحاسب الآلي المستخدم في ارتكاب الجريمة، وكيفية المحافظة على الأدلّة التي يحتويها الحاسب، وكذلك كيفية التعامل مع كافة الأجهزة الحديثة واستخراج الأدلّة منها.

والحاصل أنّه مع ظهور الجرائم الإلكترونية التي باتت تتخذ أنماطا جديدة وتجمع بين ذكاء المجرم (الذكاء الإنساني) وذكاء الأجهزة الرقمية (الذكاء الإصطناعي) أصبح لا يجدي معها إتباع الأساليب التقليدية في تحصيل الدليل لإثباتها، ممّا أدىّ إلى تدعيم جهات التحقيق بأساليب إجرائيّة مستحدثة تتفق وعملية البحث عن الدليل الرقمي من حيث طبيعته وطبيعة البيئة التي يتواجد بها.

وهذا وقد تزايد قلق المجتمع الدولي إزاء التصاعد المطرد للجريمة، وتطوّرها المتلاحق واقترانها بالتقدم التقني، وإزدادت قناعة المجتمع بالحاجة الماسة للمواجهة الشاملة من خلال التعاون الدولي في المواد الجنائية بوصفه –حجر الزاوية– في أيّة إستراتيجية ناجحة لمكافحة الإجرام، واعتباره سمة بارزة للعلاقات الدولية.

ولقد أصبح التعاون الدولي في المجال الجنائي، ظاهرا وبوضوح على صعيد الممارسة الدولية، ودعت إلى قيامه معظم المواثيق الدولية والإقليمية والمتخصصة لضمان المواجهة، وبأنّ هناك حاجة ضرورية وملحّة، ومبرّرات قويّة لتوحيد الجهود الدولية لمكافحة الجريمة بصفة عامّة والجريمة الالكترونية بصفة خاصّة.

لذلك يجب أن ينظر إلى هذا التعاون بمفهوم شمولي، لاستيعاب الصور المختلفة لمجالات التعاون (القضائية والأمنية)، وبأنّ أسس التعاون هدفها مكافحة الجريمة وتقديم المجرمين إلى العدالة، لا يتأتى ذلك إلاّ من خلال إتباع أساليب دولية تهدف إلى تفعيل التعاون الدولي بغرض عدم إفلات المجرمين من العقاب، و هو الأمــر الذي سوف نعالجه من حيث البحث مدى الاستناد على الأساليب الوطنية للتحقيق في الجرائم الإلكترونية، في (المبحث الأول)، ثم التطرق إلى الأساليب الدولية للتحقيق في الجرائم الإلكترونية في (المبحث الثاني).

المبحث الأول: الأساليب الوطنية للتحقيق في الجرائم الإلكترونية

إنّ لقواعد الإثبات أهمية خاصّة، حيّث أنّ الحق موضوع التقاضي يتجرد من كل قيمة إذا لم يقم الدليل على الواقعة التي يستند إليها، فالدليل هو صعب الواقعة أو هو النتيجة التي تحققت باستعمال وسائل الإثبات المختلفة أي إنتاج الدليل، ويقصد بهذا الإثبات الأساليب المتعلقة بالبحث عن الأدلّة وإقامتها أمام القضاء، وتقديرها من جانبه، فالإثبات هو مجموع الأساليب المنتجة لليقين.

فالإثبات في المواد الجنائية، ما هو إلاّ كافة الأدلة التي تؤكدّ وقوع الجريمة، وتحقق حالة اليقين لدى القاضي لإدانة المتهم، أو ترجح حالة الشك لديه فيقضي بالبراءة، أو هو كل ما يؤدي إلى إظهار الحقيقة، ولأجل الحكم على المتهم، يجب ثبوت وقوع الجريمة في ذاتها وأنّ المتهم هو المرتكب لها.

كما يقضي الإثبات في المواد الجنائية، إتباع القاضي الجزائي لمجموعة من الأساليب الإجرائية الوطنية للوصول إلى هدف أساسي وهو إظهار الحقيقة، وفي إطار الدعوى الجنائية، فإنّ وسائل الإثبات يحكمها حريّة الإثبات الجنائي من جهة، ومن جهة أخرى تخضع هذه الوسائل للشرعية الإجرائية، بمعنى لابد من مراعاة الأحكام القانونية التي وضعها المشرع عند جمع وتقديم كل وسيلة من وسائل الإثبات من طرف المحققين أو الشرطة القضائية وغيرهم، كما ينبغي على المحققين أثناء جمع أدلّة الإثبات ألاّ يعتمدوا على الوسائل غير الشرعية كالعنف والإكراه.

غير أن ظهور الجريمة الإلكترونية، والتي أصبحت تمثل ضربات من ضروب الذكاء الإجرامي الجديد، أدّى إلى عدم كفاية الأساليب الإجرائية التقليدية لجمع الدليل الإلكتروني، وبالتّالي إثبات قيام هذه الجريمة ومعاقبة المجرم الالكتروني على اقترافها، نظرا لما تثيره طبيعتها غير المادية من إشكاليات وما تؤديه التقنية الحديثة من دور في ارتكابها، وما توفره لها من مسرح غالبا ما يكون أقل ظهورا لحقائق موضوع البحث وأدلته، وذلك لوقوعها في عالم إفتراضي، وطبيعة أدلتها غير الملموسة.

ومن أجل مكافحة هذا النوع من الإجرام، كان لابّد من تطوير أساليب التحري والتحقيق الوطنية، بصورة تتلاءم وخاصيتها غير المادّية للأدلة التي تخلّفها، بالإضافة إلى استحداث نوع من الأساليب الإجرائية تتماشى وطبيعة هذه البيئة التقنية.

فقد أدّى التقدم الالكتروني إلى ظهور علامات بارزة في معالم نظام الإثبات الجنائي، تتمثل في إستحداث وسائل علمية جديدة تستطيع التغلب على كل محاولات المتهم لتضليل العدالة وكشف ما قد يطمسه من آثار في سعيه نحو إثبات براءته بشتى الطرق، وإذا كانت الجريمة المعاصرة قد تغيرت أبعادها وتميّزت بسمات خاصّة وأنماط جديدة، فإنّه يصبح من الضروري أن يتغير تبعا لذلك أسلوب كشفها وطريقة إثباتها، يصبح الدليل المادي لإرتباطه بالتطور العلمي ذا دور رئيسي في كشف الجريمة المعاصرة وتقديم أدلّة الإدانة فيها، فغالبا ما يترك الجاني عند ارتكاب جريمته آثار مادية مكان الجريمة، لأنّه مهما إحتاط وحرص ومحا كل الآثار الناجمة عن الجريمة، إلاّ أنه وفي النهاية لابد وأن يترك أي أثر والسبب في ذلك في رأي العلماء الحالة النفسية والانفعالات التي تصاحب الجاني والقلق الذي يسيطر عليه سواء أثناء أو بعده[1].

ويصعب حتى هذه اللحظة في غالبية الأنظمة القانونية أن نحدد إلى أي مدى تكفي الأساليب التقليدية لاستخلاص الأدلة من أجل مباشرة تحقيقات ناجحة في مجال الجرائم الإلكترونية؟ وهل لابد من استخدام أساليب حديثة تتلائم مع طبيعة هذا النوع من الجريمة ؟

لذا سيتم التفصيل في أساليب التحقيق الوطنية في الجرائم الإلكترونية بالتطرق للأساليب التقليدية و الحديثة التي حددّها القانون والمتمثلة في التفتيش والضبط في الجريمة الإلكترونية (المطلب الأول)

المطلب الأول: التفتيش والضبط في الجريمة الإلكترونية

يحق لكل فرد من أفراد المجتمع التمسك بحق سريّة حياته الخاصّة وحماية هذا الحق من الانتهاك، سواء كانت هذه السرّية تتمثل في شخصه أو مراسلاته أو معلوماته المخزّنة في حاسوبه أو نظامه المعلوماتي، غير أنّه في بعض الأحيان يتم إنتهاك هذا الحق وكشف هذه السريّة في سبيل الوصول

[1]– حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، 2017، ص 39.

إلى الحقيقة، وهذا الخرق يكون بموجب إجراء نصّ عليه القانون هو التفتيش[1]، والذي يراد به التقصي والبحث عن الأدلة سعيا وراء ضبطها بقصد الاستعانة القانونية بها لإدانة الجاني[2].

وعليه ينبغي القيام بضبط ما يترتب عليه التفتيش وتحريزه بطريقة علمية حتى لا يفقد قيمته القانونية، حال تفقده أمام القضاء إذا تطلب الأمر ذلك، لذلك يعدّ التفتيش والضبط من وسائل الإثبات التي ينبثق عنها أدلة تفيد الإدانة حال توافرها[3].

الفرع الأول: التفتيش في الجريمة الإلكترونية

يعد التفتيش من أساليب التحقيق ذات الخطورة الخاصّة لكونه من الأساليب التي تمسّ حق الإنسان في الخصوصية، وبما يشكل ذلك إنتهاكا للحياة الآمنة المستقرة التي ضمنتها الدساتير والمواثيق، وكونه من الإجراءات الخطرة، فإنّ المشرع قنّنهُ ليكون في ضمانة سلطات التحقيق.

والتفتيش في الجرائم الإلكترونية له طبيعة خاصّة ومتميّزة عن التفتيش التقليدي ، حيث أنّه ينصب على جهاز الحاسب الآلي الذي يعمل طبقا لتعليمات محددة سلفا، يستقبل البيانات ويخزنها ويقوم بمعالجة استخراج النتائج المطلوبة، وهو متصل بالشبكة للحصول على المعلومات وتبادلها عبر الشبكات والبريد الإلكتروني، فهو تفتيش في برامج ومكونات غير مادّية، إلا أنّه يخضع في إجراءاته للضوابط التي حددّها قانون الإجراءات الجزائية وما يستلزمه من وقوع الجريمة، و إتهام شخص أو أشخاص معيّنين بارتكاب جريمة، وأن تكون هناك دلائل تفيد في كشف الحقيقة في أجهزة الحاسب الآلي و الأنترنيت خاصّة بالمتهم أو غيره من الأشخاص وإذا ما توافر كل ذلك، جاز لسلطة التحقيق تفتيش جهاز الحاسب الآلي وملحقاته المكونّة له المادّية والمعنوية، وذلك من أجل ضبط أدلة الجريمة، وما يحتمل أن يكون قد استعمل في ارتكابه أو نتج عنها أو وقعت عليه، وكل ما شأنه أن يكشف عن الجريمة[4].

لذا سنتناول فيما يلي: مفهوم التفتيش في الجرائم الإلكترونية ومحل التفتيش فيها بالإضافة إلى شروط صحة إجراء التفتيش في هذه الجرائم الإلكترونية.

---

[1]– سامي جلال فقي حسين، المرجع السابق، ص 49.

[2]– محمد فتحي محمد أنور عزّت، تفتيش شبكة الأنترنيت لضبط جرائم الإعتداء على الآداب العامة والشرف والاعتبار التي تقع بواسطتها، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين الشمس، 2010، ص 348.

[3]– محمد فتحي محمد أنور عزّت، المرجع نفسه ، نفس الصفحة.

[4]– حازم محمد حنفي، المرجع السابق، ص 39–40.

أولا/ مفهوم التفتيش في الجريمة الإلكترونية :

يعتمد التحقيق في جميع مراحله على مجموعة من الإجراءات الهادفة إلى كشف الجريمة والوصول إلى دليل مادي ملموس في شأن الجريمة موضوع التحقيق، ويعد التفتيش أهم إجراءات التحقيق تختص بإجرائه سلطة التحقيق استلزمته وقوع الجريمة فهو مرتبط بها ارتباط تاما، فكلما وقعت جريمة استدعى الأمر إتخاذ هذا الإجراء، فكثيرا ما يكشف عن أدلة الجريمة فيتوقف مصير الدعوى عن النتائج المتوصل إليها من خلاله، والجدير بالذكر أن غالبية التشريعات لم تضع تعريفا للتفتيش بل اكتفت بتجديد شروطه وبيان كيفية إجرائه أي أنها ابقت على التعريف بالتفتيش عاما، فهو ينطبق على كافة أنواعه، أكان ذلك للأشخاص أو للمساكن أو للرسائل أو للسيارات، وقد أجمع الفقه على استبعاد التفتيش في المحلات العامة، أو ما لا يمكن أن يعتبر أنّه مستودع للسّر، أمّا من حيث طبيعته فهو عمل من أعمال التحقيق، ممّا ينفي عن أعمال الاستدلال صفة التفتيش[1].

1. تعريف التفتيش:

لابد لمعرفة مكونات كل عمل لإيجاد تعريف يحدد الإطار القانوني له، أمّا بالنسبة للتفتيش فلم تتضمن التشريعات العربية تعريفا محددّ له، بل اكتفت بالإشارة إلى أنّه إجراء من إجراءات التحقيق، لعدم جعل التفتيش مقيدا أو محدّدا بشكل ضيق، واتجاه هذا النقص القانوني، وجد الفقهاء المجال الواسع للعمل على إيجاد بعض التعاريف له.

ويعرف **التفتيش لغة:** من الفِعل فَتَشَ أي الفَتْشُ والتَّفْتيشُ: الطلبُ والبحثُ، وفتَشْت الشيء فتْشاً وفتَّشَه تفْتيشاً مثله. قال شمر: فتَّشْت شعر ذي الرّمة أَطلُب فيه بيتاً.[2]

والمفتش: إسم فاعل وهو من تقيمه السلطة أو إحدى الدوائر العمومية للمراقبة والبحث عن الخلل[3].

كما يعرف أيضا: الطلب والبحث وهو مشتق من الجزء الثلاثي فتّش بفتح فاء الفعل وعينه ولامه، والتفتيش هو الطلب والتحقيق وهو مشتق من الفعل فتّش، وفتش الشيء أي تفحصه، وفتّش عنه، سأل واستقصى في الطلب[4].

---

[1]– سليم علي عبده، التفتيش في ضوء أصول المحاكمات الجزائية الجديدة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، 2006، ص 24-25.

[2]– ابن منظور، لسان العرب، الطبعة الأولى، دار المعارف، القاهرة، مصر، ص 3341.

[3]– الوسيط الحديث، منجد عربي– عربي، الطبعة الأولى، دار أيوب للمنشورات، بانتة، الجزائر، 2013، ص 477.

[4]– عبد الله بن عبد العزيز عبد الله الخثعي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، مذكرة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص 20.

أما اصطلاحا فهنالك عدة تعريفات: منها أنه: "إجراء من إجراءات التحقيق تقوم به سلطة حدّدها القانون، يتم بالبحث في مستودع السّر عن أدلة الجريمة التي وقعت وكل ما يفيد في كشف الحقيقة، ويتمثل مستودع السرّ في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه"[1].

و يعرّف أيضا بأنه: "إجراء تقوم به السلطة القضائي و للإطلاع على محل يتمتع بحرمة خاصّة للبحث عن الأدلّة اللاّزمة للتحقيق الجنائي".

كما عرّفه البعض بأنّه: "ذلك الإجراء الذّي رخصّ الشارع فيه بالتعرض لحرمة ما بسبب جريمة وقعت أو ترجّح وقوعها، وذلك تغليبا للمصلحة العامّة على مصالح الأفراد الخاصّة واحتمال الوصول إلى دليل مادّي يفيد في كشف الحقيقة [2]".

ويعرّف أيضا بأنّه: "البحث في محل يتمتع بحر حق السرّية عن أدلة الإثبات أو النفي في جريمة أُرتكبت أو يخشى إرتكابها بالإطلاع عليها وضبطها عند الاقتضاء أو البحث في مثل ذلك المحل عن أشخاص وجب القبض عليهم أو فكّهم من حجز غير مشروع أو عن أشياء اقتضى ضبطها، ممّا يتعلق بجريمة ارتكبت أو يخشى ارتكابها[3]"

وعرّف أيضا بأنّه: "بحث بوليسي أو قضائي عن عناصر الدليل في جريمة ما، ويكون وفقا لقواعد قانونية خاصّة أن ينفد في المسكن الخاص بأي شخص أو في أي مكان آخر، حيث يمكن أن توجد أشياء يكون اكتشافها مفيدا في إظهار الحقيقة"[4].

و يعرف التفتيش قانونا[5] أنّه: "الإطلاع على محل منح له القانون حرمة خاصة باعتباره مستودع سّر صاحبه، فلا يجوز الإطلاع عليه أو على ما بداخله إلاّ في الأحوال المنصوص عليها في القانون أو

---

[1]– علي حسن محمد طوالبة، التفتيش الجنائي على نظم الحاسوب و الأنترنيت، الطبعة الأولى، عالم الكتب الحديثة، أربد، الأردن، 2004، ص 10.

[2]– عبد الحميد الشواربي، إذن التفتيش في ضوء الفقه والقضاء، منشأة المعارف، الإسكندرية، بدون سنة نشر، ص 09.

[3]–خالد مختار الفار، إسماعيل بابكر محمد، المرجع السابق، ص 15.

[4]– أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مجلّة المحلّية العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، 2013، ص 87.

[5]– لا يوجد في القانون الجزائري أي تعريف للتفتيش بالرجوع إلى قانون الإجراءات الجزائية نجد أن المشرع اكتفى بذكر شروطه وأحكامه والجهة المخول لها قانونا إجراءه وذلك في المواد 44 إلى 47 مكرر والمادة 64 وكذا المواد من 79 إلى 83من ق.إ.ج تاركا تعريفه للفقه ، كذلك هو الحال بالنسبة للمشرع الفرنسي والمشرع المصري بل اكتفوا بذكر طبيعته وشروطه.

برضا صاحبه، وقد يكون محل تفتيش الشخص[1]، أو المسكن[2]، أو محل آخر ألحقه القانون في حكم المسكن"[3].

وعرّف أيضا بأنّه: "البحث عن شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، ويقتضي التفتيش إجراء البحث في محل له حرمة خاصة، وقد أحاط القانون هذا التفتيش بضمانات عديدة أو هو ما يتعلق بالمتهم أو بغيره"[4].

أما عن تعريف التفتيش في الجريمة الإلكترونية: فمدلوله القانوني بالنسبة للجرائم التقليدية، لا يختلف عنه بالنسبة للجرائم الإلكترونية، وإذا كانا يشتركان في كون الهدف فيهما مشترك وهو الوصول إلى دليل يثبت الجريمة، إلاّ أنهما يختلفان في محل الجريمة، كون التفتيش في الجرائم التقليدية يتمحور حول التفتيش المادي للأدلّة، في حين التفتيش في الجرائم الإلكترونية يتعلق بتفتيش محتويات الحاسوب المادّية والمعنوية، والتي تتطلب كفاءة ومهارة عالية لإجرائه.

وفي الجرائم الإلكترونية يعدّ الدخول غير المشروع إلى الأنظمة المعلوماتية والتنقيب في البرامج المستخدمة أو في ملفات البيانات المخزّنة، عما قد يتصل بجريمة وقعت، إجراء يفيد في كشف الحقيقة عنها وعن مرتكبها، وتقتضيه مصلحة وظروف التحقيق في الجرائم الإلكترونية، لذا فهو إجراء جائز

---

[1]– يقصد بالشخص كمحل قابل للتفتيش: البحث في أجزاء جسمه وملابسه وحقائبه أو أشياء يحملها أو تكون في حيازته بقصد العثور على الأدلّة التي قد تفيد في الوصول إلى الحقيقة في الجريمة التي قامت الدلائل على اتهامه بارتكابها أو على حيازته لأشياء تفيد في كشف حقيقتها، هذا وإن كان تفتيش الأعضاء الخارجية للإنسان كاليدين والقدمين والفم لا يثير أي صعوبة، إذ يجوز فض يد الشخص وفتح فمه لإخراج ما يخفيه، إلاّ أنّ تفتيش أعضاء الجسم الدّاخلية كالمعدّة والدم والبول كانت محل خلاف بين من يجيز ذلك ومن لا يجيز ذلك، وقد تم الأخذ بإجازة ذلك في أحكام القضاء، فأجازت الإستعانة بطبيب في إجراء عملية غسيل معدّة المتهم للبحث عن آثار مادة مخدرة ضبط متلبسا بتعاطيها. أنظر: طارق فوزي الفقّي، المرجع السابق، ص 100.

[2]– يقصد بالمسكن محل التفتيش: المكان الذي يقيم فيه المتهم وملحقاته التابعة له، والمقصود بالملحقات: المنافع التابعة له والتي تعتبر جزءا مكملا للمنزل كالحديقة، وما به من حجرات ...إلخ، ولا يشترط لكي يعتبر المكان منزلا أن يكون مقيما فيه بصفة دائمة، بل يكفي أن يكون معدّا لإقامته ولو لفترة قصيرة، وقد يكون للشخص أكثر من مسكن في حيازته ويجعله مستودعا لسّره ويستطيع أن يمنع الغير من الدخول إليه إلاّ بإذنه. أنظر: طارق فوزي الفقّي، المرجع نفسه ، ص 101.

[3]– عبد الله بن عبد العزيز بن عبد الله الخثعي، المرجع السابق، ص 20.

[4]–عبد العال الديربي، محمد صادق، الجرائم الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 298.

قانونا ولو لم ينص عليه صراحة باعتباره يدخل في نطاق التفتيش بمعناه القانوني ويندرج تحت مفهومه[1].

وعرّف البعض التفتيش في الجرائم الإلكترونية بأنّه: "الاطلاع على محل منحه القانون حماية خاصّة، باعتباره مستودع سّر صاحبه ويستوي في ذلك أن يكون هذا المحل جهاز آلي أو أنظمة أو شبكة الأنترنيت"[2].

ويعرّف أيضا بأنّه: "إجراء من إجراءات التحقيق يهدف إلى البحث في نظام حاسوبي معيّن بإذن قضائي مسبق، سواءا كان هذا النظام مكونّا من حاسب واحد أو عدّة حواسيب مرتبطة فيما بينها بشبكة في محل له حرمة منحه إياه القانون، والغرض استخراج أدلة معلوماتية ممثلّة بالمعلومات أو البيانات، والتي تساعد في كشف الحقيقة في جريمة من نوع جناية أو جنحة وقعت و جار التحقيق فيها"[3].

كما يعرّف التفتيش أيضا أنه : "الدخول إلى الأنظمة المعلوماتية للبحث والتنقيب في البرامج المستخدمة، أو في ملفات البيانات المخزنة، كما قد يتصل بجريمة وقعت، وإجراء يفيد في كشف الحقيقة عنها وعن مرتكبيها"[4].

والتفتيش في الجرائم الإلكترونية يكون محلّه كل مكونات الحاسب الآلي المادّية والمعنوية، وشبكات الإتصال الخاصة به، بالإضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، ويتطلب تفتيش الحاسب الآلي أشخاص لديهم خبرة ومهارة تقنية في نظم الحاسب الآلي، كخبراء البرامج ومديري النظم المعلوماتية[5].

من خلال التعريف السابقة يتضح لنا بما لا يدع مجالا للشك بأنّ التفتيش عمل من أعمال التحقيق، الغاية منه البحث عن الأدلة التي يتوخى منها كشف الحقيقة بغية الاهتداء إلى الشخص

---

[1]–هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص 74. وأنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 38. وأنظر أيضا: حسين بن سعيد الغافري، المرجع السابق، ص 472.

[2] –علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنيت، المرجع السابق، ص 11.

[3] –سامي جلال فقّي حسين، المرجع السابق، ص 55.

[4]–عبد الله بن عبد العزيز بن عبد الله الخثعي، المرجع السابق، ص 36.

[5] –عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلّة الجنائية والطب الشرعي، الرياض، 2007، ص20.

المتهم بها، وهو يجرى بعد فتح باب التحقيق في جريمة ما، أي أنّ التفتيش ما هو إلاّ وسيلة للإثبات المادي[1] لأنه إجراء يستهدف ضبط أشياء مادية قد تساعد في إثبات وقوع الجريمة وإسنادها إلى المتهم المنسوب إليها ارتكابها، والتفتيش في الجرائم الإلكترونية مرحلة من أخطر مراحل حال إتخاذ الإجراءات الجزائية ضد مرتكب جرائم الإعتداء على نظم المعالجة الآلية، كون محل التفتيش هو نظام المعالجة الآلية، وهو محل استفسار فقهي متزايد يوما بعد يوم فيما يخص الجانب غير المادي له، فهو لا يمكن أن يكون إلاّ معلومات إلكترونية ليس لها أي مظهر محسوس في العالم الخارجي[2].

2. أهمية التفتيش في الجريمة الإلكترونية:

إن التفتيش يساعد في كشف الخفايا، وتوضيح أمور كثيرة لها أهمية في التحقيق، وإلاّ لما تعمّد المتهم إخفائها أو إيداعها مكمن الأسرار، وتلك الأهمية قد تتعلق بالواقعة أو بأطرافها[3]، فالنسبة للواقعة فقد يكشف التفتيش عـــــدة أمور منها ما يتعلق بثبوت وقوعها و مكان ارتكابها، و يمكن بيان ذلك في مايلي:

أ. ثبوت وقوع الجريمة:

مما لاشك فيه أنّ التفتيش في المكان المحتمل حدوث الواقعة بها كما ورد ببلاغ الشاهد أو المبلغ أو المجني عليه، وبين ما إذا كانت الواقعة قد حدثت أولا أم لا.

ب. وقت مكان الواقعة:

يساعد التفتيش المحقق في تحديد وقت الحادث، كما لو وقع المحقق على آثار بقايا كبريت، فيدل على أن توقيت ارتكابها ليلا، كما يفيد في تحديد المكان، ولكن بالطبع بالنسبة للجريمة الإلكترونية فإنّها من الجرائم العابرة للحدود، ممّا يصعب تحديد مكانها .

---

[1]– الإثبات المادي: هو إقامة الدليل على وقوع الجريمة أولاّ وعلى إسنادها للمتهم ثانيا، وحدّد الفقهاء طرقا خاصّة في الإثبات الجزائي بشروط خاصة مع الاستعانة بقواعد الإثبات في المواد المدنية منها: الإثبات بالكتابة، بالشهادة، الإقرار، اليمين والإثبات بالقرائن. أنظر: رياض النعمان، المعجم القانوني، الجزء الأول، دار أسامة للنشر والتوزيع، الأردن، 2013، ص 289.

[2]– رشيدة بوكر، المرجع السابق، ص 394.

[3]–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 184.

أما بالنسبة لأطراف الخصومة فالتفتيش يساعد المحقق الجنائي في كشف الباعث، وتحديد شخصية الجاني وحرفته، ودرجة خطورته، وأسلوبه الإجرامي، وعلاقته بالمجني عليه، ويمكن تناوله كالآتي[1]:

أ- تحديد الباعث الدافع :

قد يكشف التفتيش عن كراهية الجاني للمجني عليه عند العثور على أوراق بخط يد الجاني تفيد رغبته في الانتقام وتهديده للمجني عليه.

ب- تحديد شخصية الجاني :

حالة تفتيش المحقق لمسرح الجريمة وعثوره على البطاقة الشخصية أو لمستند رسمي خاص بالجاني الأمر الذي يوصل إليه بسهولة.

ت-تحديد حرفته ودرجة خطورته وأسلوبه الإجرامي:

بالعثور على أسطوانات بها برامج فك الشفرات أو برامج فيروسات أو كتب خاصّة بأشهر جرائم الكمبيوتر، أو شهادات علمية تدل على أنّ المتهم متخصص ومحترف في مجال الكمبيوتر والشبكات.

كما قد يوضح أسلوبه الإجرامي سواءا في نوعية المسروقات التي يستولي عليها أو في طريق الدخول إلى شبكة المعلومات أو المواقع الإلكترونية المنتشرة على الأنترنيت، وارتكابه الواقعة ودرجة خطورته الإجرامية، وهذه الأشياء كلها هامة للمحقق الجنائي بلا شك في تحديد الأسلوب الذي يسلكه في التعامل مع المتهم سواءا عند الضبط أو عند توجيه الاتهام.

ث-تحديد عدد الجناة وعلاقتهم بالمجني عليه:

تفتيش مسرح الجريمة المعلوماتي من شأنه أن يلقي الضوء على تعدد الجناة أو أنّ الجاني شخص واحد، ويظهر ذلك جليّا عند إجراء تفتيش للنظام المعلوماتي، وما قد يسفر عنه من العثور على أدوات وأجهزة إلكترونية استخدمت في ارتكاب الواقعة[2].

3. خصائص التفتيش في الجريمة الإلكترونية:

إنّ التفتيش ينطوي على خاصية الإجبار، بمعنى أنّ الإنسان يخضع له عادة مجبرا، فالتفتيش تعرض قانوني، ينطوي على انتهاك لحرمة الإنسان، أيا كان وعاءه فقد يكون وعاء هذا السّر، أو مستودعه هو السّر ذاته، وملابسه وما معه من أمتعة، وقد يكون مسكنه وما إلى ذلك من أماكن لها

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 185.

[2]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع نفسه، ص 186.

حرمة، وقد يكون السّر في رسائله و أوراقه أو في حاسوبه، ويخضع من يباشر التفتيش حياله، لهذا التعرض، احتراما للقانون الذي يفرضه لمصلحة المجتمع أو إدعانا لرجال الشرطة في تنفيذ إختصاصهم، أو ما كلفوه قانونا، والمهم أنّ هذا الإجراء تباشره السلطة التي اختصها به القانون سواءا رضي به من بوشر حياله أم لم يرضى[1].

والواقع أنّ من النّاس من يرضى به أحيانا في طويّة نفسه، إلاّ أنّه لا اعتداء بهذا الرضا، إذ أنّ للسلطات المختصّة أن تتخذ ما تضمن به تنفيذه عند عدم الإستجابة، إذ أنّ تفتيش الشخص يستلزم تقييد حركته المدّة اللاّزمة لإجراء التفتيش، ممّا قد يستتبع القوة وهذا طبعا في الحدود اللازمة للتغلب عن كل مقاومة من جانب الشخص المطلوب تفتيشه، وللبحث عن الأدلّة[2] المادية الملموسة أو الأدلة الإلكترونية (غير الملموسة)[3].

أ- خاصية الجبر والإكـــــــراه:

ينطوي التفتيش على عنصر الجبر أو الإكراه، فهذا الإجراء الحساس والمهم يشكل مساسا بحرّية الفرد، لأنّه عندما تصدر السلطة القضائية المختصة أمر التفتيش، فإن هذا الأمر يشكل إجبارا لمن صدر بحقّه، لأنّ مباشرة هذا الأمر بحقّه يكون دون إرادته، فقد يمسّ التفتيش حرمته، إذا كان التفتيش واقعا على شخصه، أو يمسّ حرمة مسكنّه، إذا كان التفتيش يمسّ مكان سكنه أو حرمة رسائله ومستنداته، وقد يمسّ التفتيش معلوماته وبياناته المخزّنة في حاسوب إذا كان التفتيش ينصب على جهاز الحاسوب العائد له[4].

---

[1]- منى جاسم الكواري، التفتيش شروطه وحالات بطلانه، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2008، ص 35.

[2]-الأدلة التي تفيد في كشف الحقيقة نوعان: مادية و قولية، فالأدلة المادية " هي التي تنبعث من عناصر مادية ناطقة بنفسها وتؤثر في اقتناع القاضي بطريق مباشر، إذ قد يترك الجناة في مكان الجريمة بعض الأدوات التي استخدمت في ارتكابها أو بصمات أصابع أو أقدام أو غير ذلك من الظواهر المادية التي تفيد القاضي في الإثبات، أمـّا الأدلة القولية: فهي من عناصر الشخصية المتمثلة فيما يصدر عن الغير من أقـــوال تؤثر في اقتناع القاضي بطريق غير مباشر من خلال تأكده من صدق= =هذه الأقوال. أنظر: علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2006، ص 461.

[3]- منى جاسم الكواري، المرجع السابق، ص 35. و أنظر أيضا: عادل فتحي صابر شريف، تفتيش غير المتهم، رسالة للحصول على درجة دكتوراه، كلية الحقوق، جامعة حلوان، مصر، 2010، ص 111.

[4]- سامي جلال فقي حسين، المرجع السابق، ص 57.

فالتفتيش عبارة عن تعرض قانوني لحرّية المتهم أو لحرمة مسكنه كما سبق الذكر، هذه الحرمة التي كفلها الدستور والقانون بالحماية، فالقانون يوازن بين حق المجتمع في العقاب، دفاعا عن مصالحه التي تنتهك بارتكاب الجرائم، وبين مدى تمتع الفرد بحريته أمام هذا الحق، فيبيح إجراء التفتيش جبرا عن إرادة صاحب الشأن متى توفّرت وروعيت ضمانات معيّنة[1].

وبالتالي فإنّ الإكراه والجبر عنصر أولي في التفتيش، والإجراء الذي لا تتوافر فيه هذه الخاصية لا يمكن اعتباره تفتيشا، ومن تم إذا انعدم الجبر وتوافر الرضاء، فإنّ هذا الإجراء يعتبر مجرّد إطلاع ومعاينة.

ب-خاصية المساس بحق السّر:

إن إجراء التفتيش ينطوي على المساس بحق الإنسان في السرّ، الذي يمثل أحد مظاهر الحق في الخصوصية، والذي يعني حق الفرد في ممارسة شؤونه الخاصّة بعيدا عن تطفل الآخرين، لذلك كان له الحق في أن يخلوا إلى نفسه، كما أن له حرمة حياته الخاصة، فالأشخاص والمساكن حرمة[2]، وهي موضع لإمتياز استثنائي هو الحق في السرّ، والقانون يعترف للشخص بهذا الحق، و إحتفاظه بخصوصياته وأسراره، وهذه الحرمة لا يقصد بها حماية حق ملكية المسكن أو الرسائل، فالقانون لم يقصد بذلك حماية حق الملكية أو حق مالي آخر يتعلق بها، لأنّ هذه الحقوق محل تنظيم خارج هذا الأساس، فالملكية ليست شرطا لازما لوجود حرمة المسكن أو الرسائل[3].

والحق في السرّ أيّا كان مستودعه، الشخص، مسكنه، رسائله، معلوماته أو ما يعبّر عنها بحرمة الحياة الخاصّة، يجد أساسه في فطرة الإنسان وتمليه عليه ضرورات الحياة الإجتماعية، وهكذا فإنّ هذا الحق، يعد من الحقوق المقدسة لأنه ضمان لأمن الإنسان وراحته وهدوءه وحرّيته الفردية[4].

---

[1]- منى جاسم الكواري، المرجع السابق، ص 36.

[2]- مبدأ حرمة المسكن من المبادئ الأساسية في التشريع الإسلامي وهذا المبدأ منصوص عليه صراحة في القرآن الكريم، في قوله تعالى:" يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ * فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ"* الآية 27-28 من سورة النور.

ومن الأحاديث النبوية فيما يتعلق بحرمة المسكن قوله صلى الله عليه وسلم: "من اطلع في بيت قوم من غير إذنهم حل لهم أن يفقأوا عينه" وقوله صلى الله عليه وسلم: "إنّما جعل الله الإذن من أجل النظر.

[3]-علي أحمد عبد الزعبي، المرجع السابق، ص 465. وأنظر أيضا: عادل فتحي صابر شريف، المرجع السابق، ص 113

[4]- سامي جلال فقي حسين، المرجع السابق، ص 69.

ويترتب على كون التفتيش يتضمن مساسا بالحق في السرية، أن يخرج من نطاقه كل إجراء يمس سرا لأحد، وإن تضمن تقييدا للحرية الفردية، أو إعتداء على حق آخر، ولا يعد تفتيشا الإجراء الذي يقع على شيء مكشوف أو ظاهر كالمزارع والحقول والأشياء المتروكة، حيث يحقّ لكل إنسان الإطلاع على ما فيها، أو إذا تخلىّ الشخص عن سرّه، أو كشف عما يحويه، فإنّ قواعد التفتيش لا تحميه[1].

وقد أكدت إعلانات حقوق الإنسان والاتفاقيات الدولية على ضرورة حماية خصوصية الإنسان وعدم المساس بها: فالإعلان العالمي لحقوق الإنسان لسنة 1948[2] ، نصّ في المادة 03 على ما يلي: "لكل فرد الحق في الحياة والحريّة وسلامة شخصه".

كما نصّت المادة 12 منه على أنّه: "لا يجوز تعريض أحد ليتدخل تعسفي في حياته الخاصّة أو في شؤون أسرته، أو مسكنه أو مراسلاته أو لحملات تمس شرفه وسمعته، ولكل شخص الحق في أن يحميه القانون من مثل هذا التدخل أو تلك الحملات".

كما نصّت اتفاقية بودابست لمكافحة جرائم المعلوماتية لسنة 2001 في المادة 1/15 على ما يلي: "يجب على كل طرف أن يحرص على تأسيس، وتنفيذ، وتطبيق السلطات والإجراءات المنصوص عليها في القسم الحالي والتي تخضع للشروط والاحتياجات المقررة في قانونه الدّاخلي، والذي يجب أن يتضمن حماية كافية لحقوق الإنسان وحرياته، وعلى الأخص الحقوق النّاشئة على الالتزامات التي تعهد بها في ظل اتفاقية المجلس الأوربي عام 1950 لحماية حقوق الإنسان وحرياته الأساسية، والإتفاقيات الدولية للحقوق المدنية والسياسية للأمم المتحدّة لسنة 1966، والاتفاقيات العالمية الأخرى المطبقة والخاصّة بحقوق الإنسان، والتي يجب أن تتكامل مع مبدأ التناسب".

كما أجمعت دساتير العالم على ضرورة حماية خصوصية الإنسان وعدم المساس بها التي في الأحوال يقررها القانون، فنصّت المادة 26 من دستور الإمارات العربية المتحدّة لسنة 1971[3] في الباب الثالث و الذي جاء تحت عنوان الحريات و الحقوق و الواجبات العامة على أنّ: "الحريّة

---

[1]– منى جاسم الكواري المرجع السابق، ص 37.

[2]– الإعلان العلمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة 217 ألف (د–3) المؤرخ في 10 كانون الأول، ديسمبر 1948.

[3]– أنظر بهذا الشأن إلى دستور الإمارات العربية المتحدة، الجريدة الرسمية ، السنة الأولى، بتاريخ 1971/12/31، المعدل في سنة 2009.

الشخصية مكفولة لجميع المواطنين، ولا يجوز القبض على أحد أو تفتيشه أو حجزه أو حبسه إلاّ وفق أحكام القانون".

ونصّت المادة 7 من دستور المملكة الأردنية الهاشمية لسنة 1952[1] علـــى أنّ "الحريّة الشخصية مصونة"، وأضافت المادة 10 منه على أنّ: "للمساكن حرمة فلا يجوز دخولها إلاّ في الأحوال المبينة في القانون، وبالكيفية المنصوص عليها فيه".

أمّا فيما يخص سريّة وسلامة مراسلات الفرد، فنصّت المادة 18 من الدستور على أنّه: "تعتبر جميع المراسلات البريدية والبرقية والمخاطبات الهاتفية وغيرها بأمر قضائي وفق أحكام القانون".

ونصت المادة 54 من الدستور المصري لسنة 2014 و المعدل بتاريخ 2019/04/23 على أنّ: "الحريّة الشخصية حق طبيعي وهي مصونة لا تمس، فيما عدا حالة التلبس لا يجوز القبض على أحد إلاّ بأمر قضائي مسببا يستلزمه التحقيق"[2].

ونصّت المادة 47 من الدستور الجزائري[3] علـــى أنّه: " لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر معلل من السلطة القضائية."

هذه المادة تدل على أن المشرع الجزائري سعى لحماية الحياة الخاصة للمواطن في كل جوانبها ومنها حرمة مراسلاته واتصالاته ومحادثاته السرية والخاصة سواء الشفوية أو الهاتفية أي كانت طبيعتها أو الوسيلة أو التقنية التي تمت بها، وجرم المشرع كل تعد على تلك الحقوق بنصوص قانونية أوردها بالذكر في قانون العقوبات في المادة 304 وما يليها.

كما اصدر المشرع الجزائري القانون رقم 04/18 الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات الالكترونية بموجبه أكد على سرية المراسلات والاتصالات الالكترونية بالإضافة إلى

[1]– الدستور الأردني، متاح على الموقع الإلكتروني: http://www.parliament.jo/node/137، تاريخ الزيارة 2017/08/10 على الساعة 11:00.

[2]– الدستور المصري لسنة 2014، مشار إليه على الموقع الإلكتروني:http://www.youm7.com تاريخ الزيارة 2017/09/16 على الساعة 16:00.

[3]– دستور الجمهورية الجزائرية الديمقراطية الشعبية، المعدل سنة 2020، الصادر بالمرسوم الرئاسي رقم 20–442، المؤرخ في 30 ديسمبر 2022، الجريدة الرسمية العدد 82، الصادرة في 30 ديسمبر 2020، ص 13.

واجب المحافظة على المعلومات الإسمية للمشتركين، وقرر عقوبات منصوص عليها في هذا القانون في حالة الانتهاكات التي قد تطال الحق في الخصوصية [1].

كما كرس الدستور الجزائري إلى جانب حماية الحق في الخصوصية التأكيد على حماية المعطيات الشخصية بداية، تزامنا مع التعديل الدستوري لسنة 2016، والمعاد تأكيده بموجب تعديل سنة 2020، بموجب أحكام المادة 47 منه، والتي نصت في فقرتها الرابعة على أن : "حماية الأشخاص الطبيعيين عند معالجة المعطيات ذات الطابع الشخصي حق أساسي ."

وبعد التكريس الدستوري لهذه الحماية وتأكيده على أنها حق أساسي يضمنه القانون، قام المشرع بعد حوالي سنتين من التعديل الدستوري بإعداد القانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي[2]، والذي أضاف بدوره لبنة تشريعية هامة في وقت نمت فيه المظاهر التكنولوجية والرقمية في جميع المناحي والتي أسهمت في تداول المعلومات الشخصية لاسيما عبر مواقع التواصل الاجتماعي، ومختلف مواقع الأنترنت، كلها أسباب دافعة وبقوة إلى التشريع في هذا الجانب الذي وإن كان مستجدا في الكثير من جوانبه، إلا أنه متجدد وسريع التطور، مما يقتضي تكييف منظومتنا القانونية صوب هذا المنحى لإيجاد الحلول المناسبة حفاظا وصونا للحقوق والحريات.

ت-خاصية البحث عن الأدلّة :

إنّ الغاية من إجراء التفتيش هو الحصول على الأدلّة، ويختلف نوع الدليل باختلاف محل التفتيش، فإذا كان محل التفتيش شخصا أو مكانا يتمتع بالحرمة وكان البحث جاريا عن سلاح الجريمة أو المخدرّات أو غيرها من الأشياء المادية الملموسة، فإنّ الهدف من التفتيش هو الحصول على دليل

---

[1]- القانون رقم 18-04، المؤرخ في 10 ماي 2018، يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية العدد27، الصادرة بتاريخ 13 ماي 2018.

[2]- يقصد بالمعطيات ذات الطابع الشخصي كل معلومة بغض النظر عن دعامتها متعلقة بشخص معرف أو قابل للتعرف عليه بصفة مباشرة أو غير مباشرة لا سيما الرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الاجتماعية.

ما يمكن الإستدلال به على خطورة المعالجة للمعطيات الشخصية خاصة الآلية منها، ارتباطها الوثيق بالحياة الخاصة التي هي جزء لا يتجزأ من الحريات الفردية. أنظر في هذا الصدد:

-DECAUX Emanuel, la protection de la vie privée au regard des données informatiques, droit fanda mentaux, n° 7,janvier 2008-decembre 2009,p2.

مادي[1]، يفيد في كشف مرتكب الجريمة سواء كان فاعلا أو شريكا أو محرضا أو في تبرئة شخص معين[2].

فمعظم التشريعات الجنائية نظمت القواعد القانونية للبحث عن الأدلة المادية الملموسة، ولم تنظم سوى تشريعات محددّة قواعد التفتيش عن الأدلة الإلكترونية أو الأدلة غير الملموسة، والتفتيش الذي نحن بصدده هو التفتيش عن الدعامات المعلوماتية بالدرجة الأساس، وذلك لأنّ التفتيش عن الأدلة المادية تنطبق عليها القواعد الإجرائية التقليدية. أمّا هذا النوع من التفتيش فيحتاج إلى قواعد إجرائية خاصة بسبب عدم إمكانية تطبيق معظم القواعد التقليدية عليها، وذلك لأنّ تفتيش نظم الحاسوب يحتاج إلى قواعد قانونية خاصّة بسبب طبيعة هذه الأدلة التي يمكن استخلاصها من هذه النظم عن طريق التفتيش، فعلى سبيل المثال يمكن محو وإتلاف هذه الأدلة بسهولة قبل وصول يد القائم بالتفتيش إليها، وقد يتسبب هذا الأخير في محو وإتلاف الدليل إذا لم يتمتع بخبرة فنيّة كافية في مجال تقنيات الحاسوب[3].

ثانيا : محل التفتيش في الجريمة الإلكترونية

يتم إجراء التفتيش لنظم المعلوماتية من خلال الوعاء الذي يحوي هذه النظم، ويقصد به جهاز الحاسب الآلي والذي يتكون من مكونات ماديّة التي هي عبارة عن مجموعة من الوحدات لكل منها وظيفة محددة، وتتصل هذه الوحدات مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل، ومجموعة هذه الوحدات تكون ما يسمى بمعدات الكمبيوتر وهذه الوحدات هي: (وحدة الإدخال، ووحدة الذاكرة، ووحدة الحساب والمنطق، ووحدة التحكم، ووحدة الذاكرة المساعدة، ووحدة الإخراج) ولا غنى أيضا عن توضيح المكونات المنطقية للحاسب، والتي هي عبارة عن برامج النظام وبرامج التطبيقات، كما أن له شبكات اتصال بعدية سلكية ولاسلكية على المستوى الوطني والمستوى الدولي.

وجهاز الحاسب الآلي قد يعمل بمفرده أو يعمل من خلال شبكة اتصالات ويقصد بها: اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لاسلكيا أو هي حزمة من أجهزة الحاسبات المتصلة معا، وقد تكون الأجهزة موجودة في نفس الموقع فتسمى شبكة محلية، كما قد تكون موزعة

[1]– سامي جلال فقي حسين، المرجع السابق، ص 73.

[2]– سليم علي عبده، المرجع السابق، ص 33.

[3]– سامي جلال فقي حسين، المرجع السابق، ص 73.

في أماكن متفرقة يتم ربطها عن طريق خطوط التليفون ويطلق عليها في هذه الحالة شبكة واسعة النطاق[1].

يضاف إلى ذلك أنّ الحاسب الآلي لمكوناته المختلفة تستلزم لتشغيلها وجود مجموعة من الأشخاص أصحاب الخبرة والتخصص في مجال تقنية المعلومات، وهم مشغلو الحاسب وخبراء البرمجة سواءا كانوا مخططي برامج تطبيقات أم مخططي برامج النظم، والمحلّلين ومهندسي الصيّانة و الإتصالات ومديري النظم المعلوماتية[2].

والسؤال الذي يمكن طرحه في هذا الصدد ما مدى خضوع مكونات الحاسب الآلي وشبكات الحاسب الآلي للتفتيش؟ وهل هناك قواعد فنيّة لتفتيشه؟.

1. مدى قابلية المكونات المادية للتفتيش:

تحكم الإجراءات القانونية الخاصة بالتفتيش فحص المكونات المادية للحاسب الآلي بحثا عن أي دليل له علاقة بالكشف عن الجريمة الإلكترونية و مرتكبيها، ويدخل في نطاق التفتيش طالما تم وفقا للإجراءات القانونية المقررة ، مع الأخذ بعين الإعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، إلا أن حكم هذه المكونات يتوقف على طبيعة المكان الموجود فيه، سواء في الأماكن العامة أو الأماكن الخاصة[3]، إذ للمكان أهمية في مجال التفتيش فإذا كانت موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته كان لها حكمه فلا يجوز تفتيشه، إلاّ في الحالات التي يجوز فيها تفتيش مسكنه، وبنفس الضمانات والإجراءات المقررة قانونا مع مراعاة التمييز بين ما إذا كانت مكونات الحاسب الآلي المراد تفتيشها منعزلة عن غيرها من الحواسيب الأخرى أو متصلة بحواسيب أخرى أو بنهاية طرفية في مكان آخر كمسكن غير المتهم[4].

فإذا كانت هناك بيانات مخزّنة في أوعية هذا النظام الأخير من شأنها كشف الحقيقة، تعيّن مراعاة الحقوق والضمانات التي يستلزمها المشرّع لتفتيش هذه الأماكن. أمّا لو وجد شخص يحمل مكونات

---

[1]–الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامعي، الإسكندرية، 2011، ص 378–379.

[2]– أحمد يوسف الطحطاوي، الأدلة الإلكترونية، ودورها في الإثبات الجنائي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2015، ص 299.

[3]– عزيزة رابحي، التفتيش في نظم المعالجة الآلية للمعطيات، مقال منشور بمجلة القانون والعلوم السياسية، العدد03، جانفي 2016، منشورات معهد الحقوق، المركز الجامعي، ولاية النعامة، ص 395.

[4]–حازم محمد حنفي، المرجع السابق، ص 42.

الحاسب الآلي المادية، أو كان مسيطرا عليها أو حائزا لها في مكان من الأماكن العامّة، كانت عامّة بطبيعتها كالطرق العامّة والميادين و الشوارع، أم كانت من الأماكن العامّة بالتخصيص كالمقاهي و المطاعم والسيارات العامّة، فإنّ تفتيشها لا يكون إلاّ في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال[1].

وتفتيش تلك المكونات لا يعني البحث عن البصمات والآثار الماديّة كما في الجرائم التقليدية، وإنما يعني البحث عن الأجهزة والملحقات المرتبطة بالحاسب الآلي نفسه لإثبات قيامه بالجريمة من خلال تلك الأجهزة من عدمه كالبحث عن جهاز ROUTER، دليل على دخوله للأنترنيت، ووجود ماسح ضوئي SCANNER، أو جهاز طابعة ليزر ألوان قد يكون دليلا على قيامه باستخدام جهاز الحاسب الآلي في تزوير وطباعة العملات النقدية، وما إلى ذلك من أجهزة وملحقات خاصّة بالجهاز[2].

2. مدى قابلية المكوّنات المنطقية للحاسب الآلي للتفتيش[3]:

قد يرد التفتيش على المكونات المنطقية للحاسب الآلي، المتمثلة في المعلومات المعالجة إلكترونيا، ولعل الصورة المعتادة والمثال العملي الذي يمكن تقريره هو فحص البرمجيات الذي يعدّ من الوسائل الرئيسية في الكشف عن الجرائم الإلكترونية، مثل الدخول غير المشروع إلى نظم الغير، فوجود برمجيات غير مصنفة تعمل في بيئة الاختراق أو تساعد عليه، كما هو الشأن في برمجيات المسح

---

[1]– هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997، ص 74. وأنظر: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 41. وأنظر أيضا: حازم محمد حنفي، المرجع السابق، ص 42–43. وأنظر: محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 277.

[2]– حازم محمد حنفي، المرجع السابق، ص 43.

[3]– المكونات المنطقية هي نفسها المكونات المادية وهي مجموعة البرامج والوثائق المتعلقة بتشغيل وحدة معالجة البيانات، وتنقسم هذه الكيانات المنطقية إلى نوعين:

أ/– الكيانات الأساسية: تضم كل البرامج الضرورية من أجل استخدام أفضل للحاسوب وملحقاته، وهي مندمجة في الجهاز نفسه مثل أنظمة التشغيل وأنظمة البرمجة.

ب/– الكيانات التطبيقية: تضم البرامج التي تمكن مستخدم الجهاز من أن ينفذ بواسطته عملا محدد بدقة ومتصلا باحتياجات هذا المستخدم الخاصّة والذي يسعى لمواجهة مشكلة ما. حيث تساعد المستخدم في عمله من أمثلتها برامج معالجة النصوص وجداول البيانات الإلكترونية، وبرامج قواعد البيانات، وبرامج التحليل الإحصائي. أنظر: علي حسن الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنيت، المرجع السابق، ص 24.

للكشف عن الأبواب المفتوحة، يمكن أن يشكل دلالة كافية على ارتكاب الشخص لجريمة الدخول غير المشروع للحاسب الآلي إذا استتبع ذلك اعترافا شفويا بارتكاب الجريمة[1].

وإذا كان الأمر قد انتهى إلى صلاحية مكونات الحاسب المادية كمحل يرد عليه التفتيش، فإنّ إمتداد ذلك إلى مكوناته المنطقية هو محل جدل كبير حول صلاحياتها لأن تكون موضوعا للتفتيش[2] كما يلـــي[3]:

أ. **الرأي الأول:** يرى بجواز ضبط البيانات الإلكترونية بمختلف أشكالها، و يستند هذا الرأي في ذلك إلى القوانين الإجرائية عندما تنص على إصدار الإذن بضبط (أي الشيء) فإنّ ذلك يجب تفسيره بحيث يشمل بيانات الحاسب المحسوسة وغير المحسوسة، لأنّ الهدف من التفتيش هو ضبط الأدلة التي تفيد في كشف الحقيقة. و يمتد هذا المفهوم ليشمل البيانات الإلكترونية بمختلف أشكالها.

ب. **الرأي الثاني:** عكس الرأي الأول، ويرى عدم انطباق المفهوم المادي على بيانات الحاسب غير المرئية أو غير الملموسة، لذا فإنّه يقترح مواجهة هنا القصور التشريعي عن طريق النص صراحة على أنّ تفتيش الحاسب الآلي لابد أن يشمل (المواد المعالجة عن طريق الحاسب الآلي أو بيانات الحاسب الآلي). بحيث تصبح الغاية الجديدة من التفتيش بعد التطور التقني الذي حدث بسبب ثورة الاتصالات عن بعد هو البحث عن الأدلة المادية أو أي مادة معالجة بواسطة الحاسب الآلي.

ت. **الرأي الثالث:** هذا الرأي نأى بنفسه عن البحث عمّا إذا كانت كلمة شيء تشمل البيانات المعنوية بمكونات الحاسب الآلي أم لا فذهب إلى أنّ النظرة في ذلك يجب أن تستند إلى الواقع العملي والذي يتطلب أن يقع الضبط على بيانات الحاسب الآلي إذا اتخذت شكلا ماديّا.

---

[1]– دلال مولاي ملياني، التفتيش في جرائم تكنولوجيا الإعلام و الاتصال، مقال منشور بمجلة القانون والعلوم السياسية، العدد 03، ، منشورات معهد الحقوق، المركز الجامعي النعامة، جانفي 2016، ص 295.

[2]– رشيدة بوكر، المرجع السابق، ص 397. وانظر أيضا: راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقني المعلومات، دراسة تطبيقية على إمارة أبوظبي، مقال منشور ضمن مجلة الدراسات الإستراتيجية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الإستراتيجية، العدد 131، 2008، ص 58.

[3]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 42–44. وانظر أيضا : حسين بن سعيد الغافري، المرجع السابق، 476 وما بعدها، وأنظر: محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 278–279.

و يذهب رأي فقهي إلى أنه في تحديد مدلول الشيء بالنسبة لمكونات الحاسب الآلي يجب عدم الخلط بين الحق الذهني للشخص على البرامج و الكيانات المنطقية وبين طبيعة هذه البرامج والكائنات، وإنّما يتعين الرجوع في ذلك إلى تحديد مدلول كلمة المادة في العلوم الطبيعية، فإذا كانت المادة تعرّف بأنها كل ما شغل حيزا ماديا في فراغ معيّن وأنّ الحيّز يمكن قياسه والتحكم فيه، وكانت الكيانات المنطقية أو البرامج تشغل حيّزا ماديا في ذاكرة الحاسب الآلي ويمكن قياسها بمقياس معيّن، وإنّها أيضا تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر أو واحد، فإنّها تعدّ طبقا لذلك ذات كيان مادي وتتشابه مع التيار الكهربائي الذي إعتبره الفقه و القضاء في فرنسا ومصر من قبيل الأشياء المادية. وفي الولايات المتحدة الأمريكية تم تعديل القاعدة رقم 34 من القواعد الفيدرالية الخاصّة بالإجراءات الجنائية لسنة 1970 لتنّص على السماح بتفتيش أجهزة الحاسب الآلي والكشف عن الوسائط الإلكترونية بما في ذلك البريد الإلكتروني والبريد الصوتي والبريد المنقول وعن طريق الفاكس.

3. مدى خضوع شبكات الحاسب الآلي للتفتيش:

الأمر هنا يتعلق بمسألة على درجة كبيرة من الخطورة تتعلق بالتفتيش عن بعد وذلك نتيجة لطبيعة التكنولوجيا الرقمية، فالبيانات التي تحتوي على أدلّة قد تتوزع عبر شبكة حاسوبية في أماكن مجهولة بعيدة تماما عن الموقع المادي للتفتيش وإن ضل من الممكن الوصول إليها من خلال حاسبات إلكترونية تقع في الأبنية الجاري تفتيشها. وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتّى في بلد آخر. وفي حين أنّ سلطات في بعض البلدان قد لا تنزعج من أن تقودها تحقيقاتها إلكترونيا إلى اختصاص قضائي سيادي آخر، إلاّ أنّ السلطات في ذلك الإختصاص السيادي الآخر قد تشعر بالانزعاج وهذا يزيد من تعقيد مشاكل الجريمة الإلكترونية[1] وتستطيع أن نميز في هذه الصورة بين ثلاثة احتمالات.

أ. **الإحتمال الأول:** إذا كانت المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى.

يثير هذا الإحتمال تساءل هام في ألمانيا يتعلق بمدى إمكانية الحق في التفتيش إذا تبيّن أنّ الحاسب أو النهاية الطرفية في منزل المتهم متصلّة بجهاز أو نهاية طرفية في مكان آخر مملوك لشخص غير المتهم. يرى الفقه الألماني إمكانية إمتداد التفتيش إلى سجلات البيانات التي تكون في موقع آخر

[1]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 44.

استنادا إلى مقتضيات القسم 103 من قانون الإجراءات الجنائية الألماني. وذلك عندما يكون مكان التخزين الفعلي خارج المكان الذي يتم فيه التفتيش[1].

ونجد تطبيقات هذا الرأي في المادة 88 من قانون تحقيق الجنايات البلجيكي الصادر في 2000/11/23 التي تنص على: "إذا أمر قاضي التحقيق بالتفتيش في نظام معلوماتي، أو في جزء منه فإنّ هذا البحث يمكن أن يمتد إلى نظام معلوماتي آخر يوجد في مكان آخر غير مكان البحث الأصلي، ويتم هذا الإمتداد وفقا لضابطين: أولهما إذا كان ضروريا لكشف الحقيقة بشأن الجريمة محل البحث، و الثاني إذا وجدت مخاطر تتعلق بضياع بعض الأدلة نظرا لسهولة عملية محو أو إتلاف أو نقل البيانات محل البحث".

وذات الشيء نجده في القانون الإتحادي الأسترالي حيث لم تعد صلاحيات التفتيش المتصلة بالأدلّة الإلكترونية تقتصر على مواقع محددّة، فقد توخى قانون جرائم الأنترنيت لسنة 2001 إمكانية أن تتوزع بيانات الأدلّة على شبكة الحاسب الآلي، ويسمح هذا القانون بعمليات تفتيش البيانات خارج المواقع التي يمكن اختراقها من خلال حاسبات توجد في الأبنية الجاري تفتيشها[2].

ويشير مصطلح "البيانات المتحجرة في حاسب ما" إلى أيّة بيانات متحجرة في جهاز تخزين على شبكة حاسبات يشكل الحاسب الآلي جزءا منها" فلا توجد حدود جغرافية محددّة، ولا أي اشتراط بالحصول على موافقة طرف ثالث غير أن المادة **(3LB)** بقانون الجرائم لسنة 1914، والتي أدرجها قانون جرائم الأنترنيت، تشترط إخطار شاغل المبنى النّائي قدر الإمكان عمليّا، وهذا قد يكون أكثر تعقيدا ممّا يبدوا عليه، إذا أنّه في مسار إجراء عملية بحث من خلال بيئة مرتبطة شبكيا، فإنّ المرء لا يكون متأكدا دائما من مكان وجوده[3].

ب. **الاحتمال الثاني:** وهو الاحتمال الذي تكون فيه المعطيات المراد تفتيشها تقع خارج الإقليم الجغرافي لدولة معينة.

---

[1]– هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، المرجع السابق، ص 77.

[2]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 45.

[3]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع نفسه، ص 45-46.

من المشاكل التي تواجه سلطة الإدعاء في جمع الأدلة، قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمين في ذلك شبكة الاتصالات المعلوماتية مستهدفين عرقلة الإدعاء في جمع الأدلّة والتحقيقات، و في هذه الحالة فإنّ امتداد الإذن بالتفتيش إلى خارج الإقليم الجغرافي لدولة أخرى وهو ما يسمّى بالولوج أو التفتيش عبر الحدود قد يتعذر القيام به بسبب تمسك كل دولة بسيادتها. لدى فإنّ جانب من الفقه يرى بأنّ التفتيش الإلكتروني العابر للحدود لابد وأن يتم في إطار اتفاقيات خاصة ثنائية أو دولية تجيز هذا الامتداد تعقد بين الدول المعنية. وبالتالي فإنّه لا يجوز القيام بذلك التفتيش العابر للحدود في غياب تلك الإتفاقية، أو على الأقل الحصول على إذن الدولة الأخرى، وهذا ما يؤكد على أهمية التعاون الدولي في مجال مكافحة الجرائم الإلكترونية[1].

وكتطبيق لهذا الإجراء، فقد حدث في ألمانيا أثناء جمع إجراءات التحقيق عن جريمة غش وقعت في بيانات حاسب آلي، فقد تبيّن وجود اتصال بين الحاسب الآلي المتواجد في ألمانيا وبين شبكة اتصالات في سويسرا حيث يتم تخزين بيانات المشروعات فيها.

وعندما أرادت سلطات التحقيق الألمانية ضبط هذه البيانات، فلم تتمكن من ذلك إلاّ عن طريق التماس المساعدة الذي تم بالتبادل بين الدولتين.

وفي حالة أخرى ساور الشك، الشرطة اليابانية بأنّ مجموعة من المخربين قد استخدمت أجهزة الكمبيوتر في الصين والولايات المتحدة في مهاجمة العديد من المواقع الخاصّة بالحكومة اليابانية على الشبكة، وقد طالبت الشرطة اليابانية كلا من بكين وواشنطن بتسليم بيانات الدخول المسجلة على أجهزة الكمبيوتر في كل من هاتين الدولتين حتى يتمكنوا من الوصول إلى جذور هذه العملية الإرهابية[2].

4. القواعد الفنيّة لتفتيش الحاسب الآلي:

ليست هناك قواعد محددة تحكم عملية تفتيش الحاسب الآلي (الحاسوب) من الناحية الفنية، إذ يعتمد التفتيش الفنّي للحاسوب على الشخص الذي يقوم بتفتيشه وهو يختار الطريقة المناسبة حسب ظروف وملابسات كل جريمة ووضعية الحاسب الآلي المراد تفتيشه. وفي هذا الصدد أصدرت وزارة

[1]– هلالي عبد اللاه أحمد، تفتيش نظم الحاسب وضمانات المتهم المعلوماتي، المرجع السابق، ص 87. وأنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 46.

[2]– محمد حمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2013، ص 144.

العدل الأمريكية مرشدا فيدراليا لتفتيش الحواسيب في الولايات المتحدة الأمريكية [1]، ولإنجاح الخطوات المتبعة في عملية تفتيش الحاسب الآلـــــي: حدد المرشد الفيدرالي الأمريكي لتفتيش وضبط الحاسب الآلـي أربـع خطـوات يمكـن للقـائم بـالتفتيش اتباعهـا لزيـادة احتماليـة نجـاح عمليـة التفتـيش وهـي كالتالـــــي:

أ. **تجميع فريق التفتيش**[2] : يتكون فريق التفتيش من ثلاثة أشخاص: هم كل من القائم بالتفتيش الذي يعد قائد الفريق، والمدعي العام والخبير الفنّي الذي له دراية فنية في مجال تقنية الحاسوب، وتكون المهام موزعة بين أعضاء الفريق، إذ يقوم القائم بالتفتيش بتفتيش بتوجيه عملية التفتيش والقيام بكل الإجراءات القانونية المتعلقة بالتفتيش، أمّا الخبير الفني فيقوم بتفتيش الحاسوب، ويقوم المدعي العام بمراجعة إذن التفتيش والتأكد من تطابق جميع الإجراءات القانونية مع التعديل الرابع للدستور الأمريكي والمادة 41 من قانون الإجراءات الجنائية الفيدرالي الأمريكي ويذهب جانب من الفقه العربي إلى الأخذ بأن فريق التفتيش والضبط يتكون من:

- المشرف على التحقيق: ويتولى إدارة العملية في مسرح الجريمة وتوزيع الهام على أعضاء الفريق.
- فريق آخذ الإفادات: ويتحدد عددهم حسب حجم الجريمة وعدد المتهمين والشهود في محل الحادث.
- فريق الرسم والتصوير: ويتكون من شخص واحد أو أكثر ومهمة هذا الفريق هو إجراء المخطط لمحل الحادث والتقاط الصور الفوتوغرافية وتحديد مواقع أجهزة الحاسوب في المكان.
- فريق التفتيش العملي: ويضم شخصا واحدا أو أكثر حسب الحاجة ومهمة هذا الفريق إجراء التفتيش الفنّي على الحاسوب.
- فريق التأمين والقبض: وهو الفريق المكلف بالسيطرة على مسرح الجريمة ومخارج ومداخل المكان وإلقاء القبض على المشتبه بهم وغيرها من الإجراءات الضرورية.

---

[1]–سامي جلال فقي حسين، المرجع السابق، ص 197.

[2]–علي عدنان الفيل، إجراءات التحري وجمع الأدلّة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 52–53، وأنظر أيضا: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في لجرائم المعلوماتية، المرجع السابق، ص 666–668.

- فريق ضبط وتحرير الأدلّة: ويتكون هذا الفريق من شخصين أو أكثر من خبراء الحاسوب، يقومون بضبط الأدلّة المعلوماتية التي يتم الحصول عليها من التفتيش ووضعها في الأوعية المعدّة لضبطها ووضع العلامات عليها.
- خبراء مسرح الجريمة العادية: مثل خبير البصمات وخبير الأسلحة...الخ.

غير أنّ هذا العدد كبير نسبيا مقارنة بفريق التفتيش المذكور سابقا، لذلك نرى بأنّه لابد أن يكون الفريق مكونا من ثلاثة أشخاص فقط هم:

- القائم بالتفتيش: وهو الذي يتولى اتخاذ الإجراءات القانونية والأمنية اللاّزمة لإجراء التفتيش، وينفذ خطة التفتيش عبر مساعديه من رجال الشرطة.
- الخبير الفنّي: يتولى مهمة تفتيش الحاسوب وضبط الأدلة المتحصلة منها على مساعده الفنّي.

ب. التعرف على نظام الحاسب محل التفتيش:

بعد تشكيل فريق التفتيش، يبدأ الشخص لمكلف بالتفتيش (المحقق) مهامه بمحاولة التعرف على نظام الحاسوب المراد تفتيشه، وذلك بمعرفة الشكل المميز للحاسبات الإلكترونية وملحقاتها ومسمى كل منها، والهدف من استخدامه وما هي احتمالات توظيفه لارتكابه أيّ من الجرائم الإلكترونية، حيث أنّ عدم تعرّفه عليها قد يؤدي إلى إهمالها أو حتى إتلافها دون قصد أو تعديل البيانات الموجودة فيها نتيجة الجهل بها، ليس هذا فحسب بل لابدّ أن يلّم المحقق بكيفية التعامل مع تلك المكونات من أجهزة وملحقات و وسائط تخزين بصفتها أدلّة محتملة[1].

إنّ صعوبة تفتيش الحاسوب تكمن في كون الحاسوب إمـا غير مرتبط بالشبكة كما قد يكون مرتبط بها، فالحاسوب الغير مرتبط بالشبكة تكون المعلومات محصورة في الحاسوب فحسب، أمّا الحواسيب المرتبطة ببعضها بشبكة فإنّ المعلومات المطلوبة قد تكون في مكان آخر وبالتالي صعوبة الوصول إليها.

وبالتالي فإنّ أهمية الحصول على معلومات نظام الحاسوب تبرز في حالة واحدة فقط هي عندما يقررّ فريق التفتيش إجراء التفتيش في موقع وجود الحاسوب، ففي هذه الحالة يحتاج فريق التفتيش جمع المعلومات الممكنة حول نظام الحاسوب وذلك لكي يتمكن الخبير من تفتيش الحاسوب وتهيئة البرامج والوسائل اللاّزمة لذلك، فقد يفاجئ الخبير عند مباشرته التفتيش أنّ الحاسوب يعمل بنظام غير مألوف،

[1]– علي عدنان الفيل، إجراءات التحري وجمع الأدلّة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 22-23.

ففي هذه الحالة لن يتمكن من إجراء التفتيش، لهذا يجب على فريق التفتيش ضبط الحاسوب بأكمله ونقله إلى المختبرات لغرض إجراء التفتيش[1].

وقد يقوم فريق التفتيش باتخاذ إجراء تفتيش الحاسوب خارج المكان المتواجد فيه، إذ يقوم الخبير بضبط الحاسوب مع ما هو ضروري من ملحقاته ونقله إلى المختبر لإجراء التفتيش عليه، إلاّ إذا كان هذا الحاسوب مرتبطا بالشبكة ففي هذه الحالة على الخبير الفنّي محاولة إجراء التفتيش في مكان وجود الحاسوب لأنّه من المحتمل أن تكون الملفات مخزّنة في مكان آخر غير الحاسوب المراد تفتيشه ويؤدي ذلك إلى صعوبة الوصول إليها إذا تم فصل الحاسوب عن الشبكة المرتبط بها.

ت. وضع خطة لتنفيذ التفتيش:

بعد التّعرف على نظام الحاسوب يقوم فريق التفتيش بوضع الخطة الملائمة لتنفيذ التفتيش، ووضع خطة التفتيش هو مسؤولية رئيس الفريق، إذ يقررّ حجم المهمّة ونوع الدليل الذي يتم البحث عنه وكيفية إجراء التفتيش وتوزيع الأدوار والمسؤوليات على بقية أعضاء الفريق.

وليست هناك خطة ثابتة يعتمد عليها فريق التفتيش في كل قضية، إذ تختلف خطة التفتيش بإختلاف ظروف وملابسات كل قضية، ومن الضروري على فريق التفتيش وضع خطه بديلة بالإضافة إلى الخطة الأصلية، إذ قد يفاجئ الفريق بأمور غير متوقعة أثناء التفتيش، فقد يكون الحاسوب مشفرا مثلا وقد يحتاج فك الشفرة مدة طويلة وبرامج عديدة لذلك يجب أن تكون الخطة البديلة جاهزة في هذه[2] الحالة وهي نقل الحاسوب إلى المختبر لإجراء التفتيش عليها والوصول إلى الملفات المطلوبة.

وخطة التفتيش يجب أن تكون خطة شاملة إبتداءا من الدخول إلى مكان الموجود فيه الحاسوب وانتهاء بضبط الأدلّة المطلوبة والموجودة في الحاسوب محل التفتيش، ويمكن أن تكون الخطة العامة لإجراء التفتيش كالآتي:

- إعداد خريطة للموقع الذي يتم تفتيشه ويوجد فيه جهاز الحاسوب محل التفتيش وتحديد مكان جهاز الحاسوب ونوعه.
- توزيع المهام بين أفراد الفريق ليتمكن كل عضو من فريق التفتيش معرفة دوره ليتسنى له معرفة مهمته والتحضير لها بدقّة، ويتم ذلك من خلال إعداد خطة الهجوم بحيث تكون الخطة واضحة

[1]– سامي جلال فقي حسِن، المرجع السابق، ص 200.

[2] – سامي جلال فقي حسِن، المرجع السابق، ص 201.

ومفهومة لدى أعضاء الفريق، وتكون الخطة معززّة بالرسومات والخرائط التي توضح عملية الإقتحام لمكان تواجد الحاسوب المطلوب تفتيشه.

- تأمين التيار الكهربائي لتجنب التلاعب أو التخريب عن طريق قطع التيار أو تعديل الطاقة.
- السيطرة على مداخل ومخارج مكان التفتيش لمنع أي شخص من الدخول أو الخروج من المكان لحين انتهاء التفتيش.
- إبعاد جميع الأشخاص الموجدين بالقرب من جهاز الحاسوب المراد تفتيشه لضمان عدم التلاعب به لحين إكمال التفتيش.
- إبقاء الخطة في نطاق السريّة لحين انتهاء إجراء التفتيش، إذا أنّ تسرّب معلومات عن خطة التفتيش ومكان وزمان القيام بها قد يؤدي إلى وصول المعلومات إلى المتهمين وبالتالي إتلاف الملفات التي تحتوي البيانات والمعلومات المراد ضبطها والمخزّنة في جهاز الحاسوب وبالتالي ضياع معالم الجريمة[1].

وبالتالي فإنّ الخطة أعلاه مناسبة لتصبح قاعدة عامّة يستعان بها في إجراء تفتيش أنظمة الحاسوب في مختلف الجرائم الإلكترونية مع إمكانية تعيين الخطة حسب ظروف وملابسات كل قضيّة، فإمكانية نجاح أي خطة يعتمد بالدرجة الأولى على العناصر البشرية التي تتولى وضع الخطة الملائمة لكل جريمة، بالإضافة إلى الأشخاص الذين يتولون تنفيذ الخطة، فأي خطأ في تنفيذ الخطة قد يؤدي إلى فشلها و بالتالي صعوبة الحصول على الأدلة المطلوبة من الحاسوب فالقائم بالتفتيش أو رئيس فريق التفتيش عليه أن يختار الأشخاص المناسبين الذين يتولون تنفيذ الخطة التي يرسمها لتفتيش الحاسوب محل الجريمة الإلكترونية ليضمن نجاح الخطة التي وضعها إلى درجة كبيرة.

ث. أسلوب تفتيش الحاسب الآلي[2]:

يمكن تفتيش الحاسب الآلي بأربعة أساليب هي:

- تفتيش الحاسوب في موقعه وطبع نسخ ورقية من الملفات التي تم ضبطها يتم تفتيش الحاسوب بموجب هذه الطريقة في مكان وجود الحاسوب محل التفتيش إذ يقوم الخبير الفنّي بتفتيش الحاسوب بحثا عن الملفات المطلوبة وبعد العثور على تلك الملفات يقوم الخبير بطبع نسخ ورقية

[1]– سامي جلال فقي حسين، المرجع السابق، ص 202.

[2]– سامي جلال فقي حسين، المرجع نفسه، ص 206–207. وأنظر أيضا: علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 48–49.

من الملفات التي تم ضبطها، غير أنّ هذه الطريقة منتقدة لأنّ اختيار هذه الطريقة يؤدي إلى فقدان قدر كبير من المعلومات الضرورية والمهمّة للتحقيق، ومن هذه المعلومات، تاريخ و وقت الملف، اسم الملف السّري، وغيره من المعلومات إذ أنّ طبع الملفات على الورق يؤدي إلى عدم ظهور هذه المعلومات على الورق وبالتالي خسارة كل المعلومات.

- تفتيش الحاسوب وعمل نسخة إلكترونية من الملفات التي تم ضبطها.

بموجب هذه الطريقة يقوم الخبير بتفتيش الحاسوب وعند إيجاد الملفات المطلوبة يقوم الخبير بنسخ هذه الملفات وخزنها على أية واسطة خزن، كالأقراص مثلا ويتم هذا الإجراء في مكان وجد الحاسوب.

وهذه الطريقة ملائمة إذا كان الحاسوب محل التفتيش هو حاسب شخص غير مرتبط بشبكة معيّنة، كذلك إذا كان جهاز الحاسوب غير محكم بكلمة سر يصعب الدخول إليها، إذا أنّ ضبط الحاسوب بالكامل ونقله إلى المختبر لا يتم اللجوء إليه إلاّ إذا كان الحاسوب نفسه بمكوناته المادية هو أداة الجريمة وليس واسطة خزن المعلومات فقط.

وبالتالي فإنّ هذه الطريقة تعتبر المثلى لضبط الملفات محل الجريمة لأنّ جهاز الحاسوب هنا مجرد واسطة خزن الملفات، ولا فائدة من ضبط الحاسوب ما دام قد يتم الحصول على الملفات المطلوبة وخزنها على واسطة خزن، كالأقراص المغناطيسية وغيرها من وسائط الخزن، عكس الطريقة الأولى التي يكون فيها الدليل الذي يضبط عند تفتيش الحاسوب ناقص المعلومات.

- نسخ ذاكرة الحاسوب بالكامل في موقع الحاسوب وخزنها على واسطة خزن يقوم الخبير بموجب هذا الأسلوب بنسخ ذاكرة الحاسوب بالكامل في موقع وجود الحاسوب وخزنها على واسطة خزن ومن تم إجراء التفتيش في المختبر واستخراج الملفات المطلوبة.

وتعتبر هذه الطريقة غير ملائمة، وذلك لأنّ القرص الصلب لجهاز الحاسوب قد يحتوي على عدد هائل من المعلومات وقد تكون مخزّنة عليه ملفات شخصية لا تشكل أهمية بالنسبة للجريمة التي تم تفتيش الحاسوب بسببها وبالتالي يتم انتهاك حق الخصوصية لحائز الحاسوب، بالإضافة إلى ذلك فإنّ هذه الطريقة غير مفضلة إذا كان جهاز الحاسوب مرتبطا مع الشبكة، ففي هذه الحالة لا تتم الاستفادة من نسخ ذاكرة الحاسوب بشكل مثالي، لأنّه من المتوقع أن تكون هناك ملفات مخزنة على الشبكة أو في نهاية طرفية أخرى بعيدة عن مكان وجود الحاسوب محل التفتيش.

- ضبط جهاز الحاسوب بالكامل وإزالة ملحقاته ونقله إلى المختبر لتفتيشه يتم ضبط جهاز الحاسوب بالكامل في مكان وجوده إذ يقوم الخبير المختص بإزالة الملحقات غير الضرورية والمرتبطة بالحاسوب كالطابعات والسماعات الخارجية وغيرها ومن تم نقل الحاسوب إلى المختبر تمهيدا لتفتيشه أو ضبطه كمبرر جرمي.

إنّ هذه الطريقة تستخدم عندما يكون جهاز الحاسوب أداة إرتكاب الجريمة كمكونات مادية حيث أنّ من بديهيات التحقيق ضبط أداة الجريمة سواء كان ذلك في الجرائم التقليدية، أو في الجرائم الالكترونية، ويمكن استخدام هذا الأسلوب أيضا في حال مواجهة الخبير المختص صعوبات في الدخول إلى الحاسوب لإجراء التفتيش على الملفات كأن يكون الحاسوب محميا بكلمة سر أو تكون الملفات مشفرة أو مخفيّة وغيرها من الصعوبات وبالتالي ضرورة نقل الحاسوب إلى المختبر لتفتيشه.

ثالثا /ضوابط التفتيش في الجريمة الإلكترونية:

سبق القول بأنّ التفتيش إجراء قانوني خطير يمسّ بالحرّية الشخصية للأفراد، لذلك أحاطتهُ التشريعات الإجرائية بمجموعة من الضوابط الموضوعية وأخرى إجرائية، الهدف منها تحقيق الموازنة بين المصلحة الإجتماعية وردع المجرمين وبين حقوق الأفراد وحرياتهم الأساسية.

1. الضوابط الموضوعية للتفتيش في الجرائم الإلكترونية:

يقصد بالضوابط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية و بصفة خاصة في الجرائم الإلكترونية الضوابط اللازمة لإجراء تفتيش صحيح و يمكن حصر فيما يلي: دافع التفتيش، نطاقه، والغاية منه.

أ. دافع التفتيش:

إن التفتيش بوصفه إجراء من إجراءات التحقيق يكون عادة عند وقع جريمة من الجرائم وإسنادها إلى شخص معين سواء بصفته مرتكبا مباشرا أو مساهما فيها أو توفر أدلة أو قرائن على وجود اشياء تفيد في إثبات الجريمة أو الكشف عنها ويقصد بالسبب الدافع إلى التفتيش الحصول على الدليل في تحقيق قائم بقصد كشف الحقيقة [1]، وعليه فالتفتيش في القواعد العامّة بوصفه إجراء من إجراءات التحقيق لا يصّح إصدراه ولا يعتبر مشروعا إلاّ إذا صدر لضبط جريمة من نوع جناية أو جنحة واقعة بالفعل أو ترجح وقوعها ونسبتها للمتهم، مع توافر الدلائل الكافية لنسبة الجريمة إليه[2].

[1]–علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والأنترنيت، المرجع السابق، ص 62.

[2]–خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 209.

وبناءا عليه وتطبيقا على الجرائم الإلكترونية فإنّ دافع التفتيش المتعلق بهذا النوع من الجرائم يخضع لذات الضوابط السابقة الذكر والمتمثلة فيما يلـــي:

أ-1 وقوع جريمة إلكترونية: والجريمة الإلكترونية[1]هي كل فعل غير مشروع مرتبط باستخدام الحاسب الآلي لتحقيق أغراض غير مشروعة[2].

ويشترط أن تكون هذه الجريمة جناية أو جنحة وتم استبعاد المخالفات لأنها قليلة الأهمية ولا تستحق التعّرض لحرّيات الأشخاص أو انتهاك خصوصياتهم بالإضافة إلى أن تكون هذه الجريمة قد وضعت فعلا، فلا يجوز القيام بهذا الإجراء لضبط أدلة في جريمة مستقبلية ولو قامت التحريات والدلائل الجدّية على أنّها ستقع بالفعل[3].

أ-2 ضرورة الاشتباه في شخص معيّن أو اتهامه بارتكاب الجريمة أو المشاركة فيها: فلا يكفي لقيام سبب التفتيش وقوع جريمة إلكترونية بل لابد أن يكون هناك إتهام موجّه ضد شخص معيّن، أو أن تتوافر في حق الشخص المراد تفتيشه دلائل كافية تدعوا إلى الاعتقاد بأنّه قد ساهم في ارتكاب الجريمة الإلكترونية سواءا بوصفه الشخصي[4]. ويمكن القول بأن تعبير الدلائل الكافية في مجال الحاسب الآلي هي مجموعة من المظاهر أو الأمارات المعنية التي تقوم على المضمون العقلي والمنطقي لملابسات الواقعة وكذلك على خبرة حرفية القائم بالتفتيش والتي تؤيد نسبة الجريمة الإلكترونية إلى شخص معيّن سواءا بوصفه فاعلا أو شريكا[5].

ومعنى ذلك أن تتوافر في حق المراد تفتيشه دلائل قوية وكافية تبني إلى الاعتقاد بأنه ساهم في ارتكاب الجريمة الإلكترونية، ولا يقتصر ذلك على مجرد تجميع القرائن والأدلة التي تفيد وقوع

---

[1]- أدرج المشرع الجزائري فصلا خاصا –الفصل السابع- في قانون العقوبات يتعلق بهذا النوع من الجرائم وهي جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7.

[2]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيقات الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 49.

[3]- أسامة بن غانم العبيدي، المرجع السابق، ص 97.

[4]- صورية بوربابة، قواعد الأمن المعلوماتي، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، بلعباس، 2016-2017، ص 254.

[5]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيقات الإبتدائي في الجريمة المعلوماتية، المرجع السابق، ص 50.

الجريمة ونسبتها إلى فاعلها، بل يجب أن تتضمن كذلك المعلومات والقرائن التي تعزز موقف المشتبه فيه وتنفي عنه ارتكابه للجريمة

كما يجب أن يكون الاتهام جديا ومبنيا على أدلة أو قرائن قانونية، وعليه يتعين على الجهة التي تمنح الإذن بالتفتيش أن تراقب هذه الإجراءات، فالتفتيش لا يجوز إجراءه إلا إذا كان هناك احتمال للعثور على دليل من ورائه.

ب-**نطاق التفتيش:**

يقصد بنطاق التفتيش محله أو المستودع الذي يحتفظ فيه المرء بأسراره التي تتضمنه[1]، ومحل التفتيش يجب أن يكون ممّا يتمتع بحرمة المسكن أو الشخص أو الرسائل.

ويأخذ محل التفتيش في الجريمة الإلكترونية حكم المسكن أو الشخص في الجريمة التقليدية والشخص كمحل لتفتيش نظم الحاسب الآلي قد يكون من مستغلي أو مستخدمي الحاسب الآلي أو من خبراء البرامج سواء كانت برامج نظام أو برامج تطبيقات، وقد يكون من المحللين، أو مديري النظم المعلوماتية وفي جميع الأحوال يقصد بالشخص كمحل قابل للتفتيش كل ما يتعلق بكيانه المادي وما يتصل به[2].

أمّا المسكن أو المنزل وما في حكمهما كمحل لتفتيش نظم الحاسب الآلي كافة محال الإقامة والملحقات المخصصّة لمنافعها والتي يشغلها الشخص سواءا بصفة دائمة أو مؤقتة، وسواءا كانت ثابتة أم متنقلة متى وجدت فيها مكونات الحاسب الآلي المادية أو المنطقية أو شبكات إتصال خاصّة[3].

ويشترط في المحل سواءا في الجرائم التقليدية أو الإلكترونية شرطان همـــــا:

ب-1 أن يكون معّينا: يشترط لصة التفتيش أن يكون محله معينا دقيقا نافيا للجهالة، أي أن يتم تحديد المكان المراد تفتيشه بدقّة وبالنسبة لمحل التفتيش في الجرائم الإلكترونية فإنّه ينبغي تحديد المعلومات والبيانات المراد البحث عنها وضبطها تحديدا نافيا للجهالة حسب القواعد العامّة، غير أنّ تحديد محل التفتيش في الجريمة الإلكترونية يثير صعوبة في التوصل إلى هذه المعلومات أحيانا بسبب تداخل وتشابك الملفات التي تحوي هذه المعلومات وصعوبة فصلها عن بعضها البعض، لذلك

[1]- صورية بورباية، المرجع السابق، ص 255.

[2]-حسين بن سعيد الغافري، المرجع السابق، ص 490-491.

[3]-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 215.

فإنّ القائم بالتفتيش يضطر أحيان إلى القيام ببحث عام للتوصل إلى هذا الدليل وهذا يخالف القواعد العامّة في وجوب تحديد المحل تفتيشه وبالتالي يكون هناك انتهاك لحق الخصوصية[1].

ب-2 أن يكون موضوع التفتيش ممّا يجوز تفتيشه: قد يمنح القانون محل الجريمة حصانة معيّنة فيمنع إجراء التفتيش على الرغم من توافر شروطه، ويرجع سبب منح القانون الحصانة لمحل معيّن بسبب تعلقها بمصلحة معيّنة عامّة أو فردية يرى المشرع بأنّها أولى بالرعاية من مصلحة التحقيق التي يتطلبها إجراء التفتيش أي لا يكون هناك حظر[2]على التفتيش[3].

---

[1]- سامي حسن الحسيني، النظرية العامّة للتفتيش، الطبعة الأولى، دار النهضة العربية، القاهرة، 1972، ص 129.

[2]- من أهم حالات الحظر من عملية التفتيش ما يتعلق بالحصانات وهي:

أ- الحصانة الدبلوماسية: هذا الحق يتمتع به أعضاء السلك الدبلوماسي أثناء قيامهم بالوظيفة في دولة معيّنة، إذ ليس بالإمكان لاتخاذ أي إجراء ضد أعضاء السلك الدبلوماسي ما داموا يؤدون وظائفهم العملية، وهذه الحصانة لا تكون إلاّ من خلال مدّة عملهم، وتشمل جل أفراد البعثة الدبلوماسية وحتى مقرّها إذا لا يجوز دخوله إلاّ بإذن من طرف رئيس البعثة، فإذا افترضنا أنّ الجريمة الإلكترونية ارتكبت بواسطة جهاز حاسوب موجود بمقر البعثة الدبلوماسية، فلا يجوز إتخاذ أي إجراء قضائي من شأنه المساس بمقر البعثة كتفتيش المقر بغية ضبط الحاسوب لان مقر البعثة يتمتع بالحصانة.أما فيما يخص المبعوث الدبلوماسي فتسري الحصانة على جميع مراسلاته فلا يجوز ضبطها أو الإطلاع عليها، غير أن عدم قضاء الدولة المعتمد لديها لا يعني إعفائه من الخضوع لقضاء دولته التي يمثلها فإذا إرتكب جريمة يمكن لسلطات الدولة المعتمدة طلب اتخاذ الإجراءات القانونية بحقه لدى الدولة التي يمثلها.

ب- الحصانة القنصلية: لا ترقى هذه الحصانة إلى مستوى الحصانة الدبلوماسية، إلا أنّه لا يجوز التفتيش أو الدخول إلى مقر البعثة القنصلية إلاّ بإذن من رئيس البعثة القنصلية أو رئيس البعثة الدبلوماسية، وتتمتع كافة ملفات ووثائق القنصلية بالحصانة فلا يجوز الاستيلاء عليها أو على موجودات القنصلية، ولا يجوز مراقبة الاتصالات الهاتفية والإلكترونية بمقر البعثة، فإذا ارتكبت جريمة إلكترونية عن طريق أحد الحواسيب العائد لمقر البعثة فلا يجوز دخوله إلاّ بإذن من رئيس البعثة.

أمّا إذا ارتكب عضو البعثة جريمة الكترونية بحاسوبه الخاص، جاز للدولة المستضيفة اتخاذ الإجراءات القانونية بحقه ومنها تفتيش حاسوبه، أنظر: سهيل حسين الفتلاوي، الدبلوماسية بين النظرية والتطبيق، دار الثقافة، عمان، الأردن، 2006، ص169 وما بعدها.

ت- الحصانة البرلمانية: وهي حق دستوري معترف به لعضو مجلس النواب يمارس مهامه البرلمانية سواءا بإبداء الرأي في المجلس أو في لجانه، قد يستجوب ويسأل أعضاء الحكومة أو قد يوجه اتهامات إلى السلطة التنفيذية، وقد يثبت لاحقا عدم صحة الاتهامات أو قد يرتكب جريمة في غير حالة التلبس، ففي هذه الأحوال لا يجوز اتخاذ الإجراءات القانونية بحقه وبالأخص= =الإجراءات التي تمس حريته وحرمة مسكنه كإلقاء القبض أو تفتيش مسكنه أو مكتبه أو سيارته إلاّ بعد رفع الحصانة الديبلوماسية عنه من قبل مجلس النواب. أنظر سامي جلال فقي حسين، المرجع السابق، ص 137.

[3]- سامي جلال فقي حسين، المرجع نفسه، ص 131.

ت-الغاية من التفتيش :

الغاية الأساسية من إجراء التفتيش هي الحصول على الأدلّة التي تساهم في كشف الحقيقة المرتكبة، ففي الجرائم التقليدية تكون غاية التفتيش هي ضبط الأدلة الماديّة التي تفيد في كشف الحقيقة، أما الغاية من التفتيش في الجرائم الإلكترونية هي الحصول على الأدلّة الالكترونية التي تساعد في الوصل إلى الحقيقة في جريمة إلكترونية وقعت وجار البحث فيها[1].

وحتى تتحقق الغاية من التفتيش في الجريمة الالكترونية لابد من أن تتوافر علامات قوّية وقرائن تدل على وجود أشياء أو أجهزة أو معدّات إلكترونية في المكان أو لدى الشخص المراد تفتيشه تفيد في كشف الحقيقة.

وبالتالي إذا ما تحققت الغاية من التفتيش، يحقّ للسلطات المختصة بالتحقيق الدخول إلى النظام المعلوماتي أو إلى جزء منه بغرض التفتيش على ذلك انظام أو المعطيات المخزنة به[2].

2-الضوابط الإجرائية للتفتيش في الجرائم الإلكترونية :

يقصد بها تلك الإجراءات التي أوجب المشرع مراعاتها عند إجراء عملية التفتيش ، والهدف من وضع هذه الشروط هي إحاطة عملية التفتيش بإجراءات و شكليات تضمن صحة و دقة النتائج التي يصل إليها القائم بالتفتيش و إحاطة المتهم بضمانات كافية للحفاظ علي حرياته الفردية ، وأبرز هذه الشروط ما يلي:

أ. الميقات الزمني لإجراء التفتيش :

مفاد هذا الشرط أنه يتعين على الشخص القائم بالتفتيش أن يتقيد بالوقت المحدد قانونا لمباشرة هذا الإجراء بمعنى آخر أن يجريه القائم به خلال فترة زمنية عادة ما يحدّدها المشرع وذلك حرصا على تضييق نطاق الاعتداء على الحرية الفردية وحرمة المسكن[3].

وتحديد الميقات الزمني على نظم المعلومات والشبكات، قد يكون سببا في إخفاء الأدلّة ومن تم عرقلة سير التحقيق، لكون أدلّة الجرائم الإلكترونية عبارة عن كيانات غير ماديّة يمكن إخفاء أدلتّها

[1]- سامي جلال فقي حسين، المرجع نفسه، ص 127.

[2]- فايز محمد راجح غلاب، المرجع السابق، ص 327.

[3]- عائشة بن قارة مصطفى، المرجع السابق، ص 110.

بسرعة متوقعة إذا ما علم الجاني مسبقا بالوقت الذي سيتّم فيه، لذلك تطرقت التشريعات الحديثة إلى إضافة الجرائم الإلكترونية ضمن الجرائم التي تستثنى من قيد المدّة الزمنية للتفتيش[1].

غير أنّ هناك استثناءات أخرى يجوز فيها الخروج عن الميعاد المحدد للتفتيش وبالتالي يصبح إجراءه في أي ساعة من ساعات الليل أو النهار في إحدى الحالات التّالية:

- حالة رضا المتهم بالتفتيش رضا حرّا صريحا و عن علم بالسبب.
- حالة الضرورة القصوى.
- الأماكن التي تستقبل الناس بدون استثناء كالمقاهي.
- في حالة الجرائم الإرهابية [2].
- ضرورة حضور بعض الأشخاص أثناء إجراء تفتيش المساكن ومن في حكمها.

يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون لإجراء التفتيش وذلك حتى يطمئن الخاضع للتفتيش إلى سيره وفقا للقانون، وللحيلولة دون تعسف القائم بالتفتيش[3].

غير أنّه استثني من تطبيق أحكام حضور الأشخاص إذا تعلق الأمر بالجرائم الإلكترونية، ولعل الأمر راجع إلى خصوصية هذه الجرائم التي لا تحتمل تأخير التفتيش، بالإضافة إلى إضفاء نوع من السرّية أثناء جمع الدليل الالكتروني، كون أنّ هذا الدليل ذو طبيعة خاصّة من حيث سرعة تعديله والتلاعب فيه حتّى عن بعد.

كما أنّ هذه الضمانة أو الشرط بدأت تتضاءل أهميته في الدول التي بدأت تأخذ بإجراء التفتيش عن بعد[4].

ب-محضر التفتيش:

يعرّف محضر التفتيش بأنّه الشهادة التي يعلن بمقتضاها المحققون ورجال الضبطية القضائية ما شاهدوه من وقائع وما اتخذوه بشأنها من إجراءات وما توصلوا إليه من نتائج والمحضر يعّد الصورة

---

[1]- فايز محمد راجح غلاب، المرجع السابق، ص 329-330.

[2]- عائشة بن قارة مصطفى، المرجع السابق، ص 111.

[3]-محمد عمر الغياثين، المرجع السابق، ص 125.

[4]- يقصد بالتفتيش عن بعد: قيام المحقق بالتفتيش وهو جالس في مكتبه باستخدام برامج خاصّة تحمل في طابعها قاعدة التفتيش عن الجريمة، ويثير هذا الإجراء العديد من المشاكل القانونية أهمها: التعدي على الخصوصية، التعدي على سيادة دول أخرى، ذلك لأنّه يعد من قبيل التجسّس وانتهاك حواسيب هذه الدول، ،خاصة إذا كانت هذه الدول لا تعترف بمشروعيته هذه البرمجيات. أنظر: عائشة بن قارة مصطفى، المرجع السابق، ص 109-110.

المكتوبة للتفتيش. وذلك فمن الضروري لصحته باعتباره عملا من أعمال التحقيق أن يتم إثباته عن طريق كافة إجراءاته وما أسفر عنه من نتائج في محضر خاص به، ولم يتطلب القانون شكلا خاص للمحضر، ما يعني أنّه لا يشترط لصحته سوى ما تستوجبه القواعد العامّة في المحاضر بشكل عام، حيث يجب أن ينطوي على البيانات التي توجبها القواعد العامّة في تحرير المحاضر وهي: أن يكون مكتوبا باللغة الرسمية، وأن يكون مؤرخا بتاريخ تحريره وموقعا من كاتبه ومبيّنا به كافة الإجراءات التي تم التفتيش بشأنها[1].

و فيما يخص محضر تفتيش وسائل التقنية الحديثة، فإنّه يلزم أن يكون المحقق ذو خبرة فنيّة تتعلق بتقني المعلوماتية، عند تحريره للمحضر، وله أن يستعين بخبير في وسائل التقنية الحديثة بما تتطلبه من خبرة في معالجة البيانات أو المعلومات وذلك حتّى يمكن للمحقق أن يغطي جميع الجوانب الفنيّة في عملية التفتيش، بالإضافة إلى المحافظة على الأدلة المتحصل عليها من الجريمة الإلكترونية، وحمايتها من كل تلف أو مسح أو تحريف[2].

ونرى أن تحرير محضر عن عملية التفتيش يعتبر لازما، وذلك لتمكين الجهات القضائية المختصة بنظر مدى احترام الإجراءات المتطلبة في عملية التفتيش ومن ثم بسط رقابتها عن شرعية هذا الإجراء.

الفرع الثاني: الضبط فـــــي الجرائم الإلكترونية

يترتب على عملية التفتيش التي تتم في إطار الشروط الموضوعية و الشكلية نشوء الحق في ضبط الأشياء التي تفيد في كشف الحقيقة عنها و عن مرتكبيها ،و يعد الضبط إجراء من إجراءات التحقيق (أسلوب من أساليب التحقيق) التي تؤدي إلى جمع الأدلّة الإلكترونية و الأثر المباشر المترتب عن عملية التفتيش حيث أنّ النتيجة الطبيعية التي ينتهي إليها التفتيش هي ضبط الأدلّة.

و الأساس القانوني للضبط هو العلاقة التي تربط بينه وبين الأشياء المتعلقة بالجريمة التي يشملها التحقيق والتي تفيد في كشف الحقيقة ما كان منها ضد المشتبه فيه أو ما كان في مصلحته.

ولقد تعوّدت جهات التحقيق في الجرائم التقليدية أن يقع الضبط على الأشياء المادية فقط بوصفها أدلّة ماديّة للجريمة التي يجري التفتيش بشأنها، لكن في مجال الجرائم الإلكترونية فإنّ الطبيعية

[1]– بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ص 100.

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 224–225.

العلمية المعقدة للدليل الإلكتروني الذي يوجب التفتيش عنه وضبطه لإثبات هذا النوع من الجرائم تجعله يختلف عن الدليل التقليدي. فالبيئة الافتراضية لا تنتج سلاحا ناريّا أو سكينا وإنّما تنتج نبضات رقمية تشكل قيمة وجوهر الدليل الإلكتروني.

الأمر الذي يتطلب تعريف الضبط في الجرائم الإلكترونية، وتحديد نطاقه بالإضافة إلى قواعد إحراز وتأمين المضبوطات الإلكترونية.

أولا / تعريف الضبط في الجرائم الإلكترونية و نطاقه:

يقصد بالضبط وضع اليد على شيء مرتبط بجريمة تمتّ ويفيد في كشف الحقيقة عنها وعن مرتكبيها، وهو من حيث طبيعته القانونية قد يكون من إجراءات الاستدلال أو التحقيق. فإذا كان الشيء في حيازة شخص واقتضى الأمر تجريده من حيازته وقت ضبطه[1] كان الضبط بمثابة إجراء تحقيق، أما إذا كان نزع الشيء قد تم دون الاعتداء على حيازة قائمة، فيكون الضبط بمثابة إجراء استدلال[2].

ويعرّف الضبط في البيئة المعلوماتية: "وضع اليد على الدعائم المادية المخزّنة فيها البيانات الإلكترونية أو المعلومات التي تتصل جريمة إلكترونية وقعت، وتفيد في كشف الحقيقة عنها وعن مرتكبها"[3].

أما عن نطاق الضبط في الجرائم الالكترونية، فالضبط لطبيعته وبحسب تنظيمه القانوني وغايته، فهو لا يرد إلاّ على الأشياء، أمّا الأشخاص فلا يصلحون أن يكونوا محلاّ للضبط بالمعنى الدقيق، وإذا كان قانون الإجراءات يتحدث في بعض النصوص عن ضبط الأشخاص وإحضارهم، فإنّه يعني القبض عليهم وإحضارهم، والقبض نظام قانوني يختلف تماما عن ضبط الأشياء[4].

---

[1]–إنّ الضبط يتميز بأنّه قيد على حيازة الفرد أو ملكيته لمال معيّن لمصلحة التحقيق فذاتيته ناشئة من تصادم حتى التحقيق مع الحيازة أو الملكية، أمّا التفتيش فإنّه يتميّز بأنّه يقيّد حقا غير مالي وهو ما يطلق عليه حرمة المسكن أو حرمة الأشخاص.

أنظر: توفيق محمد الشاوي، حرمة الأسرار الخاصّة ونظرية عامّة للتفتيش، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006، ص 133.

[2]– خالد عياد الحلبي، المرجع السابق، ص 168.

[3]– محمد حمد عمر الغياثين، المرجع السابق، ص 157.

[4]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 284.

ولا يفرّق القانون في مجال الضبط بين المنقول والعقار فكلاهما يمكن ضبطه، كذلك فإنّه يستوي أن يكون الشيء المضبوط ملوكا للمتهم أو لغيره، والقاعدة أنّ الضبط لا يرد إلاّ على شيء مادي أمّا الأشياء المعنوية فلا تصلح بطبيعتها أن يكون محلاّ للضبط والشرط اللاّزم لصحته أن يكون الشيء مفيدا في كشف الحقيقة فكل ما يحقق هذه الغاية يصلح ضبطه[1].

1- ضبط الأشياء الماديّة للحاسب الآلـــــــي:

إنّ ضبط المكونات الماديّة للحاسب الآلي وملحقاته الذي يشمل على جهاز الحاسوب ومكوناته لأساسية والثانوية لا تثير أية صعوبة، لأنّ الضبط يرد على الأشياء ماديّة كالدعامة الماديّة للبرامج والأسطوانات والأشرطة[2].

وبالرغم من عدم وجود خلاف حول ضبط مكونات الحاسب الآلي الماديّة ومواجهتها إجرائيا بالنصوص التقليدية، فإنه توجد بعض التشريعات الغريبة تجير ضبط مكوّنات الحاسب الآلي المادّية، وتنقسم هذه التشريعات الإجرائية إلى اتجاهين هما:

أ. **الاتجاه الأول:** تجيز بعض التشريعات اتخاذ أي إجراء أو أي شيء لازم لجمع أدلّة الجريمة والحفاظ عليها، منها قانون الإجراءات الجنائية الكندي في المادة487 منه أو قانون الإجراءات الجنائية اليوناني في المادة 251[3]. وفي لوكسمبورج يمكن القول بصفة عامّة بأنّ الضبط يشمل كل الأشياء التي تكون مفيدة في إظهار الحقيقة، بما يتسّع ليشمل بالطبع المكونات الماديّة للحاسب الآلـــــــي[4].

ب. **الاتجاه الثاني:** تنص بعض التشريعات صراحة على تفتيش وضبط مكونات الحاسب المادية منها: قانون إساءة استعمال الحاسب الآلي في انجلترا الصادر سنة 1990 وقانون المنافسة في كندا[5].

---

[1]- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 54.

[2]- عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنّفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007، ص 373.

[3]- فتوح الشاذلي، عفيفي كامل، المرجع السابق، ص 140.

[4]- محمد حمد عمر الغياثين، المرجع السابق، ص 157.

[5]- فتوح الشاذلي، عفيفي كامل، المرجع السابق، ص 140.

2. ضبط الأشياء المعنوية (الكيانات المنطقية) للحاسب الآلـــــي:

اختلفت التشريعات الإجرائية والاتجاهات الفقهية حول مسألة ضبط الأشياء المعنوية والكيانات المنطقية والتي لا تصلح بطبيعتها لأن تكون محلا لوضع اليد وهي مجرّدة من دعامتها الماديّة المثبتة عليها وانقسمت في ذلك إلى اتجاهين:

أ. **الاتجاه الأول:** يرى أصحاب هذا الاتجاه بأنّه لا يمكن تصور إجراء الضبط على الكيانات المنطقية لانتفاء الكيان المادي عنها، وبالتالي عدم صلاحية البيانات المخزّنة آليا لأن تكون محلا للضبط بالكيفية المنصوص عليها بموجب النصوص التقليدية لانتفاء الطابع المادي عن هذه البيانات في حال تجردها من الدعامة المادية[1]. ومن التشريعات التي أخذت بهذا الاتجاه قانون الإجراءات الجنائية الألماني.

ب. **الاتجاه الثاني:** يرى أنصار هذا الاتجاه أنّه لا يوجد ما يمنع من أن ينصب الضبط في المكونات المعنوية كالمعلومات والبيانات، مستندين في ذلك إلـــى أنّ غاية التفتيش هو ضبط الأشياء التي تفيد في كشف الحقيقة، وأن هذا المفهوم يمتد ليشمل المعلومات والبيانات[2].

ومن أنصار هذا الاتجاه الفقه والتشريع في بلجيكا وكندا في المادة 7/29 من قانون الإثبات الكندي والتي تنص على أن: " تفتيش وضبط الدفاتر والسجلات الخاصّة بمؤسسة مالية، يقتصر على تفتيش المكان بغرض تفقده وأخذ نسخة من المواد المكتوبة، يستوى في ذلك أن تكون السجلات مكتوبة أم في شكل إلكتروني" .

هذا الخلاف دعا المشرع الجنائي في بعض الدول إلى تطوير النصوص التشريعية المتعلقة بمحل التفتيش والضبط ليشمل فضلا عن الأشياء المادية المحسوسة، البيانات المعالجة إلكترونيا، أو إصدار تشريعات تتعلق بالجرائم الإلكترونية تتضمن القواعد الإجرائية المناسبة لهذه الصورة من البيانات، وهو ما نصت عليه المادة 39 من قانون تحقيق الجنايات البلجيكي، المدخلة في التقنين بمقتضى القانون

[1]– سعيداني نعيم، المرجع السابق، ص 159. وأنظر أيضا: محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 291.

[2]– محمد طارق عبد الرؤوف الخن، المرجع نفسه، نفس الصفحة. وأنظر أيضا: سليمان أحمد فضل، المرجع السابق، ص 321–322.

الصادر في 2000/11/23، حيث يشمل الحجز وفقا لهذا النصّ على الأشياء المادية، وعلى البيانات المعالجة إلكترونيا[1].

ونحن بدورنا نرى بأنّ الاختلاف بين هاذين الاتجاهين هو اختلاف ظاهري، فالاتجاه الأول يشترط لضبط المعلومات أن تكون مخزّنة في وسيط إلكتروني، وهذا ما لا يشترطه الإتجاه الثاني. والواقع أنّ المعلومات لا يمكن أن تكون مجرّدة عن وسيط التخزين، سواء كان ذاكرة الحاسب الآلي، أم قرصا ممغنطا.

كما أن المكونات المعنوية تشغل حيّزا ماديّا في ذاكرة الحاسب الآلي، وعليه فإنّ هذه المكونات يمكن ضبطها ضمن وسائط التخزين، مع مراعاة الإجراءات الواجب إتباعها أثناء عملية ضبط هذه المكوّنات.

ثانيا/ قواعد تحريز وتأمين المضبوطات الإلكترونية:

إنّ الدليل الالكتروني يخضع في ضبطه إلى قواعد تحريز الأدلة الجنائية عموما، إلاّ أنّه ونظرا إلى الطبيعة الخاصّة له، فإنّ عملية ضبطه وتحريزه[2] والتأمين عليه تحتاج إلى بعض الإجراءات الخاصة لحمايته فنيّا وصيانته من إمكانية العبث به، وبالتالي المحافظة على سلامة هذه المضبوطات الإلكترونية ومن هذه الإجراءات ما يلي[3]:

---

[1]– علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المرجع السابق، ص 58.

[2]– إحراز المضبوطات الالكترونية يتم وفق طرق وأساليب تقنية تتفق مع الطبيعة الإلكترونية لهذه البيانات ومن هذه الطرق نذكر على سبيل المثال:

أ– طريق النسخ: تتم من خلال نسخ المضبوطات الالكترونية باستخدام برامج معدّة خصيصا لهذا الغرض، كبرنامج (LAPLINK). حيث يتم أخذ نسخة من تلك المضبوطات الالكترونية ومن تم يتم لصقها وخزنها بإسم معيّن على إحدى وسائل النقل (CD.DVD) الخاصّة بالجهة القائمة بالضبط وتبقى بعهدتها إلى حين انتهاء التحقيق. ويمكن الاحتفاظ بنسخة منها لدى المحضرين بالمحكمة خشية من الضياع أو التلف. أنظر: أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، دار النهضة العربية، القاهرة، 2010، ص 158.

ب– طريق التجميد: تتم من خلال تجميد التعامل بالكمبيوتر أو النظام المعلوماتي الذي تتواجد بداخله هذه المضبوطات الإلكترونية أو على الأقل تجميد القسم الصلب الذي يحمل تلك المضبوطات، وذلك من خلال برامج معدّة خصيصا لذلك الغرض، أنظر: عائشة بن قارة مصطفى، المرجع السابق، ص 116.

[3]–غازي عبد الرحمان هيان الرشيد، المرجع السابق، ص 566–567. أنظر أيضا: شرف الدين وردة، عيساني علي، المساعدة القضائية الدولية المتبادلة في مجال جمع الأدلة الرقمية، وفقا للإتفاقية العربية لمكافحة جرائم تقنية المعلومات

1. تحديد المادة الإلكترونية المراد ضبطها:

نظرا لسهولة التلاعب في بيانات الأنظمة المعلوماتية وشبكاتها، وبدون ترك أي آثار، فإنه يتعين على المحقق عند تحديد البيانات المراد ضبطها، وضع علامة مادية خاصّة عليها وينقلها إلى أقراص أو أشرطة ممغنطة، ثم يقوم المحقق ومشغل النظام بتسجيل بياناته على هذه الأشرطة، ثم يتم وضعها في علب مخصّصة لحفظها والتوقيع عليها وختمها، على أن تنظم هذه الإجراءات بمحضر، يوقع عليه حسب ما تقتضيه الأحكام القانونية الخاصّة بضبط الأشياء وحفظها.

2. **تأمين البرامج المضبوطة قبل تشغيلها** : على المحقق، في حالة ضبط البرامج الالكترونية أن يعمل على تأمين هذه البرامج فنيّا، بعمل نسخة كاملة وسليمة منها، قبل البدء بتشغيلها من قبل الخبراء وبواسطة أنظمة معلوماتية مأمونة من جانبه، وإذا تم تشغيل هذه البرامج بغير الطريقة التي صممت فيها، قد تتحول إلـــى برنامج تدمير، وبالتالي يفقد الدليل.

3. **الالتزام باتباع القواعد الفنية الخاصة بكيفية نقل الأحراز الالكترونية وحملها:**

تحتاج البيانات الالكترونية المضبوطة والمفرغة على الأقراص إلى عناية خاصة من التلف أو الضياع. لذا لابد عند نقلها مراعاة عدم تعريضها للأتربة، ولأشعة كهرومغناطيسية حتى لا يتم إتلاف محتوياتها.

4. **مراعاة ظروف الحرارة والرطوبة المناسبة لتخزين الأحراز الإلكترونية:**

عند تخزين الأقراص والأشرطة الممغنطة التي تم ضبطها يجب مراعاة ظروف التخزين من حيث درجة الحرارة والرطوبة المناسبة لحفظها.

5. **ضبط الأقراص والأشرطة الأصلية، وعدم الاقتصار على ضبط نسخها:**

و هنا لابد أن يرد الضبط على الأقراص والأشرطة الممغنطة الأصلية، مع تمكين الجهة التي تحوزها من نسخها لاستخدامها كي لا يتوقف أو يعاق استمرارها في مباشرة أنشطتها، خاصة في حالة تأخر المحاكمة.

وأضافت المادة 4/19 من الاتفاقية ما يلي: "يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أيّة إجراءات أخرى يرى أنّها ضرورية من أجل تحويل سلطاته المختصّة، سلطة إصدار الأمر لأي شخص لديه معلومات عن تشغيل النظام أو الإجراءات المطبقة من أجل حماية البيانات المعلوماتية

لسنة 2010، مداخلة للمشاركة في فعاليات الملتقى الدولي حول أدلّة الإثبات الجنائية في التشريعات المقارنة المنعقد يومي 25-26 أبريل 2018، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، ص 21-22.

التي تضمن تقديم كل المعلومات الضرورية على نحو معقول يسمح بتطبيق الإجراءات المشار إليها في الفقرتين 1 و2". وبالتالي لتسهيل عملية التفتيش يمكن استشارة مثلا مديري النظام الذين لديهم معرفة جيّدة عن النظام المعلوماتي محل البحث.

أمّا بالنسبة للتفتيش في حـــالة اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان خارج الدولة، أجازت المادة 32 من الإتفاقية إمكانية الدخول بغرض التفتيش والضبط في أجهزة موجودة خارج الحدود الإقليمية لدولة أخرى بدون إذنها في حالتين ففي **الحالة الأولى:** إذا تعلق التفتيش بمعلومات أو بيانات مباحة للجمهور، أما **الحالة الثانية** إ ذا رضي صاحب أو حائز هذه المعلومات بهذا التفتيش.

و فيما يخص ضبط البيانات المعلوماتية المخزّنة نصّت المادة 3/19 من الاتفاقية على ما يلي: "يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصّة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين الأولى و الثانية، وهذه الإجراءات تشمل السلطات التالية:

أ- ضبط أو الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه، أو إلى دعامة تخزين معلوماتية.

ب- التحقق والتحفظ على نسخة من هذه البيانات المعلوماتيّة.

ت- المحافظة على سلامة البيانات المخزّنة.

ث- منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي".

ثالثا/ المعالجة الإجرائية للتفتيش و ضبط البيانات المعلوماتية وفقا الاتفاقات الدولية و التشريعات الداخلية المقارنة:

لقد نصّت الإتفاقيات الدولية والتشريعات الداخلية المقارنة على تفتيش وضبط البيانات المعلوماتية المخزّنة و سيتم التفصيل فيها على النحو الوارد أدناه:

1- المعالجة الإجرائية للتفتيش وضبط البيانات المعلوماتية وفقا للاتفاقيات الدولية :

أ- **اتفاقية بودابست لمكافحة الجريمة الإلكترونية لعام 2001.**: نصت اتفاقية بودابست لعام 2001 على التفتيش وضبط البيانات المخزّنة على النحو التّالـــــي:

أ-1- 1بالنسبة لتفتيش البيانات المعلوماتية المخزّنة : نصّت هذه الاتفاقية صراحة على حق الدول الأعضاء في تفتيش النظم المعلوماتية وحثها على تجسيد هذا الحق بكل وضوح في قوانينها الإجرائية

وذلك من خلال نص المّادة 1/19 والتي نصّت على ما يلي: "يجب على كل طرف أن يتبنّى الإجراءات التشريعية وأيّة إجراءات أخرى يرى أنّها ضرورية من أجل تخويل سلطاته المختصة سلطة التفتيش أو الولوج بطريقة متشابهة:

- لنظام معلوماتي أو لجزء منه وكذلك للبيانات المعلوماتية المخزّنة فيه وعلى أرضه .
- لدعامة تخزين معلوماتية تسمح بتخزين بيانات معلوماتية".

أ-1-2 التفتيش في حالة اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة: نصّت المادة 2/19 من الاتفاقية على ما يلي: "يجب على كل طرف أن يتبنّى الإجراءات التشريعية وأيّة إجراءات أخرى يرى أنّها ضرورية من أجل التأكد ممّا إذا كانت سلطاته تقوم بالتفتيش أو الولوج بطريقة مشابهة لنظام معلوماتي معيّن أو جزء منه وفقا للفقرة "1" بند "أ" وأنها تملك أسبابا تدعوا للاعتقاد بأنّ البيانات التي تسعى إليها مخزنة في نظام معلوماتي آخر أو في جزء منه على أرضه، وأنّ هذه البيانات يمكن الوصول إليها بشكل قانوني سواءا من خلال النظام الأولى أو من خلال كونها مهيأة من أجله، وأنّ هذه السلطات المذكورة ستكون قادرة على التوسع العاجل لنطاق التفتيش أو الولوج بطريقة مشابهة لنظام آخر".

أ-1-3 التفتيش في حالة اتصال حاسب المتهم بحاسب آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة:

نصت عليه المادة 23 من الاتفاقية على أنه:" يجب على الأطراف أن تتعاون مع بعضها البعض، وفقا للأحكام العامة للتعاون الدولي المنصوص عليها في الاتفاقية، من أجل تطبيق الأصول الدولية المتصلة بالتعاون في المواد الجنائية، والاتفاقيات المعتمدة على التشريعات المتماثلة أو النظيرة أو القوانين المحلية، إلى أوسع نطاق ممكن، من أجل التنقيب والتحري أو الإجراءات الجنائية المتعلقة بالجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو لجمع أدلة ذات شكل إلكتروني للجريمة الجنائية."

أ-2 ضبط البيانات المعلوماتية المخزنة: نصت المادة 3/19 من الاتفاقية على أنه:" يجب على كل طرف أن يتبنى الإجراءات التشريعية التي يراها ضرورية من أجل تخويل سلطاته المختصة سلطة ضبط أو الحصول بطريقة مشابهة على البيانات المعلوماتية وفقا للفقرتين 1 و2، وهذه الإجراءات تشمل السلطات التالية:

أ-ضبط أو الوصول بطريقة مشابهة إلى نظام معلوماتي أو جزء منه، أو إلى دعامة تخزين معلوماتية.

ب-التحقق والتحفظ على نسخة من هذه البيانات المعلوماتية.

ج-المحافظة على سلامة البيانات المخزنة.

د-منع الوصول إلى هذه البيانات أو رفعها من النظام المعلوماتي.

ب- الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لسنة 2010: نصّت كذلك الإتفاقية العربية لمكافحة جرام تقنية المعلومات لسنة 2010 على إمكانية تفتيش وضبط البيانات المعلوماتية المخزّنة.

ب-1 تفتيش البيانات المعلوماتية المخزّنة : نصت المادة 26 من الاتفاقية على أنّه: "تلتزم كل دولّة بتبنّي الإجراءات الضرورية لتمكين سلطاتها المختصّة من التفتيش أو الوصول إلـــى:

- تقنية معلومات أو جزء منها والمعلومات المخزّنة فيها أو مخزّنة عليها.
- بيئة أو وسيط تخزين معلومات تقنية المعلومات والذي قد تكون معلومات التقنية مخزّنة فيه أو عليه".

ب-1-1 تفتيش في حالة إتصال حاسب المتهم بحاسب آلي آخر أو نهاية طرفية موجودة في مكان آخر داخل الدولة: نصّت المادة 2/26 على ما يلي: "تلتزم كل دولة طرف بتبنّي الإجراءات الضرورية لتمكين السلطات المختصّة من التفتيش أو الوصول إلى تقنية معلومات معيّنة أو جزء منها بما يتوافق مع الفقرة (1-أ) إذا كان هناك اعتقاد بأنّ المعلومات المطلوبة مخزّنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانونا أو متوفرّة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى".

ب-1-2 التفتيش في حالة اتصال حاسب المتهم بحاسب آلي آخر أو نهاية طرفية موجودة في مكان آخر خارج الدولة: طالما أنّ التفتيش عن بعد يمتد إلى إقليم بلد أجنبي، فلابد من ضرورة التوصل إلى اتفاق دولي يضمن التعامل الدولي فيما بين السلطات المختصّة، والقول بغير ذلك يجعل من هذا الإجراء العابر للحدود تهديدا لسيادة الدول وهذا ما نصّت عليه المادة 39 والمتعلقة بالمساعدة المتبادلة بين الدول العربية المصادقة على هذه الإتفاقية.

ب-2 ضبط البيانات (المعلومات) المخزّنة : بالرجوع إلى نص المادة المادة 27 من الاتفاقية والمتعلقة بضبط المعلومات المخزّنة نجد أنها نصت على مايلي: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصّة من ضبط وتأمين معلومات تقنية المعلومات التي

يـتّم الوصـول طـرق بتبنـي الإجـراءات الضـرورية لتمكـين السـلطات المختصّـة مـن ضـبط وتـأمين معلومات تقنية المعلومات التي يتّم الوصول إليها حسب الفقرة 1 من المادة 26 من هذه الإتفاقية و هذه الإجراءات تشمل صلاحيات

- ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين تقنية المعلومات.
- عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها.
- الحفاظ على سلامة معلومات تقنية المعلومات المخزّنة.
- إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها".

2- **المعالجـة الإجرائيـة للتفتيش وضبط البيانـات المعلوماتيـة المخزّنـة وفقا للتشريعات الداخليـة المقارنة:** نظرا لخصوصية الجريمة الالكترونية وخطورتها، فإنّ بعض التشريعات الجزائية رصدت لها إجراءات خاصّة بها في مجال التفتيش والضبط.

أ- **التشريع الفرنسي:** أخذ المشرع الفرنسي بمبدأ التقييد الزمني لإجراء التفتيش، حيث يجب أن يكون بعد الساعة السادسة صباحا وقبل التاسعة ليلا وهو ما نصّت عليه المادة 59 ق.إ.ج.ف[1].

يتم التفتيش والضبط حسب المادة 56 ق.إ.ج.ف[2] ، حيث يحرّر ضابط الشرطة القضائية محضرا بضبط الأوراق المستندات، المعطيات المعلوماتية أو أية أشياء أخرى موجودة بحوزة أشخاص يشتبه

[1]-Art 59 de C.P.P.F dispose que : sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures.

[2]- عدّلت المادة 56 بموجب المادة 41 من القانون رقم 2004/575، المؤرخ في 21 جوان 2004، المتعلق بالثقة في الاقتصاد الرقمي ومسّ التعديل الفترة الأولى حيث و بعد مصطلح المستندات يضاف مصطلح المعطيات المعلوماتية، وبعد مصطلح أوراق يضاف مصطلح المعلومات. وفي الفقرة الثانية " المستندات" تستبدل المستندات أو المعطيات المعلوماتية. أما الفقرة الخامسة تستبدل بثلاث فقرات: "يتم ضبط المعطيات المعلوماتية، اللازمة لإظهار الحقيقة عن طريق وضع تحديد العدالة إمّا دعامة التخزين لهذه المعطيات، أو نسخة أجريت في ظل وجود الأشخاص الحاضرين عملية التفتيش.

- إذا تم إجراء نسخة في إطار هذا الإجراء يمكن القيام بأمر من وكيل الجمهورية بالحذف النهائي للمعطيات المعلوماتية، من على دعائم التخزين والتي لم توضع تحت يد العدالة، إذا كانت حيازة هذه المعطيات المعلوماتية أو استخدامها غير قانوني أو خطير على أمن الأشخاص أو الممتلكات.

- ولا يجوز لضباط الشرطة القضائية إلاّ بموافقة وكيل الجمهورية أن يضبط غير الأشياء، المستندات والمعطيات المعلوماتية اللازمة إظهار الحقيقة ".

في أنهم ساهموا في ارتكاب جريمة أو يحوزون أوراقـــا أو معلومات أو أشياء لها علاقة بالأفعال الإجرامية.

يتم فورا جرد كل الأشياء والمستندات المضبوطة وتوضع أحراز مختومة، ويتم ضبط المعطيات المعلوماتية اللاّزمة لإظهار الحقيقة عن طريق وضع تحت يد العدالة إمّا دعامّة التخزين لهذه المعطيات، أو نسخة أجريت في ظل وجود الأشخاص الحاضرين عملية التفتيش.

إذ تم إجراء نسخة في إطار هذا الإجراء، يمكن القيام بأمر من وكيل الجمهورية بالحذف النهائي للمعطيات المعلوماتية، من على دعائم التخزين والتي لم توضع تحت يد العدالة، إذا كانت حيازة هذه المعطيات المعلوماتية أو استخدامها غير قانوني أو خطير على أمن الأشخاص أو الممتلكات.

ولا يجوز لضباط الشرطة القضائية إلاّ بموافقة وكيل الجمهورية أن يضبط غير الأشياء المستندات والمعطيات المعلوماتية اللاّزمة لإظهار الحقيقة.

كما قام المشرّع بإدخال تعديل على قانون الإجراءات الجزائية بإضافته للمادة 1/57[1] ، إليه وذلك بموجب المادة 1/17 من القانون رقم 239/2003 حيث أجاز لضباط الشرطة القضائية أو تحت مسؤوليتهم، أعوان الشرطة القضائية خلال عملية تفتيش قائمة وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية، الدخول من خلال منظومة معلوماتية موجودة بالمبنى الذي يجرى به التفتيش إلى معطيات تفيد التحقيق الجاري والمخزّنة في هذه المنظومة أو في منظومة معلوماتية أخرى بما أنّ هذه المعطيات يتم الدخول إليها أو تكون متاحة من المنظومة الأولى.

إذ تبين مسبقا بأنّ هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى أو متاحة للمنظومة الأولى، مخزّنة في منظومة معلوماتية أخرى تقع خارج الإقليم الوطني، يمكن لضباط الشرطة القضائية جمعها وفقا لشروط الدخول المنصوص عليها في الاتفاقيات الدولية النّافذة[2].

يمكن نسخ المعطيات التي تم الحصول عليها ضمن القواعد المقررة في هذه المادة في أي دعامة تخزين إلكترونية، تكون قابلة للحجز والوضع في أحراز مختومة وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

[1]-Art 57/1 alinéa 1 de C.P.P.F dispose que : «les officiers de police judiciaire ou, sous leur responsabilité, les agents de police judiciaire peuvent, ou cours d'une perquisition effectuée dans les conditions prévues par le présent code, accéder par un système informatique implanté sur les lieux ou se déroule la perquisition a des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, des lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial …. » Crée par loi N° 2003-239 pour la sécurité intérieure 2003-03-18 art, 171 JORF du 18 mars 2003.

[2]- Vu , art 57/1 alinéa 2 de C.P.P.F.

كما نصّت المادة 57 من ق.إ.ج.ف علـــى أن يجرى التفتيش بحضور الشخص صاحب المسكن، فإذا تعذر عليه الحضور فيجرى التفتيش يعينه، وإذا تعذر ذلك فبحضور شاهدين مختارين من قبل ضابط الشرطة القضائية من غير الموظفين الخاضعين لسلطته الإدارية.

وفي حالة تفتيش أماكن يشغلها أشخاص ملزمون قانونا بكتمان السّر المهني، يجب أن تتخذ مقدما جميع التدابير اللّازمة لضمان احترام ذلك السّر ويتمثل في التدابير المتخذة عند تفتيش مكتب أو منزل المحامي وهو ما نصّت عليه المادة 1/56 من ق.إ.ج.ف[1]، كذلك هو الحال بالنسبة لمكتب طبيب أو موثق أو وكيل دعوى أو محضر قضائي وهو ما نصّت عليه المادة 3/56 ق.إ.ج.ف.

أ-1 تفتيش وضبط البيانات المعلوماتية في مرحلة التحقيق الابتدائي: في هذا الصدد نصّت المادة 76 ق.إ.ج.ف علـــى" أنّـه لا يجـوز تفتـيش المسـاكن ومعاينتهـا وضـبط الأشـياء المثبتـة للتهمـة أو مصادرة الممتلكات المنصوص عليها في المادة 131-21 ق.ع.ف إلاّ برضا صريح من الشخص الذي ستتخذ ضده هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة فيذكر ذلك في المحضر مع الإشارة إلى رضاه." إلاّ أنّه يمكن الخروج عن هذه القاعدة إذا اقتضت ضرورات التحقيق في جناية أو جنحة معاقب عليها بالسجن لمدّة تساوي أو تفوق خمس(5) سنوات أو إذا برّره البحث عن الممتلكات المصادرة وفقا للمادة 131-21 من ق.ع.ف[2]، و يكون ذلك وفقا للشروط المنصوص عليها في المادة 4/76 ق.إ.ج.ف.

---

[1]-ART 56/1 de C.P.P.F. dispose que : (L n° 2005-1549 du 12 Déc 2005, art 37) « les perquisitions dans le cabinet d'un avocat ou son domicile ne peuvent être effectuées que par un magistrat et en présence de bâtonnier ou de son délégué, à la suite d'une décision écrite et motivées prise par ce magistrat, qui indique la nature de l'infraction ou des infraction sur lesquelles portent les investigations, les raisons justifiant la perquisition et l'objet de celle-ci, le contenue de cette décision et porte dès le début de la perquisition à la connaissance du bâtonnier ou de son délégué par le magistrat celui-ci et le bâtonnier ou son délègue ont seuls le droit de consulter ou de prendre connaissance des documents (L.N° 2010-1 du 4 jan 2010) ou des objet se trouvent sur les lieux préalablement à leurs éventuelle saisie. Aucune saisie ne peut concerner des documents (L.n°2010-1 du 4 janv2010) ou des objets relatifs à d'autre infractions que celles mentionnées dans la décision précitée. Les dispositions du présent alinéa sont édictées a peine de nullité ».

[2]-Art 131-21 du C.P.F dispose que : «L.N° 2007-797 du mars 2007, art 66) la peine complémentaire de confiscation et encourue dans les cas prévus par la loi ou le règlement, elle est également encourue de plein droit pour les crimes et pour les délits punis d'une peine d'emprisonnement d'une durées supérieure a un an, à l'exception des délits de presse. »

« la confiscation porte sur tous les biens meubles ou immeubles, quelle qu'en soit la nature divis ou indivis, ayant servira a commettre l'infraction ou qui étaient destinés à la commettre, et d'ont le condamné est propriétaire ou, sous réserve des droits de propriétaire de bonne foi, dont il a libre disposition »

« Elle porte également sur tous les biens qui sont l'objet ou le produit direct ou indirect de l'infraction à l'exception des biens susceptible de restitution à la victime. Si le produit de l'infraction à été mêlé a des fonds d'origine licite pour l'acquisition d'un ou plusieurs biens, la confiscation peut ne porter sur ces biens qu'a concurrence de la valeur estimée de ce produit».

أ-2 التفتيش وضبط البيانات المعلوماتية عند فتح تحقيق قضائي: قام المشرع بتعديل نصوص التفتيش بالقانون رقم 45 المؤرخ في 21 جوان 2004 المتعلق بالثقة في الاقتصاد الرقمي، حيث قام بإضافة عبارة "المعطيات المعلوماتية" بعد عبارة أشياء في المادة 94 من ق.إ.ج.ف، و ذلك بموجب المادة 42 لتصبح المادة على النحو التالي: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة، أو لمصادرة الممتلكات المنصوص عليها في المادة 131-21 ق.ع.ف.

وإذا حصل التفتيش في مسكن المتهم، فعلى قاضي التحقيق أن يلتزم بأحكام المواد 57 و59 وهذا ما نصّت عليه المادة 95 من ق.إ.ج.ف.

أمّا إذا حصل التفتيش في مسكن غير لمتهم استدعي صاحب المنزل الذي يجرى تفتيشه ليكون حاضرا وقت التفتيش، فإذا كان غائبا أو رفض الحضور، أجري التفتيش بحضور اثنين من أقاربه أو أصاهره الحاضرين بمكان التفتيش، فإذا لم يوجد أحد منهم فبحضور شاهدين، وعلى قاضي التحقيق أن يلتزم بأحكام المواد 2/57 و59. وعلى قاضي التحقيق أن يتخذ جميع الإجراءات اللاّزمة لضمان إحترام كتمان سر المهنة وحقوق الدفاع.

تطبق أحكام المواد 56 و1/56 5/56 على التفتيش الذي يجريه قاضي التحقيق وهو ما نصّت عليه المادة 96 ق.إ.ج.ف.

كما نصّت المادة 97 ق.إ.ج.ف[1] على أنّه إذا اقتضى الأمر أثناء إجراء التحقيق وجوب البحث عن مستندات أو معطيات معلوماتية فإنّ لقاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها.

« La confiscation peut en outre porter sur tout bien meuble ou immeuble défini par la loi ou le règlement qui réprime l'infraction ».

« S'il s'agit d'un crime ou d'un délit puni d'au moins cinq ans d'emprisonnement et ayant procuré un profit direct ou indirect, la confiscation porte également sur les biens meubles ou immeuble, quelle qu'en soit la nature, divis, appartenant au condamné lorsque celui-ci mis en mesure de s'expliquer sur les bien dont la confiscation est envisagée, n'a pu en justifier l'origine.

« L'lorsque la loi qui réprime le crime ou le délit le prévoit, la confiscation peut aussi porter sur tout ou partie des biens appartenant au condamné quelle qu'en soit la nature meubles ou immeubles, divis ou indivis…….de son aliénation ».

[1]-عدّلت المادة 97 بموجب المادة 43 من قانون رقم 2004-575، المؤرخ في 21 جوان 2004، المتعلق بالثقة في الاقتصاد الوطني، متاح على الموقع الإلكتروني: https:// wipolex.wipo.int

حيث نصّت المادة 43 على أن تعدل المادة 97 ق.إ.ج.ف كما يلي:

يجب جرد وحتم كل الأشياء المستندات أو المعطيات المعلوماتية الموضوعة تحت يد العدالة، ويتم ضبط المعطيات المعلوماتية اللاّزمة لإظهار الحقيقة عن طريق وضع تحت يد العدالة إمّا دعامّة التخزين لهذه المعطيات أو نسخة أجريت لها بحضور الأشخاص الحاضرين".

ب- التشريع الإماراتـــــــي:

لو نتفحص القوانين الخاصة بمكافحة جرائم تقنية المعلومات[1] وقانون الإجراءات الجزائية الخاص بدولة الإمارات العربية المتخذّة نجد بأنها لم تنصّ على تفتيش وضبط الحاسب الآلي بمكوناته المادية والمعنوية، وكذلك هو الحال بالنسبة للتفتيش في حالة إتصال حاسب المتهم بحاسب آلي آخر ونهاية طرفية موجودة في مكان آخر داخل أو خارج الدولة ما يطلق عليه التفتيش عن بعد بالرغم من أنها تعتبر من الدول الموقعة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010.

ج - التشريع الأردنـــــــي:

تنص المادة 13 الفقرة "أ" من قانون الجرائم الالكترونية لسنة 2015[2] على تفتيش المكونات المادية والمعنوية للحاسب الآلي بقولها: "مع مراعاة الشروط والأحكام المقررّة في التشريعات النافذة ومراعاة حقوق المشتكي عليه الشخصية يجوز لموظفي الضابطة العدلية بعد الحصول على إذن من المدعي العام المختص أو من المحكمة المختصة، الدخول إلى أي مكان تشير الدلائل إلى استخدامه لارتكاب أي من الجرائم المنصوص عليها في هذا القانون، كما يجوز لهم تفتيش الأجهزة والأدوات والبرامج و

- الفقرة الأولى: بعد مصطلح "مستندات" تضاف عبارة "أو المعطيات المعلوماتية".
- الفقرة الثانية: تستبدل عبارة "الأشياء والمستندات بعبارة الأشياء المستندات أو المعطيات المعلوماتية".

[1]- صدرت في دولة الإمارات العربية المتحدة عدّة قوانين نظمت موضوعات التجارة والمعاملات الإلكترونية منها:

أ- مرسوم بقانون إتحادي رقم 3 لسنة 2003 بشأن تنظيم قطاع الاتصالات، الجريدة الرسمية العدد 411 السنة الرابعة والثلاثون بتاريخ 2004/03/14.

ب- القانون الاتحادي رقم 1 لسنة 2006 المتعلق بالمعاملات والتجارة الإلكترونية، الجريدة الرسمية العدد 422 السنة السادسة و الثلاثون بتاريخ 2006/01/31.

ت- قانون اتحادي رقم 2 لسنة 2006 مكافحة جرائم تقنية المعلومات.

ث- مشروع قانون اتحادي لسنة 2009 بشأن المعلومات الائتمانية في دورته السابعة.

ج- مرسوم بقانون إتحادي رقم 5 لسنة 2012 المتعلق مكافحة جرائم تقنية المعلومات. أنظر: عبد الرحيم بن بوعيدة ، ضياء علي أحمد نعمان ، موسوعة التشريعات الإلكترونية المدنية و الجنائية – التشريع المغربي و العربي و الفرنسي الاتفاقيات العربية و الأوروبية و الدولية، الجزء الأول، الطبعة الأولى، المطبعة و الوراقة الوطنية، مراكش ، 2010،ص 235-306.

[2]- مشار إليها في قانون الجرائم الإلكترونية الأردني لسنة 2015، الجريدة الرسمية العدد 5631، ص 5635.

أنظمة التشغيل والشبكة المعلوماتية والوسائل التي تشير الدلائل في استخدامها لإرتكاب أي من تلك الجرائم وفي جميع الأحوال على الموظف الذي قام بالتفتيش أن ينظم محضرا بذلك ويقدمّه إلى المدعي العام المختص".

كما تنص المادة 13 الفقرة "ب" من قانون الجرائم الالكترونية لسنة 2015[1] ،على ضبط المكونات المادية والمعنوية للحاسب الآلي بقولها: "مع مراعاة الفقرة "أ" من هذه المادة ومراعاة حقوق الآخرين ذوي النيّة الحسنة وباستثناء المرخص لهم وفق أحكام قانون الاتصالات ممّن لم يشتركوا بأي جريمة منصوص عليها في هذا القانون، يجوز لموظفي الضابطة العدلية ضبط الأجهزة والأدوات والبرامج وأنظمة التشغيل والشبكة المعلوماتية والوسائل المستخدمة لإرتكاب أي من الجرائم المنصوص عليها أو يشملها هذا القانون والأموال المتحصلّة منها و التحفظ على المعلومات والبيانات المتعلّقة بإرتكاب أي منها".

د- التشريع اليمني:

فيما يخص تفتيش مكونات الحاسب الآلي الماديّة أخضعها المشرّع اليمني للقواعد التقليدية في المواد من 131-144[2].ق.إ.ج.ي، أمّا فيما يخص تفتيش مكونات الحاسب الآلي المعنوية، فلم يتناول القانون اليمني هذه المسألة. كذلك هو الحال بالنسبة لتفتيش شبكات الحاسوب إذ تعّد إحدى المشكلات التي تعيق إجراء التحقيق حيث أنّ نصوص التفتيش تهدف إلى البحث عن الأدلة الماديّة التي تفيد في كشف الحقيقة، والتّي تستند إلى عناصر ماديّة إضافة إلى أنّ تطبيق النصوص السابقة يقتصر على الأجهزة المتواجدة داخل لاخارجها.

هـ- التشريع الجزائري:

عند تعديل المشرّع الجزائري لقانون الإجراءات الجزائية بالقانون رقم 22/06 المؤرخ في 20 ديسمبر 2006[3]، استحدث أحكام خاصّة بالتفتيش لتتلاءم مع الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات نظرا لخصوصية هذه الجرائم، كذلك هو الأمر حين أصدر القانون رقم 04/09 المتعلق

[1] – مشار إليها في قانون الجرائم الإلكترونية الأردني لسنة 2015، ص 5635.

[2]– قرار جمهوري بالقانون رقم 13 لسنة 1994 بشأن الإجراءات الجزائية ،المؤرخ بتاريخ 8 جمادى الأول 1415 الموافق لـ 12 أكتوبر 1994 ،الجريدة الرسمية العدد 19/4 .

[3]– القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية.

بالقواعد لخاصّة للوقاية من الجرائم المتصلّة بتكنولوجيا الإعلام والإتصال، لهذا سنتطرق للمعالجة الإجرائية للتفتيش وضبط الحاسب الآلي في التشريع الجزائري وفقا للقوانين على النحو التالـــــــي:

هـ.أ-المعالجة الإجرائية للتفتيش والضبط في الجرام الماسة بأنظمة المعالجة الآلية للمعطيات وفقا لقانون الإجراءات الجزائية:

إذا كان أمر التفتيش من الإجراءات الأمنية الضرورية للكشف عن الحقيقة والقبض على المجرم والحد من نشاطه لتحقيق الأمن والإستقرار إلأ أنه لا يتم إلا في أحوال يجيزها القانون، وهذا حفاظا لمقتضيات المصلحة العامة وحماية لحقوق الإنسان لهذا سنتناول هذه المعالجة بالدراسة في حالتين والتي يمكن بمناسبتهما إجراء التفتيش في حد ذاته همـــا:

التفتيش و الضبط في حالة الجناية أو الجنحة المتلبس بها والتفتيش والضبط في حالة التحقيق الابتدائي والقضائي.

هـ-1-أ التفتيش وضبط الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالة التلبس بالجريمة:

تقتضي عملية التفتيش وضبط الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في حالة التلبس بالجريمة توفر مايلي:

- **الحصول على إذن مسبق من قبل السلطة القضائية المختصّة:**

بالرجوع إلى المواد 44 وما بعدها من ق.إ.ج.ج يلاحظ أن الإذن بالتفتيش أمر لازم في جميع الأحوال سواء في حالة التلبس أو في غير أحوال التلبس والسلطة المختصة بإصداره هي النيابة العامة ممثلة في الشخص وكيل الجمهورية وقضاة التحقيق ممثلا في شخص قاضي التحقيق.

و في هذا الصدد نصّت المادة 44 ق.إ.ج.ج على ما يلي: "لا يجوز لضباط الشرطة القضائية الإنتقال إلى مساكن الأشخاص الذين لم يظهر أنهم ساهموا في الجناية، أو أنهم يحوزون أوراقا أو أشياء لها علاقة بالأفعال الجنائية المرتكبة لإجراء تفتيش إلاّ بإذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق مع وجوب الاستظهار بهذا الأمر قبل الدخول إلى المنزل أو الشروع في التفتيش.

و يكون الأمر كذلك في حالة التحري في الجنحة المتلبس بها أو التحقيق في إحدى الجرائم المذكورة في المادتين 37 و40 من هذا القانون.

" يجب أن يتضمن الإذن المذكورة أعلاه بيان وصف الجرم موضوع البحث عن الدليل وعنوان الأماكن التي سيتم زيارتها وتفتيشها وإجراء الحجز فيها، وذلك تحت طائلة البطلان.

تنجز هذه العمليات تحت الإشراف المباشر للقاضي الذي أذن بها والذي يمكنه عند الاقتضاء أن ينتقل إلى عين المكان للسهر على احترام أحكام القانون.

إذا أكشفت أثناء هذه العمليات جرائم أخرى غير تلك التي ورد ذكرها في إذن القاضي فإنّ ذلك لا يكون سببا لبطلان الإجراء العارضة".

وبالرجوع لنفس المادة نجد أن المشرع تطلب لتفتيش منزل المتهم الحصول على إذن قضائي، وبذلك يكون قد خالف المشرّع الفرنسي الذي غالبا ما يتفق معه في نصوصه القانونية، حيث نصّ المشرّع الفرنسي على جواز التفتيش في حالة التلبس بدون الحاجة إلى إذن طبقا لنص المادة 1/56 ق.إ.ج.ف[1].

- حضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:

طبقا لنص المادة 45 ق.إ.ج.ج تتم عمليات التفتيش على النحو التالـــي:

1- إذا وقع التفتيش في مسكن شخص يشتبه في أنّه ساهم في إرتكاب الجناية فإنّه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضباط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين لسلطته.

2- إذا جرى التفتيش في مسكن شخص آخر يشتبه بأنّه يحوز أوراقا أو أشياء لها علاقة بالأعمال الإجرامية، فإنّه يتعيّن حضوره وقت إجراء التفتيش، وإن تعذر ذلك اتبع الإجراء المنصوص عليه في الفقرة السابقة.

ولضباط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم في الفقرة الأولى أعلاه الحق في الإطلاع على الأوراق أو المستندات قبل حجزها.

من خلال المادة يتضح بأنّ المشرع الجزائري أوجب ضرورة حصول إجراء التفتيش المتعلق بالمساكن وملحقاته بحضور المتهم عندما يتم تفتيش مسكنه من قبل الضبطية القضائية.

[1] -Art 56/1 du C.P.P.F dispose que : « si la nature de crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents, (L.n° : 2004-575 du 21 juin 2004, Art.41) « données informatique » ou outre objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces (L.n° : 2004-575 du 21 juin 2004 ,Art , 41). « information ou objet relatifs aux faits incriminés, l'officier de police judicaire se transporte sans désemparer au domicile de ces derniers pour y t procéder à une perquisition dont il dresse procès-verbal. »

كما نصت المادة 47 مكرر ق.إ.ج.ج على ما يلي: "إذ حدث أثناء التحري في الجريمة متلبس بها أو التحقيق متعلق بإحدى الجرائم المذكورة في المادة 47 الفقرة 3 من هذا القانون أن كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر[1] أو محبوسا في مكان آخر، وأنّ الحال يقتضي عدم نقله إلى ذلك المكان بسبب مخاطر جسيمة قد تمس بالنظام العام، أو لاحتمال فراره، أو اختفاء الأدّلة خلال المدّة اللازمة لنقله، يمكن أن يجرى التفتيش بعد الموافقة المسبقة من وكيل الجمهورية أو قاضي التحقيق وبحضور شاهدين مسخرين طبقا لأحكام المادة 45 من هذا القانون أو بحضور ممثل يعيّنه صاحب المسكن محل التفتيش".

غير أنّه وبموجب التعديل الذي ألحقه المشرّع على قانون الإجراءات الجزائية بموجب القانون 22/06 استثنى تطبيق هذا الشرط وبعدم حضور المتهم أو الشاهدين عندما يتعلق الأمر ببعض الجرائم ومنها الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات[2].

و هو ما يعّد إقرار المشرّع بخطورة هذا النوع من الجرائم، وخوفا من قيام المتهم بالجريمة من طمس معالمها ومحو آثارها.

- **ميعاد التفتيش والضبط في الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات:**

أباح المشرّع الجزائري إجراء تفتيش المساكن من الساعة الخامسة صباحا إلى الساعة الثامنة مساءا كقاعدة عامة، وهو ما نصّت عليه المادة 47 /2،1 من قانون إ.ج.ج غير أنه وضع استثناء على ذلك، وهو جواز دخول المنازل وتفتيشها في أي وقت من اليوم ليلا ونهارا دون أن يتقيد القائم بالتفتيش بالمعاد الزمني له .

وبالرجوع إلى الاستثناء الوارد في المادة 3/47 ق.إ.ج.ج والذي يتعلق بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف، فإنّ إجراء التفتيش فيها يصبح في أي

---

[1]– التوقيف للنظر: هو إجراء بوليسي، يأمر به ضابط الشرطة القضائية، يتمثل في وضع شخص يريد التحفظ عليه في مركز الشرطة أو الدرك الوطني لمدّة معيّنة قانونا، وذلك من أجل الوصول إلـــــى الحقيقة، ويعد التوقيف للنظر من المسائل الدستورية، حيث أعتبر الدستور الجزائري التوقيف للنظر في مجال التحريات الجزائية، يخضع للرقابة القضائية ولا يمكن أن يتجاوز 48 ساعة، ولا تمدّد هذه المدّة إلا استثناء،و وفقا للشروط المحددة في القانون.

[2]– نصت المادة 45 فقرة أخيرة ق.إ.ج.ج والمعدلة بالأمر 22/06 على أنّه: "لا تطبق هذه الأحكام إذ تعلق الأمر بجرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال و الإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف ...".

ساعة من ساعات النهار أو الليل سواء تعلّق الأمر بمحل سكني أو غير سكني، وذلك بناءا على إذن مسبق من وكيل الجمهورية المختص، كما يجوز لقاضي التحقيق كذلك أن يقوم بأيّة عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك وهو ما نصّت عليه المادة 4/47 ق.إ.ج.ج.

و المشرع الجزائري عندما استثنى الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من ميعاد التفتيش، يكون قد أدرك ميزة هذه الجرائم، من حيث قابليته الدليل الإلكتروني فيها للمحو والتدمير في أقل من ثانية.

هـ-1-ب التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في مرحلة التحقيق الإبتدائي (التحقيق الأولي في غير حالة التلبس): تخول المادة 64 من ق.إ.ج.ج لضباط الشرطة القضائي حق دخول المساكن في حالة البحث التمهيدي الذين يقومون به في غير حالة التلبس، حيث تنص هذه المادة على أنّه: "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلاّ برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ويجب أن يكون هذا الرضا مكتوبا بخط اليد صاحب الشأن، فإن كان لا يعرف الكتابة فإمكانه الاستعانة بشخص يختاره بنفسه ويذكر ذلك في المحضر مع الإشارة إلى رضاه.

و تطبق فضلا عن ذلك أحكام المواد من 44 إلى 47 من هذا القانون.

غير أنّه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المنصوص عليها في المادة 3/47 من هذا القانون، تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر."

فهذه المادة اشترطت وجود الرضا وأن يكون صريحا ومكتوبا صادرا من الشخص الذي سيتخذ إجراء التفتيش ضده وهذا يتعارض مع التفتيش كإجراء من إجراءات التحقيق الذي يتم جبرا دون مراعاة لرضا الشخص صاحب المسكن، وبالتالي عدم تطبيق الضمانات الواردة بهذه المادة بخصوص التفتيش المتعلق بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

هـ-1-ت التفتيش والضبط في الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات في مرحلة التحقيق القضائي:

نصّت المادة 79 ق.إ.ج.ج على أنّه: "يجوز لقاضي التحقيق الإنتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته ويستعين قاضي التحقيق ويحررّ محضرا بما يقوم به من إجراءات".

يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة وهو ما نصّت عليه المادة 81 ق.إ.ج.ج.

- **الميعاد القانوني للتفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات:**

عندما يتعلق الأمر بجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لقاضي التحقيق دخول المساكن وتفتيشها في أي وقت خارج الميعاد القانوني المنصوص عليه في المادة 1/47 من ق.إ.ج.ج، وهو ما يستشف أيضا من استقراء أحكام المادة 82 ق.إ.ج.ج وله أن يأمر ضباط الشرطة القضائية المختصين القيام بذلك طبقا لنص المادة 4/47 ق.إ.ج.ج.

- **حضور صاحب المسكن أثناء عملية التفتيش والضبط في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات :**

بالرجوع إلى نصّ المادة 82 و83[1] ق.إ.ج.ج والمتعلقة بحضور أشخاص معيّنين عملية التفتيش، والتي تحيلان إلى المادة 45 ق.إ.ج.ج (تنص على حضور المتهم أو ممثله أو شاهدين) والمادة 47 ق.إ.ج.ج (تنص على تحديد وقت التفتيش بين الخامسة والثامنة مساء كقاعدة عامّة لها استثناءاتها) يجوز لقاضي التحقيق القيام بالتفتيش في الجرائم المنصوص عليها في المادة 3/47 ق.إ.ج.ج منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، دون حضور هؤلاء الأشخاص.

هـ.ب ضبط الأدلة:

إن الهدف من التفتيش هو ضبط الدليل، وفي هذا الصدد تتم عملية الحجز وفقا للقواعد المقررة في نص المادة 84 ق.إ.ج.ج كاحترام إجراءات التحقيق وخاصة سر المهنة وحقوق الدفاع بما يكفل أمن وسيرة وسلامة المعطيات في المنظومة المعلوماتية، حيث نصّت المادة 84 ق.إ.ج.ج على ما يلي:

---

[1]– تنص المادة 82 ق.إ.ج.ج على ما يلي: إذا حصل التفتيش في مسكن المتهم فعلى قاضي التحقيق أن يلتزم بأحكام المواد من 45 إلى 47. غير أنه يجوز له وحده في المواد الجنايات أن يقوم بتفتيش مسكن المتهم في غير الساعات المحددة في المادة 47 على أن يباشر التفتيش بنفسه وأن يكون ذلك بحضور وكيل الجمهورية".

أمّا المادة 83 ق.إ.ج.ج فتنص على ما يلي: "إذا حصل التفتيش في مسكن غير مسكن المتهم، استدعي صاحب المسكن الذي يجرى تفتيشه ليكون حاضرا وقت التفتيش. فإذا كان غائبا أو رفض الحضور أجري التفتيش بحضور إثنين من أقاربه أو أصهاره الحاضرين بمكان التفتيش فإن لم يوجد أحد منهم فبحضور شاهدين لا تكون ثمة بينهم وبين سلطات القضاء تبعيّة.

وعلى قاضي التحقيق أن يلتزم بمقتضيات المادتين 45، 47 ولكن عليه أن يتخذ مقدما جميع الإجراءات اللاّزمة لضمان احترام سرّ المهنة وحقوق الدفاع".

"إذا اقتضى الأمر أثناء إجراء تحقيق وجوب البحث عن مستندات فإن قاضي التحقيق أو ضابط الشرطة القضائية المنوب عنه وحدهما الحق في الإطلاع عليها قبل ضبطها، ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في إحراز مختومة.

ولا يجوز فتح هذه الأحراز والوثائق إلاّ بحضور المتهم مصحوبا بمحاميه أو بعد استدعائهما قانونا كما يستدعى أيضا كل من ضبطت لديه هذه الأشياء لحضور الإجراء ولا يجوز لقاضي التحقيق أن يضبط غير الأشياء والوثائق النافعة في إظهار الحقيقة أو التي قد يضرّ إفشاؤها بسير التحقيق ويجوز لمن يعنيهم الأمر الحصول على نفقتهم، وفي أقصر وقت على نسخة أو صورة فوتوغرافية لهذه الوثائق التي بقيت مضبوطة إذا لم تَحُلْ دون ذلك مقتضيات التحقيق".

هـ.2 المعالجة الإجرائية للتفتيش وحجز المعطيات المعلوماتية وفقا للقانون رقم 04/09:

ينص المشرع الجزائري على القواعد الإجرائية لتفتيش المنظومات المعلوماتية وحجز المعطيات المعلوماتية في الفصل الثالث من القانون 04/09 كما يلي:

هـ-2-أ تفتيش المنظومة المعلوماتية:

اشترط المشرع الجزائري لإجراء عملية التفتيش في المعطيات المخزنة في المنظومة المعلوماتية إعمال قاعدة الحضور، حيث نصّت المادة 5 من قانون 04/09 على ما يلي: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، الدخول بغرض التفتيش ولو عن بعد إلـــــى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزّنة فيها.

ب- منظومة تخزين معلوماتية

في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعوا للاعتقاد بأنّ المعطيات المبحوث عنها مخزّنة في منظومة معلوماتية أخرى أنّ هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصّة مسبقا بذلك.

إذا تبين مسبقا بأن المعطيات المبحوث عنها والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزّنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإنّ الحصول عليها يكون بمساعدة السلطات الأجنبية المختصّة طبقا للاتفاقيات الدولية ذات الصّلة ووفقا لمبدأ المعاملة بالمثل.

يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها". وهذه المادّة تتعلّق بشروط صحة تفتيش المنظومة المعلوماتية.

ولهذا حاول المشرع غلق منافذ إفلات المجرم في هذا النوع من الجرائم التي تتسم بالتعقيد والتطور الدائم في استخدام تقنية الحوسبة والاتصال/ مما أجاز معه للسطات المكلفة بالتفتيش تسخير كل شخص مختص في مجال عمل المنظومة المعلوماتية قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهامها.

هـ-2-ب حجز المعطيات المعلوماتية :

نصّ عليه المشرّع الجزائري في المواد 6، 7و8 من قانون 04/09 كما يلـــي:

" عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزّنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنّه ليس من الضروري حجز كل المنظومة، يتم نسخ كل المعطيات محل البحث وكذا المعطيات اللاّزمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز والوضع في أحراز وفقا لقواعد المقررّة في قانون الإجراءات الجزائية. "

ويجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجرى بها العملية.

غير أنّه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستعمال لأغراض التحقيق، شرط ألاّ يؤدي ذلك إلى المساس بمحتوى المعطيات (المادة 06 من قانون 04/09).

وبهذا يكون المشرع قد أجاز فسخ وإفراغ المعطيات على دعامة تخزين إلكترونية تكون قابلة للحجز مثل الأقراص المرنة والأقراص المضغوطة والذاكرة الومضية.

أمّا إذا إستحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 6، لأسباب تقنية يتعيّن على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة (المادة 7 من قانون 04/09).

ويمكن للسلطة التي تباشر التفتيش أن تأمر بإتخاذ الإجراءات اللازمة لمنع الإطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك (المادة 8 قانون 04/09).

المطلب الثاني: المعاينة والخبرة في الجرائم الالكترونية

تعتبر المعاينة من أهم أساليب التحقيق، نظرا لما يمكن أن توفره من أدلة إثبات الجريمة، وتزداد أهميتها في الجرائم الإلكترونية، وذلك راجع إلى الطبيعة الخاصّة للسلوك الإجرامي فيها بالإضافة إلى اعتبارها من الجرائم المستحدثة، ممّا استوجب ابتكار أساليب خاصّة بالمعاينة و الخبرة كأسلوب لإستجلاء الحقيقة في هذا المجال.

لذلك سنتعرض في إلى مفهوم المعاينة في الجرائم الإلكترونية(الفرع الأول) ، ومفهوم الخبرة في الجرائم الإلكترونية (الفرع الثاني).

الفرع الاول: المعاينة في الجرائم الالكترونية

تعتبر المعاينة من بين الإجراءات التي تباشرها سلطات التحقيق والتي تؤدي للوصول إلى الدليل المستمد من الواقعة الإجرامية، عن طريق البحث والتعقيب عن الحقيقة من حيث ثبوت التهمة ونسبتها إلى المتهم من عدمه، وباعتبار أنّ المعاينة لها أهمية قصوى فسوف نتناولها من عدّة جوانب كالتالي: تعريف وأهمية المعاينة في الجريمة الالكترونية، وشروط صحّة معاينة مسرح الجريمة الالكترونية.

أولا / تعريف المعاينة وأهميتها في الجريمة الالكترونية :

يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقة عن جريمة وعن مرتكبها، وبالتّالي يجب على السلطات المختصة الانتقال إلى أماكن وقوع الجريمة فور ارتكابها، حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير أو إزالة الآثار المادّية للجريمة التي تساعد في التنقيب عن الحقيقة[1].

[1]– عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية، بحث مقدم إلى المؤتمر الإقليمي حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة 26-2008/04/27، مقر جامعة الدول العربية، ص 16 مشار إليه على الموقع الإلكتروني:

http://www.arabic.center.com/public/event/paper/paper/2-4 تاريخ الزيارة: 2018/10/26، الساعة 19:00.

كما تعرف أيضا بأنّها: "إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التي تفيد في كشف الحقيقة"[1].

ويقصد بالمعاينة في القانون الجنائي بأنّها إثبات مباشر ومادي لحالة الشيء أو الشخص معيّن ويكون ذلك من خلال الرؤية أو الفحص المباشر للشيء بواسطة باقي الإجراءات[2].

ممّا يعني من خلال التعاريف السابقة، أنّ جوهر المعاينة هو ملاحظة وفحص حسّي مباشر لمكان أو شخص أو شيء له علاقة بالجريمة وإثبات حالته والكشف والتحفظ على كل ما يفيد في كشف الحقيقة.

أمّا المعاينة في الجريمة الالكترونية فيقصد بها معاينة الآثار التي يتركها مستخدم الشبكة المعلوماتية أو الأنترنيت، وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية[3].

وتحتل المعاينة مكان الصدارة في الجرائم التقليدية على ما عدها من إجراءات البحث الأخرى بحكم مركزها المحوري ولدورها في تصورّه وقوع الجريمة وظروف وملابسات ارتكابها وتوفير الأدلّة المادّية من المادّة التي تجمع عن طرقها وتمحيص وتقييم الأدلة الأخرى والتنسيق بينهما في ضوء المعلومات التي تتوافر، بما يكفل في ذات الوقت التخطيط السليم لعمليات البحث والتحقيق الجنائي وتطورها، غير أنّ دورها في مجال كشف غموض الجرائم الإلكترونية، وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها، إلى نفس الدرجة من الأهمية، ويمكن رد ذلك إلى أنّ هناك على الدوام تقريبا مسرحا للجريمة التقليدية جرت عليه الأحداث، وتركت آثارها المادّية التي تنبثق منه الأدلّة، والمعاينة في مسرح الجريمة تتيح المجال أمام الباحث والمحقق الجنائي للكشف عن طريق المعاينة الآثار المادية التي خلّفها ارتكاب الجريمة، والتحفظ على الأشياء التي تفيد في التحقيق الجاري بشأنها.

---

[1]– سليمان أحمد فضل، المرجع السابق، ص 286.

[2]– حازم محمد حنفي، المرجع السابق، ص 54.

[3]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 153.

بينما لا يوجد عادة مسرح مماثل للجريمة الالكترونية المرتكبة، وأقرب تشبيهها لمسرحها، قد يكون في الموقع أو المكتب الذي توجد فيه المعدّات والأنظمة الالكترونية، التي كانت محلاّ للجريمة أو أداتها[1].

ويقلل مثل هذا المسرح إلى حد كبير من فرص إفصاحه عن الحقائق المراد التوصل إليها من وراء معاينته لسببين رئيسيين هما: أنّ الجرائم التي تقع بواسطة الأنظمة الالكترونية قلّما ينجم عن إرتكابها آثار مادّية، كما أنّ عددا كبيرا من الأشخاص يكون قد تردّد على مسرح الجريمة الفترة الزمنية الطويلة نسبيا، التي قد تنقضي عادة بين ارتكاب الجريمة واكتشافها، ممّا يفسح المجال لحدوث تغيير أو تلف أو عبث بالآثار المادية أو زوال بعضها وهو ما يثير الشك حول الدليل المستمد من المعاينة[2].

و في كل الأحوال عند تلقي بلاغ عن وقوع إحدى الجرائم الالكترونية وبعد التأكد من البيانات الضرورية في البلاغ يتم الانتقال إلى مسرح الجريمة لمعاينته، غير أنّ هذا الانتقال لا يكون إلى العالم المادي وإنّما إلى القضاء الالكتروني.

ويتم معاينة الجريمة الالكترونية بالانتقال إلى هذا العالم الافتراضي إمّا من قبل قاضي التحقيق أو ضابط الشرطة القضائية كالتالي[3]:

- من مكتبه بالمحكمة من خلال جهاز الحاسوب الخاص به.
- اللجوء إلى مقهى الأنترنيت Internet Café
- اللجوء إلى مكان عمل مزوّد خدمة الأنترنيت.

كما يجوز له الانتقال من خلال مقرّ مكتب الخبير التقني المختص إذا سمح له القانون بذبك، وهذا ما نجده في مصر من خلال إدارة مكافحة الجرائم الإلكترونية التابعة لوزارة الداخلية.

ومن هنا يستوجب على سلطة التحقيق الانتقال إلى العالم الافتراضي بالسرعة الكافية من أجل منع زوال ومحو آثار الجريمة[4].

---

[1]– حازم محمد حنفي، المرجع السابق، ص 57–58.

[2]– عبد الله حسين علي محمود، سرقة المعلومات المخزّنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2001، ص 365–366.

[3]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، مرجع سابق، ص 156–157.

[4]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع نفسه، ص 158–164.

ثانيا : شروط صحّة معاينة الجريمة الإلكترونية

حتى تحقق المعاينة الهدف المرجو منها في كشف غموض الجريمة والتوصل إلى الفاعل لابدّ من مراعاة عدّة شروط أهمها[1] :

أ. **سرعة الانتقال إلى مكان وقوع الجريمة الالكترونية:** على السلطة المختصة بالتحقيق الانتقال فور وصول خبر وقوع الجريمة إلى علمها إلى مكان الواقعة، ضمانا لعدم تغيير شكل مسرح الجريمة عن الوضع والحالة التي تركه الجاني عليها و الحصول على شهود للواقعة [2].

ب. **السيطرة والتحكم على مكان وقوع الجريمة الإلكترونية** : عند وصول سلطة التحقيق لمكان الحادث لمعاينته، و السيطرة عليه لابد من إتباع ما يلـــي:

- منع أي شخص من مبارحة مكان الواقعة حتى تنتهي الضبطية القضائية من تحرياتها.
- منع تواجد أي شخص داخل مسرح الجريمة حتى لا يؤدي إلى تغيير الآثار والأدلة المستمدة من الواقعة سواءا بقصد أو بخطأ.
- حماية كل ماله علاقة بالحادث من وسائل وأشياء و أشخاص.
- قيام الخبراء كل حسب اختصاصه برفع الآثار بمسرح الجريمة، و أول خبير يقوم بعمله هو خبير التصوير.

ت. **التسلسل في المعاينة:** لضمان إجراء المعاينة بصورة مرتبة ومتسلسلة يجب على السلطة المختصّة بالتحقيق مراعاة نقطتين أساسيتين الأولى تحديد نقاط البدء في المعاينة. أما الثانية عدم الانتقال من مكان لآخر إلاّ بعد التأكد تماما من معاينته وعدم ترك أيّة أشياء به.

ث. **الدقة والعناية الفائقة في معاينة مسرح الجرائم الإلكترونية:** وذلك بوصف المنطقة التي ارتكبت فيها الجريمة، وإذا كانت هذه الأخيرة داخل مبنى فيجب معاينة كل منافذ الدخول والخروج، وكذا وصف المحتويات بما هو مرتبط بالجريمة، كأجهزة الكمبيوتر والماسح الضوئي، الطابعة، والأسطوانات المدمجة، وغيرها من الوسائل المستخدمة في اقتراف الجريمة الالكترونية.

---

[1] – نظرا لما تقتضيه السرعة في معاينة مسرح الجريمة الافتراضية، أجاز القانون الأمريكي 2703 UCODE 18، لعضو النيابة العامة CTC من إمكانية إرسال رسالة إلى مزوّد خدمة الأنترنيت يلزمه فيها بالتحفظ على السجلات المطلوبة، إلى حين صدور أمر من المحكمة باتخاذ هذا الإجراء أو غيره.

[2]– سرحان حسن المعيني، المرجع السابق، ص 42.

ج. **التحفظ على مسرح الجرائم الإلكترونية [1] بعد المعاينة:** والعلّة في ذلك واضحة وهي إمكانية العودة إليه كلّما أراد المحقق كشف غموض أو التأكد من آثار معينّة.

ح. **تدوين المعاينة:** ويكون ذلك كتابيا ورسميا وتصويريا كتصوير أجهزة الحاسب الآلي المضبطة بمجل ارتكاب الجريمة والأجهزة الطرفية المتصلّة بها، مع التركيز بصفة خاصّة على الأجهزة الخلفية للحاسب الآلي وملحقاته، مع مراعاة تسجيل تاريخ و وقت ومكان التقاط كل صورة.

ثالثا: نطاق إعمال المعاينة في الجرائم الالكترونية

يعتمد المحقق لإجراء المعاينة في الجرائم الالكترونية بحثا عن الأدلة الالكترونية، على فحص مكونات الحاسب الآلي الخاصة بالجاني والمجني عليه وكذا أنظمة الاتصال بالأنترنيت.

1- المعاينة الواقعة على مكونات الحاسب الآلـــــــــي:

تعتبر الحواسيب مصدرا غنيّا بالأدلة الإلكترونية خاصة الحواسيب الشخصية التّي تعد بمثابة أرشيف لسلوك الفرد ونشاطاتهم ورغباتهم، لذلك فإنّ عملية فحص هذه الحواسيب تمثّل نقطة البداية في الكشف عن خطايا الجريمة الإلكترونية باعتبار هذه الأجهزة وسيلة تنفيذها أو محل وقوعها[2].

و فيما يخصّ المعاينة الواقعة في الجرائم الإلكترونية، يجب التمييز بين حالتين أساسيتين:

الحالة الأولى هي المعاينة الواقعة على المكونات المادّية للحاسب الآلي، أما الحالة الثانية فتخص المعاينة الواقعة على المكونات المعنوية أو المنطقية للحاسب الآلي.

أ. **معاينة المكونات المادية للحاسب الآلي:** كمعاينة أشرطة الحاسب، مفاتيح التشغيل، والأقراص وشاشة العرض و غيرها. فلا توجد أيّة صعوبة مادية لتقرير صلاحية مسرح الجريمة الذي يضم هذه المكونات لمعاينتها من طرف ضابط الشرطة القضائية، وكذا وضع الأختام في الأماكن التي

[1]- يراد بمسرح الجريمة الرقعة المكانية التي حدثت فوقها الواقعة الإجرامية بكافة جزيئاتها ومراحلها وخاصّة الإجرامي، بمعنى أن يحدد كل تغيير قد طرأ على الكيان المادّي الذي يعلوا سطح المكان الذي شهد حدوث الجريمة فوقه. كما يقصد بمسرح الجريمة أيضا: مجموعة الأماكن التي تشهد مراحل تنفيذ الجريمة وتحتوي على الآثار المختلفة من ارتكابها، أو المكان الذي تنبثق منه معظم الأدلة. أنظر: عبد الفتاح عبد اللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2011، ص 20-21.

[2]- جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه، تخصص قانون كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018، ص 59.

تمت معاينتها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها مع إخطار وكيل الجمهورية ذلك[1].

ب.معاينة المكونات المعنوية أو المنطقية للحاسب الآلي: يفترض في القائمين بهذه المعاينة الإلمام الجيد بأجهزة الحاسب الآلي وبرامجه نظرا لأن التفتيش يتم داخل جهاز الحاسب نفسه وما يحويه من برامج وبالتالي ضبط كل ما يفيد في كشف الحقيقة[2]. غير أنّ الجرائم الواقعة على برامج الحاسب الآلي وبياناته، تثير عدّة صعوبات تحول دون فاعلية المعاينة أو فائدتها.

ذلك لأنّ برامج الحاسب الآلي مثلا غالبا ما يشوبها عيب أو قصور ولو جزئي في أداء وظيفتها، وهذا من شأنه أن يؤثر في الحاسب فيجعله محل شك تهتز معه قيمة الدليل.

2- معاينة أنظمة الاتصال بشبكة الأنترنيت :

أحيانا لا يكفي معاينة مكونات الحاسب الآلي وحدها لاستخلاص الدليل الالكتروني إنّما يتطلب من المحقق أيضا فحص أنظمة اتصال الحاسب بشبكة الأنترنيت، ويقصد بها من الناحية الإجرائية: تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة الاتصال بالأنترنيت. وعملية معاينة هذه الأنظمة يشمل بالأساس فحص مسار الأنترنيت، والنظام الأمني، وكذا فحص الخادم[3].

ويتم التفتيش في شبكة الأنترنيت عن طريق بيانات المتهم على الشبكة، فمن خلال الحاسب يمكن الولوج إلى البريد الإلكتروني الخاص بالمتهم وفحص رسائل التهديد التي قام بإرسالها للضحيّة مثلا، أو معرفة حسابه على مواقع التواصل الاجتماعي وكلمة المرور الخاصة به. ومن خلال حسابه يمكن التعرف أيضا على ما قام به من نشر أفكار متطرفة أو إشاعات كاذبة أخلت بالسلم والأمن الاجتماعي[4].

ونظرا لخطورة المعاينة ونتائجها التي تترتب عليها الكثير في التحقيقات، وإمكانية إجرائها عبر شبكة الأنترنيت، والولوج إلى الحاسب المراد معاينته عن طريق بعض البرامج المختلفة لذلك يجب مراعاة عدّة نقاط قبل معاينة الجرائم الالكترونية:

- الإعداد الجيّد قبل المعاينة لعدم تسرب الأدلة أو إتلافها.

---

[1]- فتوح شادلي وعفيفي كامل عفيفي، المرجع السابق، ص 356.

[2]- حازم محمد حنفي، المرجع السابق، ص 56.

[3]- جمال براهيمي، المرجع السابق، ص 64.

[4]- حازم محمد حنفي، المرجع السابق، ص 56.

- اصطحاب الخبراء المتخصصين لمرافقة فريق التحقيقات.
- لابدّ من وجود مجموعة من البرامج المختلفة معهم قبل المعانية، خاصّة تلم المتعلقة باستعادة الملفات المحذوفة (RECOVRY) وبرامج كسر كلمة المرور (PASSWORD BREAK) وبرامج فحص الهواتف المحمولة مثل (MOBILE EDIT) (OXYGENE).
- يجب أن تكون المعلومات المتوافرة عن الموقع المراد معاينته كافية وتشمل كافة الجوانب من مساحة وخطورة ومعوقات وصول ومعوقات فحص ومعاينة.
- يجب اصطحاب وسيلة توليد كهرباء بديلة وآمنة (UPS) حتّى لا ينقطع التيار الكهربائي أثناء الفحص وهو ما يهدّد بإتلاف مكوّنات أجهزة الحاسب الآلي وبالتالي تلف الدليل.

كما أنّ هناك بعض الإجراءات لابد من اتخاذها عند القيام بالمعاينة مثل[1]:

- تصوير الجهاز وملحقاته ووضعه في المكان الذي يوجد فيه.
- فحص سلة المهملات لمعرفة الملفات التي تم حذفها مؤخرّا، بالإضافة إلى استخدام برامج إعادة الملفات المحذوفة نهائيا.
- التحفظ على المستندات الخاصّة بالإدخال وكذلك ملحقات الحاسب الآلي المادّية والورقية والمرتبطة بالجريمة وما قد يوجد عليها من آثار.
- الحرص على عدم إتلاف أي بيانات يتم استخراجها من الجهاز، وكذلك التأكد من وجود نسخة منها محفوظة على الحاسب نفسه.
- الفحص بدقة لكل ملفات الجهاز وخاصة ملفات LOG FILE للتعرف على جميع العمليات التي قام بها مستخدم الجهاز والمواقع التي ارتادها على الشبكة العالمية (الأنترنيت) وكذلك أسماء حساباته في مواقع التواصل الاجتماعي وكلمات المرور الخاصة به.

رابعا: المعالجة الإجرائية للمعاينة في الجريمة الإلكترونية وفقا للاتفاقيات الدولية والتشريعات الداخلية المقارنة:

1- المعالجة الإجرائية للمعاينة في الجريمة الإلكترونية وفقا للاتفاقيات الدولية:

[1]- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 172-174. أنظر أيضا: أحمد يوسف الطحطاوي، المرجع السابق، ص 134-135. وأنظر أيضا: هشام محمد فريد رستم، المرجع السابق، ص 60-61. وأنظر أيضا: حازم محمد حنفي، المرجع السابق، ص 57. وأنظر أيضا سليمان أحمد فضل، المرجع السابق، ص 290-291.

بالنسبة للاتفاقيات الدولية لم تتطرق لإتفاقية بودابست لسنة 2001، ولا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 لهذا الإجراء، على النحو التالي:

2- المعالجة الإجرائية للمعاينة في الجريمة الإلكترونية وفقا للتشريعات الداخلية المقارنة :

فيما يخص التشريعات المقارنة أخضعت إجراء المعاينة الالكترونية للأحكام العامةّ لمعاينة الجرائم التقليدية كالتالي:

أ- التشريع الفرنسي:

نصّ المشرع الفرنسي على إجراء المعاينة في المواد من 92 إلـــــــى غاية 5/99 ق.إ.ج.ف وفي هذا الخصوص نصّت المادة 92 ق.إ.ج.ف على أنّه: " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء المعاينات اللاّزمة أو للقيام بتفتيشها ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته ويستعين قاضي التحقيق دائما بكاتب تحقيق ويحررّ محضرا بما يقوم به من إجراءات"[1].

كما يجوز لقاضي التحقيق إذا استلزمت ضرورات التحقيق، الانتقال صحبة كاتبه بعد إخطار وكيل الجمهورية بمحكمته إلى كامل التراب الوطني للقيام بجميع إجراءات التحقيق على أن يخطر بذلك مقدما وكيل الجمهورية بالمحكمة التي سينتقل إلى دائرتها وينوّه في محضره عن الأسباب التي دعت إلى انتقاله وهو ما نصّت عليه المادة 93 ق.إ.ج.ف[2].

وفي فرنسا يمكن إجراء المعاينة عن طريق المحضر أو الخبير بناءا على طلب المعني المادة 145 قانون المرافعات المدنية الفرنسي بعد موافقة القاضي المختص بناءا على طلب على عريضة، خاصة إذا كانت المعاينة تجرى في مكان خاص حتى ولو كان مفتوحا للجمهور مثل قهوة أنترنيت، ولا يجوز للخبير أن يجري إلا المعاينات المادية فقط. فلا يستطيع أن يرتب عليها نتائج أو يقدم تفسيرا لما يراه

[1]-Art 92 du C.P.P.F dispose que : « le juge d'instruction peut se transporter sur les lieux pour y effectuer toutes constatations utiles ou procédé a des perquisitions, il en donne avis au procureur de la république ; qui a la faculté d'accompagner.
Le juge d'instruction est toujours assisté d'un greffier.
Il dresse d'un procès verbale de ces opérations.

[2]-Art 93 du C.P.P.F (L n° 75-701 du Aout 1975) si la nécessité de l'information l'exigent, le juge d'instruction peut, après en avoir donner avis au procureure de la république son tribunal ,se transporter avec son greffier dans tout l'étendue du territoire national, a l'effet d'y procédé a tous actes d'instruction à charge par lui d'aviser, au préalable le procureur de la république du tribunal dans le ressort du quel il se transporte, il mentionne sur son procès verbale les motifs de son transport.

و لا يقدم رأيا فيها، ولكنه يمكن أن يرفق صورا شمسية فيها. أمّا المعاينات الفنّية التي لا يستطيع القيام بها إلاّ الخبير التقني فهي التي يمكن للخبير أن يقدم فيها رأيه وتفسيره ونتائجه لما يراه [1].

كما حرص المشرّع الفرنسي على حماية مسرح الجريمة من أي تغيير قبل القيام بالإجراءات الأولية لتحقيق الجنائي وهو ما نصت عليه المادة 55 ق.إ.ج.ف[2].

و إن كانت أحكام هذه المادة تنصرف إلى أغلب الجرائم التقليدية، إلاّ أنّه يمكن تطبيقها عند معاينة مكونات الحاسب الآلي المادية. وفي حالة ما إذا كان الفاعل يهدف إلى عرقلة بالوصول إلى الحقيقة، فإنّه يخضع لأحكام المادة 434-4 ق.ع.ف[3]. والتي تعاقب بالحبس لمدّة 3 سنوات وبالغرامة تصل إلى45.000 أورو.

ب-**التشريع الإماراتي :**

في هذا الصدد يجب التمييز بين حالتين:

- حالة المعاينة في الجريمة المتلبس بها ، حيث نصّت المادة 42 ق.إ.ج.إ [4] :" يجب على مأمور الضبط القضائي في حالة التلبس بالجريمة الإنتقال فورا لمحل الواقعة لمعاينة الآثار المادية للجريمة و يحافظ عليها ،و يثبت حاله الأماكن و الأشخاص و كل ما يفيد في كشف الحقيقة. "
- حالة المعاينة في الجرائم الغير متلبس بها نصت المادة 71 من ق.إ.ج.إ على:" أن ينتقل عضو النيابة العامة إلى مكان ليثبت حالة الأشخاص و الأماكن و الأشياء المتصلّة بالجريمة

[1]- جميل عبد الباقي الصغير، المرجع السابق، ص 28.

[2]- Art 55 du C.P.P.F dispose que : « dans les lieux ou un crime a été commis, il est interdit de sous peine de l'amende prévue pour les contraventions de la 4eme classes, à toute personne son habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélèvements quelconques ».

[3]- Art 434-4 du C.P.F dispose que : est puni de trois ans d'emprisonnement de 45000€ d'amende le fait en vue de faire obstacle à la manifestation de la vérité :

1° « de modifier l'état des lieux d'un crime ou d'un délit soit par l'apport, le déplacement ou la suppression d'objets quelconques ;

2° « de détruire, soustraire, receler ou altérer un document public ou privé ou un objet de nature a faciliter la découverte d'un crime ou d'un délit, la recherches des preuves ou la condamnation des coupable.

Lorsque les faits prévus au présent article sont commis par une personne qui, par ses fonctions est appelé à concourir à la manifestation de la vérité, la peine a porté à cinq ans d'emprisonnement et à 75000€ d'amende.»

[4]- قانون رقم 35 لسنة 1992، والمتعلق بإصدار قانون الإجراءات الجزائية، الجريدة الرسمية لدولة الإمارات العربية المتحدة، العدد 233مكرر، السنة 22، بتاريخ 1992/01/26.

و كل ما يلزم إثبات حالته.وإذا استدعى الحال اتخاذ إجراء في جهة تقع خارج دائرة اختصاصه فيمكنه ندب عضو النيابة العامة المختصة للقيام بتنفيذه."

ت-**التشريع الأردنـــــــي:**

في هذا الصدد يجب التمييز بين حالتين:

- المعاينة في الجرم المشبوه: نصّت المادة 1/29 من قانون أصول المحاكمات الجزائية على أنّه: "إذا وقع جرم مشهود يستوجب عقوبة جنائية، يجب على المدعي العام الانتقال حالا إلى موقع الجريمة." ويقوم بتحضير محضرا بالحادثة وكيفية وقوعها ومكانها ويدوّن أقوال من شاهدها ومن كانت لديه معلومات عنها أو معلومات تفيد التحقيق، ويصادق أصحاب الإفادات المستمعة على إفادتهم وإذا امتنعوا عن التوقيع يصرح بذلك في المحضر.طبقا لنص المادة 30 من قانون أصول المحاكمات الجزائية، و يجوز للمدعي العام منع أي شخص موجود في البيت أو في المكان الذي وقعت فيه الجريمة من الخروج منه أو الابتعاد عنه حتى يتم تحرير المحضر طبقا لنصّ المادة 1/31 من قانون أصول المحاكمات الجزائية الأردني، وهذا في حالة الجريمة المشهودة.
- معاينة جريمة غير مشهودة: نصّت المادة 43 من نفس القانون على أنّه: "إذا اطلع المدعي العام في الأحوال الخارجة عما هو مبيّن في المادتين 29 و42 بوقوع جناية أو جنحة موجود في منطقته عن طريق الإخبار أو بصورة أخرى أو علم بأن الشخص مرتكب الجناية أو الجنحة موجود في منطقته ، فيتولى إجراء التحقيقات والتوجه بنفسه إلى مكان الحادث إذا لزم الأمر لينظم فيه المحاضر اللاّزمة طبقا لإجراءات التحقيق المنصوص عليها في هذا القانون."

ث-التشريـــــــع المصري:

نظم المشرّع المصري بدوره الانتقال للمعاينة في مرحلة جمع الاستدلالات حيث يجب على مأموري الضبط القضائي أن يقبلوا الشكاوى والتبليغات التي ترد إليهم بشأن الجرائم، وأن يبعثوا بها فورا إلى النّيابة العامّة ويجب عليهم وعلى مرؤوسهم أن يحصلوا على جميع الإيضاحات ويجروا معاينات اللاّزمة لتسهيل تحقيق الوقائع التي تبلغ إليهم، أو التي يعلنون بها بأيّة كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللاّزمة للمحافظة على أدلّة الجريمة. ويجب أن تثبت جميع الإجراءات التي يقوم بها مأمور الضبط القضائي في محاضر موقع عليها منهم يبيّن بها وقت إتخاذ الإجراءات ومكان حصوله ويجب أن تشمل تلك المحاضر زيادة على ما تقدم توقيع الشهود والخبراء ومكان حصوله ويجب أن تشمل تلك المحاضر زيادة على ما تقدم توقيع الشهود والخبراء الذين سمعوا، وترسل

المحاضر إلى النّيابة العامّة مع الأوراق والأشياء المضبوطة. وهذا ما نصت عليه المادة 24 ق.إ.ج.م.

أمّا في حالة التلبسّ بالجريمة، نصّت المادة 1/31 ق.إ.ج.م على ما يلي: "يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة أن ينتقل فورا إلى محل الواقعة ويعيّن الآثار المادّية للجريمة ويحافظ عليها ويثبت حالة الأشخاص وكل ما يفيد كشف الحقيقة ويسمع أقوال من كان حاضرا أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبها. ويجب عليه وفقا للمادة 2/31 أن يخطر النّيابة العامّة فورا بانتقاله ويجب على النّيابة العامّة بمجرّد إخطارها بجناية متلبس بها الانتقال فورا إلى محل الواقعة.

كما نصّت المادة 32 من نفس القانون على أنّ "لمأمور الضبط القضائي عند انتقاله في حالة التلبس بالجرائم أن يمنع الحاضرين من مبارحة محل الواقعة أو الابتعاد عنها حتى يتم تحرير المحضر وله أن يستحضر في الحال من يمكن الحصول منه على إيضاحات بشأن الواقعة".

أمّا في حالة فتح تحقيق قضائي، نصّت المادة 90 من نفس القانون على ما يلي: "ينتقل قاضي التحقيق إلى أي مكان كلّما رأى ذلك ليثبت حالة الأمكنة والأشياء و الأشخاص و وجود الجريمة مادياّ و كل ما يلزم إثبات حالته"

ج- التشريع الجزائري:

يجب التمييز في هذا الصدد بين ثلاثة حالات:

- **الإنتقال للمعاينة في الجرائم المتلبس بها:** نصّت المادة 1/42 من قانون .إ.ج.ج و التي تنص على مايلـــــي: "يجب على ضابط الشرطة القضائية الذي بُلّغ بجناية في حالة التلبس أن يخطر و كيل الجمهورية على الفور ثم ينتقل بدون تمهل إلى مكان الجناية و يتخذ جميع التحريات اللازمة" "وعليه أن يسهر على المحافظة على الآثار التي يخشى أن تختفي"

و حرصا من المشرع الجزائري على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، جعل المادة 43 من قانون.إ .ج.ج تحظر على كل شخص لا صفة له موجود في مكان ارتكاب جناية، أن يقوم بإجراء أي تعديل أو تغير على حالة الأماكن التي وقعت فيها الجريمة،أو انتزاع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي،و فرض عقوبة في نفس المادة تتمثل في غرامة من 200 إلى 1.000 دج،غير أنه أستثني من هذا الحظر حالة ما إذا كانت هذه التغيرات أو نزع الأشياء من أجل السلامة و الصحة العمومية أو تستلزمها معالجة المجني عليهم. أما إذا كان

الفاعل يهدف من وراء طمس الآثار أو نزع الأشياء عرقلة سير العدالة يعاقب بالحبس من ثلاثة أشهر إلـــــــى ثلاثة سنوات و بغرامة من 1000 إلـــــى 10.000 دج.

- **الانتقال للمعاينة في حالة التحقيق الابتدائي:** يقوم ضابط الشرطة القضائية، وتحت رقابتهم أعوان الشرطة القضائية بالتحقيقات الابتدائية بمجرد أن يعلموا بوقوع الجريمة إما بناءا على تعليمات و كيل الجمهورية و إما من تلقاء أنفسهم (المادة 63 من ق.إ.ج.ج)

أما في حالة تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة فيها، لابد من مراعاة شرطين أساسين نصّت عليهما المادة 64 ق.إ.ج.ج كما يلي:

الشرط الأول: رضا صريح من الشخص الذي تتخذ لديه هذه الإجراءات.

الشرط الثاني:أن يكون هذا الرضى بتصريح مكتوب بخط يد صاحب الشأن، فإن كان لا يعرف الكتابة، يمكنه الاستعانة بشخص يختاره بنفسه. ويذكر ذلك في المحضر مع الإشارة صراحة لرضاه.

أمّا إذا تعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 3/37 ق.إ.ج.ج، فتطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر.

الانتقال للمعاينة في حالة تحقيق قضائي: يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، كما يستعين قاضي التحقيق كالعادة بكاتب التحقيق يحرّر محضرا بما يقوم به من إجراءات وهو ما نصّت عليه المادة 79 ق.إ.ج.ج.

الفرع الثاني: الخبرة في الجرائم الالكترونية

منذ ظهور الجرائم الإلكترونية ،تستعين سلطات التحقيق بأصحاب الخبرة الفنية المتميزة في مجال الحاسب الآلي، و ذلك بغرض كشف غموض الجريمة، أو تجميع أدلتها و التحفظ عليها، أو مساعدة المحقق في إستخلاص جوانب الغموض في العمليات الإلكترونية الدقيقة ذات الصلة بالجريمة محل التحقيق ،و يلاحظ أن نجاح الإستدلالات و أعمال التحقيق في هذه الجرائم يكون مرتهنا بكفاءة و تخصص هؤلاء الخبراء.

لذلك كان لزوما التعرض في هذا الفرع إلـــــى مفهوم الخبرة في الجرائم الإلكترونية ، ثم آلية عمل الخبير الإلكتروني، ثم أسلوب الجمع بين الخبرة الفنية و الكفاءة المهنية، و القيود التي ترد على عمل الخبير في الجرائم الإلكترونية، وأخيرا المعالجة الإجرائية لهذا الإجراء.

أولا: مفهوم الخبرة في الجرائم الإلكترونية

تعد الخبرة أهم الوسائل التي يلجأ إليها القاضي أو المحقق لاستجلاء حقيقة الجريمة المرتكبة وإسنادها إلى المتهم أو تحديد شخص الفاعل سواءا كانت هذه الجريمة ذات طابع تقني معلوماتي ترتكب في الوسط الإلكتروني، أم كانت جريمة تقليدية.

فإستعانة المحقق أو القاضي بالخبير في مجال الجرائم الإلكترونية، يكاد يكون ضرورة لا يمكن الاستغناء عنها، نظرا للطابع الفنّي الخاص بأساليب إرتكابها والطبيعة غير المادية لمحل الاعتداء[1]، وبالتالي فإنّ للخبرة أهمية في مجال كشف الجرائم الإلكترونية وضبط الأدلّة المترتبة عليها.

1- تعريف وأهمية الخبرة و الخبير الإلكتروني:

يقصد بالخبرة بصفة عامّة: "الاستشارة الفنيّة التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصّة لا تتوافر لديه[2]".

وتعرّف أيضا بأنها: " إستعانة القاضي بأشخاص مختصين في مسائل يفترض عدم إلمام القاضي بها للتغلب على الصعوبات الفنيّة أو العلمية التي تتعلق بوقائع النّزاع، وذلك بالقيام بأبحاث فنيّة وعلمية واستخلاص النتائج منها"[3].

و الخبرة وسيلة من وسائل الإثبات التي تهدف إلى كشف بعد الأدلّة أو تحديد مدلولها بالاستعانة بالمعلومات العلمية والفنية والتي لا تتوافر سواء لدى المحقق أو القاضي.

و تقدم الخبرة عونا ثمينا لجهة التحقيق والقضاء ولسائر السلطات المختصة بالدعوى الجنائية في أداء رسالتها، فبدونها يتعذر الوصول إلى الرأي السديد بشأن المسائل الفنيّة التي يكون على ضوئها كشف الجوانب الحقيقية المبنية على الأصول والحقائق العلمية.

وتقتضي الخبرة شرط التخصص والتعمق من قبل المتصف بها، فالخبير هو ذلك الشخص الضليع بعلم من العلوم عن طريق مهارة فنية عالية، سواء كان ذلك من خلال الدراسة الخاصة التي تلقاها أو

---

[1]- فايز محمد راجح غلاب، المرجع السابق، ص 362.

[2]- عائشة بن قارة مصطفى، المرجع السابق، ص 138.

[3]- مراد محمود الشنيكات، الإثبات بالمعاينة والخبرة في القانون المدني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008، ص 98. وأنظر أيضا: أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية، دار الفكر الجامعي، الإسكندرية، 2016، ص 18.

الخبرة الطويلة التي اكتسبها بمرور السنين مكنته من الالمام بالمهنة ودقائقها الجزئية التي تصعب على العامة.

والقاضي متخصص في العلوم القانونية، ولا يمكن له الإلمام بباقي العلوم لكثرة تنوعها وتعددها، فكان لزاما عليه أن يستعين بدوي الاختصاص في مختلف أنواع المعارف والعلوم لإبداء رأيهم فيها ليكون الحكم القضائي مبنيا على أساس من الوضوح فيأخذ برأي الأطباء في قضية طبيّة، والمهندسين في قضية هندسية وهكذا فضلا عن المختبرات العلمية التي يقوم عليها أخصائيون لمعرفة حقائق الأشياء المتنازع عليها، كمختبرات الطب الشرعي وما تقوم به من عمليات[1].

وإذا كانت للخبرة تلك الأهميّة في الجرائم التقليدية، فإنّ أهميتها تزداد وتصبح ضرورية بل وحتمية في إثبات الجرائم الإلكترونية، حيث تتعلق بمسائل فنيّة معقدة ومحل الجريمة فيها غير مادي، والتطور في أساليب ارتكابها سريع ومتلاحق، ولا يكشف غموضا إلاّ متخصص وعلى درجة كبيرة من التميّز في مجال تخصصه، فإجرام الذكاء والفن لا يكشفه إلاّ ذكاء وفن مماثلين وذلك من خلال الخبرة التقنية، والتي تعد أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة تكنولوجيا المعلومات و الأنترنيت، فهي تؤدي دورا لا يستهان به إتجاه نقص المعرفة القضائية الشخصية لظاهرة الأنترنيت، ويظهر ذلك جليّا في فشل جهات التحقيق في جمع الأدلّة الإلكترونية، بل أن المحقق في كثير من الأحيان يدمّر الدليل الفني كنتيجة خطأ أو إهمال في التعامل معه. ولذلك بات من الضروري الإستعانة بالخبرة في مجال الجريمة الإلكترونية[2].

أمّا فيما يخصّ الخبير الإلكتروني[3]، فيعّرف على أنّه: "الشخص الذي تعمق في دراسة عمل من الأعمال الإلكترونية وتخصص في أدائه فترة زمنية طويلة، ممّا أكسبه خبرة علمية بحيث أصبح ملمّا

---

[1]– أنيس حسيب السيد المحلاوي، المرجع السابق، ص 23.

[2]– عائشة بن قارة مصطفى، المرجع السابق، ص 139.

[3]– يطلق كذلك على خبير الجرائم الإلكترونية بالخبير الإلكتروني الرقمي إلاّ أننا نرى مصطلح الخبير الإلكتروني كاف للتعبير عن الهدف منه، ذلك أنّ الخبير الرقمي لا يستطيع العمل إلاّ من خلال الأوعية التي توجد فيها الأدلّة الرقمية وهذه الأوعية هي الأجهزة الإلكترونية، وبالتّالي فهذه التسمية تحصيل حاصل، ولا حاجة لنا بها، إذا أنّها من قبيل التزيّد في صك مصطلح ينتشر استعماله يوما بعد يوم.

بتفاصيله، ممّا جعله متفوقا على الشخص العادي، كما جعله قادرا على إعداد الرأي الإلكتروني الرقمي في الأمور المتصلة بهذا العمل"[1].

و أهم صعوبة تواجه نظم الخبرة تتمثل في تكوين الخبير المناسب الذي سيتم الإستعانة به، باعتبار أنّ الخبرة في مجال المعلوماتية لا تعتمد على الشروط التقليدية الخاصّة بتعيين الخبير، بل يتطلب الأمر شروط تتلاءم مع التطورات الطارئة في مجال تكنولوجيا المعلومات والجرائم الواقعة عليها خاصّة في المسائل الفنيّة والعلمية[2].

فيحتاج الشخص لكي يكون خبيرا قضائيا في مجال الجريمة الإلكترونية بشكل خاص، أن يتمتع بشروط خاصّة، حيث يجب أن يكون مؤهلا ومهنيا ومتحصلا على شهادات ودراسات عليا في فرع التخصص، وأن يخضع للتدريب العملي والقانوني مع استمراريته للتدريب والدراسة خلال مسيرته الوظيفية من أجل مواكبة كل جديد يطرأ على تخصصه لأداء مهمته[3]. و بالتالي على الخبير في مجال كشف الجرائم الإلكترونية أن يكون ملمّا بالجوانب الفنيّة والتقنية، ومنها ما يلـــــــي:[4]

- المعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسي والفرعي والأجهزة الطرفية الملحقة به وكلمات المرور و أكواد التشفير، وغيرها.
- طبيعة بيئة الحاسوب والشبكة من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين ووسائل الاتصالات.
- المواضيع الرقمية المحتمل تواجد فيها أدلّة الإثبات والصور أو الأشكال التي تتخذها.
- الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة.
- الكيفية التي يمكن بواسطتها نقل الأدلة إلى الأوعية دون إتلافها.
- التمكن من تحويل أدلّة الإثبات غير المرئية إلى أدلّة مقروءة والمحافظة على الأدلّة المستخرجة بصورة نسخ أو مطبوعات بشكل يمكن للقاضي أن يفهمها ويستوعبها.

---

[1]– شريف نصر أحمد، النظرية العامّة للخبرة في المواد الجنائية، رسالة دكتوراه في الحقوق، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2010، ص 240–241.

[2]– سليمان أحمد فضل، المرجع السابق، ص 342.

[3]– سليمان أحمد فضل، المرجع نفسه، ص 342.

[4]– فايز محمد راجح غلاب، المرجع السابق، ص 362.

وبالتّالي فإنّ اختيار الخبير في مجال الجرائم الإلكترونية يتحدد بنوعية الجريمة المرتكبة وأنواع الحاسبات والشبكات والبرامج المستخدمة فيها، وقد لا يوجد خبير لديه معرفة متعمّقة في كافة أنواع الحاسبات وبرمجياتها وشبكاتها، كما أنّه لا يوجد خبير قادر على التعامل مع أنواع الجرائم التي تكون هذه الوسائل الإلكترونية محلاّ لإرتكابها أو أداة لها[1].

ولقد حصر قانون الدليل الخاص بولاية كاليفورنيا في الولايات المتحدة الأمريكية الخبراء و الشهود الإلكترونيين في كل مـــن[2]:

- المبرمج الذي قام بتحرير البرنامج واختياره.
- محلل النظم الذي صممّ وحددّ برنامج الحاسب الآلي الذي أنتج الدليل.
- المشغل الذي يقوم بتشغيل البرنامج.
- مهندس الصّيانة الإلكتروني الذي يقوم على صيانة الجهاز الأصلي.
- مبرمجي صيانة النظام والمسؤولين عن سريّة عمل الحاسب الآلي المستخدم في تنفيذ برامجه.
- طاقم عمليات البيانات الذي يعّد البيانات بالصورة التي يستطيع الحاسب قراءتها.
- أمناء مكتبة الأشرطة المسؤولين عن توفير الأشرطة والأسطوانات المشتملة على البيانات المصدرية الصحيحة.
- موظفي المدخلات والمخرجات و المسؤولين عن معالجة المدخلات والمخرجات يدويا قبل وبعد أداء العمل.

2- أنواع الخبرة في المجال المعلوماتي :

الخبرة في المجال المعلوماتي قد تكون خاصة وقد تكون عن طريق المؤسسات التعليمية، وقد تتم عن طريق جهات الضبط القضائي، وهكذا يمكن للقاضي الجزائي اختيار الخبير المعلوماتي من إحدى الفئات التالية:

أ. **الجهات الخاصّة:** تعد أقوى أنواع الخبرات على الإطلاق لكونها تنطلق من مفهوم السعي إلى خلق فرص منافسة حقيقية بين المنظمات الخاصة وهي تضم الخبرة الفردية التي تعد أهم مظاهر الخبرة في مجال تكنولوجيا المعلومات، حيث أنّ المؤسسات الكبرى المتخصصة في مجال تكنولوجيا

[1]- فايز محمد راجح غلاب، المرجع السابق، ص 362-363.

[2]- شريف نصر أحمد، المرجع السابق، ص 242. وأنظر أيضا: أنيس حسيب السيد المحلاوي، المرجع السابق، ص 106-107.

المعلومات و الأنترنيت تعمل جاهدة على الإستعانة بأشخاص تثبت كفاءتهم في مجال الحاسب الآلي، حتى وإن لم يكونوا من أصحاب الدراسات الأكاديمية، فقد ثبت علميا أنّ هناك أشخاص يتمتعون بمهارات خاصّة وبموهبة في التعامل مع استعمال الحاسب و الأنترنيت دون أن يتجاوز تحصيلهم العلمي المرحلة الثانوية أو السنوات الجامعية الأولى مثل (بيل كيتس) BILL Gates، وهو أمهر مبرمجي نظم التشغيل، وذات الأمر ينطبق على الهكرة ومخترقي الأنظمة[1].

ب.المؤسسات التعلمية : لما كانت الأنترنيت تعدّ أحد منتجات العلم في حركته، فإنّه يمكن القول وبحق أنّ أقوى مظاهر الخبرة التي يمكن الاستعانة بها لمواجهة الجريمة الإلكترونية أن تكون من خلال المؤسسات التعليمية. وهذه المؤسسات تعتمد منهج علمي غير تجاري هدفها بالتأكيد تطوير العلم ليقضي على المشكلات التي تواجه البشرية.

ولقد قامت عدّة مؤسسات تعليمية بتكوين قاعدة خبرة كبيرة فيها التكون على أهبّة الاستعداد لمواجهة الجريمة الإلكترونية، ومثل ذلك دراسات الحاسب الآلي التي تتطور بشكل فائق في جامعة "ستانفورد" كذلك معهد التكنولوجيا في "ماساشوستس"، الذي قدّم للبشرية خبراء على درجة عالية من التفوق[2] .

ج. جهات الضبط القضائـــــــي:

قامت بعض الدول وعلى رأسها الولايات المتحدة الأمريكية بإعداد أجهزة متخصصّة للخبرة في الإجرام عبر الأنترنيت، فقد أسسّ فرعا تابعا لمكتب التحقيقات الفيدرالي FBI أطلق عليه "المخبر الإقليمي الشرعي للحاسوب" مقترة (سان دييجو) SAN DIEGO، والذي تم افتتاحه في نوفمبر سنة2000 لكي يكون بيت خبرة عام متعدد النواحي القضائية، غرضه مكافحة التصعيد الخطير في الجريمة الإلكترونية، من خلال التصنيف والتحليل للدليل الرقمي، وأهم ما يقوم به هذا المخبر التقاء العديد من منظمات الضبط القضائي من أجل التعاون فيما بينها[3].

ثانيا: آلية عمل الخبير الإلكتروني

يقوم الخبير الإلكتروني بفحص الأجهزة الإلكترونية المتعلقة بالجريمة سواءا كانت حواسيب شخصية أم مخدّمات لدى مزوّد خدمة الأنترنيت، وعليه يجب على الخبير الإلكتروني أن يكون قادرا على القيام بالمهام التالية:

---

[1]– سليمان أحمد فضل، المرجع السابق، ص 342.

[2]– خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، المرجع السابق، ص 298–299.

[3] طارق فوزي الفقي، المرجع السابق، ص 174.

1- حجز البيانات:

هناك مبدأ شهير في مجال المعلوماتية الشرعية، يعرف باسم "مبدأ لوكارد التبادلي" ويقصد به أنّ أي شخص يدخل إلى مسرح الجريمة، يجب أن يأخذ منه شيئا، ويترك خلفه شيئا ما. فمثلا إذا أرسل شخص رسالة إلكترونية تحمل مضمونا احتياليا إلى أحد الأشخاص، فإنّ هذه الرسالة سوف تخزّن على المخدمّات الموجودة لدى مزوّدة خدمة الأنترنيت مع التاريخ والوقت، إضافة إلى مسار الرسالة وعنوان رقم النفاذ.

لذلك يجب على الخبير الإلكتروني أن يقوم في بادئ الأمر بعملية حجز للبيانات المتعلمة بالجريمة الموجودة لدى مزوّد الخدمة إضافة إلى حجز الأجهزة التي تحتوي هذه البيانات، والتي تكون بحيازة المشتبه به أو في مسرح الجريمة[1].

2- حفظ البيانات:

يقوم الخبير الإلكتروني في هذه المرحلة بنسخ البيانات التي تم حجزها، بحيث يصبح لديه منها نسختان: الأولـــى: يتم تخزينها في الأجهزة الرقمية التي تم حجزها، بحيث تبقى محفوظة بشكل جيد، أما النسخة الثانية : عبارة عن نسخة طبق الأصل، يتم إجراء عملية الاختبار أو الفحص عليها.

3- استعادة البيانات :

يجب على الخبير الإلكتروني أن يستعيد البيانات المحذوفة، وذلك باستخدام أحد برامج استعادة البيانات، وهو أمر ضروري من أجل إعادة بناء القضية، فمثلا يمكن للخبير أن يستعيد جميع الرسائل التي قام الجاني بحذفها عن طريق تتبع الأثر الذي تتركه هذه الرسائل على جهاز التخزين[2].

4- تحليل البيانات :

فـــي هذه المرحلة، يقوم الخبير الإلكتروني بعملية تقييم محتوى البيانات الإلكترونية، بحيث يفحصها بدقّة من أجل تحديد وسائل الجريمة ودوافعها والغرض منها.

5- إعادة بناء القضية:

وهي العملية التي يقوم بها الخبير، بعد تجميع وتحليل البيانات والمعلومات التي تم الحصول عليها نتيجة البحث، من أجل توضيح ما حصل بين المجرم والضحيّة أثناء ارتكاب الجريمة، فالدليل

[1] محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 334-335.

[2] محمد طارق عبد الرؤوف الخن، المرجع نفسه، ص 335. أنظر أيضا: طارق فوزي الفقي، المرجع السابق، ص 178.

الإلكتروني الذي تم الحصول عليه يحتوي على آثار سلوكية للمجرم، مثل الكلمات التي استخدمها المجرم في تصفح الأنترنيت، والمواقع التي قام بتصفحها، فالربط بين السلوكيات يؤدي إلى معرفة وقت ومكان ارتكاب الجريمة، والطريقة التي تمت بها، وكيفية وصول الجاني إلى ضحيّته.

6- كتابة التقريـــــــر:

يتضمن تقرير الخبرة، النتائج التي توصل إليها الخبير من خلال عملية البحث ومن النتائج التي يجب أن يتضمنها التقريـــــر ما يلـــــي:

أ. مواصفات مسرح الجريمة الافتراضية.

ب. ملخص عن عملية الجريمة التي تم القيام بها.

ج. إعادة رواية أحداث القضيّة.

د. ملخص النتائج.

هـ. اقتراحات الخبير الإلكتروني.

وينصح أن يكون التقرير متسلسلا من حيث بناء الأحداث، وأن يكون مختصرا من النّاحية التقنية، ومكتوبا بأسلوب بسيط وواضح، حتّى تتمكن المحكمة من فهمه بسهولة [1].

ثالثا: أسلوب الجمع بين الخبرة الفنية والكفاءة المهنية :

نتيجة التطور التكنولوجي المستمّر، فإنّ الخبير الإلكتروني يعتبر من أهم أعوان المحقق والباحث الجنائي، هؤلاء يقدمون أعمالا تؤدي إلى مصادر الأدلّة الجنائية الإلكترونية وبالتّالي كشف الجرائم الإلكترونية، وصول إلى نتائج إيجابية.

غير أنّه يمكن أن يكون بين المتهمين والشهود في جرائم الحاسب الآلي أشخاص لم يبلغوا درجة الخبير من العلم والمعرفة وبالتالي يصعب عليهم إدراك مصطلحاته الفنيّة. وعليه ينبغي البحث عن أسلوب خاص يجمع بين الخبرة الفنيّة والكفاءة المهنية للقيام بإجراءات التحقيق مع الأشخاص ذوي العلاقة بجريمة الحاسب الآلي، ومن الممكن حيال ذلك إتباع الخطوات التاليـــــة[2]:

---

[1]- محمد طارق عبد الرؤوف الخن، المرجع السابق، ص 335-336. أنظر أيضا: طارق فوزي الفقي، المرجع السابق، ص 178.

[2]-أنيس حسيب السيد المحلاوي، المرجع السابق، ص 108. وأنظر أيضا: محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المرجع السابق، ص 348-349. وأنظر أيضا: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص 236-237.

الخطوة الأولى: تبادل المعلومات بين المحقق وخبير الحاسب الآلي وذلك قبل البدء في التحقيق وأخذ أقوال الشهود والمشتبه فيهم أو استجواب المتهميّن، بحيث يشرّح المحقق للخبير أهمية ترتيب المتهمين والشهود وطريقة توجيه الأسئلة إليهم، ومن جهة أخرى يقوم الخبير بشرح الأبعاد الفنيّة والنقاط التي ينبغي استجلائها من الأشخاص وكافة المصطلحات الحاسوبية التي يمكن استخدامها مع بيان معاينتها ليتم الاستفادة منها عند ضرورة.

الخطوة الثانية: يتم حصر النقاط المطلوب استجلائها من قبل الخبير والمحقق قبل البدء في التحقيق ليتولى المحقق بعد ذلك ترتيب النقاط.

الخطوة الثالثة: يتم أخذ أقوال الشهود واستجواب المتهمين من قبل المحقق وبحضور الخبير، الذي يجوز له توجيه الأسئلة الفرعية أثناء الاستجواب وفق الكيفية التي يتم الإتفاق عليها مسبقا قبل البدء في التحقيق.

الخطوة الرابعة: التنسيق بين المحقق والخبير في الحصول على البيانات المخزّنة في الحاسب الآلي وملحقاته الخاصّة بالشاهد أو المتهم الذي تم التحقيق معه، مع مراعاة أنّ هذا الأخير لا يجوز إجباره على تقديم دليل يدينه.

ويمكن للمحقق أو الخبير أن يتوصلا إلى تلك البيانات وأساليب فتحها من خلال التحقيق مع الأشخاص ذوي العلاقة بجرائم الحاسب الآلي أو الأنترنيت علما بأنّ أقل خطأ في مثل هذه الحالات يقضي على كافة البيانات المخزّنة في الحاسب الآلي.

رابعا: القيود التي ترد على عمل الخبير في الجرائم الإلكترونية

يرتبط عمل الخبير في مجال الجرائم الإلكترونية بالمشروعية، فليس له أن يلجأ إلى أساليب غير مشروعة من أجل المهمّة المكلف بها. ولعل ما يثور من تساؤل في هذا الشأن عن مدى الحق للخبير في الإستعانة بهكرة (المحترفين في مجال الحاسوب) و مرتكبي الجرائم الإلكترونية؟

نشير بداية إلى أنّ كبرى الشركات قد دعت من منتصف عام 1999 إلى التعاقد مع الهكرة تجنبا لاختراقاتهم، إلاّ أن مدى قبول ذلك أو عدم قبوله يظل دوما للقضاء في مدى تقبل دليل مستمد من استعانة الخبير بهكرة ومن تم فإنّه على الرغم من استعانة الخبير بمجرم معلوماتي للتعرف على أسلوب إرتكاب الجريمة الإلكترونية لا يجعل منه خبيرا في الدعوى، إذ أن الأمر في نهاية المطاف

مرجعه للخبير ثم لقاضي الموضوع وما ذلك المجرم إلاّ مساعد للخبير، وفي ذلك سابقة للكونجرس الأمريكي من استدعاء أحد كبار الهكرة للإدلاء بشهادته أمامه[1].

ولتنظيم الخبرة في الجريمة الإلكترونية وفقا للاتفاقيات الدولية، لم تنظم إتفاقية بودابست لعام 2001 ولا الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية الخبرة الإلكترونية.

أمّا بالنسبة للتشريعات، فهناك من نظم أعمال الخبرة في مجال الجرائم الإلكترونية مثل قانون البلجيكي، الصادر في 23 نوفمبر 2000. حيث نصّت المادة 88 منه على أنّه: "يجوز لقاضي التحقيق، والشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللاّزمة عن كيفية تشغيل النظام، وكيفية الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزّنة أو المحمولة أو المنقولة، على أن يتم ذلك بالطريقة التي تريدها جهة التحقيق"[2].

خامسا: المعالجة الإجرائية للخبرة في الجريمة الإلكترونية وفقا للتشريعات الداخلية المقارنة: من بين التشريعات التي أخضعت الخبرة في الجريمة الإلكترونية للأحكام العامة للخبرة التقليدية وهذا لعدم وجود نصوص خاصّة تنظمها:

1- التشريع الفرنسي :

نظم المشرع الفرنسي أحكام الخبرة التقليدية في المواد 156 إلى 169-1 من قانون الإجراءات الجزائية، حيث نصّت المادة 1/156 من قانون إ.ج.ف على أنّه: "لجهات التحقيق أو الحكم عندما تعترض لها مسألة ذات طابع فني أن تأمر بندب خبير إمّا بناءا على طلب النيابة العامّة وإمّا من تلقاء نفسها أو من الخصوم". وأضافت المادة 2/156 أنّه إذا رأى قاضي التحقيق أنّه لا موجب للإستجابة لطلب خبرة فعلية أن يصدر في ذلك أمرا مسبّبا في أجل شهر من تاريخ استلامه الطلب ويكون قراراه غير قابل للطعن. هذا ونصّت عليه المادة 3/156 من نفس القانون علـــــى أن يقوم الخبراء بأداء مهامهم تحت مراقبة قاضي التحقيق أو القاضي الذي تعيّنه الجهة القضائية التي أمرت بإجراء الخبرة.

---

[1]- طارق فوزي الفقّي، المرجع السابق، 180-181.

[2]- عائشة بن قارة مصطفى، المرجع السابق، ص 139-140.

أمّا فيما يخص اختيار الخبراء فقد يكونون من بين الأشخاص الطبيعيين أو المعنويين المشار إليهم في الجدول الوطني الذي تعده محكمة الطعن بالنقد أو محاكم الاستئناف. و يمكن أن يتم اختيار خبراء غير مقيديّن في ذلك الجدول من طرف الجهات القضائية، وهذا ما نصّت عليه المادة 157 قانون إ.ج.ف[1].

كما يجب أن تحدد دائما في قرار ندب الخبراء مهمتهم التي لا يجوز أن تهدف إلاّ إلى فحص مسائل ذات طابع فنّي وهو ما نصّت عليه المادة 158 من قانون إ.ج.ف و قاضي التحقيق قد يختار خبير واحد أو عدّة خبراء للقيام بمهمّة الخبرة و هذا ما نصّت عليه المادة 159 قانون إ.ج.ف[2].

كما نصت عليه المادة 161-1/1 من قانون إ.ج.ف على أنه: "يجب على قاضي التحقيق أن يبلّغ نسخة من أمر تعيين الخبير إلى كل من وكيل الجمهورية والأطراف، الذين يمكنهم خلال 10 أيام أن يطلبوا من قاضي التحقيق أن يعدل أو يكمل الأسئلة المطروحة على الخبير وأن يضيف إلى الخبير المعيّن خبيرا من اختيارهم."

وأضافت المادة 161-2/1 من قانون إ.ج.ف.أنه في حالة ما إذا لم يستجب قاضي التحقيق إلى تلك الطلبات فعليه أن يصدر أمر مسبّبا، ويكون ذلك الأمر أو السكوت عن إصداره أصلا قابلا للإستئناف في مهلة 10 أيام أمام رئيس غرفة التحقيق الذي يفصل بموجب مقررّة غير قابلة للطعن .

و لا تطبق هذه المادة في حالة ما إذا كانت أعمال الخبرة وإيداع التقرير من طرف الخبير يجب أن تنجز استعجالا و لا يمكن تأجيلها خلال 10 أيام المذكورة سابقا، أو إذا كان التبليغ المشار إليه من شأنه أن يعرقل التحقيق. وهذا ما أشارت إليه المادة 161-3/1 من قانون إ.ج.ف.

عند انتهاء الخبراء من أعمال الخبرة يحررون تقريرا، يجب أن يشتمل على وصف ما قاموا به من أعمال ونتائجها،و يوقعون على تقاريرهم مع الإشارة إلى أسماء و وظائف الأشخاص الذين ساعدوهم، تحت رقابتهم ومسؤوليتهم، من أجل إنجاز المهام الموكلّة إليهم[1].

---

[1]-Art 157 du C.P.P.E (L n° 2004-130 du 11 février 2004, art54) : « les experts sont national choisis parmi les personnes physique ou morales qui figurant sur la liste national dressée par la cour de cassation ou sur une des listes dressées par les cours d'appel dans les conditions prévues par la loi n°71-498 du 29 juin 1971 relative aux experts judiciaires »V..L n° 71-498 du 29 juin 1971 .C.pr ,civ, App ,V° experts judiciaires .
A titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes.

[2]-Art 159 (L n° 85-1407 du 30 décembre 1985) : Le juge d'instruction désigne l'expert chargé de procéder à l'expertise.
Si les circonstances le justifient, il désigne plusieurs experts.
Dernier al . abrogé par Ln° 93-1013 du 24 aout 1993.

أ- التشريع الإماراتي:

نضّم المشرع الإماراتي الخبرة في المواد 137-138-139 في التعليمات القضائية للنّيابة العامة تحت عنوان "ندب الخبراء في المسائل الفنيّة"[2].

حيث نصّت المادة 137 على أنّه: "يجوز لأعضاء النيابة العامّة ندب الخبراء المتخصّصين فيما يعرض من لهم من أمور فنيّة كندب المحاسبين والمراجعين والمهندسين وأساتذة الجامعات أو غيرهم إذا اقتضى التحقيق ذلك، ويجب على عضو النيابة أن يضمن قراره بندب الخبير بيان المهمّة المكلف بها، وأن يمّكنه من الإطلاع على أوراق التحقيق المتعلقة بتلك المهمّة والتصريح له بالإطلاع على غيرها من الأوراق أو السجلات لدى أي جهة بحسب نوع المهمّة والغرض الذي يقتضيه التحقيق."

وإذا كان الخبير المنتدب ممّا يحلفون يمينا قبل مزاولة المهنة فلا يلزم تحليفه اليمين قبل مباشرة المهمة المكلف بها، أمّا غيرهم من الخبراء، فيجب أن يؤدي اليمين القانونية أمام عضو النّيابة قبل مباشرتها بأن يحلف يمينا بأن يؤدي المهمّة الموكلة إليه بالصدق والأمانة وهذا ما نصّت عليه المادة 138 من ذات التعليمات.

و على عضو النيابة أن يحدد للخبير في قرار الندب ميعادا لتقديم تقريره، وله أن يستبدل به خبير آخر إذا لم يقدم التقرير في الميعاد المحدّد أو استدعى التحقيق ذلك. وهو ما نصت عليه المادة 139 من ذات التعليمات.

ب-التشريع الأردني:

حقيقة لم يتطرق المشرع الأردني صراحة للخبرة إلا في مرحلة التحقيق الابتدائي، في المواد من 39 إلى 41 من قانون الأصول المحاكمات الجزائية.

حيث نصت المادة 39 على أنه: " إذا توقف تمييز ماهية الجرم وأحواله على معرفة بعض القانون والصنائع، فعلى المدعي العام أن يستصحب واحدا أو أكثر من أرباب الفن والصنعة،" كما نصت المادة 40 على أنه:" إذا مات شخص قتلا أو بأسباب مجهولة باعثة على الشبهة فيستعين المدعي العام بطبيب أو أكثر لتنظيم تقرير بأسباب الوفاة و بحالة جثة الميت"، أما المادة 41 فقد نصت على

---

[1]-Art 166/1 du C.P.P.E dispose que : « lorsque les opérations sont terminées, les experts rédigent un rapport qui doit contenir la description desdites opérations ainsi que leurs conclusion (L° 2003-239 du 18 mars 2003 , art ,16)

« Les experts signent leurs rapports et mentionnent les noms et qualités des personnes qui les ont assistés, sous leur contrôle et leur responsabilité, pour la réalisation des opérations jugées par eux nécessaire a l'exécution a la mission qui leur a été confiée

[2]-عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي، المرجع السابق، ص 600.

أنه:" يتعين على الأطباء والخبراء المشار إليهم في المادتين 39 و40 من قانون العقوبات أن يقسموا قبل مباشرتهم العمل يمينا بأن يقوموا بالمهمة الموكلة إليهم بصدق وأمانة".

يتضح مما سبق ذكره أنه يجوز للنيابة العامة لموظفي الضابطة العدلية في حالة الجرم المشهود، تعيين خبير أو أكثر من أرباب الفن والصنعة، حين يتوقف تمييز ماهية الجرم وأحواله على معرفة بعض الفنون والصنائع، كما يجوز أن تستعين هذه الجهات بطبيب أكثر في حالة ما إذا مات شخصا قتلا أو لأسباب مجهولة لتنظيم تقرير لأسباب الوفاة وبحالة جثة الميت، واللجوء إلى الخبر في حالة الجرم المشهودة لا يعتبر عملا من أعمال التحقيق الأولي بل من أعمال التحقيق الابتدائي تحل فيه النيابة العامة محل قاضي التحقيق، لذا كان لابد من تحليف الخبير اليمين القانونية.

ت-التشريع المصري:

نضم المشرع المصري أحكام الخبرة التقليدية، ضمن قانون الإجراءات الجنائية في المواد 29 و85-89 و292 منه. حيث أجاز قانون الإجراءات الجزائية المصري الإستعانة بالخبراء لكل من مأمور الضبط القضائي والنّيابة العامّة وقاضي التحقيق. حيث نصّت المادة 29 منه على ما يلـــي: " لمأموري الضبط القضائي أثناء جمع الإستدلالات أن يسمعوا أقوال من يكون لديه معلومات عن الوقائع الجنائية ومرتكبها وأن يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ويطلبوا رأيهم شفهيا أو بالكتابة. ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلاّ إذا خيف ألاّ يستطاع فيما بعد سماعه الشهادة بيمين".

إذا استلزم إثبات الحالة الإستعانة بطبيب أو غيره من الخبراء يجب على قاضي التحقيق الحضور وقت العمل وملاحظته المادة 1/85 من قانون إ.ج.م وإذا اقتضى الأمر إثبات الحالة بدون حضور قاضي التحقيق نظرا إلى ضرورة القيام بأعمال تحضيرية أو تجارب متكررة أو لأي سبب آخر، وجب على قاضي التحقيق أن يصدر أمرا يبيّن فيه أنواع التحقيقات وما يرد إثبات حالته المادة 2/85 من قانون إ.ج.م.

ويجوز في جميع الأحوال أن يؤدي الخبير مأموريته بغير حضور الخصوم، طبقا للمادة 3/85 من نفس القانون.

يجب على الخبراء أن يحلفوا أمام قاضي التحقيق يمينا على أن يبدوا رأيهم بالذمة وعليهم أن يقدموا تقريرهم كتابة المادة 86 قانون إ.ج.مصري.

يحدد قاضي التحقيق ميعادا للخبير ليقدم تقريره فيه[1]، وللقاضي أن يستبدل به خبيرا آخر إذا لم يقدم التقرير في الميعاد المحدّد طبقا لنص المادة 87 قانون إ.ج.م.

ولقد حرص المشرع على إفساح سبيل الدفاع أمام المتهم، لذلك اعترف له بالحق في أن يستعين دائما بخبير استشاري[2] يودع تقريره لملف الدعوى ليكون تحت نظر المحكمة عند مناقشة تقرير الخبير المنتدب من قبل المحقق.

وعلى الرغم من أن نص المادة 88 ق.إ.ج.م لم يتكلم إلاّ عن حق المتهم في الإستعانة بخبير استشاري، إلاّ أنّه ينبغي الإعتراف بهذا الحق لكل من المدعي المدني و المسؤول عن الحقوق المدنية، وذلك من باب المساواة بين الخصوم في توفير وسائل الدفاع المؤدية إلى إظهار الحقيقة [3].

ونصّت المادة 292 ق.إ.ج.م على ما يلـــــي: "للمحكمة سواءا من تلقاء نفسها أو بناءا على طلب الخصوم، أن تعيّن خبير واحدا أو أكثر في الدعوى".

ث-التشريع الجزائري:

لم يعرف التشريع الجزائري الخبرة بل بين الغرض منها في قانون الاجراءات المدنية والادارية من خلال نص المادة 125: " تهدف الخبرة إلى توضيح واقعة مادية تقنية أو علمية محضة للقاضي،" أما المشرع الجنائي فقد بين مباشرة إجراءات الإحتكام للخبراء من خلال نص المادة 143- 156 قانون الإجراءات الجزائية وسمي هذه القسم بالخبرة.

ورغم عدم تضمين المشرع الجزائري لنصوص خاصّة تتعلق بالجريمة الإلكترونية، وكذلك نقص الخبرة في مجال تكنولوجيا المعلومات، إلا أنّ هناك إمكانية تطبيق الأحكام المتعلقة بالخبرة في الأحكام العامة على الجرائم الإلكترونية، و في هذا الصدّد نصّت المادة 143 علـــى أن : "لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فنّي أن تأمر بندب خبير، إما بناءا على طلب النيابة العامّة وإمّا من تلقاء نفسها أو من الخصوم.

---

[1]- تنص المادة 88 ق.إ.ج.م على أنّه: "للمتهم أن يستعين بخبير استشاري ويطلب تمكينه من الإطلاع على الأوراق وسائر ما سبق تقديمه للخبير المعيّن من قبل القاضي على أن لا يترتب على ذلك تأخير السير في الدعوى".

[2]- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتية، المرجع السابق، ص 599.

[3]- تقرير الخبير يعتبر من الأدلة، أما إجراء ندب الخبير فهو من إجراءات جمع الأدلة، ولذلك تحرك الدعوى الجنائية به، باعتباره إجراء من إجراءات التحقيق حتّى لو كانت النيابة العامّة لم تباشر قبله أي إجراء. أنظر: عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الإبتدائي في الجرائم المعلوماتي، المرجع نفسه، ص 595.

وإذ رأى قاضي التحقيق أنّه لا موجب للاستجابة لطلب خبرة فعليه إصدار أمر مسببا في أجل (30) يوما من تاريخ استلامه الطلب.

وإذا لم يبث قاضي التحقيق في الأجل المذكور، يمكن الطرف المعني إخطار غرفة الإتهام مباشرة خلال 10 أيام، ولهذه الأخيرة أجل 30 يوما للفصل في الطلب تسري من تاريخ إخطارها، ويكون قرارها غير قابل لأي طعن".

و يقوم الخبراء بأداء مهمتهم تحت مراقبة قاضي التحقيق أو القاضي الذي تُعيّنه الجهة القضائية التي أمرت بإجراء الخبرة ".

أمّا عن اختيار الخبير، يكون من بين الخبراء المسجلين بالجدول الذي تعدّه المجالس القضائية بعد استطلاع رأي النيّابة العامّة، وقد يختار خبراء ليسوا مقيدين في الجدول بقرار مسبب من الجهات القضائية وهذا ما نصّت عليه المادة 144 الفقرة 1 و 3 من ق.إ.ج.ج.

يكون أداء اليمين بالنسبة للخبير المقيد في الجدول مرّة واحدة عند تقييده بينما يلزم الخبير المعيّن من خارج الجدول[1] أداء اليمين لكل مهمّة محددّة بذاتها طبقا لنص المادة 145قانون إ.ج.ج.

و للخبير في سبيل القيام بمهامه والحصول على معلومات تفيده في مجال الخبرة التي كلّف برفع تقرير خبرة بشأنها، الاستماع لكل شخص يرى ضرورة لسماعه، باستثناء المتهم الذي لا يحق للخبير الاستماع لأقواله، إلا بواسطة قاضي التحقيق وبحضوره فقط [2].

يجب تحديد المدّة التي يجب على الخبير أو الخبراء إنجاز المهام المناطة بهم خلالها. غير أنّه يجوز تمديدها بقرار مسبب من قاضي التحقيق، بناءا على طلب من الخبير أو الخبراء، وعليهم إيداع تقاريرهم في الميعاد المحددّ لهم، فمن حق الجهة التي انتدبتهم استبدالهم، وعليهم أن يقدّموا نتائج أبحاثهم، وأن يردّوا الأشياء التي سلمت لهم بهدف القيام بمهامهم، في ظرف 48 ساعة، و لا يكون ذلك حائلا دون مجازاتهم تأديبيا، والتي قد تصل إلى عقوبة الشطب من جدول الخبراء.

ولقد استحدث المشرع الجزائري بموجب الأمر 02/15 المؤرخ في 23 يوليو 2015[1] نظاما في الباب الأول من الكتاب الثاني تحت عنوان "في حماية الشهود و الخبراء والضحايا" من المواد 65

[1]– الخبير من خارج الجدول القضائي والذي يتم انتدابه من قبل قاضي التحقيق بموجب طلب من النيابة العامّة أو الخصوم، أو بدون طلب هو ما يطلق عليه بالخبير الاستشاري.

[2]– نظر المادة 151 من قانون إ.ج.ج.

مكرر 19 إلـــى 65 مكرر 28، حيث تنص المادة 65 مكرر 19 على ما يلي: "يمكن إفادة الشهود والخبراء من تدبير أو أكثر من تدابير الحماية غير الإجرائية و/أو الإجرائية المنصوص عليها في هذا الفصل إذا كانت حياتهم أو سلامتهم الجسدية أو حياة أو سلامة أفراد عائلاتهم أو أقاربهم أو مصالحهم الأساسية معرضّة لتهديد خطير، بسبب المعلومات التي يمكن تقديمها للقضاء، والتي تكون ضرورية لإظهار الحقيقة في قضايا الجريمة المنظمة أو الإرهاب أو الفساد".

من خلال النصّ نلاحظ أنّ المشرع بسط حماية لكل من الشهود والخبراء فقط، رغم ذكر الضحايا في العنوان إلاّ أنّه لم يتعرض لهم.

ويوجد بالمعهد الوطني للأدلّة الجنائية وعلم لإجرام ببوشاوي الجزائر العاصمة مصلحة الخبرات الخاصّة بالدلائل الرقمية[2]، كما تضمنت المديرية العامّة للأمن الوطني ومصالحها في بعض الولايات قسم خاص بالخبرة الرقميةُ، يتكون من خبراء متخصصين في تحليل و استعادة البيانات المحذوفة وتتبع عنوان **(CIP)** ومعالجة الصور ومطابقتها ومعرفة الصور التي تم تركيبها، وكذلك الخبرة المتعلقة برسائل الهاتف النقال[3].

المطلب الثالث : الأساليب المستحدثة للتحقيق في الجرائم الإلكترونية

ذكرنا سابقا مجموعة من الأساليب التقليدية لجمع الدليل الإلكتروني التي لا تكفي لإثبات هذا النوع الجديد من الجرائم، وتبين لنا مدى التعقيد الذي أحدثته ثورة الإتصالات في مسألة استخلاصه، وهو ما يؤدي إلى إفلات العديد من المجرمين من العقاب، وعلى ذلك كان لزاما أن يلحق التطور طرق الحصول على هذا الدليل الجنائي وذلك من خلال تكريس أساليب أخرى مستحدثة تتناسب والطبيعة التقنية لهذه الجرائم الإلكترونية وللدليل الإلكتروني الذي يصلح لإثباتها، لكي يمكن عن طريقها الوصول إليه، ونقصد بذلك تكريس تقنية المعلومات لجمع الدليل الإلكتروني[4].

---

[1]– الأمر 02/15 المؤرخ في 23 يوليو 2015، يعدّل ويتمم الأمر 155/66 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائرية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، السنة الثالثة والأربعون، الصادرة في 24 ديسمبر 2006، ص 33.

[2]– القرار الوزاري المؤرخ في 14 أبريل 2007 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للأدلّة الجنائية وعلم الإجرام، الجريدة الرسمية للجمهورية الجزائرية، العدد 36، الصادرة في 3 يونيو 2007، ص 14–17.

[3]– فايز محمد راجح غلاب، المرجع السابق، ص 370.

[4]– رشيد بوكر، المرجع السابق، ص 440.

من هذه الأساليب المستحدثة، سنتطرق إلى إعتراض المراسلات وتسجيل الأصوات والتقاط الصور في (الفرع الأول)، ثم نتناول التسرّب في (الفرع الثاني) وأخيرا إستحداث إجراءات أخرى في مجال التحري والتحقيق في الجرائم الإلكترونية (الفرع الثالث).

الفرع الأول: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

إنّ عصرنة الاتصالات والمواصلات والتطور الهائل في فضاء التكنولوجيا جعل حركة تنقل الأشخاص و الممتلكات والمعلومات سهلة التداول في فترة وجيزة لمسافات بعيدة بين أطراف متعددّة ممّا نتج استغلالها باستعمالها لارتكاب الجرائم، ولهذا أصبح من الصعب إنجاز البحث والتحري ضد المشتبه فيهم والتعرف على هويتهم ومكان إقامتهم ووجهتهم خلال تحركاتهم، وللتحكم في أماكن معيّنة وما يحضر فيها، جاء النصّ على شرعية المراقبة التقنية لنشاطاتهم لضرورات التحقيق في جمع الأدلّة الأولية[1].

أولا: اعتراض المراسلات (السلكية واللاّسلكية)

للأحاديث الشخصية والمكالمات التليفونية حرمة تستمد من حرمة الحياة الخاصّة لصاحبها، وتتضمن حرمة الأحاديث الشخصية والمكالمات التليفونية حمايتها ضد جميع وسائل التصنّت والاستماع والنشر، فلا يجوز مطلقا تسجيل الأحاديث الشخصية والمكالمات التليفونية أو مراقبتها بأيّة وسيلة[2]، والمقصود بالمراقبة هنا تعتمد التسجيل بأيّة طريقة سواءا مباشرة أو غير مباشرة، وسّيان كانت على الاتصالات السلكية كالهواتف، أو اللاسلكية، ويقصد بها البرامج أو الإذاعات ونضيف إليها البرامج الإلكترونية والمعلومات التي تبث عبر أجهزة الحاسب الآلي[3].

وعرفت لجنة خبراء البرلمان الأوروبي بمناسبة اجتماعها المنعقد بسترسبورغ في 2006/10/06 لدراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية عملية اعتراض المراسلات بأنّها: "عملية مراقبة سرّية المراسلات السلكية واللاّسلكية وذلك في إطار البحث والتحري عن الجريمة وجمع الأدلّة أو المعلومات حول الأشخاص المشتبه فيهم أو في مشاركتهم في ارتكاب الجرائم[4]".

---

[1]– قادري أعمر، أطر التحقيق، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013، ص 68.

[2]– عبد الله بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، المرجع السابق، ص 779.

[3]– ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012، ص 148.

[4] رشيدة بركر، المرجع السابق، ص 441–442. وأنظر أيضا: عبد الرحمن خلفي، المرجع السابق، ص 72.

و المراسلات يمكن أن تكون كتابية كالرسائل البريدية والبرقيات أو تكون شفوية كالاتصالات التليفونية سواءا سلكية أو اللاّسلكية[1]، والاختلاف بينهما يكمن فقط في الوسيلة المستعملة من قبل المرسل إلى المرسل إليه.

كما أنّ المراسلات التي تصلح لإجراء اعتراضها يجب أن تتسم بالخصوصية، ولكي تكون كذلك يلزم أن يتوفر لديها عنصران أساسيان هما:العنصر الموضوعي يتعلق بموضوع ومضمون الرسالة في حد ذاتها بمعنى أن تكون الرسالة ذات طابع شخصي وسرّي أو خاص فيما تخبر به، والعنصر الشخصي يراد به إدارة المرسل في تحديد المرسل إليه ورغبته في عدم السماح للغير بالإطلاع على مضمون الرسالة[2].

فالتصنت وبث تسجيل الكلام المتفوه به بصفة خاصّة أو سريّة من طرف شخص أو عدّة أشخاص في أماكن خاصّة وعمومية يعتبر من العمليات التي وضعت بشكل محكم ومرتّب يهدف في النهاية إلى رصد الدليل الذي سوف يثقل كاهل المجرم الإلكتروني إذا خصّ الإجراءات في هذا الإتجاه وحده. فالملاحظ أنّ هذه الترتيبات التقنية يتم وضعها دون علم المعنيين ودون موافقة مسبقة من هؤلاء المعنيين بالمراقبة، و من خلالها يتم رصد كل كلمة أو كل المحادثات بين هؤلاء وهذا الكلام أو الحوار يتم أولاّ التقاطه ثم تثبيته بتسجيله وبثه عند الحاجة ومن تم يستعمل كدليل يواجه به المتهم ويستوي في ذلك أن يكون الكلام بصفته خاصّة أو بشكل سرّي[3].

ويبدوا أنّ المراقبة المسلطّة على التواصل بين الأشخاص عن طريق الهاتف من خلال تسجيل المكالمات تعد الأخطر من اعتراض المراسلات، فالمؤكد أن الوسائل التقنية الحديثة بلغت درجة عالية من التطور بوجود أجهزة دقيقة بإمكانها تسجيل والتقاط المكالمات في أي مكان وبالرغم من مدى الخطورة المشار لها على حق الإنسان في احترام خصوصية المقررّة دستوريا، فإنّ الفقه القانوني

---

[1]– تماشيا مع ظهور الهاتف النقال كوسيلة إتصال وفتح المجال أمام القطاع الخاص لتقديم خدمات الاتصال ثم إصدار مراسيم تنفيذية تتضمن الموافقة على منح رخص لإقامة واستغلال شبكة عمومية للمواصلات اللاّسلكية الخلوية من نوع GSM وهي المراسيم 219/01 و09/04 حيث ألزم مقدم الخدمة من خلالها ضمان عدم التعرض لحرمة الاتصالات الخاصّة والبيانات الشخصية للمشتركين إلاّ في حالة وجود طلب رسمي من قبل السلطات المختصة. أنظر: صورية بوربابة، المرجع السابق، ص 281.

[2]– نعيم سعيداني، المرجع السابق، ص 178.

[3]– زبيخة زيدان، المرجع السابق، ص 157–158.

الحديث اعتبر ذلك استثناءا على القواعد العامّة غايته تحقيق التوازن بين حق في الخصوصية والسرّية وحق المجتمع في التصدي للجريمة لتحقيق الأمن والسلامة للفرد[1].

و لاعتراض يتم باستخدام وسائل فنيّة Des Moyens Techniques تتعلق بالتصنت L'écoute أو التحكم Le Controle أو مراقبة محتوى الاتصالات La Surveillance Du Contenu Des Communications و الحصول على المحتوى بطريقة مباشرة من خلال طريقة الولوج إلى داخل النظام المعلوماتي واستخدامه، أو بشكل غير مباشر عن طريق استخدام أجهزة التصنت L'emploi De D'ecoute Dispositifs و يمكن أن تشتمل وسائل الاعتراض على تسجيل البيانات[2] Un Enregistrement Des Données.

ولعل من أهم المراسلات الإلكترونية التي يهتم القائمين بالتحقيق بإخضاعها لعملية الاعتراض والمراقبة والتي تمثل مصدرا غنيا لأدلّة إثبات الجرائم الإلكترونية، المراسلات عبر البريد الإلكتروني، والذي هو بمثابة نظام للتراسل بإستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه إلاّ عن طريق كلمة المرور[3].

و البريد الإلكتروني لم يسلم من الاقتحام من قبل مجرمي المعلوماتية بل أنّه يعتبر الميدان الخصب لتدخلاتهم سيما بعد رواج التسوّق والمعاملات التجارية الإلكترونية أو ما يعرف بالتجارة الإلكترونية وذلك كله رغم ما توصلت إليه التكنولوجيا الحديثة بابتكار نظام التشفير لحماية البريد الإلكتروني من هواة الإجرام[4].

ثانيا: تسجيل الأصوات و التقاط الصور

يقصد بتسجيل الأصوات أو التقاط الصور تسجيل المحادثات الشفوية التي يتحدث بها الأشخاص بصفة سرّية أو خاصّة وفي مكان عام أو خاص وكذلك إلتقاط صورة لشخص أو عدّة أشخاص يتواجدون في مكان خاص[5].

---

[1]– زبيخة زيدان، المرجع السابق، ص 158.

[2]– هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، المرجع السابق، ص 79–80.

[3]– زبيخة زيدان، المرجع السابق، ص 159.

[4]– زبيخة زيدان،المرجع نفسه، ص 160.

[5]– عبد الرحمن خلفي، المرجع السابق، ص 73.

ويتم استخدام هذه الوسائل في المحلات السكنية والأماكن الخاصّة والأماكن العامّة، فأمّا المحلات السكنية فنعني بها المنازل المسكونة وكل توابعها، بينما الأماكن العامّة يقصد بها كل مكان معدّ لإستقبال الكافّة أو فئة معيّنة من النّاس لأي غرض من الأغراض. أمّا المكان الخاص فهو مكان غير معدّ للسكن يستعمل لمزاولة نشاط كالمحلات التجارية [1].

فحق الإنسان في حياته الخاصّة يتفرع عنه حقّه في عدم التقاط صورة له دون موافقته، كما يتضمن هذا الحق في إمكانية بث أو نشر صورته أو استغلالها دون إذنه، بالإضافة إلى اعتراض الشخص على المساس بصورته أو تحريفها أو تغيير ملامحها عن طريق المونتاج [2].

ورغم الاعتراف بهذا الحق، إلاّ أنّ الفقه المقارن لم تتحد كلمته حول ماهية ومضمون هذا الحق، فذهب جانب منه إلى اعتبار أنّ لكل شخص سلطة الإعتراض على نشر صورته دون رضاه، ويستوي في ذلك إنتاج الصورة بالطرق التقليدية كالرسم على الورق أو القماش أو الزجاج أو النحث...الخ، أو بالوسائل الميكانيكية والتقنية الحديثة، دون أن يكون له حق الإعتراض على التقاط صورته، لأنّ ذلك يتعارض مع الطبيعة الاجتماعية للإنسان، الذي هو عضو في المجتمع يخرج لرؤية الناس ويحتك بهم، ومن جهة أخرى يصعب توفير الحماية له ضد التقاط صورته من النّاحيتين القانونية والواقعية، على اعتبار أنّ الفعل المذكور يتم عادة خفية دون علم صاحبه، ويضل أمره مجهولا بالنسبة له إلى الوقت الذي يتم نشر الصورة فيما بعد[3].

وذهب جانب آخر إلى اعتبار أنّ الشخص له الحق على إنتاج وإعادة إنتاج صوره الخاصّة[4].

وفي المقابل ذهب فريق ثالث (وهم غالبية الفقهاء)، إلى القول بأنّ الحق في الصورة يعطي لصاحبه سلطات أوسع تتعدّى مجرّد الإعتراض على نشر صورته، لتشمل أيضا الإعتراض على التقاط صورته، ويبرّرون ذلك أنّه من غير المنطقي السماح بالتقاط صور الأشخاص دون تمكينه من

---

[1]– عبد الرحمن خلفي، المرجع السابق، ص73.

[2]– عملية المونتاج (Montage): هي اختيار وتجميع المناظر ووصل بعضها ببعض في جميع مراحلها وهي مرحلة ضبط اللقطات من حيث طول كل منها ومكانها وتوقيتها، ومعالجة الوثائق الصوتية لشخص ما أو لصورته، بقصد الحصول على وثيقة موحدّة في =ظاهرها ولا تتطابق مع حقيقة ما قيل أو رئى. أنظر: ممدوح خليل بحر، حماية الحياة الخاصّة في القانون الجنائي، مكتبة دار الثقافة للنشر والتوزيع، عمان 1996، ص 402.

[3]– علاء الدين عبد الله الحواصنة وبشار طلال المومني، النظام القانوني للصورة الفوتوغرافية، مجلة الشريعة والقانون، العدد 53، جامعة الإمارات العربية المتحدة، 2013، ص 224–225.

[4]- Ravanas (J), la protection des personnes contre la réalisation et la publication de leur image ,L.D.J ,Paris ,1978,P 236-237.

نشرها، وأنّ صعوبة توفير الحماية الواقعية والقانونية لا تصبح سببا يبرّر إلتقاط الصورة خفية أمرا مشروعا[1].

ما يمكن قوله في هذا الصدد، هو أنّ التصوير خفية بقدر ما يفيد حتما في كشف الحقيقة ويسّهل إثبات كثير من الجرائم الغامضة التي يتعذر إثباتها بالوسائل التقليدية، ولكنه في الوقت ذاته يمثل انتهاكا صارخا لحرمة الحياة الخاصة للأفراد.

أمّا فيما يخص تسجيل أحاديث المتهم وشركائه عن واقعة معيّنة من الوقائع، فبصرف النظر عن مكان التسجيل الذي يمكن أن يكون عامّا كالشارع أو خاصا كالمسكن وبصرف النظر عن الأداة التي يتم بها، فالأساس في العملية هو الكلام المتفوه به، الذي قد يعتبر دليلا لإظهار الحقيقة.

ثالثا: الضمانات المقرّرة لاعتراض المراسلات

إنّ أسلوب اعتراض المراسلات (السلكية أو اللاّسلكية)، وتسجيل الأصوات والتقاط الصور دون علم أصحابها، أثبت جدارته في كشف وإثبات الكثير من الجرائم منها الجريمة الإلكترونية، إلاّ أنه يعتبر اعتداء على سرّية مراسلاتهم اتصالاتهم التي كفلتها معظم الدساتير والتشريعات بالحماية. لذلك يجب إحاطة هذه الإجراءات بضمانات قانونية تعمل على منع تعسف السلطات العامّة وتصون الحرّية الفردية، وتتمثل أهمها فيما يلي:

1- صدور أمر بإعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور :

السلطة القضائية هي المختصة عموما بإصدار هذا الأمر[2] ويعد ذلك ضمانة لازمة لإعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور، فلا يجوز قيام ضباط الشرطة القضائية القيام بالإجراءات السابقة دون صدور أمر إليه من السلطة المختصة، لكونها من إجراءات التحقيق وليسمن إجراءات التحري وجمع الأدلّة ولابّد أن يشمل الإذن جميع العناصر المتعلقة بنوع الجريمة التي اقتضت ضرورة التحري أو التحقيق وطبيعة المراسلة أو الاتصال[3].

كما يجب تحديد مدّة سريان الأمر باعتراض المراسلات السلكية واللاّسلكية أو تسجيل الأصوات أو التقاط الصور، وعلى القائم بتنفيذ هذا الأمر التقيّد بالمدّة التي حددّها له الأمر، سواءا صدر إليه

---

[1]- علاء الدين عبد الله الخواصنة وبشار طلال المومني، المرجع السابق، ص 255.

[2]- تختلف الجهة القضائية المخول لها قانونا اعتراض المراسلات السلكية أو اللاّسلكية وتسجيل الأصوات والتقاط الصور، في القوانين الإجرائية لأغلب الدول كما سنرى لاحقا عن موقف التشريعات المقارنة من هذه الإجراءات.

[3] - رشيدة بوكر، المرجع السابق، ص 444.

من قاضي التحقيق أم من النّيابة العامّة، و الهدف من تحديد هذه المدّة هو منع السلطة القائمة بهذا الإجراء من التعسف.

2- تسبيب الأمر بإعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور:

يقصد به المبرر الشرعي والضرورة الملّحة التي تستدعي القيام بعملية اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور، وتتحقق هذه الضرورة عندما يكون من الصعب الوصول إلى نتيجة تهم مجريات التحري والتحقيق دون اللجوء إلى هذه العملية، وفي هذا الشأن يشترط على الجهة القضائية المختصة قبل منح الإذن بتنفيذ العمليات المذكورة، تقدير جدواها وجديّة دواعيها والفائدة كل هذه العناصر للتأكد ممّا إذا كانت كافية لخرق مبدأ حرمة الحياة الخاصّة. فإذا ارتأى بأن التسبيب غير كاف رفض طلب الإذن[1].

بمعنى لا يشترط ذكر الأسباب بالتفصيل، بل يكفي الإشارة إلى القرائن والدلائل التي تبرز إصدار الأمر بإيجاز بالقدر الذي يمّكن القضاء من رقابة المحقق ومعرفة ما إذا كان هذا الأمر قد صدر بناءا على أسباب جدّية وكافية أم على مجرّد شكوك واحتمالات.

3- تحرير محضر لعملية اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور:

يجب تحرير محضر عن كل من الإجراءات المذكورة، لكي تكون حجّة على الكافّة كما يجب أن يحددّ في المحضر تاريخ بداية وانتهاء هذه الإجراءات وتوقيع محرّره[2].

4- سريّة اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور:

ينبغي أن تنفذ هذه العمليات في سرّية تامة ودون علم أو رضا المشتبه فيه أو صاحب الأماكن مع مراعاة عدم المساس بالسرّ المهني[3]. وبما أنّ اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من إجراءات التحقيق الإبتدائي الذي يتميّز بطابع السرّية بالنسبة للجمهور والعلانية بالنسبة للخصوم، فإنّه يسري على هذه الإجراءات ما يسري على التحقيق الإبتدائي من قواعد وضمانات، منها حضور المتهم أو محاميه إجراءات الإطلاع على المراسلات والصور والأصوات بعد تسجيلها من أجل الاطمئنان إلى سلامة الإجراء.

---

[1]- جمال براهيمي، المرجع السابق، ص 96.

[2]- عبد الرحمن خلفي، المرجع السابق، ص 74.

[3]- رشيدة بوكر، المرجع السابق، ص 442. وأنظر أيضا: جمال براهيمي، المرجع السابق، ص 98.

رابعا: المعالجة الإجرائية لإجراء اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور وفقا لتشريعات المقارنة:

بالنسبة لتنظيم إجراء اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور من طرف التشريعات المقارنة، فقد أرست هذه الأخيرة نصوص جديدة ذات طبيعة خاصة تتلائم مع التطور الحاصل في حقل الجريمة الإلكترونية، حيث ضمنت قوانين إجراءاتها الجنائية هذا الإجراء، غير أنّ معظم التشريعات العربية لم تنص على إجراء تسجيل الأصوات باستثناء المشرع الجزائري. و هو ما سنوضحه كالآتـــــي:

أ- التشريع الفرنسي:

كان المشرع الفرنسي السبّاق إلى تبني إجراءات اعتراض المراسلات السلكية و اللاّسلكية وتسجيل الأصوات والتقاط الصور ضمن إجراءات التحري والتحقيق الجنائي من خلال قانون إجراءاته الجزائية لعام 1991. ولقد نظم المشرع الفرنسي هذه الإجراءات كما يلـــــي:

أ.**1 بالنسبة لإعتراض المراسلات السلكية واللاّسلكية:** نظم المشرع الفرنسي هذا الإجراء في المواد من100 إلى 100-7 قانون إ.ج.ف حيث نصّت المادة 100 من قانون الإجراءات الجزائية على ما يلي: " في الجنايات أو الجنح إذا كانت العقوبة تفوق سنتين، يمكن لقاضي التحقيق إذا دعت مقتضيات البحث والتحري أن يأمر باعتراض وتسجيل ونسخ المراسلات التي تتم عن طريق وسائل الإتصال. هذه العمليات تجرى تحت سلطة و رقابة قاضي التحقيق، يكون الأمر بالإعتراض مكتوبا، وليس له طابع قضائي وغير قابل لأي طعن"[1].

كما نصّت المادة 101-1 منه على ما يجب أن يتضمنه الإذن كنوع الجريمة وطبيعة الإتصال محل الإعتراض والمدّة، وحددّت المادة 100-2 ق.إ.ج.ف مدّة سريان هذا الإجراء بقولها: "الأمر المتخذ يكون لمدّة أقصاها أربعة أشهر، ولا يمكن تجديده إلاّ ضمن نفس الشروط الشكلية والزمنية".

[1]- Art 100 du C.P.P.F stipule : « En matière criminelle et en matière correctionnelle, si la peine en courue est égale ou supérieur à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception , l'enregistrement et la transcription de correspondances émise par la voie de télécommunication ces opérations sont effectuées sous son autorité et son contrôle . La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours » modifie par loi n° 91-646 du 10 juillet 1991-art 2 JORE 13 juillet 1991 en vigueur le 1er octobre 1991.
Art 101-1 stipule : « la décision prise en application de l'article 100 doit comporter tous les éléments d'identification de la liaison à intercepter, l'infraction qui motive le recours à l'interception ainsi que la durée de celle-ci ».

على أن لاتتجاوز المدة الإجمالية للاعتراض سنة أو عندما يتعلق هذا الإجراء بأحد الجرائم المنصوص عليها من المادة 706-73 و706-1/73.

هذا و أضافت المادة 100-3 من نفس القانون أنّ لقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو هيئة موضوعة تحت سلطة أو وصاية الوزارة المكلفّة بالإتصالات السلكية أو اللاّسلكية أو كل عون مؤهل بتشغيل الشبكة أو مقدمي خدمات الإتصال الإلكترونية المرخصة من اجل القيام بتركيب جهاز الإعتراض.

ويجب على قاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه تحرير محضر عن عملية الإعتراض، ويحدد فيه تاريخ بداية وانتهاء وساعة هذا الإجراء وهو ما نصّت عليه المادة 100-4 من ق.إ.ج.ف.

مع ملاحظة أنّه في فرنسا ومنذ صدور القانون 204/2004 المؤرخ في 2004/03/09 المعدل لقانون الإجراءات الجزائية أصبح الإذن باعتراض المراسلات من اختصاص قاضي التحقيق والاعتقال وهذا ما نصّت عليه المادة 706-95 ق.إ.ج.ف[1]، بحيث إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في الجريمة المنصوص عليها في المادة 706-73، يجوز لقاضي الحريات والاعتقال بالمحكمة العليا، بطلب من وكيل الجمهورية أن يأذن باعتراض، تسجيل، نسخ المراسلات عن طريق وسائل الإتصال السلكية واللاّسلكية، لمدّة لا تتعدي شهر واحد، قابلة للتجديد مرّة واحدة ضمن نفس الشروط الشكلية والزمنية.

وقد أجاز المشرّع الفرنسي بموجب القانون رقم 2016-731[2] المؤرخ في 03 جوان 2016 ، المتعلق بتعزيز مكافحة الجريمة المنظمة و الجرائم الإرهابية وتمويلها وتطوير فعالية وضمانات الإجراءات الجزائية، لقاضي الحريات والاعتقال بطلب من وكيل الجمهورية أن يأذن بالولوج عن بعد إلى المراسلات المخزّنة عن طريق الإتصالات الإلكترونية حيث نصّت المادة 706-95-1 على أنّه: "إذا اقتضت ضرورات التحري في الجرائم المنصوص عليها في المادة 706-73 و706-73-1

[1]-Art 706-95 du C.P.P.E stipule :« si les nécessité de l'enquête de flagrance ou de l'enquête préliminaire relative à l'un des infractions entrant dans le champ d'application de l'article 703-73 l'exigent, le juge de libertés et de la détention de tribunal de grande instance peut, à la requête du procureur de la république, autoriser l'interception , l'enregistrement de la transcription de correspondances émise par la voix des télécommunications selon les modalités prévus par les articles 100, deuxième alinéa, 100-1, 100-3 à 100-7 pour une durée maximum d'un mois , renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention ».

[2]-Art 2 de la loi n° 2006-731 DU 3 JUIN 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et amélioration l'efficacité et garanties de la procédure pénal (1), JORF n°0129 du 4 juin 2016 texte n°1.

يجوز لقاضي الحريات والاعتقال، بطلب من وكيل الجمهورية، أن يأذن بناءا على أمر مسبب، الولوج عن بعد دون علم المعنيين، إلى المراسلات المخزنة عن طريق الاتصالات الإلكترونية بواسطة معرف معلوماتي. المعطيات التي تم التوصل إليها يمكن حجزها وتسجيلها أو نسخها على أي دعامة تخزين وهذا بطبيعة الحال في مرحلة البحث والتحري.

أما في مرحلة التحقيق أجاز المشرع لقاضي التحقيق أن يأذن بالولوج عن بعد إلى المراسلات المخزّنة عن طريق الاتصالات الإلكترونية، حيث نصّت المادة 706-95-2 على ما يلي: "إذا اقتضت ضرورات التحقيق في الجرائم المنصوص عليها في المادة 706-73 و706-73-1 يجوز لقاضي التحقيق أن أذن بناءا على أمر مسبب الولوج عن بعد دون علم المعنيين، إلى المراسلات المخزّنة عن طريق الاتصالات الإلكترونية بواسطة معرف معلوماتي المعطيات التي تم التوصل إليها يمكن حجزها وتسجيلها أو نسخها على أيّة دعامة تخزين".

كما أن المشرع الفرنسي نصّ على إجراء جمع البيانات الفنيّة للاتصال من خلال تعديل الذي أجراه على قانون الإجراءات الجزائية بموجب القانون رقم 2016-731 السالف الذكر[1]، حيث يمكن الإذن بهذا الإجراء سواءا في مرحلة التحقيق أو مرحلة البحث والتحري و نظمه في المواد من 706-95-4 إلى 706-95-10 من ق.إ.ج.ف.

حيث نصّت المادة 706-95-4 على أنه: "إذا اقتضت ضرورات التحري في إحدى الجرائم المنصوص عليها في المواد 706-73 و 706-73-1 يجوز لقاضي الحرّيات والاعتقال بطلب من وكيل الجمهورية الإذن لضباط الشرطة القضائية باستخدام آلة أو جهاز تقني المنصوص عليهم في 1° من المادة 226-3 من قانون العقوبات بهدف جمع البيانات الفنية للاتصال، والتي تسمح بالتعرف على التجهيزات الطرفية أو رقم اشتراك المستخدم، وأيضا البيانات المرتبطة بتحديد موقع التجهيزات الطرفية المستخدمة".

كما نصّت المادة 706-95-5 على ما يلي: "إذا اقتضت ضرورات التحقيق في إحدى الجرائم المنصوص عليها في المواد 706-73 و706-73-1 ق.إ.ج،ف يجوز لقاضي التحقيق بعد إطار وكيل الجمهورية، الإذن لضابط الشرطة القضائية باستخدام آلة أو جهاز تقني المنصوص عليهم في 1° من المادة 226-03 من قانون العقوبات بهدف جمع البيانات الفنيّة للاتصال، والتي تسمح

[1] - Art 3 de la loi n° 2016 -731 du 3 juin 2016 renforçant la lutte contre le crime organisé , le terrorisme et leur (1). financement et amélioration l'efficacité et les garanties de la procédure pénale

بالتعرف على التجهيزات الطرفية أو رقم اشتراك المستخدم، وأيضا البيانات المرتبطة بتحديد موقع التجهيزات الطرفية المستخدمة".

و بالنسبة للإذن الصادر في المواد 706-95-4 و 706-95-5 يجب أن يكون مكتوبا ومسبب وغير قابل للطعن وهو ما نصّت عليه المادة 706-95-6 ق.إ.ج.ف فبالنسبة للأمر الصادر من قبل قاضي الحريات والاعتقال يكون لمدّة أقصاها شهر قابلة للتجديد مرّة واحدة، أمّا بالنسبة للإذن الصادر من قبل قاضي التحقيق فيكون لمدّة شهرين قابلة للتجديد وفقا لنفس الشروط على أن لا تتجاوز المدّة الإجمالية للعمليات ستة أشهر نص المادة 706-95-4 و706-95-5 ق.إ.ج.ف.

كما نصّ المشرع على حكم خاص بجريمة الاعتراض المعلوماتي أو جريمة التصنت على المراسلات ضمن جرائم الحياة الخاصّة، وذلك بمعاقبة كل من يقوم وبسوء نيّة باعتراض أو تحويل أو استخدام أو الكشف عن المراسلات الواردة أو المرسلة عن طريق إلكتروني أو بتركيب المعدّات المصممّة للقيام بمثل هذه الاعتراضات وذلك بموجب الحكام الخاصّة بالمادة 226-15[1] عقوبات المعدل والتي تحدد العقوبة بالسجن لمدّة سنة واحدة وغرامة مالية مقدرة بـــ 45.000 يورو.

أ.2 بالنسبة لتسجيل الأصوات و التقاط الصور:

نضم المشرع الفرنسي هذا الإجراء في المواد من 706-96 إلـــــى 706-102 ق.إ.ج.ف، كما نص على إمكانية الإذن به في التحقيق فقط دون مرحلة البحث والتحري، حيث نصّت المادة 706-96 مـــن ق.إ.ج.ف بأنّه:" يجوز لقاضي الحرّيات والاعتقال بطلب من وكيل الجمهورية، أن يأذن لضباط أو أعوان الشرطة القضائية، بوضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصّة أو سريّة من طرف شخص أو عدة أشخاص داخل أماكن أو سيارات خاصّة أو عمومية، أو التقاط صورة لشخص أو عدة أشخاص يتواجدون في مكان خاص.

ومن أجل وضع الترتيبات التقنية المشار إليها في الفقرة الأولى، يمكن لقاضي الحريات والاعتقال أن يأذن بالدخول إلى سيارة أو مكان خاص ولو خارج المواعيد المحددّة في المادة 59 من هذا القانون

[1]Art 225-15 du C.P.E stipule : « le fait commis de mauvais foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivé ou nom à destination à adresser à des tiers , ou d'un prendre .frauduleusement connaissance ,est puni de même peine d'un d'emprisonnement et de 45.000 Euros est puni de même peines le fait , commis de mauvaise foi, d'intercepter , de détourner , d'utiliser, ou de divulguer des correspondances émises , transmises ou reçue par la voie électronique , ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions » modifie par loin n° 2013-1168 du 18 décembre 2013 art 23.

وبغير علم أو رضا مالك أو حائز السيارة أو شاغل هذه الأماكن أو أي من الأشخاص الذين لهم حق على تلك الأماكن والسيارات، تنجز هذه العمليات التي لا يكون الغرض منها إلاّ وضع الترتيبات التقنية تحت رقابة قاضي الحريات والاعتقال. أحكام الفقرة السابقة تطبق أيضا على العمليات التي يكون الغرض منها تفكيك الترتيبات التقنية التي تم وضعها".

يكون الإذن الصادر وفقا للمادة 706-96 لمدّة أقصاها شهر قابلة للتجديد مرّة واحدة وفقا لنفس الشروط (المادة 706-98ق.إ.ج.ف).

وتنص المادة 706-96-1 أيضا على ما يلي: "إذا اقتضت ضرورات التحقيق في الجرائم المنصوص عليها في المادة 706-73 و 706-73-1 يجوز لقاضي التحقيق بعد إخطار وكيل الجمهورية، أن يأذن لضباط أو أعوان الشرطة القضائية، بوضع الترتيبات التقنية، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصّة أو سريّة من طرف شخص أو عدّة أشخاص داخل أماكن أو سيارات خاصّة أو عمومية أو التقاط صور لشخص أو عدّة أشخاص يتواجدون في مكان خاص.

ومن أجل وضع الترتيبات التقنية المشار إليها في الفقرة الأولى، يمكن لقاضي التحقيق أن يأذن بالدخول إلى السيارة أو مكان خاص ولو خارج المواعيد المحددّة في المادة 59 من هذا القانون وبغير علم أو رضا مالك أو حائز السيارة أو شاغل هذه الأماكن أو أي من الأشخاص الذين لهم الحق على تلك الأماكن والسيارات، إذ تعلق الأمر بمحل سكني كان يجب إجراء العملية خارج المواعيد المنصوص عليها في المادة 59، فإنّ هذا الإذن يصدر من قبل قاضي الحرّيات والاعتقال، بطلب من قاضي التحقيق، تنجز هذه العمليات التي لا يكون الغرض منها إلاّ وضع الترتيبات التقنية تحت سلطة ورقابة قاضي التحقيق. أحكام الفقرة السابقة تطبق أيضا على العمليات التي يكون الغرض منها تفكيك الترتيبات التقنية التي تم وضعها".

وبالنسبة للإذن المنصوص عليه في المواد 706-95 و 706-96-1 يكون بناءا على أمر مسبب، ويضم كل العناصر التي تسمح بالتعرف على السيارات أو الأماكن الخاصة أو العامة، وبيان نوع الجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها، هذه التدابير لا تكون قابلة لأي وجه من أوجه الطعن، وهو ما نصت عليه المادة 706-97 ق.إ.ج.ف.

يكون الإذن الصادر في المادة 706-96 لمدة أقصاها شهر قابلة للتجديد مرة واحدة، وفقا لنص الشروط وبالنسبة للإذن، الصادر وفقا للمادة 706-96-1 لمدة أقصاها شهرين قابلة للتجديد وفقا

لنفس الشروط على أن لا تتجاوز المدة الإجمالية سنتين كحد أقصى وهو ما نصت عليه المادة 706-98 ق.إ.ج.ف

يكون الإذن الصادر وفقا للمادة 706-96-1 لمدّة أقصاها شهرين، قابلة للتجديد وفقا لنفس الشروط على أن تتجاوز المدّة الإجمالية للعمليات سنتين كحد أقصى (م 706-98 ق.إ.ج.ف).

أما عن تحرير محضر تسجيل الأصوات و التقاط الصور، نصّت المادة 706-100 من ق.إ.ج.ف على ما يلي: "يحررّ وكيل الجمهورية، قاضي التحقيق أو ضابط الشرطة القضائية المكلف وفقا للمادة 706-96 و 706-96-1، محضرا عن كل عملية من عمليات وضع الترتيبات التقنية وعمليات الإلتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري. ويجب أن يذكر هذا المحضر تاريخ وساعة بدء العمليات و انتهائها. توضع التسجيلات في أحراز مختومة ومقفلة".

ينسخ وكيل الجمهورية، قاضي التحقيق أو ضابط الشرطة القضائية المكلف وفقا للمواد 706-96 و706-96-1 الصور أو ضابط المحادثات المسجلّة والمفيدة في إظهار الحقيقة في محضر يودع بالملف وهو ما نصّت عليه المادة 706-96-101 ق.إ.ج.ق.

كما نصّت المادة 706-102 على أن: "يتم تدمير التسجيلات الصوتية أو السمعية البصرية، بناءا على طلب من وكيل الجمهورية أو النّائب العام، عند انقضاء الدعوى العمومية بالتقادم، ويحررّ محضر عن عملية التدمير".

ب- التشريع الإماراتـــــــي:

نصّت المادة 75 من ق.إ.ج.إ علـــى ما يلي:" لعضو النّيابة العامّة بموافقة النّائب العام أن يضبط لدى مكاتب البريد جميع المكاتبات والرسائل والجرائد و المطبوعات و الطرود ولدى مكاتب البرق جميع البرقيات، و أن يراقب ويسجل المحادثات بما في ذلك السلكية واللاّسلكية متى استوجبت مقتضيات التحقيق ذلك".

ت- التشريع الأردنـــــي:

نضّم المشرع الأردني بدوره مسألة ضبط الرسائل ومراقبة المكالمات الهاتفية، حيث نصّت المادة 88 من قانون أصول المحاكمات الجزائية على: " للمدعي العام أن يضبط لدى مكاتب البريد كافة

الخطابات والرسائل والجرائد والمطبوعات والطرود ولدى مكاتب البرق كافة الرسائل البرقية، كما يجوز له مراقبة المحادثات الهاتفية متى كان لذلك فائدة في إظهار الحقيقة".[1]

وأجازت المادة 3/89 من نفس القانون للمدعي وحده الإطلاع على الرسائل والبرقيات المضبوطة حال تسلمه الأوراق في غلافها المختوم، فيحتفظ بالرسائل والبرقيات التي يراها لازمة لإظهار الحقيقة، أو التي يكون أمر إتصالها بالغير مضرّا بمصلحة التحقيق. ويسلم ما بقي إلى المشتكي عليه أو إلى الأشخاص الموجهة إليهم.

كما نصّ المشرّع الأردني صراحة على جريمة الاعتراض المعلوماتي[2]و حددّ عقوبتها من خلال المادة 05 من قانون أنظمة المعلومات رقم 30 لسنة 2010، وذلك بمعاقبة كل من قام قصدا بالتقاط أو اعتراض أو بالتصنت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أي نظام معلومات بالحبس مدّة لا تقلّ عن شهر ولا تزيد على سنة أو بغرامة لا تقل عن مائتي دينار (200) ولا تزيد على ألف دينار (1.000) أو بكلتا هاتين العقوبتين. وكذلك بموجب المادة 76 و80 من قانون الاتصالات المعدل والمتمم لسنة 2011 [3].

ث- التشريع الـــــجزائري:

في إطار الإجراءات الحديثة التي جاء بها المشرع الجزائري بموجب القانون رقم 06-22 المعدّل والمتمم لقانون الإجراءات الجزائية، استحدث هذه العمليات من خلال الفصل الرابع من الباب الثاني من الكتاب الأول تحت عنوان "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور"، وقد ضمنّه ستّة مواد من المادة 65 مكرر 5 إلى المادة 65 مكرر 10.

---

[1]- نظم المشرع الإماراتي إجراء ضبط الرسائل وتسجيل المحادثات السلكية واللاسلكية ضمن قانون الاجراءات الجزائية بالفرع الثاني بعنوان المعاينة والتفتيش وضبط الأشياء من الفصل الأول بعنوان مباشرة التحقيق من الباب الثاني معدل بتحقيق النيابة العامة. للمزيد من التفاصيل أنظر القانون رقم 35 لسنة 1992، بشأن إصدار قانون الاجراءات الجزائية، الجريدة الرسمية لدولة الإمارات العربية ،المرجع السابق، ص 9.

[2]- المشرع الأردني لما نصّ صراحة على جريمة الاعتراض غير المشروع كان يهدف إلى تشجيع استخدام أنظمة المعلومات والشبكات المعلوماتية وانتشارها من خلال حماية مستخدميها الذين يحرصون على ضمان السريّة والخصوصية ولحماية معلوماتهم المالية والشخصية وغيرها.

[3]- قانون الاتصالات الأردني رقم 13 لسنة 1995 الجريدة الرسمية رقم 4072، بتاريخ 1995/10/01، ص 2939، المعدّل بموجب القانون رقم 21 لسنة 2011 والصادر بالجريدة الرسمية بتاريخ 2011/04/21، ص 5156.

من خلال إستقـــــراء المادة 65 مكرر ق.إ.ج.ج نجد أنّ المشرع الجزائري يقصد باعتراض المراسلات[1]، اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاّسلكية، وهاته المراسلات هي عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض.

كما نجد أن المشرّع الجزائري حددّ المقصود بالمراسلات التي تتم عن طريق وسائل الإتصال السلكية واللاّسلكية، كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتبات أو صور أو أصوات أو معلومات مختلفة[2] عن طريق الأسلاك أو البصريات أو اللاّسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطسية .

أما فيما يخص تسجيل الأصوات فإن المشرع الجزائري لم يعطي تعريفا صريحا لها، بل عرفها ضمنيا في نص المادة 65 مكرر من ق.إ.ج.ج على أنها:" وضع واستعمال الوسائل والترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وبث التسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة اشخاص يتواجدون في أماكن خاصة.

و طبقا لنص المادّة 65 مكرر 5 ق.إ.ج.ج فإنّه لا يمكن لضابط الشرطة القضائية اللجوء إلى العمليات المذكورة سابقا إلاّ بعد أن يحصل على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي.

---

[1]– ما يمكن ملاحظته في هذا الصدد أنّ المشرع الجزائري استعمل مصطلح "إعتراض" في نص المادة 65 مكرر 5 ق.إ.ج.ج. وما بعدها، بينما استعمل مصطلح مراقبة للتعبير عن الفعل ذاته في نص المادة 03 من القانون 04/09 وكان حري به الثبات على مصطلح واحد.

كما أن المشرع الجزائري لم يتصد لضبط تعريف للمراقبة الإلكترونية لا في مواد قانون الإجراءات الجزائية ولا في مواد القانون رقم 09-04 تاركا ذلك للفقه، **فالمراقبة الإلكترونية** تعني التصنت من ناحية وتسجيل من ناحية أخرى ومحلها الأحاديث الشخصية والمحادثات السلكية واللاسلكية، فهي تنصب على المراسلات الإلكترونية مهما كان نوعها أو البرنامج الذي تمت بواسطته، حيث اهتم القائمين بعملية المراقبة بإخضاع كل المراسلات الإلكترونية لعملية الإعتراض والمراقبة.

ولم يشترط المشرع استخدام أي جهاز لتحقق المراقبة ليحذوا بذلك حذو الموقف الذي استقر عليه كل من الفقه والقضاء في مصر.

[2]– عرفت المادة 2/2 من القانون 09-04 الإتصالات الإلكترونية بأنها: " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتبات أو صور أو أصوات أو معلومات مختلفة، بواسطة أية وسيلة إلكترونية." ما يلاحظ في هذه المادة أن المشرع لم يضع جزاء على مخالفة هذا الإجراء، كما أنه أغفل ترتيب المسؤولية الجزائية في حالة القيام بإجراءات مراقبة الاتصالات الالكترونية دون إذن من السلطة القضائية، ونهيب بالمشرع أن يستدرك هذه النقطة ويشير إليها.

وعلى وكيل الجمهورية أو قاضي التحقيق قبل منح هذا الإذن تقديره فائدة إجراء الإعتراض وجدّيته وملائمته لسير إجراءات الدعوى من خلال معطيات التحرّيات التي قامت بها الضبطية القضائية مسبقا.

ويجب أن يتضمن الإذن المذكور، كل العناصر التي تسمح بالتعرّف على الاتصالات المطلوب التقاطها، كتحديد رقم الهاتف واسم المشترك، وتحديد الأماكن المقصودة سكنية أو غيرها، وتحديد الجريمة التي تبرر اللجوء إلى هذه التدابير ويسلّم الإذن مكتوبا لمدّة أقصاها 4 أشهر قابلة للتجدد حب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية (المادة 65 مكرر 7 ق.إ.ج.ج) وهي نفس المدّة التي حددّها المشرّع الفرنسي في المادة 100 ق.إ.ج.ف.

ولقد حددّ المشرّع الجزائري الجرائم التي يجوز فيها مباشرة اعتراض المراسلات وتسجيل الإتصالات والتقاط الصور[1]، وهذه الجرائم محددّة على سبيل الحصر في المادة 65 مكرر 5 ق.إ.ج.ج منها الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات، نظرا لخصوصيتها ولعدم كفاية الإجراءات التقليدية لجمع الدليل التقني واستكمال مقتضيات التحقيق.

يحرر ضابط الشرطة القضائية المأذون له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات وكذا عن عمليات وضع الترتيبات التقنية[2] وعمليات الإلتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري ويذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها وهو ما نصّت عليه المادة 65 مكرر 9 ق.إ.ج.ج.

---

[1]– نجد المشرّع الجزائري أيضا أعطى تصريحا للجهات القضائية باستعمال إجراء الاتصالات الإلكترونية في إطار الوقاية من بعض الجرائم التي يحتمل أن تشكل خطرا على أمن الدولة وهي كما حددّتها المادة 4 من قانون 04/09، الأفعال الموصوفة = بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة، وجرائم الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أو الاقتصاد الوطني.

[2]– اللاّفت للانتباه هو أنّ المشرّع وبغية تسهيل عملية وضع الترتيبات التقنية يسمح لمحققين وبمن يستعينون بهم من مختصين بالدخول إلى المساكن أو المحلات أو غيرها في أي وقت يريدون ودون طلب موافقة أصحاب هذه المحلات ودون استشارتهم، والأخطر من ذلك كله فإنّ دخول هذه المحلات والمساكن يتم دون مراعاة أبسط القواعد الواجبة الإحترام والتي تقيدّ زمن التفتيش توقيته والمنصوص عليه في المادة 47 من ق.إ.ج.ج و المحظورة قبل الساعة الخامسة صباحا وبعد الساعة الثامنة مساءا إلاّ بطلب من صاحب المنزل، وقد أكدّت المادة 65 ق.إ.ج.ج وجوب السماح بالدخول في الحالات والأوضاع المشار لها بالنصّ عليه في الإذن المسلم بغرض وضع تلك الترتيبات. أنظر زبيخة زيدان، المرجع السابق، ص 161–162.

وقد أعطى المشرع الجزائري حماية قانونية خاصة لسرية المراسلات والاتصالات للأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، من خلال القانون 18-07، وبتحليلنا لأحكامه نجده نص صراحة على وجوب الموافقة المسبقة، حيث لا يمكن القيام بمعالجة المعطيات ذات الطابع الشخصي إلا بالموافقة الصريحة للشخص المعني.

كما حمى المشرّع الجزائري الإعتداء على الاتصالات والمراسلات بأيّة تقنية كانت و وسّع من مجال حماية الاتصالات والمراسلات. حيث نصّت المادة 303 من ق.ع.ج على ما يلي:" كل من يفض أو يتلف رسائل أو مراسلات موجّهة إلى الغير وذلك سوء نيّة وفي غير الحالات المنصوص عليها في المادة 137 يعاقب بالحبس من شهر (01) إلى سنة وبغرامة من 25.00دج إلى 100.00دج أو بإحدى هاتين العقوبتين فقط".

كما نصّت المادة 303 مكرر المضافة لقانون العقوبات لسنة 2006[1]على ما يلي: "يعاقب بالحبس من ستة أشهر(06) إلى ثلاثة سنوات (03) وبغرامة من خمسون ألف دينار(50.000) إلى ثلاثمائة ألف دينار جزائري(300.000) كل من تعمد المساس بحرمة الحياة الخاصّة وبأيّة تقنية كانت وذلك بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصّة أو سرّية بغير إذن صاحبها أو رضاه و عن طريق إلتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه.

و يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في المادة بالعقوبات ذاتها المقرّرة للجريمة التّامة، و يضع صفح الضحيّة حدّا للمتابعة الجزائية" .

وما تجدر الإشارة إليه في هذا الصدد هو أنّه في جريمة الإعتراض لا يشترط أن تكون المعلومات سرّية وإنّما وسيلة إرسالها سرّية ، ذلك أنّ الأساس في جريمة الاعتراض غير المشروع هو حماية حرّية الاتصالات وعدم إعاقة سيرها أو اعتراضها حتّى ولو لم تكن المعلومات سرّية ولكن أطراف الاتصال أرادوا أن تكون بوسيلة سريّة وغير علنية.

[1]- نجد المشرّع الجزائري أيضا أعطى تصريحا للجهات القضائية باستعمال إجراء الاتصالات الإلكترونية في إطار الوقاية من بعض الجرائم التي يحتمل أن تشكل خطرا على أمن الدولة وهي كما حددّتها المادة 4 من قانون 04/09، الأفعال الموصوفة بجرائم الإرهاب أو التخريب والجرائم الماسة بأمن الدولة، وجرائم الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة، أ الاقتصاد الوطني.

الفرع الثاني: التسرب

مع تطور الإجرام وسبلة المتضمن استعمال وسائل تؤدي إلى إخفاء آثار الجريمة وتضليل المحققين والعدالة، أصبح من الصعوبة بمكان الكشف عن الجريمة بمعزل عن أعضائها. وهو ما دفع بعض الدول إلى إستحداث إجراء ضمن قوانينها يكفل كشف هذه الجرائم نظرا لاحتمال ارتكابها في المستقبل، يسمى هذا الإجراء التسرب[1].

و ترجع العلّة في استحداث مثل هذا الإجراء إلى عجز أساليب البحث والتحري التقليدية والتي لم تعد كافية وفعالة للكشف عن الجرائم المستحدثة من بينها الجريمة الإلكترونية، وموضوع التسرب يعتبر جديد بالنسبة للكثير لهذا يتساءل العديد منهم عند تطرقهم لكلمة التسرب لأول وهلة عن مدلول وضع هذه الكلمة لهذا سنحاول التطرق إلى تعريف التسرب ثم شروطه وأهم طرق التسرب في مجال الجريمة الالكترونية وأخيرا معالجة هذا الإجراء.

أولا: تعريف التسرّب

يعرف التسرب لغة أنه :

مشتق من الفعل تسرّب تسرّبا. أي دخل وانتقل خفية، وهو الولوج والدخول بطريقة تسللية إلى مكان ما أو جماعة معيّنة وجعلهم يعتقدون بأنّ المتسرب ليس غريبا عنهم، بل واحد منهم [2]، ولكلمة التسرب كلمة مرادفة لها هي الإختراق وهي مستخدمة في الكثير من الكتب والمؤلفات القانونية وتعني إختراق يخترق الناس، مشى وسطهم[3].

أما اصطلاحا:

فللتسرب عدّة مرادفات كالتوغل أو الإختراق وهي تقنية يسمح بموجبها الدخول لوسط مغلق كجماعة إجرامية أو شبكة تتاجر في مواد ممنوعة، ممّا يفيد إقحام عنصر أجنبي عن الجماعة المراد اختراقها، وهذا بالذّات ما يطلق عليه الزرع. ليكون عينا عليها يرقب أعمالها ويرصد تصرفاتها. أي زرع أحد الضباط أو أعوان الضبطية القضائية ممّن تتوفر فيهم بعض الموصفات الخاصّة وسط مجموعة إجرامية، بقصد مراقبتها من الداخل، معرفة الإمكانيات الماديّة والبشرية والتنظيمية للمجموعة من

[1]– حبيب عباسي، المرجع السابق، ص 381.

[2]– سهيل حسيب سماحة، معجم اللّغة العربيّة، الطبعة الأولى، مكتبة سمير، 1984، ص 130.

[3]– القاموس الجديد للطلاب، علي بن هادية، بن لحسن البليمن، الجيلالي بن حاج يحي، المؤسسة الوطنية للكتاب، الجزائر، بدون سنة، ص20.

أساليب عمل ووسائل اتصال وتنقل وغيرها، حتى تتمكن المصالح الأمنية من مكافحة إجرامهم وتقديمهم للعدالة وإثبات التهم عليهم[1].

ويراد بالتسرب العملية المحضر لها والمنظمة، المراد من القيام بها التوغل داخل وسط لمعرفة حقيقة معرفة جيّدة من خلال نشاطه البارز وكشف الخفي فيه، ويكون هذا الوسط محدّدا مسبقا بطبيعته والعمل من أجل الاستعلام عنه ومعرفة أدق تفاصيله وخصوصياته وأسراره حسب تطلعات الجهات الأمنية وفائدة المصلحة [2].

ويعرّفه البعض بأنّه: "تقنية من تقنيات التحري والتحقيق الخاصة تسمح لضابط أو عون شرطة قضائية بالتوغل داخل جماعة إجرامية وذلك تحت مسؤولية ضابط شرطة قضائية آخر مكلف بتنسيق عملية التسرّب، بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء الهوية الحقيقية، ولتقديم المتسرب لنفسه على أنّه فاعل أو شريك" [3].

ويلاحظ ممّا سبق ذكره، أنّ التسرّب عملية معقدّة تتطلب أن يدخل العون المكلف بالعملية في اتصال بالأشخاص المشتبه فيهم ويربط معهم علاقات من أجل تحقيق الهدف النهائي من العملية، وتتطلب على الخصوص المشاركة المباشرة في نشاط الخليّة الإجرامية التي تسرب إليها[4].

كما تستلزم عملية التسرّب ضرورة الحصول على صورة حقيقية على الوسط المراد استكشافه لمعرفة طبيعة سيره وأهدافه، وكذلك معرفة تاريخ هذه الجماعة وكيفية نشأتها واختصاصات كل فرد من عناصرها، بالإضافة إلى الوسائل التي تعمل بها كوسائل النقل والاتصال وتحديد نقاط قوّة وضعف هذه الجماعة، وبعد أن يتم دراسة الوسط المستهدف يتم اختبار الأشخاص المناسبين للقيام بمهمة التسرّب[5].

---

[1]– قادري أعمر، المرجع السابق، ص 72.

[2]– سعيداني نعيم، المرجع السابق، ص 175.

[3]– عبد الرحمن خلفي، المرجع السابق، ص 74.

[4]– سعيداني نعيم، المرجع السابق، ص 175.

[5]– زوزو هدى، التسرّب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلّة دفاتر السياسة والقانون، مجلة جامعية محكمّة في الحقوق والعلوم السياسية، تصدر عن جامعة قاصدي مرباح، ورقلة، العدد الحادي عشر، جوان 2014، ص 118.

و في إطار القيام بعملية التسرب يلجأ الأشخاص المكلفين بهذه العملية إلى إخفاء شخصيتهم وإظهار شخصية مستعارة، قصد تفادي كشفهم من قبل عناصر الوسط الإجرامي محل الإجراء، أين يمكن أن يلحق بهم ضرر لا يوصف، إذا يؤدي إلى إفنائهم من قبل أعضاء الجماعة الإجرامية[1].

ثانيا: شروط صحّة التسرّب

باعتبار عملية التسرّب إجراء غير عادي لجمع البيانات والمعطيات الخاصّة التي تشير إلى كافة الأعمال الإجرامية، وتمكين المصالح الأمنية من معرفة الإمكانيات والأساليب المستعملة لإرتكاب الأفعال المجرّمة، إلاّ أنّه يعدّ من أخطر الإجراءات انتهاكا الحرمة الحياة الخاصّة للمتهم، لذا تمت إحاطته بجملة من الشروط يتعيّن مراعاتها عندما تقتضي ضرورات التحرّي أو التحقيق اللجوء إليه، وذلك من أجل إنجاح العملية وسيرها في ظروف سهلة تضمن أمن المتسرب وللوصول إلى الإخلاف المسطرة دون التسبب في أية أضرار أو خسائر، إن عملية التسرب تتسم بالخطورة والمجازفة خاصة بالنسبة للشخص المتسرب وبالتالي تعرض حياته للخطر، وتتمثل هذه الشروط فيما يلي:

1- الشروط الموضوعية :

يشترط للقيام بعملية التسرّب مراعاة مجموعة من الشروط الموضوعية من قبل السلطة المختصة بإجراء التسرب، خاصة وقت ومكان إجراء عملية التسرّب، نوع الجريمة، التسيب، أن يكون المتسرب فاعلا أو شريكا.

أ. السلطة المختصة بإجراء التسرّب

يتم اللجوء إلى التسرّب إذا اقتضت ضرورات التحري أو التحقيق ذلك، والجهة المختصة بإصدار أو منح الإذن بالتسرّب هو إمّا وكيل الجمهورية أو قاضي التحقيق. ففي مرحلة التحري فإنّ وكيل الجمهورية هو من يقوم بمتابعة والرقابة على تلك العملية أي هو من يأذن به وهو من يتولّى متابعة سيره من خلال ماله من مكانة في إدارة نشاط ضباط وأعوان الشرطة القضائية[2].

---

[1]- حبيب عباسي، المرجع السابق، ص 383.

[2]- هذا ما نصت عليه المادة 65 مكرر 12 غير أن ما يمكن ملاحظته في هذا الصدد أن المشرع الجزائري أغفل جانب أساسي ومهم للقيام بعملية التسرب وهو التمويل المالي لضباط الشرطة القضائية و عون الشرطة القضائية الذي يتولى القيام بعملية التسرب خصوصا وأن هاته العملية تستلزم تنقلات ومصاريف أخرى تستعمل في العملية.

وبالتّالي فإنّ قانون خوّل له أن يأمر ويراقب لا أن يتسرّب، ومن تمّ فإنّ لدينا من يراقب وهو وكيل الجمهورية ومن يقوم بدور المسؤول المباشر وهو ضابط الشرطة القضائية. ولا يمكن للوكيل الجمهورية القيام بالعملية بنفسه باعتباره من أعضاء النّيابة العامّة[1].

أمّا في مرحلة التحقيق، فإنّ قاضي التحقيق، بعد إخطار وكيل الجمهورية هو الذي يأذن بالتسرّب وهو من يقوم بمراقبته[2]. حيث يقوم بمنح إذن مكتوب لضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، إذ يصعب تصور قاضي التحقيق متنكر في زّي مجرم بحثا عن مرتكب الجريمة، فالبحث عن المجرم من مهام الشرطة القضائية, وضابط الشرطة القضائية هو من يتولّى مهمة التنسيق في عملية التسرّب[3].

ب. وقت ومكان إجراء عملية التسرّب:

باعتبار التسرّب إجراء من إجراءات التحقيق، يجعل من المتسرّب غير مقيّد بحيّز زمني يتحرك فيه، فضرورة التحقيق تبرّر عملياته طول ساعات الليل والنهار، وله أن يدخل كل الأماكن التي يمكن أن يكشف فيها الحقيقة دون قيد أو شرط، لأنّه لا يتحرك بصفة ضابط الشرطة القضائية بل هوية مستعارة [4].

ت. نـــــــوع الجريمة :

يجب أن يتم إجراء التسرّب بمناسبة جرائم محددّة على سبيل الحصر وهي:

جرائم المخدّرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلّقة بالتشريع الخاص بالصرّف وجرائم الفساد، وهذه الجرائم بعضها من نوع الجنايات والبعض الآخر من نوع الجنح، وهذه الجرائم خطيرة وآثارها وخيمة على المجتمع كالهلاك الناجم عن المخدّرات، والآثار الجسيمة التي تلحق الاقتصاد الوطني من جراء ارتكاب جرائم غسيل الأموال وغيرها من جرائم الفساد الأخرى. فهي جرائم سريعة

---

[1]– باسم محمد شهاب، عملية التسرّب، الحقيقة التشريعية، مقال منشور في مجلة الحقوق، مجلّة فصلية علمية محكمة، تصدر عن مجلس النشر العلمي، جامعة الكويت، العدد 04، ديسمبر 2013، ص 548.

[2]– زبيخة زيدان، المرجع السابق، ص 169.

[3] قادري أعمر، المرجع السابق، ص 75.

[4]– تشير الهوية المستعارة إلى كل مستند ثبوتي سواءا كان عبارة عن جواز سفر أم رخصة قيادة أم هوية عمل أو بطاقة تعريف، وتعد أحد عناصر ضمان نحاج عملية التسرّب، وهي التي تعبر عن المتسرب ولكن باسم ولقب ومكان إقامة وعمل وغير ذلك من معطيات معايرة للحقيقة.

الانتشار وعابرة للحدود الوطنية، كما أنّها تسخرّ عددا كبيرا من المجرمين، وجرائمها قائمة على التخطيط واستخدام كل الوسائل لمحو آثار الجريمة وطمس معالمها، كما أنّها تدر أموالا طائلة على الضالعين فيها[1].

ث. التسبيب :

يعتبر التسبيب أساس العمل القضائي، فمن خلاله تتبيّن العناصر التي أقنعت الجهات القضائية المختصّة لمنح الإذن وكذا العناصر التي دفعت ضابط الشرطة القضائية للجوء إلى هذا الإجراء والتي تكون ضمن موضوع طلبه الإذن. لذلك كان لزاما عند إصدار الإذن بالتسرّب سواءا من طرف وكيل الجمهورية أو من طرف قاضي التحقيق إظهار جميع الأدلّة بعد تقدير العناصر المعروضة عليه من طرف ضابط الشرطة القضائية[2].

ج. أن يكون المتسرّب فاعلا أو شريكا:

يقصد بالتسرّب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنّه فاعل معهم أو شريك لهم أو خاف.

من خلال هذا التعريف يتضح أنّ التسرّب يتم من خلال الأشخاص المؤهلون الذين تم ذكرهم فقط، والمتسرّب يمثل دور الفاعل أو الشريك أو المتخفي.

والمتسرّب ليس بالمحرض وقد قيل في وصف الأخير بأنّه مفتعل الجريمة، وهو شخص يحرّض على ارتكابها بغية الإيقاع بفاعلها وضبطه في حالة التلبس لتسليمه إلى السلطات، في حين أنّ الفاعل كان من الجائز ألاّ يرتكب الجريمة تلقائيا لو ترك وشأنه. فهذا التعريف يشير إلى التورط أكثر من التحريض أو الاستدراج، ويحوّل دور السلطات العامّة المتمثل في منع ارتكاب الجريمة إلى الدفع نحوها[3].

ويمكن للمتسرّب بوصفه فاعلا أو شريكا اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من إرتكاب الجرائم أو مستعملة في إرتكابها دون أن يعد ذلك من قبيل التحريض، كما يجوز له استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم

---

[1]– زوزو هدى، المرجع السابق، ص 121.

[2]– نعيم سعيداني، المرجع السابق، ص 176–177.

[3]– باسم محمد شهاب، المرجع السابق، ص 520–522.

الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[1].

2- الشروط الشكلية:

نظرا لما تتطلبه عملية التسرب من سرية وحيطة وحذر نتيجة خطورة العملية على حياة المتسرب حرص المشرع على حسن سير العملية واستوجب شروط شكلية يمكن إجمالها فيم يلي:

أ. صدور إجراء التسرّب بإذن قضائي:

لا تتم عملية التسرّب دون أن يحصل ضابط الشرطة القضائية على إذن[2] مسبق من قبل وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية، ويجب أن يكون هذا الإذن مكتوبا مع إحتوائه على الأسباب التي تبرّر صدوره أي وجوب أن يكون مسبّبا[3].

ذلك أنّ الأصل في العمل الإجرائي الكتابة، ولقد رتبّ المشرّع على تخلف شرط الكتابة و التسبيب في الإذن بطلانه. وينبغي أن يتضمن الإذن طبيعة الجريمة التي برّرت اللجوء إلى التسرّب وكذا تحديد هوية ضابط الشرطة القضائية المسؤول عن العملية، مع تحديد المدة الزمنية للعملية[4].

ب. مدّة تنفيذ عملية التسرّب

يجب أن يحدد في الإذن مدّة عملية التسرّب، ويمكن تجديد هذه المدة إذا اقتضت ضرورات التحري والتحقيق ذلك مع إصدار إذن آخر وفق الشروط الزمنية نفسها التي صدر فيها الإذن الأول. غير أنه في حالة ما إذا وجد المتسرّب صعوبة في الانسحاب من الشبكة، له أن يبقى لمدّة قد تصل إلى ضعف المدّة القانونية، ولو سحب المتسرّب نفسه فجأة من التنظيم الإجرامي دون التحضير لذلك فإنّه سيكون محلا للشك وسيعرض نفسه للخطر[5]، ولا يمكن أن يكون تاريخ صدور الإذن هو تاريخ بداية العملية، بل يمكن أن يكون تاريخ مباشرة العملية بعد تاريخ صدور الإذن بالعملية وبأسبوع مثلا وذلك قصد التحضير الجيد لعملية التسرب على أن يبلغ ضابط الشرطة القضائية المسؤول عن العملية وكيل الجمهورية عن تاريخ بداية العملية.

---

[1]- عبد الرحمن خلفي، المرجع السابق، ص 75.

[2]- عائشة بن قارة مصطفى، المرجع السابق، ص 121.

[3]- الإذن عبارة عن محرر رسمي صادر من جهة قضائية مختصة مسلمة إلى جهة أمنية مختصّة ممثلة في ضابط الشرطة القضائية.

[4]- قادري أعمر، المرجع السابق، ص 76.

[5]- قادري أعمر، المرجع نفسه ، ص 75. وأنظر أيضا: زبيخة زيدان، المرجع السابق، ص 121.

ثالثا: طرق التسرّب

وهي حالة تمّت دراستها في قضايا سابقة ذات الوصف إجرامي منظم وسط جماعة تتعامل في الفضاء الدولي خاصّة الاختراق عن طريق التسليم المراقب. ومن بين هذه الطرق[1] :

1- التسرّب بالبحث:

يقوم العنصر المتسرّب بنسج علاقة مع المُخبر الذي يلعب هذا الدور بحكم موقعه الهام في المنظمة الإجرامية ولرغبته في التعاون مع المصلحة المحققة، هذا الأسلوب يمكن استعماله في إطار محاربة الإرهاب وذلك بالاستفادة من إسهام المخبر بصفته شخص مسخر دون تعريض العنصر المتسرّب للخطر.

2- عملية الشراء:

تستعمل هذه الطريقة في مختلف عمليات الإتجار غير الشرعي بالمخدّرات، الأسلحة، السيارات وأشياء أخرى التي من خلالها يظهر التسليم مباشرة تورط البائعين. وهنا يقوم المتسرّب بشراء عيّنة كاختبار أو شراء شقّة على شكل عملية فعلية كما تستعمل هذه الطريقة في إطار محاربة الجرائم الإلكترونية.

3- عملية التوزيع:

هذه الطريقة تتم عن طريق تدخل المتسرّب بحيث يكشف تورط الموزعين المعتادين للمخدّرات أو التهريب أثناء تسليم جسم الجريمة.

4- الدائرة المالية:

تستعمل هذه الطريقة في قضايا تبييض الأموال والمخالفات المتعلقة بالتشريع الخاص بالصّرف من اجل كشف الآليات والبحث عن المصدر غير الشرعي للأموال عن طريق جمع سيولة يقترح العنصر المتسرّب تحويلها أو ضخّها في دائرة مالية.

أمّا في مجال الجريمة الإلكترونية، يمكن تصور عملية التسرب فيها، بدخول أو عون الشرطة القضائية إلى العالم الإفتراضي وذلك باختراقه لمواقع معيّنة وفتح ثغرات إلكترونية فيها، أو اشتراكه في محادثات غرف الدردشة أو حلقات الإتصال المباشر مع المشتبه فيهم والظهور بمظهر كما لو كان

[1]- قادري أعمر، المرجع السابق، ص 79.

مثلهم، مستخدما في ذلك أسماء أو وصفات هيئات مستعارة و وهمية سعيا منه الإستفادة منهم حول كيفية اقتحام الهاكر لموقع ما مثلا[1].

وما تجدر الإشارة إليه، هو أنّ إجراء التسرّب يثير صعوبات جمّة عند تطبيقه، حيث أنّ ذلك يتطلب ربط علاقات مع الأشخاص المشتبه فيهم و مشاركتهم في نشاط الخليّة الإجرامية[2] ، وهو ما يستلزم في بعض الحالات صرف مبالغ مادية طائلة لا تتوفر بيد المتسرّب، لإيهام الأشخاص المراد الإيقاع بهم بأنّ المنفّذ لعملية التسرب، صاحب مال طائل ونفوذ، يمكن الاعتماد عليه في الأنشطة الإجرامية.

و فيما يخص التسرّب وفقا للاتفاقيات الدولية، منها اتفاقية منظمة الأمم المتحدّة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية فكانت سباقة إلى احتواء هذا الإجراء والتي عبرّت عنه بالأعمال المستترة، كما ألزمت الدول الأطراف باتخاذ تدابير لإتاحة الاستخدام المناسب لأسلوب التسليم المراقب وما تراه مناسبا من انتهاج أساليب تحر خاصّة أخرى، مثل المراقبة الإلكترونية أو غيرها من أشكال الرقابة، والعمليات المستثيرة من جانب سلطاتها المختصة داخل إقليمها لغرض مكافحة هذه الجريمة[3] .

رابعا : المعالجة الإجرائية للتسرب وفقا للاتفاقيات الدولية والتشريعات الداخلية المقارنة:

1- المعالجة الإجرائية للتسرب وفقا للاتفاقيات الدولية:

فيما يخص اتفاقية بودابست لسنة 2001 لمكافحة الجرائم المعلوماتية[4] وكذا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، فلم تنص أي منهما على إجراء التسرّب ضمن أحكامها الإجرائية المخصصة لمكافحة الجرائم الإلكترونية.

---

[1]- رشيدة بوكر، المرجع السابق، ص 434.

[2] علاوة هوام، التسرّب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلة الفقه والقانون، العدد الثاني، المغرب، 2012، ص 63.

[3]- أنظر المادة 1/20 من اتفاقية الأمم المتحدّة لمكافحة الجريمة المنظمة عبر الوطنية.

[4]- ما يمكن قوله في هذا الصدد ونظرا لما يشكل التسرّب مساسا بحقوق الأفراد، رغم ما يحوزه من أهمية بالغة في كشف الجرائم التي يجز فيها، فقد أكد المؤتمر الدولي السادس عشر لقانون العقوبات المنعقد في بودابست 9199 على أنّه يجوز اللجوء إلى الإجراء وفق الشروط الآتية:

- يجب أن تكون الوسيلة المستخدمة متعارف عليها في نطاق القانون وتخدم حقوق الإنسان،
- الإلزامية في اتخاذ هذا الإجراء بمعنى أن لا تكون هناك وسيلة أخرى مشروعة ناجعة وأقل خطورة.
- حصر مجال هذا الإجراء في نطاق، بحيث لا يشمل إلاّ الجرائم ذات الخطر الخاص،

2- المعالجة الإجرائية للتسرب وفقا للتشريعات الداخلية المقارنة:

وعن نظام التسرّب في التشريع المقارن، اتجهت بعض التشريعات الجزائية[1] في القانون المقارن إلى الأخذ بنظام التسرب. و من هذه التشريعات:

أ- التشريع الفرنسي:

نظم المشرع الفرنسي إجراء التسرّب في المواد من 706-81 إلـــــــى 706-87 ق.إ.ج.ف حيث أجاز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرّب. وهي قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنّه فاعل معهم أو شريك لهم أو خاف[2].

ويمكن لضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عملية التسرّب والأشخاص الذين يسخرونهم لهذا الغرض، دون أن يكونوا مسؤولين جـــزائيا: القيام بما يلـــــي:

- اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرّف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال وهو ما نصت عليه المادة 706-82 ق.إ.ج.ف.

- احترام مبدأ قضائية هذا الإجراء بأن لا يتخذ إلاّ بناءا على إذن مسبق من القاضي أو تحت رقابته، أنظر حبيب عباسي، المرجع السابق، ص 386.

[1]- لم ينص المشرع الإماراتي وكذا المشرع الأردني على إجراء التسرّب كإجراء للتحري والتحقيق عن الجرائم الإلكترونية.

[2]-Art 706-81.C ,P,P,F; stipule : « lorsque les nécessités de l'enquête ou de l'instruction concernant l'un des crimes ou délits entrant dans le champ d'application des articles 706-73 et 706-73-1 le justifient, le procureur de la république ou , après avis de ce magistrat , le juge d'instruction saisi peuvent autoriser qu'il soit procédé , sous leur contrôle respectif, à une opération d'infiltration dans les conditions prévues par la présente section.

L'infiltration consiste, pour un officier ou un agent de police judiciaire spécialement habilité dans les conditions fixées par décret et agissant sous la responsabilité d'un officier de policier judiciaire chargé à coordonner l'opération, à surveiller des personnes suspectées de commettre un crime ou un délit en se faisant passer , auprès de ces personnes , comme un de leurs coauteurs , complices ou receleurs , l'officier ou l'agent de police judiciaire est à cette fin autorisée a faire usage d'une identité d'emprunt et a commettre si nécessaire les actes mentionnées a l'article 706-82, a peine de nullité , ces actes ne peuvent constituer une incitation à commettre des infractions .

L'infiltration fait l'objet d'un rapport rédigé par l'officier de police judiciaire ayant coordonné l'opération qui comprend les éléments strictement nécessaire a la constatation des infractions et ne mettant pas en changer la sécurité de l'agent infiltré et des personnes requises au sens de l'article 706-82.

كما يجب أن يكون الإذن مسلم تطبيقا للمادة 706-81ق.إ.ج.ف مكتوبا ومسبّبا وذلك تحت طائلة البطلان. ويذكر فيه الجريمة التي تبرّر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، كما يحدد الإذن مدّة عملية التسرّب التي لا يمكن أن تتجاوز أربعة (04) أشهر، ويمكن تجديد العملية ضمن نفس الشروط الشكلية والزمنية، ويجوز للقاضي الذي رخصّ بإجرائها أن يأمر في أي وقت بوقفها قبل انقضاء المدّة المحددّة. تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب، وهو ما نصت عليه المادة 706-83 ق.إ.ج.ف.

ولا يجوز إظهار الهوية الحقيقية لضباط الشرطة القضائية أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات، ويعاقب كل من يكشف هوية الضابط وأعوان الشرطة القضائية بالحبس (05) خمس سنوات وبغرامة 75.000 يورو. و في حالة ما إذا تسبّب الكشف عن الهوية في أعمال عنف أو ضرب أو جرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، تشدّد العقوبة إلى الحبس (7) سبع سنوات و بغرامة 100.000يورو. أمّا إذا تسبّب الكشف في وفاة أحد هؤلاء الأشخاص، تشدد العقوبة إلى الحبس عشر سنوات (10) و بغرامة 150.000يورو. وهذا ما نصّت عليه المادة 706-84 ق.إ.ج.ف.

و بمقتضى المادة 706-85 فإنّه إذا تقرّر وقف العملية أو عند انقضاء المهلة المحددّة في رخصة التسرّب، وفي حالة عدم تمديدها، يمكن للعون المتسرّب مواصلة النشاطات المذكورة في المادة 706-82 أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألاّ يتجاوز ذلك مدّة أربعة (04) أشهر.

ونص المشرع عن التحقيق باستعمال اسم مستعار l'enquête sous pseudonyme المادة 706-87-1.ق.إ.ج.ف

ب-التشريع الجزائري :

من ضمن المقوّمات التشريعية التي أرساها المشرّع الجزائري ضمن خطته لمكافحة الجرائم المستحدثة من بينها الجرائم الإلكترونية، عملية التسرّب وقد كان ذلك بموجب القانون 22/06، ليطبق هذا الإجراء متى اقتضت ضرورات التحري أو التحقيق ذلك، وبالتالي اصبح للضبطية القضائية الحق في استعمال هذا الإجراء للبحث عن جميع المعلومات والاشخاص المرتبطين بالجريمة.

و قد تم تنظيم هذا الإجراء وفق ثمانية مواد، من المادة 65 مكرر 11 إلى المادة 65 مكرر18.

و على غير العادة نجد أنّ المشرّع الجزائري وضع تعريف للتسرّب في نصّ المادة 65 مكرر 12 ق.إ.ج.ج علـــــى أنّه: "يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنّه فاعل معهم أو شريك لهم أو خاف".

ولما كان التسرّب يقتضي اختراق الوسط الإجرامي، أجاز القانون لضباط الشرطة القضائية المرخصّ لهم بإجرائه والأشخاص الذين يسخرون لهذا الغرض دون أن يكونوا مسؤولين جزائيا، القيام بما يلـــــي[1]:

ت-اقتناء أو حيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.

ث-استعمال أو وضع تحت تصرّف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني والمالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ونظرا لخطورة نظام التسرّب على الحقوق، لاسيما الحق في الخصوصية، واستناد لمبدأ المشروعية، نجد أن القانون حصر استعمال هذا الإجراء في بعض الجرائم منها الجرائم الإلكترونية والتي تعتبر من بين الجرائم الماسّة بالأنظمة المعلوماتية للمعطيات[2].

كما اشترط القانون جملة من الشروط الواجب توافرها في هذا الإجراء وإلاّ عدّ باطلا. تتمثل هذه الشروط فيمـــا يلي:

- الحصول على إذن مكتوب ومسبّب من قبل وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية.
- أن يتضمن الإذن تحديد الجريمة التي تبرّر اللجوء إليه وهوية ضابط الشرطة القضائية التي تتم العملية تحت مسؤوليته.
- أن يحدّد الإذن مدّة عملية التسرّب الذي لا يمكن أن تتجاوز الأربعة (04) أشهر مع جواز أن يأمر القاضي الذي رخصّ بإجرائها بوقفها قبل انقضاء المدّة المحددّة[3].

---

[1]- أنظر المادة 65 مكرر 14 ق.إ.ج.ج.

[2]- أنظر المادة 65 مكرر 11 إحالة إلى 65 مكرر 05 من ق.إ.ج.ج.

[3]- قام المشرع بتحديد المدة الزمنية لعملية التسرب بأن لا تتجاوز 04 أشهر مع إمكانية التجديد، ثم رجع في المادة 65 مكرر 2/17 ق.إ.ج.ج بقولها: إذا انقضت مهلة 4 أشهر دون أن يتمكن المتسرب من توقيف نشاطه في ظروف

- إمكانية تجديد العملية حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية،
- إيداع الإذن في ملف الإجراءات بعد انتهاء عملية التسرب[1].

وبطبيعة الحال فإن التسرّب يعبّر عن تضحيات جبارّة من قبل الأشخاص الممارسين له، نظرا للمخاطر الجسمية التي يمكن أن يتعرض لها المتسرّب بعد انتهاء عملية التسرّب في حياته، والتي يمكن أن تمتد إلى أفراد أسرته.

وبالتالي لابدّ من توفير ضمانات تكون كفيلة بتحقيق الحماية المتطلبة لهم، وفي هذا السيّاق نصّ القانون على عدم جواز إظهار الهويّة الحقيقية للمتسربين في أي مرحلة من مراحل الإجراءات، مع تقرير عقوبة عن هذا الفعل تتحدد كما يلي:

الحبس من خمس (05) سنوات إلى عشر (10) سنوات والغرامة من 200.00دج إلى 500.000دج، إذ تسبب الكشف عن الهوية في أعمال عنف أو شرب أو جرح على أحد الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين، الحبس من عشر (10) سنوات إلى عشرين (20) سنة والغرامة من 500.000دج إلى 1.000.000 دج، دون الإخلال، عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات، إذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص[2].

و الجدير بالذكر أنّ الموظف المسرّب والأشخاص الذين يسخرون في هذه العملية لا يمكن سماعهم كشهود عيان[3]، وعلى الرغم من أنّهم احتكوا بمرتكبي الجريمة وعرفوا خباياها وفي ذلك حماية لهم، وإن كان يجوز سماع ضابط الشرطة القضائية الذي تجرى عليه عملية التسرّب تحت مسؤوليته بوصفه شاهد على العملية[4].

الفرع الثالث: إستحداث إجراءات أخرى في مجال التحري والتحقيق في الجرائم الإلكترونية

يعتبر التحفظ العاجل على البيانات وإجراء التحفظ والإفشاء العاجلان لبيانات المرور وإجراء الأمر لإنتاج بيانات معلوماتية من الإجراءات الحديثة للتحري والتحقيق في الجرائم الإلكترونية، لمواجهة

تضمن أمنه يمكن للقاضي أن يرخص بتمديدها لمدة أربعة أشهر على الأكثر، وبالتالي لا يمكن فهم المدة المحددة للعملية أم هي إثنتي عشر أشهر لمجمل المدة الزمنية أم هي ثمانية أشهر.

[1]– أنظر المادة 65 مكرر 15 ق.إ.ج.ج.

[2]–أنظر المادة 65 مكرر 16 من ق.إ.ج.ج.

[3]– علاوة هوام، المرجع السابق، ص 66. وأنظر أيضا: زبيخة زيدان، المرجع السابق، ص 171.

[4]– أنظر المادة 65 مكرر 18 ق.إ.ج.ج.

بعض المشكلات المتعلقة بالدليل الإلكتروني والمتمثلة في سهولة التلاعب وتغيير البيانات المعلوماتية من خلال سوء تخزينها بطريقة غير دقيقة، أو محوها بطريقة عمّدية وإحدى وسائل المحافظة على سلامة هذه البيانات قيام السلطات المختصة بالتفتيش والتنفيذ لضبطها.

ويقصد **بالتحفظ العاجل على البيانات المعلوماتية المخزنة**، قيام مزوّد الخدمة بتجميع البيانات الإلكترونية وحفظها وحيازتها في أرشيف وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار اتخاذ إجراءات قانونية أخرى[1].

وفي هذا الصدد يجدر بنا الإشارة إلى أنّه من الأهمية بمكان التفرقة بين مصطلحي "التحفظ على البيانات" و "الاحتفاظ أو أرشفة البيانات" فرغم أن للكلمتين معنيين متجاورين في اللغة المعلوماتية، إذا أن عبارة يتحفظ على البيانات تعني حفظ البيانات سبق وجودها في شكل مخزّن وحمايتها من كل شيء يمكن أن يؤدي إلى اتلافها أو تجريدها من صفتها أو حالتها الراهنّة.

في حين أنّ عبارة الاحتفاظ بالبيانات تعني حفظ البيانات لدى حائزها بالنسبة لمستقبل البيانات التي في طور الإنتاج و التوالد، فأرشفة البيانات يشير إلى تجميع البيانات في الوقت الحاضر وحفظها أو حيازتها في أرشيف.

فأرشفة البيانات عبارة عن عملية تخزين للبيانات على عكس التحفظ على البيانات الذي يعني النشاط الذي يضمن للبيانات سلامتها وسرّيتها[2].

ولقد نصّت اتفاقية بودابست لمكافحة جرائم المعلوماتية لسنة 2001 على إجراء التحفظ العاجل على البيانات المعلوماتية المخزّنة في المادة 16 على أنّه: "

1. يجب على كل طرف أن يتخذ الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل السماح لسلطاته المختصة أن تأمر أو أن ترفض بطريقة أخرى التحفظ العاجل على البيانات المعلوماتية المخزّنة، وبما في ذلك البيانات المتعلقة بالمرور[3] المخزّنة بواسطة نظام معلوماتي،

---

[1]– رشيدة بوكر، المرجع السابق، ص 448.

[2]– هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص 186-187.

[3]– تعرف بيانات المرور بأنّها: كل البيانات التي تتعامل مع الإتصال، والتي تمرّ من خلال النظام المعلوماتي، أو يتم إعدادها بواسطته، والذي يعد عنصرا في سلسلة الاتصال، بالإشارة إلى مصدر الاتصال، ومكان الوصول وخط السير، والسرعة ، والتاريخ، والحجم، ومدّة الاتصال، ونوع الخدمة المؤداة. وعرّفها المشرع الجزائري في المادة الثانية فقرة "ه" من القانون 04/09 تحت مسمّى معطيات حركة السير.

وبالأخص عندما تكون هناك أسباب تدعو للإعتقاد بأنّ هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير".

2. عندما يقوم طرف بتطبيق الفقرة "أ" أعلاه، عن طريق أمر يصدر لشخص للتحفظ على البيانات المخزّنة الموجودة في حوزته أو تحت إشرافه، فإنّ هذا الطرف يجب عليه اتخاذ الإجراءات التشريعية والإجراءات الأخرى التي يراها ضرورية من أجل إجبار هذا الشخص على التحفظ وحماية سلامة البيانات المذكورة لمدّة طويلة من الزمن على قدر الضرورة، لحد أقصى 90 يوما بغرض السماح للسلطات المختصة بالكشف عنها، كما يمكن لكل طرف أن يقرّر تجديد هذا الأمر.

3. يجب على كل طرف اتخاذ الإجراءات التشريعية وأيّة إجراءات أخرى يرى أنّها ضرورية لإجبار حارس البيانات أو أي شخص يقع عليه عبء التحفظ على هذه البيانات، أن يحافظ على السرّية بالنسبة لتطبيق الإجراءات المذكورة خلال المدّة المقررّة بواسطة قانونه الدّاخلي.

4. السلطات والإجراءات المشار إليها في المادة الحالية يجب أن تكون خاضعة للمادتين 14 و15.

كما تطرقت الإتفاقية العربية لمكافحة جرائم تقنية المعلوماتية لسنة 2010 على التحفظ على البيانات المخزّنة في تقنية المعلومات، حيث نصّت المادة 23 من الاتفاقية على أنّه:[1]

1- تلتزم كل دولة بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزّنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصا إذا كان هناك اعتقاد أنّ تلك البيانات عرضة للفقدان أو التعديل.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (01) بواسطة إصدار أمر إلى شخص من اجل حفظ معلومات تقنية المعلومات المخزّنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدّة أقصاها 90 يوما قابلة للتجديد من أجل تمكين السلطات المختصّة من البحث والتقصي.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية المعلومات للإبقاء على سريّة الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الدّاخلي"

[1]- المرسوم الرئاسي رقم 14-252 مؤرخ في 08 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررّة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية للجمهورية الجزائرية، العدد 57، الصادرة 28 سبتمبر 2014، ص 07.

كما تضمن القانون 04/09 عدد من التزامات مقدمي الخدمات[1] منها ما نصّت عليه المادة 10 وهي:

تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها تحت تصّرف السلطة المذكورة مع مراعاة سرّية العمليات والمعلومات المتصّلة بها.

ولحفظ البيانات المتعلقة بحركة السير، يتعين على مقدمي الخدمات حفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، والمعطيات المتعلقة بالتجهيزات الطرفية المستعملة للإتصال، وحفظ الخصائص التقنية وتاريخ ووقت محدد ومدّة كل اتصال، والمعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها والمعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلّع عليها.

وبالنسبة لنشاطات الهاتف، يقوم المتعامل بحفظ المعطيات التي تسمح بالتعرف على مستعملي الخدمة، وكذلك تلك التي تسمح بالتعرف على مصدر الاتصالات وتحديد مكانها، وتحددّ مدّة حفظ المعطيات المذكورة بسنة واحدة ابتداءا من تاريخ التسجيل.

وتقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي الإخلال بالالتزامات المذكورة إلى عرقلة حسن سير التحرّيات القضائية، حيث يعاقب الشخص الطبيعي بالحبس من ستة (06) أشهر إلى خمس (05) سنوات. وبغرامة من 50.000دج إلى 500.000دج كما يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات[2].

ويعدّ التحفظ بالنسبة لغالبية الدول إجراءا قانونيا جديدا، فهو أداة جديدة للتنقيب والتحري في مجال مكافحة الإجرام المعلوماتي لعدّة مبرّرات[3]:

---

[1]– عرّف المشرع الجزائري مزودي الخدمات في المادة 02 الفقرة (د) من القانون رقم 04/09 على أنها:
– أي كيان عام أو خاص يقدم لمستعملي خدماته، ضمانة القدرة على الاتصال بواسطة منظومة معلوماتية و/أو نظام للاتصالات،– أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها، كما عرفتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 2 الفقرة الثانية على أنّها: "أي شخص طبيعي أو معنوي عام أو خاص يزوّد المشتركين بالخدمات للتواصل بواسطة تقنية، المعلومات أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها".

[2]– أنظر المادة 11 من ق 04/09.

[3]– هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، المرجع السابق، ص 190–193.

- قابلية البيانات للتلاشي، فإن هذه البيانات من السهل أن تخضع للتلاعب أو التغيير وهكذا يسهل فقدان عناصر إثبات الجريمة، من خلال الإهمال وممارسات التخزين غير الدقيقة، أو التغيير العمدي لها أو محوها من أجل تدمير كل عناصر للإثبات أو محوه في إطار العمليات العادّية أو الروتينية لمحو البيانات التي لم تعد حاجة إليها.

وإحدى وسائل المحافظة على سلامة البيانات تتمثل في قيام السلطات المختصة بعمل تفتيشات أو الولوج بطريقة أخرى للبيانا لضبطها أو الحصول عليها بطريقة أخرى.

ومع ذلك إذا كان حارس البيانات جدير بالثقة، كما في حالة شركة تجارية ذات سمعة طيّبة فإنّ سلامة البيانات يمكن ضمانها بطريقة أسرع عن طريق إصدار أمر بالتحفظ على البيانات لديه، وبهذا يمكن أن يكون الأمر بالتحفظ على البيانات أقل قلقا أو إخلالا بالنظام بالنسبة للأنشطة، وأقل ضررا على سمعة الشركة الأمنية، من عملية تفتيش الأماكن بغرض الضبط.

- الجرائم الإلكترونية والجرائم المتصلة بالحاسب، غالبا ما يتم إرتكابها عن طريق نقل الاتصالات بواسطة نظام معلوماتي، هذه الاتصالات يمكن أن تحوي محتوى غير مشروع، مثال ذلك مواد إباحية طفولية، فيروسات معلوماتية، أو أي تعليمات أخرى تحمل اعتداء على البيانات أو تعيق حسن أداء النظام المعلوماتي كما يمكن أيضا أن تحوي عناصر يمكن من خلالها إثبات أنّ جرائم أخرى قد تم ارتكابها مثال ذلك: حالات الإتجار بالمخدّرات أو النصب، وبناء على ذلك فإنّ التحقق من هوية مصدر أو منتهي هذه الإتصالات الخارجية يمكن أن يساعد على تحديد هوية مرتكب هذه الجرائم، ومن اجل تعيين مصدر ومنتهى هذه الاتصالات ينبغي تجهيز أو تهيئة بيانات التجارة غير المشروعة المتعلقة بهذه الاتصالات الخارجية.
- عندما تكون هذه الاتصالات تقدم محتوى غير مشروع أو دليل أفعال جنائية فإنّ صورا من هذه الاتصالات يتم الاحتفاظ بها بواسطة مقدمي الخدمات، على سبيل المثال البريد الالكتروني، التحفظ على هذه الاتصالات يكون هامّا من أجل عدم فقد عناصر الإثبات الجوهرية، فلا مراء فعلي أن إعطاء صور من هذه الاتصالات الخارجية، على سبيل المثال البريد المخزّن يمكن أن يكشف عن الجرائم التي تم إرتكابها.

إنّ سلطة التحفظ العاجل على البيانات المعلوماتية يجب أن تسمح بمواجهة هذه المشكلات وبالتالي يجب على الأطراف إنشاء أو تأسيس سلطة للأمر بالتحفظ على بيانات معلوماتية معيّنة، وبما أنّ هذا الإجراء وقتي، فإنّ الفترة الزمنية التي يتم فيها التحفظ على البيانات محدودة بحد أقصى

90 يومان ويمكن للأطراف أن يقرروا تجديد هذا الإجراء. هذا مع ملاحظة أنّ البيانات المتحفظ عليها لا يمكن الكشف عنها آليا للسلطات، فلكي يحدث ذلك، يجب اتخاذ إجراء إضافي أو أمر بالتفتيش.

من المهمّ أيضا أن توجد إجراءات للتحفظ على المستوى المحلّي تسمح للأطراف أن يقدموا المساعدة على المستوى الدولي فيما يتعلق بالتحفظ العاجل على البيانات المخزّنة داخل حدودهم، وهذا بالطبع سيساعد على ضمان أن البيانات الجوهرية لا تختفي خلال الإجراءات المطلوبة لطلب لمساعدة القضائية المتبادلة أثناء قيام الطرف المقدم إليه الطلب من الحصول على البيانات وإرسالها إلى الطرف مقدم الطلب أو الملتمس.

إلى جانب هذا الإجراء يوجد إجراء آخر وهو **التحفظ والإفشاء العاجلان لبيانات المرور**[1]، وهذا الأخير يهدف كذلك الوصول إلى البيانات المخزّنة لفحصها قبل أن يتم التلاعب بها، وكذلك لتحديد هوية مصدر الاتصال أو منتهاه. حيث تعد من الأمور الجوهرية التي تقود إلى معرفة الأشخاص الذين لهم علاقة بالجريمة الإلكترونية.

وبالرغم من أهمية هذا الإجراء في مجال التنقيب والتحري في الجرائم الإلكترونية، غير أن ما يمكن ملاحظته هو أن مقدمي الخدمات قد لا يبدوا تعاونا مع السلطات المختصة بالتحري أو التحقيق لعدم وجود ثقة بينهم وبين سلطات التحقيق، وعليه لا يكون هذا الإجراء مفيدا بالشكل المطلوب، وبالتالي يحتاج الأمر اتخاذ إجراءات أشدّ حزما كالتفتيش مع مراعاة الحقوق المتعلقة بالخصوصية وحقوق الإنسان بشكل عام، وبما يحقق التوازن بين إقامة العدالة والمحافظة على تلك الحقوق[2].

---

[1]– نصّت على هذا الإجراء اتفاقية بودابست لسنة 2001 في المادة 17 كما يلي: "

1/ من أجل ضمان التحفظ على البيانات المتعلقة بالمرور في تطبيق المادة 16، يجب على كل طرف اتخاذ الإجراءات التشريعية وأيّة إجراءات أخرى يرى أنّها ضرورية من أجل:

– التأكد من أنّ التحفظ العاجل لهذه البيانات المتعلقة بالمرور متوافر بغض النظر عمّا إذا كان مقدم خدمة واحدة أو عدة مقدمين للخدمة قد يساهموا في نقل الاتصال.

– ضمان الإفشاء السريع للسلطة المختصة للطرف أو للشخص المعيّن من قبل هذه السلطة، عن كمية بيانات مرور كافية، تسمح بتحديد هوية مقدمي الخدمات والطريق الذي تم الاتصال من خلاله.

2/ السلطات والإجراءات المشار إليها في المادة الحالية يجب أن تكون خاضعة للمادتين 14 و15."

[2]– فايز محمد راجع غلاب ، المرجع السابق ،ص 427–428

كما تناولت المادة 18 من الإتفاقية[1] إجراء آخر من الإجراءات المستحدثة في مجال التحري والتحقيق في الجرائم الإلكترونية، يمثل في **الأمر بإنتاج بيانات معلوماتية**[2]، حيث يلتزم شخص أو مقدم الخدمات بتقديم المعلومات التي تكون مخزنة في نظامه، أو تحت سيطرته إلى السلطة المختصة بموجب أمر صادر من تلك السلطة وهذا الإجراء يتناسب وطبيعة الدليل الإلكتروني كمرحلة سابقة لمرحلة التفتيش والضبط تقتضيه السرعة التي يتطلبها الحفاظ على الأدلة الإلكترونية من التلاعب بها.

كما نصّت أيضا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 على أمر تسليم المعلومات، حيث نصّت المادة 25 منها على ما يلي: "تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصّة من إصدار الأوامر إلـــــى:

1. أي شخص في إقليمها لتسليم معلومات معيّنة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.
2. أي مزوّد خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزودة الخدمة أو تحت سيطرته."

---

[1]– تنص المادة 18 من اتفاقية بودابست لسنة 2001 على ما يلي:

1/ يجب على كل طرف أن يتبنى الإجراءات التشريعية والإجراءات التي يرى أنّها ضرورية من أجل تأهيل سلطاته المختصة أن تأمـــــر:

أ.شخصا ما على أرضه بإرسال بيانات معلوماتية معينة في حوزة أو تحت سيطرة هذا الشخص، والمخزنة في نظام معلوماتي أو في دعامة تخزين معلوماتية.

ب. مقدم خدمات الذي يقدم خدماته على أرض ذلك الطرف، من أجل إرسال البيانات التي في حوزته أو تحت سيطرته والمتعلقة بالمشتركين وتلك الخدمات.

2/ السلطات والإجراءات المشار إليها في المادة يجب أن تكون خاضعة للمادتين 14 و15

3/ لأغراض المادة الحالية فإنّ تعبير البيانات المتعلقة بالمشتركين يقصد به كل معلومات تحتوي على شكل بيانات معلوماتية، أو أي شكل آخر في حوزة مقدم الخدمة، وترتبط بالمشتركين وخدماتهم، غير بيانات المرور أو المحتوى والتي من خلالها يمكن تحديد:

أ.نوع خدمة الاتصال المستخدمة، والأوضاع الفنية المنصوص عليها بالنسبة لفترة الخدمة,

ب. الهوية، العنوان البريدي أو الجغرافي، ورقم تلفون المشترك ورقم الولوج والبيانات المتعلقة بدفع الفاتورة والمبلغ المدفوع والمتوافرة على أساس عقد أو اتفاق تقديم خدمة.

ت. أية معلوماتية أخرى تتعلق بموقع تجهيزات الاتصال المتوافر على أساس عقد أو اتفاق تقديم الخدمة."

[2]– لم تنص فرنسا ولا الجزائر والأردن – وهو حال معظم الدول– ضمن تشريعاتها الداخلية على الأمر بإنتاج بيانات معلوماتية كإجراء للتحري والتحقيق عن الجرائم الإلكترونية وإن كان الحصول على البيانات المعلوماتية فيها يتم بطرق مشابهة كالتفتيش والضبط.

المبحث الثاني: الأساليب الدولية للتحقيق الجنائي في الجريمة الإلكترونية

يعتبر التحقيق الجنائي من الإجراءات التي تأتي في مقدمة محاولات مواجهة الجريمة الإلكترونية ، بموجب استحداث أساليب التحقيق والارتقاء بالمحققين من خلال تزويدهم بالتقنيات الحديثة، وحيث ساعدت هذه الأخيرة على توفير طرق جديدة في عمل المحققين ذلك انهم اصبحوا بموجبها ينتزعون الحقيقة، وذلك بالسعي إلى الإلمام بأساليب البحث الفني الجنائي خاصة في الجرائم المرتبطة في الأساليب ارتكابها بالتقنية الحديثة أي الجرائم الإلكترونية، وإيمانا من المشرع بضرورة استخدام أساليب التحقيق الجنائي التي تتناسب وطريقة الجريمة الإلكترونية استحدث وعدّل في النصوص الإجرائية وذلك طبعا في سبيل اكتشاف الجريمة وملاحقة مرتكبيها.

إن الدور الأساسي الذي تلعبه أساليب التحقيق الحديثة في التوصل إلى إثبات أو نفي الجريمة الإلكترونية واكتشاف غموضها وحل لغزها والتوصل للجاني من اجل تحقيق العدالة والأمن، وحيث تعززت بموجبها آمال القضاء والعدالة إذ حققت نتائج باهرة في مجال علوم الأدلة الجنائية، ولكنها رغم تلك النجاحات إلا أنها لطالما اصطدمت بعائق الاختصاص خاصة عندما تكون الجريمة ذات بعد دولي.

حيث أفرزت الجريمة الإلكترونية ذات البعد الدولي تحديات واضحة أمام المحققين وما زاد الأمر تعقيدا هو عدم وجود الجاني في مسرح الجريمة وكذا التباعد الزماني والمكاني بين السلوك الإجرامي والنتيجة الإجرامية يثير إشكالية التعارض مع السيادة الوطنية هو الدافع إلى اللجوء إلى التعاون الدولي كآلية لمواجهة الجريمة الإلكترونية، ضف إلى ذلك أنه في مجال التحقيق الجنائي تجلى التعاون الدولي في جملة من المعاهدات الدولية من اجل الوقاية والحد من الجرائم الإلكترونية وكذا التعاون القضائي.

لذا سنخصص هذا المبحث للحديث عن التعاون الأمني الدولي في الجرائم الإلكترونية في (المطلب الأول)، ثم نتناول التعاون القضائي الدولي في الجرائم الإلكترونية في (المطلب الثاني).

المطلب الأول: التعاون الأمني الدولي في الجرائم الإلكترونية

حتى يسهل لكل دولة الاستمرار والعيش مع غيرها من الدول فإنها تحتاج إلى قدر من الأمن والنظام، وتشكل الجريمة إحدى القضايا الرئيسية في الكثير من دول العالم، وتشغل بالحكومات والمختصين والأفراد على حد سواء، ولقد اثبت الواقع العملي أن الدولة لا تستطيع بجهودها المنفردة القضاء على الجريمة مع هذا التطور الملموس والمذهل في كافة ميادين الحياة ، فنتيجة لهذا التطور الملموس والمذهل في الاتصالات وتكنولوجيا المعلومات وظهور الأنترنيت والانتشار الواسع والسريع لها أدى إلى ظهور أنماط جديدة من الجرائم هي الجرائم الإلكترونية، والتي باتت تشكل خطرا على سرية النظم الحاسوبية أو سلامتها أو توافرها فحسب، بل تعدت إلى امن البنى الأساسية الحرجة.[1]

و مع تميز الجرائم الإلكترونية وبكونها عابرة للحدود، فان مكافحتها لا تتحقق إلا بوجود تعاون دولي على المستوى الإجرائي الجنائي، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة في الدول المختلفة، وذلك بإنشاء مكاتب متخصصة لجمع المعلومات عن مرتكبي الجرائم الإلكترونية وتعميمها.

ويكتسي التعاون الأمني الدولي أهميته البالغة في ظل الجهود الدولية الساعية إلى تدويل الجريمة وربط أطراف العالم بالمعاهدات، كما يساهم في التقارب والتجانس في الأفكار والجهود بما يخدم أعضاء المجتمع الدولي، ويقف حائلا أمام المجرمين في وسائلهم المتطورة للإفلات من العقاب، ولا شك أن هناك العديد من الدواعي الدولية اللازمة لمواجهة خطر الجرائم الإلكترونية.[2]

والتعاون الأمني باعتباره صورة من صور التعاون الدولي في مجال مكافحة الجريمة الإلكترونية يجد له أساسا في الاتفاقيات الدولية الثنائية والمتعددة الأطراف والتي لا تقتصر على دول الجوار فحسب، بل تمتد لتربط حتى بين دول تابعة لقارات مختلفة، طالما أن هذه الجريمة جعلت من العالم قرية واحدة.

لهذا تشمل دراسة التعاون الأمني الدولي في الجرائم الإلكترونية التطرق إلى تعريف وأهمية هذا الأخير في (الفرع الأول) ، ثم التطرق إلى أسس التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية

[1] - حسين بن سعيد الغافري، المرجع السابق، ص 636

[2] - حبيب عباسي، المرجع السابق، ص 518

في (الفرع الثاني)، صور هذا التعاون في (الفرع الثالث) لنصل في الأخير إلى جهود المنظمة الدولية للشرطة الجنائية في مجال التعاون الأمني(الفرع الرابع).

الفرع الأول: تعريف وأهمية التعاون الأمني الدولي في الجرائم الإلكترونية

أولت الدول فيما بينها اهتماما خاصا بالجريمة الإلكترونية، نظرا لخطورتها على الأمن والسلم الدوليين والوطنيين، فهي بمثابة أخطبوط ألقى بفروعه وأجزائه في جميع أنحاء العالم، وذلك إيمانا منها بان مكافحة هذه الجريمة لا تقتصر على ما هو مقرر في كل دولة، بل لا بد من تضافر جهود الدول فيما بينها خاصة في المسائل الأمني للوقوف في وجه المجرم الإلكتروني[1].

لذا يعد التعاون الأمني الدولي من أهم صور وأوجه التعاون الدولي في مجال مكافحة الجريمة الإلكترونية:

أولا: تعريف التعاون الأمني الدولي:

يعتبر التعاون الأمني الدولي من بين المفاهيم التي يصعب وضع تعريف جامع مانع لها، والسبب يرجع لعدة اعتبارات لعل أهمها يظهر من خلال مدى اتساع المجال والصور والأشكال التي قد يتخذها التعاون وعدم إمكان حصرها أو حصر الوسائل الجديدة والمتجددة التي من شأنها أن تجعل من هذا التعاون يشكل ظاهرة متغيرة ومتطورة بشكل مستمر[2]، كما يرجع ذلك أيضا إلى ارتباط مفهوم التعاون بمصالح الأمن، الذي يجد هو الآخر العديد من الإشكاليات في تعريفه.

حيث لم يتم الاتفاق على وضع تعريف موحد له عالميا رغم أهميته وذلك لأن الظاهرة الأمنية قد عرفت تطورات كثيرة نظرا لتطور التحولات الدولية، صنف إلى ذلك تدخل عوامل أخرى من بينها طبيعة المقاربات الأمنية المعتمدة في دراسة الأمن، وكذا تداخله مع العديد من المفاهيم، لهذا السبب نجد غياب الإجماع بين الدارسين لموضوع الأمن حول إعطائه تصور محدد[3].

[1] -حبيب عباسي، المرجع السابق، ص 519.

[2] -عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي، في مجال مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع السابق، ص15.

[3] -خديجة بتقة، السياسة الأمنية الأروبية في مواجهة الهجرة غير الشرعية، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، جامعة محمد خضير، بسكرة، 2013، ص 10.

وبالنظر إلى التعاون الأمني الدولي بمفهومه الواسع، نجد أنه يشمل مجالات مختلفة، كالمجال الشرطي والمجال القانوني والمجال القضائي، و مرد ذلك أن تحقيق الأمن يتطلب تنفيذ إجراءات تتعلق بتلك المجالات مجتمعة.

ثانيا: أهمية التعاون الأمني الدولـــــي

يكتسب التعاون الأمني الدولي أهمية باللغة في مكافحة الجريمة الإلكترونية نظرا لطبيعة هذه الجريمة وخصوصيتها، إضافة إلى اعتبارها من أخطر النظم الإجرامية الحديثة، بفضل ما يترتب عليها من أضرار وخيمة تمس جميع نواحي المجتمع الدولي والوطني على حد سواء.

ويشكل التعاون الأمني الدولي أحد المجاور الأساسية التي تبنى عليها المواجهة الفعالة للجريمة الإلكترونية، فمرتكب الجريمة سيجد نفسه بدون سياج يحميه من المسؤولية الجزائية، حتى ولو ارتكب الجريمة من خارج الدولة التي وقعت فيها أو فر إلى دولة أخرى بعد ارتكاب الجريمة، وهو ما يحمله على التفكير مليا قبل الإقدام على ارتكابها، فلا شك أن التعاون يحكم السيطرة على الجناة أيا كان موقعهم أو جنسياتهم[1].

ويمثل التعاون الدولي بين أجهزة الشرطة الجنائية المخصصة لمكافحة الجرائم الإلكترونية في الدول أحد الوسائل الهامة التي يمكن من خلالها منع الجرائم الإلكترونية أو الإقلال منها، وتؤكد التحقيقات في الجرائم عامة والجرائم الالكترونية خاصة على أهمية التعاون الأمني الدولي، حيث يستحيل على الدولة بمفردها القضاء على الجرائم الدولية العابرة للحدود، لأن جهاز الأمن في هذه الدولة أو غيرها لا يمكنه تعقب المجرمين وملاحقتهم إلا في حدود الدولة التابع لها، فملاحقة مرتكبي هذه الجرائم وتقديمهم للعدالة لتوقيع العقاب يستلزم القيام بإجراء التحريات خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، ومن هذه الإجراءات مثلا: معاينة مواقع الأنترنت في الخارج، أو ضبط الأقراص الصلبة[2].

[1] - حبيب عباسي، المرجع السابق، ص 520.

[2] - عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي، في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع السابق، ص20-21.

والتعاون الأمني الدولي لا يقتصر على إجراءات ملاحقة الأشخاص المطلوبين للعدالة وحسب، بل يتعدى الأمر ذلك يشمل مكافحة الجريمة بشقيها الوقائي والقمعي، بما يشمل العناية بحقوق المتهمين والضحايا ومراعاة حقوق الدول وسيادتها.

وعليه يعرف التعاون الأمني الدولي بأنه:« تبادل العون والمساعدة و تظافر الجهود المشتركة بين طرفين دوليين أو أكثر لتحقيق نفع أو خدمة أو مصلحة مشتركة في مجال التصدي لمخاطر الإجرام، وما يرتبط به من مجالات أخرى، مثل مجال العدالة الجنائية، ومجال الأمن، أو لتخطي مشكلات الحدود والسيادة التي قد تعرض الجهود الوطنية لملاحقة المجرمين وتعقب مصادر التهديد، سواء كانت المساعدة المتبادلة قانونية أو قضائية أو شرطية، وسواء اقتصرت على دولتين فقط أو امتدت إقليميا أو عالميا»[1].

إذن يعد التعاون الأمني الدولي ثمرة تطور العلاقات الدولية، ونتيجة حتمية لما تشهده الجريمة من تطور متلاحق يكاد يقفز في أرقامه من عام إلى آخر، حتى أصبح تطور الجريمة في حد ذاته ظاهرة دولية.

والتعاون الأمني على الصعيد الدولي ينبغي أن يرمي إلى منع ارتكاب الجرائم عن طريق العمل على كشفها في مهدها، أي في مراحلها التحضيرية، من خلال تطوير آليات البحث والتنقيب والتحري بما فيها الآليات المستحدثة بفضل التكنولوجيا الحديثة، فإذا كانت الجرائم الإلكترونية تركب بوسائل تقنية فيجب التصدي لها بالوسائل ذاتها، وهو يتطلب تحسين القدرات البشرية والتقنية للأجهزة الأمنية المعنية بمكافحة هذا النوع من الجرائم[2].

ومتى فّر المجرم خارج حدود الدولة يقف الجهاز الأمني عاجزا، لذا أصبحت الحاجة ماسة إلى وجود تعاون دولي يأخذ على عاتقه القيام بهذه المهمة[3].

---

[1] – عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي، في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع السابق، ص 19– 20. وأنظر أيضا: خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض، 2006، ص 38.

[2] –كمال حطاب، المرجع السابق، ص 386.

[3] –حسين بن سعيد الغافري، المرجع السابق، ص 637.

وتتضح أهمية التعاون الأمني من خلال تبني تكنيك متطور لإجراء التحريات والتحقيقات في مجال مكافحة الجريمة الإلكترونية، باستخدام التكنولوجيا الحديثة في الاتصال مثل الدوائر التلفزيونية، واستخدام أساليب خاصة للتحري والمراقبة، واستحداث قنوات للاتصال، والتنسيق الأمني والقضائي بين الجهات المختصة عن طريق الأقمار الصناعية وشبكة الأنترنت لتبادل المعلومات سريعا، وانتقال القاضي إلى الدول المعنية للتحقيق ولاتخاذ ما يلزم من إجراءات، ليس فقط في مرحلة التحقيق الابتدائي ولكن في مرحلة الحكم أيضا، ومراعاة تنفيذ الأحكام الأجنبية وفقا لضوابط تتفق عليها الدول فيما بينها، من خلال التوفيق بين الإجراءات الجنائية في كل من الدولتين، والاتفاق على معايير موحدة في هذا الشأن، كذلك الاتفاق على كيفية مصادرة الأموال محل الجريمة الإلكترونية عبر الحدود أو إرسال المسجونين.[1]

زيادة على ذلك فإن التعاون الأمني الدولي يؤدي إلى تدعيم فلسفة الدولة الحديثة التي من مظاهرها تحقيق العدالة الاجتماعية ورعاية حقوق الإنسان وتوفير النظم الكفيلة لمنع الجريمة وضبطها، وتقديم مقترفيها للعدالة ومحاكمتهم ، فبدون هذا التعاون لن تستطيع الدولة مواجهة الجريمة الإلكترونية، وضبط الفارين بجريمتهم من دولة إلى أخرى[2].

مما سبق ذكره، يتضح أن التعاون الأمني الدولي يساهم مساهمة كبيرة في انحسار الجريمة الإلكترونية والقضاء عليها، وهو ما يتطلب ضرورة تفاعل الدول فيما بينها و زيادة الجهود في سبيل تشجيع وتفعيل هذا التعاون، بإيجاد وسائل تعاونية في المسائل الأمنية الكفيلة بالوقاية من الجريمة أو باقتفائها وتتبع آثارها في حالة وقوعها.

الفرع الثاني: أسس التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية

بالنظر إلى الطبيعة الخاصة للجرائم الإلكترونية، فإن التعاون الأمني الدولي في سبيل مكافحتها يجب أن يعتمد على آليات متطورة تواكب تطور هذه الجرائم، ويجب أن يتم هذا التعاون الدولي على

[1] – عادل عبد العال ابراهيم خراشي، إشكاليات التعاون الدولي، في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع السابق، ص 21.

[2] – حبيب عباسي، المرجع السابق، ص 522.

أسس معينة تكفل في نهاية الأمر مكافحة هذه الجرائم بصورة بناءة، وعلى هذا فإن التعاون الأمني الدولي في مجال المكافحة والوقاية من الجرائم الإلكترونية يجب أن يقوم على الأسس التالية[1]:

1- التناول العلمي لبحث ظاهرة الجرائم الإلكترونية، وتوفير المعلومات الإحصائية والبيانات اللازمة، سواءا ما يتعلق بالجريمة ذاتها أو ما تعلق بمرتكبيها، أو ما يتعلق بسير نظام القضاء الجنائي حيث أن هذه المعلومات تساعد على التعامل مع الجرائم الإلكترونية بصورة دقيقة وفعالة، وفهم كل أبعاد هذه الجرائم، ولذا يجب إنشاء مركز دولي للمعلومات والبيانات الخاصة بتلك الجرائم على مختلف صورها وأنماطها، بما في ذلك أسماء الجناة والمتورطين معهم، والإجراءات التي اتخذت حيالهم، والتحقيقات التي جرت معهم والأحكام التي صدرت بشأنهم، وذلك حتى يسهل على كافة الدول الرجوع إليها لوضع سياساتها التشريعية والأمنية الكفيلة بمنع انتشار تلك الجرائم، أو الحد من آثارها والوقاية منها.

2- التنسيق بين المؤسسات الأمنية بآلياتها المختلفة في الساحات الأمنية الإقليمية والدولية، بما يحقق حصر معدلات الجريمة، ويحول دون انتشارها واستكمال أي نقص في المعلومات الأمنية، وذلك بالتعاون لتجميع عناصر تلك المعلومات، ليكتمل بها في النهاية كشف أبعاد الجرائم وخطط الإعداد لارتكابها، وإتاحة الفرصة لإمكان دراسة الثغرات الأمنية الدولية في المؤسسات الأمنية لدى الدول الأخرى.

ذلك لأن تبادل المعلومات والخبرات ونتائج البحوث والدراسات بخصوص الجرائم الإلكترونية، يتيح حصر الأساليب والوسائل الجديدة المستخدمة في ارتكاب هذه الجرائم، ويوسع نطاق المعرفة بأنماط المجرمين فيها وأنشطتهم الإجرامية.

3- تحديد سبل التعاون في مجال التدريب والتعاون التقني، وتحقيق التكامل الأمني بين الأجهزة الأمنية على المستوى الدولي.

4- إعداد مدونة دولية تتضمن توحيد المعايير والأركان القانونية التي تقوم عليها هذه الجرائم، ونطاق الأفعال المؤثمة فيها، مع ضمان أن يشكل نطاق التجريم كافة جوانبها ومراحلها.

[1] -سامح أحمد بلتاجي موسى، الجوانب الإجرائية للحماية الجنائية لشبكة الأنترنت، رسالة الدكتوراه في القانون الجنائي، جامعة الإسكندرية، مصر، 2010، ص 524، 525.

5- وضع استراتيجيات وقائية قادرة على خلق المناخ الملائم لأعمال المكافحة وتضييق الخناق على أنشطة تلك المنظمات الإجرامية وحرمانها من البيئة الملائمة لممارسة أنشطتهم الإجرامية، وزيادة الوعي العام لدى الجماهير بنشر كافة المعلومات عن طبيعة هذه الجرائم وأساليب مرتكبيها.

6- القيام ببعض العمليات الشرطية والأمنية المشتركة تدعيما للتعاون و صقلا للمهارات.

كما أن التعاون الأمني بين الدول يجد له أساسا في الاتفاقيات الثنائية أو المتعددة الأطراف، التي تعرب من خلالها الدول عن اقتناعها بأن مصالحها وأهدافها في مجال مكافحة الجريمة، لا يمكن الوصول إليها بالجهود الفردية وأنها تتطلب تعاون مع دولة أخرى من أجل تحقيقها بشكل أفضل على أساس أن التعاون يحقق الأهداف والمصالح المشتركة[1]، وهو ما يتفق تماما مع الجريمة الإلكترونية.

في هذا الصدد عمدت الجزائر إلى عقد اتفاقيات مع بعض الدول من أجل تحقيق تعاون معها في المسائل الأمنية، منها الاتفاق مع إسبانيا، حيث جاء هذا الأخير في سباق المساهمة في تطوير العلاقات الثنائية وتوطيد أواصر تعاونهما في هذا المجال في سياق احترام مبادئ المساواة والمعاملة بالمثل والمساعدة المتبادلة[2].

وحددت الاتفاقية أن انطباقها يكون في مجال مكافحة الإجرام، وتتمثل الجرائم التي يشملها هذا التعاون على ما يلي[3]:

- جرائم الإرهاب.
- الجرائم المرتكبة ضد حياة وسلامة الأشخاص.
- الإتجار والإنتاج والمتاجرة غير المشروعين في المخدرات والمؤثرات العقلية، وكذا الإتجار والإنتاج والمتاجرة غير المشروعين بالسلائف والواد الأولية المستعملة في صنع تلك المخدرات وتلك المؤثرات.

---

[1] - حبيب عباسي، المرجع السابق، ص 523.

[2] -أنظر ديباجة الاتفاقية الجزائرية الديمقراطية الشعبية والمملكة الإسبانية في مجال الأمن ومكافحة الإرهاب والجرام المنظم، الموقعة بالجزائر في 15 جوان 2008، المصادق عليها بموجب المرسوم الرئاسي 08 – 427 المؤرخ في 28 ديسمبر، ج.ر.ج.ج، العدد 05 تاريخ 21 جانفي 2009.

[3] -أنظر المادة 1 من الاتفاقية الجزائرية الديمقراطية الشعبية والمملكة الإسبانية في مجال الأمن ومكافحة الإرهاب والجرام المنظم.

- المتاجرة بالأشخاص والشبكات المرتبطة بالهجرات غير المشروعة.
- الاختطاف وحبس الرهائن وحجز الأشخاص.
- تزوير (إعداد وتغيير) وثائق التعريف ووثائق السفر واستعمالها غير المشروع.
- التهريب.
- تبييض الأموال الصادرة عن نشاطات غير مشروعة.
- تمويل الإرهاب.
- تزوير (إعداد وتغيير) القطع النقدية ووسائل الدفع والشيكات والسندات وتداولها بشكل تدليسي.
- سرقة السيارات و الإتجار غير المشروع فيها والنشاطات غير المشروعة المتعلقة بها.
- سرقة الأسلحة و الذخيرة والمتفجرات والمواد الأولية الإستراتيجية (المعدات النووية والإشعاعية) وإخفائها والمتاجرة غير المشروعة فيها، والمتاجرة غير المشروعة في المواد الخطيرة الأخرى وكذا في البضائع والتكنولوجيا ذات الاستعمال المزدوج.
- سرقة الممتلكات الثقافية والمواد ذات القيمة التاريخية والتحف الفنية وإخفائها والإتجار غير المشروع فيها.
- الجرائم الاقتصادية، بما فيها الجرائم الجبائية.
- الإجرام المنظم في مجال الدعارة، لا سيما التي تمس القصر، إعداد ونشر وتوزيع محتويات إباحية تضم القصر.
- الجريمة عن طريق الأنترنت، وجميع الجرائم الأخرى المرتكبة عن طريق أنظمة الإعلام الآلي.
- الجرائم المرتكبة على حساب الموارد الطبيعية والبيئية».

كما تم التعاون بين الجزائر وفرنسا أيضا في مجال الأمن ومكافحة الإجرام المنظم[1]، نظرا للتهديد الذي يشكله هذا الأخير بكل أشكاله وخدمة لمصلحة البلدين، حيث تم الاتفاق على إقامة تعاون

[1] -أنظر ديباجة الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقع بالجزائر في 25 أكتوبر 2003، المصادق عليه بموجب مرسوم رئاسي رقم 07- 375 مؤرخ في 01 ديسمبر 2007، ج.ر.ج.ج. العدد 77 بتاريخ 9 ديسمبر 2007.

عملياتي وتقني في مجال الأمن الداخلي وتبادل المساعدة[1]، كما تم تحديد المجالات التي يشملها هذا التعاون تحديدا غير حصري فيما يلي[2]:

- « مكافحة الأجرام الدولي المنظم.
- مكافحة الإتجار غير المشروع بالمخدرات والمؤثرات العقلية وسلائفهما الكيماوية.
- مكافحة الإرهاب.
- مكافحة الجرائم ذات الطابع الاقتصادي المادي لاسيما تبييض الأموال.
- مكافحة الإتجار بالبشر.
- مكافحة الإتجار بالأملاك الثقافية والتحف الفنية المسروقة.
- مكافحة التزوير والتزييف.
- مكافحة الهجرة السرية التدليس في الوثائق المتعلقة بها.
- أمن وسائل النقل الجوية والبحرية.
- مكافحة الاحتيالات المرتبطة بتكنولوجيا الإعلام والاتصال الجديدة.
- النظام والأمن العامان.
- تكوين المستخدمين.
- الشرطة الجوارية.
- الشرطة التقنية والعلمية.
- شرطة الاستعمالات.
- تقنيات المتفجرات.
- الاتصالات السلكية واللاسلكية والإعلام الآلي.
- مكافحة الإجرام عن طريق الإعلام الآلي.

يمكن لهذا التعاون أن يشمل مجالات أخرى، متعلقة بالأمن الداخلي عن طريق ترتيبات الوزراء المعنيين المسؤولين عن تنفيذ هذا الاتفاق».

[1] -مختار شبلي، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة، الجزائر، 2013، ص 234.

[2] -أنظر المادة 1 من المرسوم الرئاسي رقم 07 – 375.

وبهذا يمكن القول بأن الدول الأوربية كانت سباقة لوضع أسس للتعاون الأمني فيما بينها، ويرجع السبب في ذلك إلى الظروف التي أملتها الضرورة والواقع، وكذلك إلى الأفكار المشتركة التي كان لها تأثيرا كبيرا في بناء هذا التعاون[1].

وكمثال أيضا عن الاتفاقيات الأوربية التي أشارت صراحة إلى التعاون الأمني الدولي اتفاقية « شنجن» الموقع عليها سنة 1985 بين كل من فرنسا وألمانيا والدول الأطراف في « البونوليكس Bene Lux»، والتي تضمنت إلغاء الحدود بين هذه الدول بفضل الأخذ بأنظمة مشتركة في عدة مجالات، كالتعاون بين أجهزة الشرطة والجمارك.

وحل محل هذه الوثيقة اتفاقية تطبيق اتفاق « شنجن Schengen» الموقع عليها سنة 1990، حيث عالج الباب الثالث منها التعاون الأمني والذي نص على التزام الدول الأطراف بأن تتبادل المساعدة في المسائل الأمنية بهدف الوقاية من الجرائم وتتبعها، وحدد المظاهر التي يتخذها هذا التعاون[2].

الفرع الثالث: صور التعاون الأمني الدولي لمكافحة الجرائم الإلكترونية.

لقد أصبحت الحاجة ماسة إلى وجود كيان دولي يأخذ على عاتقة القيام بهذه المهمة خاصة في مجال تبادل المعلومات و لتعاون الأمني الدولي عدة صور أهمها:[3]

أولا : ربط شبكات الاتصال والمعلومات

تحتاج الاتصالات الشرطية إلى وسائل للاتصال تحقق السرعة الملائمة لتتمكن أجهزة العدالة الجنائية من التواصل بين سلطات التحقيق والملاحقة المختلفة، لذا عمدت الدول والمنظمات الدولية إلى تطوير الاتصال وتبادل المعلومات فيما بينها.

[1] - مختار الشبلي، المرجع السابق، ص 183.

[2] - V.Art 39 au 47, convention d'application de l'accord de schengen (19 juin 1990).

[3] - عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي، في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع السابق، ص 24.

ثانيا : تبادل المعاونة لمواجهة الكوارث والأزمات والمواقف الحرجة

تتعرض كافة دول العالم لاحتمالات وقوع كوارث ضخمة وأحداث مفاجئة بشكل لا يمكن توقعه، أو يستحيل التنبؤ بتوقيت حدوثه، أو يصعب معه مواجهته بالإمكانيات القومية للدولة التي تعرضت للكارثة بمفردها ومع وقوع مثل هذه الكوارث أو اللازمات أو المواقف الحرجة غالبا ما يكون عنصر الوقت من الأمور الحاسمة في المواجهة، الأمر الذي يحتاج إلى تكثيف خاص للجهود والخبرات والإمكانيات بشكل يصعب تحقيقه إلا بتظافر الجهود الدولية.[1]

وهذه الصورة من صور التعاون الأمني تعد من اهم الصور في مجال مكافحة الجرائم الإلكترونية لاسيما وان أجهزة العدالة الجزائية ليست بنفس المستوى والجاهزية في جميع الدول، وإنما هناك تفاوت فيما بينها، فبعض الدول متقدمة تقنيا وتكنولوجيا ولها نصيب كبير في مواجه الجرائم الإلكترونية تشريعيا وفنيا، والبعض الأخر يفتقد ذلك، من هنا كان لابد من التعاون بين الدول.

ثالثا: القيام ببعض العمليات الشرطية والأمنية المشتركة

تعقب مجرمي المعلوماتية عامة وشبكة الأنترنيت خاصة، وتعقب الأدلة الإلكترونية وضبطها والقيام بعملية التفتيش العابر للحدود لمكونات الحاسب الآلي المنطقية والأنظمة الإلكترونية وشبكات الاتصال بحثا عن ما قد تحويه من أدلة وبراهين على ارتكاب الجريمة الإلكترونية، كلها أمور تستدعي القيام ببعض العمليات الشرطية والفنية والأمنية المشتركة، والتي من شأنها تساعد في تحفيز مهارات وخبرات القائمين على مكافحة تلك الجرائم، وبالتالي وضع حد لها[2].

الفرع الرابع: جهود المنظمة الدولية للشرطة الجنائية (الإنتربول) في مجال التعاون الأمني:

تسعى منظمة الإنتربول إلى الوصل بين أجهزة الشرطة لجعل العالم أكثر أمانا، وتشجيع التعاون بين أجهزة الشرطة في الدول الأطراف وعلى نحو فعال في مكافحة الجريمة وضبط المجرمين وجمع البيانات والمعلومات المتعلقة بالمجرم والجريمة وتتبادلها فيما بينها، وذلك من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في الدول الأعضاء، كما تسعى مساعدة أجهزة الشرطة في الدول

[1] -حسين بن سعيد الغافري، المرجع السابق، ص 641-642.

[2] -سليمان أحمد فضل، المرجع السابق، ص 415.

الأطراف ودعمها وتحسين قدراتها باستمرار لمنع الإجرام ومحاربته وتطوير المعارف والمهارات اللازمة لعمل أجهزة الشرطة على الصعيد الدولي بشكل أكثر فاعلية.[1]

وبهدف توصيل اتصال فعال وآني بين أجهزة الشرطة في مختلف الدول على نحو يمكنها من تبادل المعلومات بشكل آمن وسريع، قامت منظمة الإنتربول بوضع منظومة عالمية للاتصالات الشرطية المأمونة لتوفير الاتصال بين موظفي إنفاد القانون في جميع الدول الأعضاء على نحو يمكن مستخدمي هذه المنظومة من تبادل المعلومات والبيانات الشرطية الهامة فيما بينهم والاطلاع على قواعد بيانات الإنتربول والحصول على خدماته على مدار الساعة.[2]

وقد أحدثت منظومة الاتصال تلك تطويرا جذريا على صعيد عمل أجهزة الشرطة في الدول الأعضاء إذ تمكن المحققون من الوصول إلى أدوات الإنتربول المتطورة ومن الربط بين معلومات قد تبدوا غير متصلة فيما بينها، مما ييسر بالتالي التحقيقات في الجرائم، فضلا عن أن منظومة الاتصال تلك تمكن أجهزة الشرطة وجهات إنفاذ القانون من تقصي البيانات ومقارنتها في ثواني معدودة، وذلك من خلال وصولهم المباشر إلى قواعد البيانات المتعلقة بالمجرمين المشبوهين أو بالأشخاص المطلوبين[3].

يمكن القول في هذا الصدد، أن هذه المنظومة تعد من إحدى المتطلبات الأساسية لمكافحة الجرائم الإلكترونية، التي تتطلب مثل هذا النوع من السرعة في تقفي الأثر وتبادل المعلومات حول الأجهزة مصدر الهجمات الإلكترونية ومستخدميها، بين أجهزة الشرطة في جميع الدول.

ومن الأمثلة على دور الإنتربول فيما يتعلق بالجرائم الإلكترونية، قيام القضاء اللبناني بتوقيف أحد الطلبة الجامعين في لبنان بتهمة إرسال صور إباحية القاصرة دون العشرة أعوام من موقعة على شبكة الأنترنت، وذلك إثر تلقي النيابة اللبنانية برقية من الإنتربول في ألمانيا بهذا الشأن[4].

---

[1] -محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية، الطبعة الأولى، دار الفكر والقانون، 2015، ص 131- 132.

[2] -محمد كمال محمود الدسوقي، المرجع نفسه ص 132. وأنظر أيضا: فهد عبدالله العبيد العازمي، المرجع السابق ، ص 519.

[3] -محمد كمال محمود الدسوقي، المرجع نفسه، ص 132.

[4] -كمال حطاب، المرجع السابق، ص 390.

ومن بين الإنجازات التي حققها الإنتربول في ظل مواجهته للجرائم الإلكترونية تلك العملية التي قامت بها المباحث الفيدرالية الأمريكية بالاشتراك مع الإنتربول والمتعلقة بنشر دودة الحب Love Buj عبر الأنترنت في الفلبين[1].

كذلك العملية التي قامت بها شرطة الإنتربول بالاشتراك مع الباحث الفيدرالية وكذا الشرطة الإنجليزية والتي أحرزت فيها إنجازات كبيرة سنة 1998 والمعروفة بعملية"Cathedral"، حيث حققت من خلالها تفكيك موقع منشور عليه أكثر من 75.000 صورة سلبية لدعارة الأطفال، وكذا القبض على 107 شخص في 12 دولة[2].

يتضح مما سبق ذكره، أن مواجهة الجريمة الإلكترونية ليست مهمة أجهزة الأمن فقط، فإثارة الوعي العام بخطورة الجرائم الإلكترونية وانتشارها يعد من أهم الأهداف الأساسية في مواجهة تلك النوعية من الجرائم المستحدثة، وشرح أهدافها وأبعادها وأساليب عملها وإعطاء فكرة مفصلة وواضحة لجميع دول العالم مما ترمز إليه وتستهدفه من تدمير للمؤسسات سواء الاجتماعية أو الاقتصادية أو السياسية، والتأثير على عمل وفاعلية نظم العدالة الجنائية، ثم يأتي دور الأجهزة الأمنية التي يجب أن تكون على أعلى درجة من الاستعداد والتدريب[3]والخبرة للمواجهة الفعالة والمؤثرة، فجهاز الأمن هو خط الدفاع الأخير في مواجهة الخطر المعلوماتي، خاصة وأن الثقافة القانونية للعديد من الدول لا تعترف بوضوح لهذا النوع من الجرائم التقنية بوصفها خطرا محدقا يهدد المجتمعات الإنسانية كلها دون استثناء.

المطلب الثاني: التعاون القضائي الدولي في الجرائم الإلكترونية

ليس التشريع هو الأداة المنفردة للتعاون بين الدول في مكافحة الجريمة الإلكترونية، ولكن السلطة القضائية يمكن أن تقوم بدور فعال في هذا الصدد، والتعاون القضائي ينبع من الضرورة ذاتها التي ينبع منها التعاون التشريعي.

[1] -عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي، في مكافحة الجرائم المعلوماتية وسبل التغلب عنها، المرجع السابق، ص 28.

[2] - عادل عبد العال إبراهيم خراشي، المرجع نفسه، نفس الصفحة.

[3] -تم التطرق إلى عنصر التدريب تحت عنوان: اعتماد نظام التدريب لتفعيل التحقيق في الجريمة الالكترونية، في المطلب الثاني من المبحث الثاني في الفصل الأول من الباب الثاني.

ففي غالب الأحيان يتعدى أثر الجرائم الإلكترونية حدود الدول فقد يكون مرتكب الهجوم في بلد ما ويتم شن الهجوم من حواسيب موجودة في بلد آخر وتقع الآثار المترتبة على ذلك في بلد ثالث، وقد يرتكب المجرم جميع مراحل جريمته في دولة لم تطأها قدما أصلا من قبل، لذا تقتضي فعالية التحقيق والملاحقة القضائية تتبع أثر النشاط الإجرامي من خلال تقصي أثر قناة الاتصالات بالحاسبات مصدر الهجوم وحاسوب الضحية أو بأجهزة أخرى تعمل مع مقدمي خدمات الأنترنت في دول مختلفة[1].

لتحديد مصدر الجريمة غالبا ما يتعين على أجهزة التحقيق الاعتماد على السجلات التاريخية التي تبين متى أجريت تلك التوصيلات ومن أين ومن الذي أجراها.[2]

وفي أحيان أخرى قد يتطلب إنفاذ القانون تتبع اثر التوصيل ووقف إجراءاته، وقد يكون ذلك خارج نطاق الولاية القضائية للمحقق وهو ما يحدث غالبا، فان أجهزة إنفاذ القانون تكون بحاجة إلى مساعدة من نظرائها في ولايات قضائية أخرى بمعنى الحاجة إلى ما يسمى بالتعاون القضائي، فالدول لا تتجاوز حدود سلطاتها ويمتنع عليها القيام بأي عمل قضائي أو إجراء جزائي في دولة أخرى.

ويقصد بالتعاون القضائي بين الدول:" ما تقدمه سلطات دولة لدولة أخرى من مساعدة وعون في سبيل ملاحقة الجناة بهدف عقابهم على جرائمهم، وذلك من خلال تدابير وقائية تستهدف مواجهة الصيغة غير الوطنية للجريمة وتستجمع الأدلة بمختلف الطرق، وهو ما يستغرق وقتا ويتطلب إمكانات لا تملكها سلطات قانونية لدولة واحدة ما لم تدعمها وتساندها جهود السلطات القانونية في الدول الأخرى[3]."

ويقصد به أيضا:" التعاون الواقع بين السلطات القضائية لمختلف الدول في سبيل كشف الجريمة وضبط مقترفيها وإخضاعهم للجزاء المستحق عن ارتكابهم لها[4]."

---

[1] -محمد كمال محمود الدسوقي، المرجع السابق، ص 142.

[2] -فهد عبد الله العبيد العازمي، المرجع السابق، ص 506.

[3] -ابو المعالي محمد عيسى، المرجع السابق، ص 02.

[4] -هدى حامد قشقوش، الجريمة المنظمة ، الطبعة الاولى، الدار العلمية الدولية ودار الثقافة للنشر والتوزيع، عمان، الاردن، 2011، ص 85.

كما يعرّف أيضا : "على أنه تعاون السلطات القضائية في الدول لمكافحة الجريمة الإلكترونية بهدف إجراء العمل القضائي فوق أراضيها[1]."

والتعاون القضائي في مجال الجريمة الإلكترونية يتجلى في الأساس في المساعدة القضائية(الفرع الأول)، والإنابة القضائية(الفرع الثاني) والتحقيقات المشتركة (الفرع الثالث).

الفرع الأول: المساعدة القضائية المتبادلة في مجال الجرائم الإلكترونية

تعد المساعدة القضائية المتبادلة واحدة من أهم مظاهر التعاون الدولي[2] في مكافحة الجريمة بصفة عامة، والجريمة الإلكترونية بصفة خاصة، وأكثرها فعالية في مجال تعقب مرتكبي الجرائم وملاحقتهم والقبض عليهم ومحاكمتهم و إنزال العقاب بهم.

ففيما مضى كان التعاون القضائي بين الدول محدودا لعدة أسباب أبرزها تعقيدات وبطء إجراءات تبادل المساعدة القضائية التقليدية وعدم فاعليتها، فقد يستغرق اتخاذ الإجراءات شهورا، الأمر الذي لا يتناسب مع ضرورة توخي السرعة في التعامل مع الأدلة الإلكترونية غير الملموسة وسريعة الزوال هذا من جهة.

ومن جهة أخرى قد يؤدي غياب المساعدة القضائية المتبادلة أو بطئها، إلى ان يجري المحققون في إحدى الدول التي تسعى إلى الحصول على المعلومات في حواسيب موجودة في دولة أخرى عمليات بحث عابرة للحدود هي الأخرى غير مرخص لها في النظم الحاسوبية.

لذا فانه لابد من اعتماد آليات للتعاون وتبادل المساعدة تتلاءم مع طبيعة الجرائم الإلكترونية تمكن المحققين في تلك الجرائم من الحصول على المعلومات بصورة عاجلة.

---

[1] -هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والاجرائية والتعاون الدولي، دار النهضة العربية، 2000، ص 85.

[2] -يعرف التعاون الدولي بأنه: "تبادل العون والمساعدة بين الدول وكذلك بين الدول والمحاكم الجنائية الدولية، والمنظمات الدولية، لتحقيق نفع مشترك على المستوى الوطني والدولي لمكافحه الجريمة، والقبض على مرتكبيها ومحاكمتهم وتوقيع العقوبات الرادعة عليهم بما يتناسب وجسامة الجريمة المرتكبة وما يرتبط به من مجالات أخرى كالعدالة الجنائية وتخطي مشكلات الحدود والسيادة وتحقيق الأمن وتعقب مصادر التهديد." أنظر: فاطمة محمد العطوي، المرجع السابق، ص 30 -31.

فالجريمة الإلكترونية وصفت بأنها جريمة عابرة للحدود نظرا لتجاوزها حدود الدولة الواحدة وهو ما من شانه أن يحدث واقعا يفرض التعاون بين السلطات القضائية للدول، بهدف استخلاص أدلة الإثبات التي يمكن استعمالها في إدانة مرتكبي هذه الجريمة المستحدثة.

وعليه فإن مكافحة هذه الجريمة لن تكون فعالة بعيدا عن المساعدة القضائية المتبادلة والتي تعد وسيلة حتمية في ذلك، ويرجع السبب في ذلك إلى أنها تتوزع في الغالب عبر أقاليم عدة دول مما يؤدي إلى تشتت الأدلة التي يمكن أن تستند عليها الدولة التي تنظر في هذه الجريمة وهو ما يحول دون الوصول إلى الحقيقة، وبالتالي يجد القضاء نفسه أمام فرضيتين إما معاقبة أشخاص بدون كفاية دليل الإدانة وهذا ما يشكل خرقا لمبدا المشروعية الجزائية، وإما اطلاق صراح أشخاص بعدم ثبوت الإدانة رغم ضلوعهم في هذه الجريمة.

ودراسة موضوع المساعدة القضائية المتبادلة يقتضي التطرق إلى تعريفها وذكر صورها ومجالاتها الخاصة وإجراءتها لمواجهة الجريمة الإلكترونية .

أولا: تعريف المساعدة القضائية المتبادلة:

تعرف المساعدة القضائية المتبادلة[1] بأنها: " كل إجراء قضائي تقوم به دولة من شانها تسهيل مهمة المحكمة في دولة أخرى بصدد جريمة من الجرائم"[2].

وتعرف أيضا: "قيام سلطة قضائية مختصة تابعة لدولة أجنبية باتخاذ إجراء أو أكثر من إجراءات التحقيق، وذلك لحساب سلطة قضائية مختصة تابعة لدولة أخرى من اجل الوصول إلى كشف الحقيقة في قضايا جنائية"[3].

---

[1]– أطلق المشرع الجزائري على المساعدة القضائية المتبادلة مصطلح المساعدة القضائية الدولية وذلك في إطار قانون رقم 09-04.

[2] –عادل عبد العال ابراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، المرجع السابق، ص 30. وأنظر أيضا: سالم محمد سليمان اوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1997، ص 425.

[3] –علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، رسالة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، 2011، ص 296.

يتضح من خلال التعريف السابق أن المساعدة القضائية المتبادلة تقوم على فكرة التنسيق بين السلطات القضائية التابعة لدولتين على الأقل وذلك من أجل اتخاذ إجراءات التحقيق المتطلبة في دولة ليست هي الدولة الناظرة في الجريمة بسبب أن أركان الجريمة امتدت لتشمل هاتين الدولتين وذلك من اجل ضمان إخضاع مقترفي هذه الجريمة إلى محاكمة عادلة.

والمساعدة القضائية لا تتحقق إلا من خلال خطوات ثلاث هي :[1]

1- الطلب: وتقدمه الدولة صاحب الاختصاص الجنائي بالمحاكمة، ويخضع هذا الطلب لقانون الدولة الطالبة وفي نطاق الاتفاقية التي تعقدها مع الدولة التي ستقدم المساعدة، ويتم تقديم الطلب بالطرق الدبلوماسية بحسب الأصل، ومع ذلك فان بعض الاتفاقيات الدولية تسمح بالاتصال المباشر بين جهات العدل في الدولتين كسبا للوقت.

2- فحص الطلب: وتقوم به الدولة التي ستقدم المساعدة، ويتم ذلك عن طريق التحقق من اعتبار الواقعة المطلوب تحقيقها تعد جريمة وفقا لقانون الدولة الطالبة، وفي ضوء مدى اختصاص الدولة المطلوب منها إجابة هذا الطلب وفقا لنصوص الاتفاقية التي تعقدها مع الدولة الطالبة.

3- تنفيذ المساعدة القضائية: ويتم وفقا لقواعد الدولة المطلوب منها المساعدة، فالإجراء يتم وفقا لقانون الدولة التي تنفذه.

و الاتفاقيات الدولية هي وحدها الأداة التي يمكن ان تنبع عنها الالتزامات بين الدول، ومن تم فانه بدون الاتفاقية الدولية وخارج الشروط التي تنص عليها لا يمكن للدولة أن تعتمد على مساعدة الدولة المطلوب منها على ان كل ما ليس ملزما يظل مع ذلك ممكنا وفقا لما ينص عليه القانون الداخلي في كل من الدولتين.

ثانيا: صور المساعدة القضائية المتبادلة

تتخذ المساعدة القضائية الصور التالية: تبادل المعلومات و نقل الإجراءات:

[1] -سليمان أحمد فضل، المرجع السابق، ص 421. وأنظر أيضا: عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 31-32.

1- تبادل المعلومات:

من أهم العناصر المتعلقة بالوقاية من الجريمة تبادل المعلومات والخبرات، إذ أن تقاسم المعلومات وسرعة الحصول عليها يعمل على تسهيل مهمة الأجهزة الوطنية في التحرك المناسب لمواجهة الجريمة.

لهذا يولي المجتمع الدولي تبادل المعلومات أهمية قصوى بوصفه وسيلة لمكافحة الإجرام عموما والجريمة الإلكترونية خصوصا، لما توفره المعلومات الصحيحة والموثوقة من مساندة لأجهزة تنفيذ القوانين في كافة المجالات بما في ذلك متابعة نشاط المنظمات الإجرامية، ومصادر الأموال في كافة المجالات، لذلك أوصى مؤتمر الأمم المتحدة السادس لمنع الجريمة ومعاملة المجرمين، بتطوير التبادل المنهجي للمعلومات بوصفه عنصرا رئيسيا من عناصر خطة العمل الدولية لمنع الجريمة ومكافحتها، وأوصى بأنه على منظمة الأمم المتحدة ان تنشئ قاعدة معلوماتية لإعلام الدول الأطراف بالاتجاهات العالمية في مجال الجريمة.

وهكذا ينبغي للتعاون في المسائل المتعلقة بالجريمة الإلكترونية أن يدعم بتوظيف نظم تبادل المعلومات بين الدول الأعضاء، وتقديم المساعدة التقنية الثنائية والمتعددة الأطراف إلى الدول الأعضاء باستخدام التدريب على تنفيذ القوانين والمعاهدة المتعلقة بالعدالة الجنائية على الصعيد الدولي[1]

وتبادل المعلومات يمكن أن يتحقق من خلال المنظمات والهيئات الدولية، ويشمل تبادل المعلومات والبيانات والوثائق والمواد الاستدلالية التي تطلبها سلطة قضائية أجنبية وهي بصدد النظر في جريمة ما، عن الاتهامات التي وجهت إلى رعاياها في الخارج والإجراءات التي اتخذت ضدهم وقد يشمل التبادل السوابق القضائية للجناة[2]

وتتضح أهمية التعاون الفعال بين الدول في سرعة تبادل المعلومات أو المساعدة في الحالات التي يعتقل فيها المجرمون ثم يطلق سراحهم لعدم ورود المستندات من دولة أخرى[3].

[1] -عزيز رابحي، الأسرار المعلوماتية وحمايتها الجزائية، المرجع السابق، ص 331.

[2] -عادل عبد العال ابراهيم الخراشي، المرجع السابق، ص32.

[3] -فهد عبد الله العبيد العازمي، المرجع السابق، ص532.

وتبرز أهمية تبادل المعلومات من التعاون في ميدان مكافحة الجرائم الإلكترونية التي يلجأ مرتكبيها إلى التخفي على الشبكات الإلكترونية خلف شخصيات وهمية وأسماء مستعارة، وهو ما يتطلب تعاونا بين الدول خاصة في حالة توزع النشاط الإجرامي بين أكثر من دولة، لتحديد هويه الأشخاص المشتبه في ضلوعهم في تلك الجرائم وتحديد أماكن وجودهم تمهيدا للقبض عليهم فضلا على أن تبادل الدول المعلومات بالنسبة للوسائل والأساليب التي يستخدمها مرتكبي تلك الجرائم في ارتكاب جرائمها والتي تتسم تلك الوسائل والأساليب بالتطور السريع والمستمر يسهل من مهمة التصدي لتلك الجرائم ويجب ان يتم تبادل المعلومات بشكل اكثر سرعة دون انتظار عقد اجتماعات ومؤتمرات.

حيث انه بالإمكان إصدار نشرة دورية شهرية مثلا تتضمن احدث الوسائل والأساليب في مجال الجرائم الإلكترونية على ان يتم تبادلها على مستوى الدول إما بطريقة مباشرة من دولة لدولة أو من خلال المنظمات الدولية أو الإقليمية والتي بدورها تقوم بتعميمها على الدول الأعضاء أو بطرحها على المواقع الإلكترونية الخاصة بها أو عقد الاجتماعات عن بعد بواسطة الشبكات ومناقشة تلك الخبرات.[1]

حيث تقتبس هذه الفكرة من مجرمي المعلومات ذاتهم الذين لا يدخرون جهدا ولا يقتصرون في تبادل خبراتهم في مجال الاختراق والتجسس المعلوماتي سواء من خلال مؤتمراتهم عبر شبكات الأنترنيت ومن خلال منتدياتهم المخصصة لهذا الغرض.

وفي هذا المجال تم تقديم معلومات في قضية القرصنة الإلكترونية، حيث تلقت السلطات الجزائرية شهر جويلية 2009 معلومات من سفارة ألمانيا بالجزائر مفادها أن مصالح الشرطة الألمانية اكتشفت بأن شخصا ما قام بتاريخ 30 جوان 2009 على الساعة الثامنة وخمسون دقيقة مساء باختراق قاعدة بيانات متواجدة بميونخ بألمانيا وقام بتحميل البيانات الرقمية الخاصة ب 15000بطاقة ائتمان باستعمال عنوان إلكتروني.

وبتاريخ 21 أكتوبر من نفس السنة تلقى كذلك مكتب الانتربول بالجزائر مراسلة من مكتب الانتربول بكندا مفادها أن مصالح شرطة كيبك Québec تمكنت خلال العام الماضي من القبض على شبكة إجرامية مختصة في القرصنة الالكترونية بتحميل المعطيات الرقمية المتبادلة بين الزبائن والبنك وتحويل الأموال من حسابات بنكية.

[1] -محمد كمال محمد دسوقي، المرجع السابق، ص 148-149.

على اثر هذه المعلومات تمكنت المديرية العامة للأمن الوطني من إلقاء القبض على المتهم وهو شاب جزائري وتقديمه للعدالة بتهمة القرصنة الإلكترونية المرتكبة بحق مراكز معطيات الكترونية أجنبية متواجدة بكل من ألمانيا، كندا وصدر بحقه حكم رقم 10/37560 من محكمة عنابة بتاريخ 28 جوان 2010 [1].

2- نقل الإجراءات:

يقصد بنقل الاجراءات قيام إحدى الدول بناءا على اتفاقية أو معاهدة باتخاذ إجراءات جنائية وهي جريمة ارتكبت في إقليم دولة أخرى ولمصلحة هذه الدولة متى ما توافرت شروط معينة. من أهمها التجريم المزدوج ويقصد به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة والدولة المطلوب اليها نقل الإجراءات، بالإضافة إلى شرعية الإجراءات المطلوب اتخاذها بمعنى أن تكون الإجراءات المطلوب اتخاذها مقررة في قانون الدولة المطلوب اليها عن ذات الجريمة. وأيضا الشروط الواجب توافرها أن تكون الإجراءات المطلوب اتخاذها من الأهمية بمكان بحيث تؤدي دورا مهما في الوصول إلى الحقيقة[2].

ويمكن إعمالا للقواعد المقررة أن تلتمس الدولة الطالبة من الدولة المطلوب منها المساعدة القضائية نقل الإجراءات وهي القضية التي فصل فيها مجلس قضاء باتنة بتاريخ 4 جويلية 2010 بموجب قرار رقم 10/05805 وذلك إثر إرسالية صادرة من زارة العدل الأمريكية (المكتب الفيدرالي للتحقيقات) مفادها تعرض النظام المعلوماتي لشركة أميريكية متخصصة في حماية المعلومات والبرامج الإلكترونية تسمى Sago net Work إلى الاختراق واستغلال تلك المعلومات لصالح شركات منافسة مقابل مبالغ مالية من طرف شاب جزائري وهو تقني سامي بالإعلام الآلي المتهم بتهمتي التواجد غير المشروع في الأنظمة المعلوماتية والتعامل مع معطيات غير مشروعة[3].

---

[1]- حكم غير منشور رقم 10/37560 صادر عن محكمة عنابة بتاريخ 2010/06/28. نقلا عن عصماني ليلى، صهيب سهيب غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، مجلة القانون، المجتمع والسلطة، المجلد 9، العدد 2، جامعة وهران، 2020، ص 30.

[2] -يوسف حسن يوسف، المرجع السابق، ص 151. وأنظر أيضا: حسين بن سعيد الغافري، المرجع السابق، ص645-646.

[3]- قرار غير منشور رقم 10/05580، صادر عن مجلس قضاء باتنة بتاريخ 04 جولية 2010. نقلا عن عصماني ليلى، صهيب سهيب غازي زامل، المرجع السابق، ص 29.

ثالثا: مجالات المساعدة القضائية الخاصة بمواجهة الجرائم الإلكترونية:

لا تزال العديد من الإجراءات الواردة باتفاقات المساعدة القضائية المتبادلة القائمة تتسم بنوع من التعقيد والبطء والذي لا يتناسب مع الطبيعة السريعة للجرائم الإلكترونية، لدى لابد من استحداث وسائل أخرى للتعاون أكثر فاعلية للتصدي للجرائم الإلكترونية.

ولهذا سوف نتحدث عن تلك المجالات في ضوء الاتفاقيات الخاصة بالجرائم الإلكترونية مثل اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001 ، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010. كما سنتحدث عن هذه المساعدة القضائية المتبادلة وفقا للتشريعات الداخلية المقارنة .

1- مجالات المساعدة القضائية المتبادلة في مجال الجريمة الإلكترونية وفقا للاتفاقيات الدولية:

تتنوع وتتعدد مجالات المساعدة القضائية المتبادلة في مجال مكافحة الجريمة الإلكترونية وعادة ما ترد هذه المجالات ضمن الاتفاقيات الدولية التي أبرمت لغرض مكافحتها مثل اتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001 ، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات المنعقدة في القاهرة سنة 2010.

أ. المساعدة القضائية المتبادلة وفقا لاتفاقية بودابست المتعلقة بالجريمة الإلكترونية لسنة 2001:

نصت المادة 25 من الاتفاقية على ما يلي:[1]

(1- يجب على الأطراف ان توفر لبعضها البعض مساعدة قضائية متبادلة إلى اقصى مدى ممكن لأغراض التحقيقات أو الإجراءات بالنسبة للجرائم الجنائية المرتبطة بنظم وبيانات معلوماتية أو بغرض جمع الأدلة الإلكترونية للجريمة الجنائية.

[1] - عبد الرحيم بن بوعيدة، ضياء علي احمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع السابق، ص 317.

2- يجب على كل طرف أيضا، ان يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية للوفاء بالالتزامات المنصوص عليها في المواد 27 إلى 35.

3- يمكن لكل طرف، في حالة الاستعجال، أن يقدم طلبا للمساعدة المتبادلة أو اتصالات عن طريق وسائل سريعة كالفاكس أو البريد الإلكتروني وذلك لما تقدمه هذه الوسائل من شروط كافية للأمن والتوثيق (بما في ذلك التشفير لو كان ضروريا)، مع التأكيد الرسمي اللاحق حينما يكون ذلك مطلوب بواسطة الدولة الموجه اليها الطلب، ويجب على الدولة المقدم الطلب ان توافق وأن ترد على الطلب المقدم اليها عن طريق أية وسيلة من الوسائل العاجلة للاتصال.

4- باستثناء ما يرد مخالفا ذلك صراحة في مواد هذا الفصل، فإن المساعدة المتبادلة تخضع للشروط المحددة عن طريق القانون الداخلي للطرف الموجه إليه الطلب أو عن طريق الاتفاقات المطبقة للمساعدة المتبادلة، بما في ذلك الأسباب التي بناء عليها يمكن للطرف الموجه إليه الطلب أن يرفض التعاون .يجب على الطرف الموجه إليه الطلب ألا يمارس حقه في رفض المساعدة القضائية المتبادلة بالنسبة للجرائم المنصوص عليها في المواد من 2 إلى 11 من الاتفاقية، فقط إذا كان الباعث على تقديم الطلب يتصل بجريمة ذات طبيعة مالية.

5- عندما يسمح وفقا لبنود هذا الفصل، للطرف المقدم اليه الطلب ان يخضع المساعدة المتبادلة لوجود تجريم مزدوج (مشترك)، فإن هذا الشرط يعتبر مستوفيا إذا كان السلوك المكوّن للجريمة في الطلب المقدم للطرف المطلوب منه المساعدة، يوصف بأنه جريمة جنائية في قانونه الداخلي قد صنفه في نفس طائفة الجرائم أم لا، وسواء تم تجريده بنفس المصطلح الذي نص عليه قانون الطرف الملتمس أم لا."

كما تضمنت هذه الاتفاقية المساعدة القضائية المتبادلة في مجال الإجراءات الوقتية والعاجلة وتشمل ما يلي:

- **التحفظ العاجل على بيانات الحاسب المخزنة:**

تناول هذا الإجراء المادة 29 من الاتفاقية والتي تنص على أنه:[1]

[1] - عبد الرحيم بن بوعيدة، ضياء علي احمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع السابق، ص 324.

(1- يمكن لأي طرف أن يطلب من طرف آخر أن يأمر أو يرفض بطريقة أخرى التحفظ على البيانات المخزنة بواسطة نظام معلوماتي يوجد داخل أراضي ذلك الطرف، والتي بخصوصها ينوي الطرف الملتمس أن يرسل طلبا للمساعدة المتبادلة من أجل تفتيش هذه البيانات أو الوصول اليها، أو ضبطها أو الحصول عليها ، أو إفشاء سريتها .

2-طلب التحفظ على البيانات المقدم تبعا للفقرة الأولى يجب أن يحدد:

أ. السلطة التي تطلب التحفظ.

ب. الجريمة محل التحقيق الجنائي مع ملخص للوقائع المتصلة بها.

ج. البيانات المعلوماتية المخزنة الواجب التحفظ عليها وطبيعة علاقتها مع الجريمة.

د. أية معلومات متوافرة تسمح بتحديد هوية البيانات المعلوماتية المخزنة أو موقع النظام المعلوماتي.

هـ. ضرورة إجراء التحفظ.

و. من واقع أن هذا الطرف ينوي إرسال طلب للمساعدة المتبادلة من أجل تفتيش هذه البيانات أو الوصول اليها أو ضبطها أو الحصول عليها، أو إفشاء سريتها.

3- عند تلقي الطلب من الطرف الملتمس، يجب على الطرف المقدم إليه الطلب أن يتخذ كافة الإجراءات اللازمة من اجل التحفظ بشكل عاجل على البيانات المحددة، طبقا لقانونه الداخلي، ومن اجل تلبية مثل هذا الطلب، فان التجريم المزدوج (أي اعتبار فعل جريمة من كلا الطرفين) لا يعد شرطا مسبقا لهذا التحفظ.

4- أي طرف يشترط التجريم المشترك كشرط لتلبية طلب المساعدة المتبادلة من أجل تفتيش البيانات أو الوصول اليها أو ضبطها أو الحصول عليها أو إفشاء سريتها، بمقدوره فيما يتعلق بجرائم أخرى غير تلك المشار اليها في المواد من 2-11 من هذه الاتفاقية ان يحتفظ بحقه في رفض طلب التحفظ على البيانات تبعا لهذه المادة، في الحالات التي يكون فيها سبب معقول للاعتقاد أنه في لحظة إفشاء سرية هذه البيانات، فإن شرط التجريم المزدوج لم يكن قد تم الوفاء به.

5- علاوة على ذلك يمكن رفض طلب التحفظ على البيانات فقط إذا كان:

أ- الطلب يتعلق بجريمة يعتبرها الطرف المقدم اليه الطلب جريمة سياسية، أو جريمة تتصل بجريمة ذات طبيعة سياسية.

ب-إذا كان الطرف المقدم اليه الطلب يعتقد أن تلبية الطلب قد يمس سيادته، أو أمنه، أو نظام العام، أو مصالح أخرى جوهرية.

6- إذا كان الطرف المقدم اليه الطلب يعتقد أن مجرد التحفظ لا يكفي من أجل ضمان التوافر المستقبلي للبيانات، أو انه سيلحق به ضررا بأية صورة كانت، فعليه ان يخطر على الفور الطرف الملتمس بذلك، والذي بمقدوره عندئذ ان يقرر ما اذا كان يجب المضي قدما في تنفيذ الطلب من عدمه

7- كل تحفظ على البيانات يتم بمقتضى طلب مشار اليه في الفقرة الأولى من هذه المادة يصبح صالحا لمدة 60 يوم على الأقل، حتى يتسنى للطرف الملتمس عرض طلب التنقيب عن البيانات أو الوصول اليها أو ضبطها أو الحصول عليها أو كشف سريتها، وبعد تلقي مثل هذا الطلب، يجب الاستمرار في التحفظ على البيانات حتى يتم اتخاذ قرار بشأنه.)

إن المساعدة المتبادلة في التحفظ العاجل على البيانات المخزنة في النظام المعلوماتي المنصوص عليها في المادة السابقة، هو أمر ضروري تستلزمه طبيعة الأدلة في الجرائم الإلكترونية، وذلك لتفادي أي تغيير في هذه الأدلة أو نقلها أو إتلافها ومحو أثار الجريمة، خلال المدة التي تستغرقها إجراءات طلب المساعدة القضائية المتبادلة للحصول على تلك البيانات بالطرق التقليدية.

وعملية التحفظ هي إجراء ذو طبيعة وقتية للتدخل بطريقة أكثر سرعة من مجرد تنفيذ التماس أو طلب المساعدة المتبادلة التقليدية، بالإضافة إلى ما يتميز به هذا الإجراء من سرعة، فانه يعد أقل تدخلا حيث أن هذا الإجراء لا يتطلب من سلطات الدولة الموجه اليها طلب المساعدة نزع البيانات من الجهة القائمة عليها والاستحواذ عليها، وإنما مضمون هذا الإجراء ان تقوم تلك السلطات باتخاذ الإجراءات التي تضمن ان الجهة التي بحوزتها المعلومات موضوع طلب المساعدة والتي غالبا ما تكون هذه الجهة هي مزود الخدمة أو شخص ثالث، لا تقوم بمحو هذه البيانات لحين صدور امر بتحويلها إلى سلطات إنفاذ القانون في وقت لاحق.[1]

[1] - محمد كمال محمود الدسوقي، المرجع السابق، ص 157-158.

كما يتسم هذا الإجراء بأنه ليس فيه مساس بسرية المعلومات والبيانات محل الإجراء الوقتي موضوع الطلب، فلا يتم كشفها ولا فحصها من قبل سلطات إنفاذ القانون إلا في بعض الحالات ووفقا للشروط المقررة قانونا بما يكفل حق الشخص المعني بالمعلومات في الخصوصية بسرية.

- **الإفشاء العاجل لسرية بيانات المرور المتحفظ عليها:**

يتكامل هذا المجال من التعاون مع المجال السابق، حيث نصت المادة 30 من الاتفاقية على أنه:[1]

(1- إذا اكتشف الطرف المقدم اليه الطلب أثناء تنفيذ طلب مقدم تطبيقا للمادة للتحفظ على بيانات المرور المتعلقة باتصال معين، أن مزود الخدمة في دولة أخرى ساهم في نقل الاتصال، فانه يجب عليه، ان يقوم بالإفشاء الفوري عن قدر كاف من البيانات المتعلقة بالمرور للطرف الملتمس، للتعرف على مزود الخدمة وعلى المسار الذي تم عبره هذا الاتصال.

(2- الإفشاء العاجل لسرية بيانات المرور تطبيقا للفقرة الأولى يمكن أن يتم رفضه فقط:

أ- إذا كان الطلب ينصب على جريمة يعتبرها الطرف المقدم إليه الطلب ذات طبيعة سياسية، أو جريمة تتصل بجريمة سياسية.

ب-إذا كان الطرف المقدم إليه الطلب يعتبر ان تنفيذ هذا الطلب من شانه المساس بسيادته أو أمنه، أو نظامه العام، أو أي مصالح جوهرية أخرى.)

ما يمكن ملاحظته من هذا النص أنه يعالج مسألة واقعية هامة تحدث غالبا في أرض الواقع، حيث أنه عادة ما يقوم المجرم المعلوماتي بمحاولة توزيع نشاطه الإجرامي عبر أكثر من دولة بقصد تعقيد مهمة البحث عنه وكشف هويته.

أما فيما يخص المساعدة القضائية المتبادلة في مجال سلطات التحقيق فتشمل المجالات الأتية:

- **المساعدة المتبادلة المتعلقة بالولوج إلى البيانات المعلوماتية المخزنة:**

نصت عليها المادة 31 من الاتفاقية[1] بحيث:

[1] - عبد الرحيم بن بوعيدة، ضياء علي احمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع السابق، ص326-327.

(1- يجوز لأي طرف إن يطلب من طرف آخر إن يفتش أو أن يقوم بالولوج إلى البيانات المعلوماتية المخزنة في نظام معلوماتي يتواجد على ارض هذا الطرف الآخر لضبطها أو الحصول عليها أو الكشف عنها، بما في ذلك البيانات التي تم التحفظ عليها تبعا للمادة 29.

(2- تستجيب الدولة المطالبة (المطلوب منها تقديم المساعدة) للطلب من خلال تطبيق المعاهدات الدولية والاتفاقيات والتشريعات المشار إليها في المادة 23، وفقا للنصوص القانونية الأخرى ذات الصلة والخاصة بهذا الفصل.

(3- يتم الاستجابة لهذا الطلب على وجه السرعة في حالة:

أ- إذا كانت هناك أسباب تدعو للاعتقاد أن البيانات المعنية معرضة لمخاطر الفقد أو التعديل.

ب-إذا كانت المعاهدات، أو الاتفاقيات أو التشريعات المشار إليها في الفقرة الثانية تنص على التعاون الفوري.)

تتشابه هذه المادة مع البند (ج) من الفقرة الثانية من المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية[2] والخاصة بتقديم المساعدة القضائية المتبادلة بالكامل بمقتضى قوانين الدولة متلقية الطلب ومعاهداتها واتفاقاتها وترتيباتها ذات الصلة بشان تنفيذ التفتيش والضبط.

- **الدخول عبر الحدود إلى البيانات المعلوماتية المخزنة بتصريح أو من خلال إتاحتها للجمهور:**

يعد هذا المجال والذي تضمنته المادة 32 من الاتفاقية، من مجالات المساعدة القضائية المتبادلة أفرزته طبيعة الجرائم الإلكترونية، حيث نصت تلك المادة على أنه:[3]

(يمكن لأي طرف دون تصريح من الطرف الآخر:

---

[1] - عبد الرحيم بن بوعيدة، ضياء علي أحمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع السابق، ص 327.

[2] - الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة، بتاريخ 21 ديسمبر 2010، وثيقة متاحة على موقع الشبكة القانونية العربية، إدارة الشؤون القانونية التابعة للأمانة العامة لجامعة الدول العربية، الموقع الالكتروني: WWW.ARABLEGALNET.ORG

[3] - عبد الرحيم بن بوعيدة، ضياء علي أحمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع السابق، ص 328.

أ- أن يصل إلى البيانات المعلوماتية المخزنة والمتاحة للجمهور (مصر مفتوح) بغض النظر عن موقعها الجغرافي، أو

ب-الدخول على، أو تلقي، عن طريق نظام معلوماتي يقع على إقليمه، بيانات معلوماتية مخزنة في دولة أخرى، اذا حصل الطرف على موافقة قانونية وإدارية من شخص لديه سلطة قانونية[1] للكشف عن هذه البيانات إلى هذا الطرف من خلال هذا النظام المعلوماتي).

فيما يخص هذه المادة يستحسن من باب الاحترام سيادة الدول والمجاملات الدولية، وحتى لا يثار أي إشكال بين الدول الأطراف حول تفتيش نظام معلوماتي يقع على إقليم إحداهما، إضافة شرط بالنسبة للحالة التي تقوم فيها سلطات الدولة بالدخول إلى النظام المعلوماتي الموجود في إقليم دولة أخرى وتفتيشه وضبط ما بداخله من معلومات، مفاده إخطار وإحاطة الدولة التي يقع في إقليمها النظام المعلوماتي المراد تفتيشه علما بعملية الدخول وموافقة صاحب السلطة القانونية على تلك المعلومات والبيانات.

- **المساعدة المتبادلة بخصوص جمع بيانات المرور في الوقت الفعلي:**

في كثير من الأحيان قد لا يكون بإمكان سلطات التحقيق ضمان تتبع خط سير الاتصال للوصول إلى مصدر الاتصال لإتباع أثره من خلال التسجيلات الخاصة برسائل سابقة، وذلك نتيجة قيام مزود الخدمة بحذف بيانات المرور بشكل ألي من حلقات الاتصال التي تمر بها عملية نقل الرسالة، لذلك فانه من الضروري بالنسبة لسلطات التحقيق في كل دولة أن يكون لديها القدرة على الحصول على بيانات المرور خلال الوقت الفعلي بالنسبة للاتصالات التي تمر خلال نظام معلوماتي لدى دولة أخرى.

[1] - يعرف الشخص الذي بملك سلطة قانونية للكشف عن البيانات والمعلومات الإلكترونية بانه كل شخص طبيعي او معنوي له كافة السلطات الممكنة بموجب قانون او اتفاق على البيانات والمعلومات المخزنة الكترونيا بحيث يحق له استعماله واستغلاله والتصرف فيه.

لذلك نصت المادة 33 من الاتفاقية على أنه :[1]

(1- يجب على الأطراف ان تقدم المساعدة المتبادلة إلى بعضها البعض بالنسبة لجمع بيانات المرور في الوقت الفعلي، والتي تكون مرتبطة باتصالات معينة على أرضهم، ومرسلة عن طريق نظام معلوماتي، ووفقا للأوضاع المنصوص عليها في الفقرة 2 فان هذه المساعدة، سوف تحكمها الشروط والإجراءات المنصوص عليها في القانون الداخلي

(2- يجب على كل طرف ان يقدم هذه المساعدة على الأقل فيما يتعلق بالجرائم الجنائية من حيث جمع بيانات المرور في الوقت الفعلي التي يمكن أن تكون متاحة في قضية موازية على المستوى الداخلي).

بموجب هذا النص يكون كل طرف ملزما بتجميع خط سير البيانات بصورة عاجلة وفي الوقت الفعلي لمصلحة الطرف الآخر، ولما كان تجميع بيانات المرور بصورة عاجلة في الوقت الفعلي قد يكون الطريقة الوحيدة الجوهرية لتحديد هوية مرتكب الجريمة الإلكترونية، وحيث ان هذا الإجراء أكثر تدخلا، فان الفقرة الثانية من الاتفاقية استخدمت مصطلح على الأقل لجميع الدول الأطراف على السماح بأوسع نطاق ممكن للمساعدة المتبادلة حتى في ظل غياب مبدآ التجريم المزدوج.

- **المساعدة المتبادلة في مسألة اعتراض بيانات المحتوى :**

نصت المادة 34 من الاتفاقية على أنه:[2]

(1- تقوم الدول الأطراف بالاتفاقية بتقديم المساعدات المتبادلة لبعضها البعض فيما يتعلق بعملية تجميع أو تسجيل مضمون البيانات في الوقت الصحيح والخاصة باتصالات معينة يتم إرسالها بواسطة منظومة كمبيوتر والى الحد الذي تجيزه القوانين بموجب المعاهدات والقوانين الوطنية الواجبة التطبيق.)

[1] - عبد الرحيم بن بوعيدة، ضياء علي احمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع السابق، ص328.

[2] - عبد الرحيم بن بوعيدة، ضياء علي احمد نعمان، موسوعة التشريعات الإلكترونية المدنية والجنائية، الجزء الثاني، المرجع نفسه، ص 329.

و نظرا لما يشكله هذا الإجراء من مساس بحقوق الأفراد في الخصوصية، حيث ينطوي على تجميع وتسجيل البيانات التي يتم نقلها بواسطة نظام معلوماتي، فقد تم تحديد الالتزام بتوفير المساعدة القضائية المتبادلة المتعلقة بهذا الشأن، وفي الحدود التي تسمح بها المعاهدات والقوانين الداخلية المطبقة لدى الدول الأطراف.

ب-المساعدة القضائية المتبادلة وفقا للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010:

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010 ضمن الفصل الرابع المتعلق بالتعاون القانوني والقضائي على المساعدة القضائية المتبادلة كإجراء في المواد من 32 إلى 36، حيث نصت المادة 32 من الاتفاقية على أنه:[1]

1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات لجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الإلكترونية في الجرائم
2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية من اجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين.
3- يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بشكل خطي ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الإلكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك استخدام التشفير) وتأكيد الإرسال حسب ما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات.
4- باستثناء ما يرد فيه نص في هذا الفصل فان المساعدة الثنائية خاضع للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها ان تمارس حقها في رفض المساعدة فيما يتعلق

[1] -المرسوم الرئاسي رقم 14-252 مؤرخ في 8 سبتمبر 2014 يتضمن التصديق على ألاتفاقي العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 57، السابق ذكره، ص 10.

بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية

5- حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فان هذا الشرط يعتبر حاصلا بغض النظر عما إذا كانت قوانين الدولة الطرف تصنيف الجريمة في نفس تصنيف الدولة الطرف الطالبة وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف.

كما أضافت هذه الاتفاقية مجالات جديدة للمساعدة القضائية تتناسب مع طبيعة الجرائم الإلكترونية وتتمثل هذه المجالات في:

- **الحفظ العاجل للمعلومات المخزنة في أنظمة المعلومات:**[1]

نصت عليه المادة 37 من الاتفاقية بحيث: [2]

(1- لأي دولة طرف أن تطلب المساعدة من دولة أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقني المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلبا بشأنه للمساعد المتبادلة للبحث وضبط وتامين المعلومات.

(2- يجب أن يحدد طلب الحفظ حسب الفقرة 1 ما يلي:

أ- السلطة التي تطلب الحفظ.

ب-الجريمة موضوع التحقيق وملخصا للوقائع.

ج- معلومات تقنية المعلومات التي يجب حفظها وعلاقتها بالجريمة.

د- أية معلومات متوفرة لتحديد المسؤول عن المعلومات المخزنة أو موقع تقنية المعلومات.

---

[1] -ينطبق هذا الإجراء على البيانات المخزنة au données stockées التي سبق تجميعها collectées والاحتفاظ بها archivées عن طريق حائزي البيانات les détenteurs de données، مثال ذلك مقدمي الخدمات، بيد أنها لا تنطبق على التجميع في الوقت الفعلي entemp réel والتحفظ المستقبلي على البيانات المتعلقة بالمرور أو الولوج في الوقت الفعلي إلى محتوى الاتصالات

وبالنسبة لغالبية الدول، فان التحفظ على البيانات يعد سلطة أو إجراء قانوني جديد كليا في القانون الداخلي، فهو أداة جديد للتنقيب الهام في مجال مكافحة الجرائم الالكترونية.

[2] -مرسوم رئاسي رقم 14-252، السابق ذكره، ص 12.

هـ- موجبات طلب الحفظ.

و- رغبة الدولة الطرف بتسليم طلب المساعدة الثنائية للبحث أو الوصول أو الضبط أو تامين أو كشف معلومات تقنية المعلومات المخزنة.

(3- عند استلام إحدى الدول الأطراف الطلب من دولة أخرى فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الاستجابة إلى الطلب فلا يشترط وجود ازدواجية التجريم للقيام بالحفظ.

(4- أي دولة تشترط وجود ازدواجية التجريم للاستجابة لطلب المساعدة يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الاتفاقية، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذا كان هناك سبب الاعتقاد بأنه لن يتم تلبية شرط ازدواجية التجريم في وقت الكشف.

(5- بالإضافة لذلك، يمكن رفض طلب الحفظ إذا تعلق الطلب بجريمة تعتبرها دولة الطرف المطلوب منها جريمة سياسية ومتى تم اعتبار الدولة الطرف المطلوب منها بان تنفيذ الطلب قد يهدد سيادتها أو آمنها أو نظامها أو مصالحها.

(6- حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيقات الدولة الطرف الطالبة لها أو سلامتها فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطلب.

(7- أي حفظ ناجم عن الاستجابة للطلب المذكور في الفقرة 1 يجب أن يكون لفترة لا تقل عن 60 يوما من أجل تمكين الدولة الطرف الطالبة من تسليم طلب البحث أو الوصول أو الضبط أو التامين أو الكشف للمعلومات وبعد استلام مثل هذا الطلب يجب الاستمرار بحفظ المعلومات حسب القرار الخاص بالطلب)

-الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة:

حينما يكون هناك مقدم خدمة (مزود خدمة) واحد أو عدة مزودي الخدمة قد ساهموا في نقل اتصال معين، فان التحفظ العاجل على بيانات المرور (الحفظ العاجل لمعلومات تتبع المستخدمين) يمكن أن يتم من خلالها جميعا، بيد أن هذه المادة[1] لم تحدد الوسائل التي من

[1] -المادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السابق ذكرها.

خلالها يمكن تحقيق ذلك، تاركة هذا الأمر للقانون الداخلي ليحدد الطريقة التي تتلاءم مع نظامه القانوني والاقتصادي.

و إحدى وسائل التحفظ العاجل على البيانات في مثل هذه الحالات تتمثل في قيام السلطات المختصة بإصدار أمر عاجل منفصل لكل مقدم من مقدمي الخدمة، لكن لوحظ على هذه الوسيلة أن الحصول على عدة أوامر منفصلة يمكن أن يستغرق وقتا طويلا.

لذلك فإن أحد الحلول المفضلة هو الحصول على أمر واحد ولكن سوف ينطبق على كل مقدمي الخدمة الذين ساهموا في نقل الاتصال، وهذا الأمر يتم إبلاغه بالتعاقب لكل مقدمي الخدمات المعنيين أو صاحب الشأن.[1]

حيث نصت المادة 38 على ما يلي:

1) حيثما تكشف الدولة الطرف المطلوب منها في سياق تنفيذ الطلب حسب المادة 37 لحفظ معلومات تتبع المستخدمين الخاصة بالاتصالات معينة بان مزود خدمة في دولة أخرى قد اشترك في بث الاتصال.
2) يمكن تعليق كشف معلومات تتتبع المستخدمين حسب الفقرة (1) إذا تعلق الطلب بجريمة تعتبرها الدولة الطرق المطلوب منها جريمة سياسية و متى اعتبرت الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سلامتها أو أمنها أو نظامها أو مصالحها.

- **التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة:**

يتمثل هذا الإجراء في تفتيش وضبط المعلومات التقنية حيث نصت المادة 39 من الاتفاقية على أنه[2]:

[1] -هلالي عبد اللاه احمد، كيفية المواجهة التشريعية لجرائم المعلوماتية، في النظام البحريني على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، 2011، ص 190.

[2] -المرسوم الرئاسي رقم 14- 252 المؤرخ في 8 سبتمبر، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السابق ذكره، ص 12- 13.

1) يجوز لأي دولة طرق أن تطلب من دولة طرق أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضي الدولة الطرق المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.
2) تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرق الطالبة وفقا للأحكام الواردة في هذه الاتفاقية.
3) تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضة للفقدان أو التعديل.

- **الوصول إلى معلومات تقنية المعلومات عبر الحدود:**

نصت المادة 40 من الاتفاقية على أنه:[1] يجوز لأي دولة طرف، وبدون الحصول على تفويض من دولة طرق أخرى:

1- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بعض النظر عن الموقع الجغرافي للمعلومات.
2- أن تصل أو تستقبل من خلال تقنية المعلومات في إقليمها معلومات إذا حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى الدولة الطرق بواسطة تقنية المعلومات المذكورة.

- **التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين:**

نصت عليه المادة 41 من الاتفاقية حيث:[2]

1) على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينة في إقليمها والتي تبث بواسطة تقنية المعلومات.

[1] -مرسوم رئاسي رقم 14- 252 المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السابق ذكره، ص 13.

[2] -الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السابق ذكرها.

2) على كل دولة طرق توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية).

- **التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى:**

نصت عليه المادة 42 من الاتفاقية بحيث[1]: تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينة تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية.

وخلاصة لما سبق ذكره يمكن القول بأنه على الرغم من مصادقة معظم الدول العربية على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، إلا أنه لم يتم إدراج نصوصها في القوانين الداخلية لهذه الدول على الرغم من إلزام هذه الاتفاقية الدول المنظمة إليها من القيام بذلك حسب ما ورد في المادة 2/32، لذا نقترح على الدول العربية المصادقة على هذه الاتفاقية إدراج نصوصها وأحكامها ضمن قوانينها الإجرائية الداخلية تنفيذ التزاماتها من جهة ومن أجل إمكانية اللجوء إلى المساعدة القضائية الدولية من جهة أخرى، لأن من شأن ذلك عرقلة التحقيقات وجمع الأدلة الإلكترونية في هذه الجرائم لعدم وحدة مجالات المساعدة المتبادلة وعدم شرعيتها في هذه الدول لعدم النص عليها مما يؤدي إلى إفلات المجرم المعلوماتي من العقاب نظرا لضياع الدليل الرقمي المثبت لارتكابه الجريمة.

أما عن المساعدة القضائية المتبادلة وفقا للتشريعات الداخلية المقارنة، فمن أجل تعزيز مبدأ التعاون القضائي، الذي تعد المساعدة القضائية إحدى صوره، يكمن لدول أن تلجأ إلى عقد اتفاقيات بينها إما ثنائية أو متعددة الأطراف، تضمنها أحكام خاصة بهذه المساعدة، تبين آليات و مكانيزمات تطبيقها، كما هو الحال في اتفاقية التعاون القضائي بين الجزائر والإمارات العربية المتحدة[2].

---

[1] - مرسوم رئاسي رقم 14- 252 المؤرخ في 8 سبتمبر 2014، يتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، السابق ذكره، ص 13.

[2] - مرسوم رئاسي رقم 07 – 323 مؤرخ في 23 أكتوبر 2007 يتضمن التصديق على اتفاقية التعاون القضائي والإعلانات والإنابات القضائية وتنفيذ الأحكام وتسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الإمارات العربية المتحدة، الموقعة بالجزائر في 12 أكتوبر 1983، الجريدة الرسمية للجمهورية الجزائرية، العدد 67، بتاريخ 24 أكتوبر 2007.

وكذلك الاتفاقية المبرمة بين الجزائر والسودان حول التعاون القانوني والقضائي[1].

كما نص المشرع الجزائري على المساعدة القضائية الدولية المتبادلة بين الدول في المواد من 16 إلى 18 من الفصل السادس المتعلق بالتعاون والمساعدة القضائية الدولية من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2]، حيث نصت المادة 16 منه على المساعدة القضائية المتبادلة كالآتي:

في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يكمن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني.

يمكن في حالة الاستعجال ومع مراعاة الاتفاقيات الدولية ومبدأ المعاملة بالمثل، قبول طلب لمساعدة القضائية، المذكورة في الفقرة الأولى أعلاه، إذا وردت عن طريق وسائل الاتصال الشريعة بما في ذلك أجهزة الفاكس أو البريد الإلكتروني وذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

في حين نصت المادة 17 من قانون 09 – 04 على تبادل المعلومات واتخاذ الإجراءات التحفظية كما يلي:

- تتم الاستجابة لطلبات المساعدة الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدا المعاملة بالمثل.

هذا ونصت المادة 18 من القانون 09-04 على القيود الواردة على طلبات المساعدة القضائية الدولية كالتالي:

[1] -مرسوم رئاسي رقم 07 – 325 مؤرخ في 23 أكتوبر 2007، يتضمن التصديق على اتفاقية التعاون القانوني والقضائي بين حكومة الجهورية الجزائرية الديمقراطية الشعبية وحكومة جمهورية السودان، الموقعة بالجزائر في 24 يناير 2003، الجريدة الرسمية للجمهورية الجزائرية، العدد 68، بتاريخ 28 أكتوبر 2007.

[2] -القانون رقم 09 – 04، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية، السابق ذكره، ص 16.

(يرفض تنفيذ طلبات المساعدة إذا كان من شـأنها المساس بالسيادة الوطنية أو النظام العام.

يمكن أن تكون الاستجابة لطلبات المساعدة مقيدة بشرط المحافظة على سرية المعلومات المبلغة أو بشرط عدم استعمالها في غير ما هو موضح في الطلب).

كما نص المشرّع على التعاون القضائي الدولي في الفصل السادس من قانون 20-05 المتعلق بالوقاية من التمييز و خطاب الكراهية و مكافحتها ، حيث نصت المادة 43 منه على مايلي :في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المنصوص عليها في هذا القانون و كشف مرتكبيها ،يمكن السلطات المختصة ومع مراعاة الاتفاقيات الدولية و مبدأ المعاملة بالمثل، اللجوء إلى التعاون القضائي الدولي.

يمكن في حالة الإستعجال، قبول طلبات التعاون القضائي الدولي ،إذا وردت عن طريق وسائل الإتصال السريعة، بما في ذلك أجهزة الفاكس أو البريد الإلكتروني ،و ذلك بقدر ما توفره هذه الوسائل من شروط أمن كافية للتأكد من صحتها.

في حين نصت المادة 44 من نفس القانون علـى أنه : تتم الإستجابة لطلبات التعاون القضائي الدولي الرامية لتبادل المعلومات أو اتخاذ أي إجراءات تحفظية وفقا للاتفاقيات الدولية الثنائية و مبدأ المعاملة بالمثل.

رابعا: إجراءات إعمال المساعدة القضائية المتبادلة

تعد المساعدة القضائية الدولية من أهم الأدوات المتاحة لنظام العدالة في مواجهة كافة الجرائم الدولية الخطيرة بمختلف أنواعها و أبعادها خاصة الجرائم الماسة بالمعلوماتية و التي يرتكبها اليوم أشخاص أو مجموعات أو تنظيمات إجرامية ، فهي تبقى ضمانة قانونية لعدم إفلات مرتكبي الجرائم من العقاب كونها آلية رئيسية للحصول على المزيد من أدلة الإثبات الإلكترونية و تبادلها ، فالدول تخول لبعضها البعض بناءا على الاتفاقيات و المعاهدات كانت ثنائية أو متعددة الأطراف تبادل المعلومات اللازمة و اتخاذ كافة الإجراءات الدولية وفقا لمبدأ التعاون القضائي و قواعد المعاملة بالمثل.

فتقديم المساعدة القضائية في مجال العدالة الجنائية بين الدول يهدف بالدرجة الأولى إلـــــى تبسيط الإجراءات و تذليل الصعوبات للوصول إلى ضمان محاكمة عادلة بعيدا عن اختلاف الأنظمة القانونية بين الدول، وعادة ما يتم تقديم المساعدة القضائية بناءا على طلب تقدمه الدولة الطالبة وفقا للاتفاقية المحررة كتابيا بينها و بين الدولة المطلوب منها وفي حالة غيابها يتم الرجوع إلى الاتفاقيات المتعددة الأطراف ذات الصلة بالمساعدة القضائية، كما يرجع للأطراف المعنية الاتفاق على تطبيق الاتفاقية كاملة أو جزءا منها هو ما نصت عليه صراحة أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في فصلها الرابع تحت عنوان التعاون القانوني و القضائي[1]. علـى أن يتم تنفيذها من قبل الجهة المختصة لذلك، وبما أن المساعدة القضائية المتبادلة تعد نظاما رسميا يتم بين السلطات القضائية التابعة لدولتين فأكثر، فإنه يتعين تحديد الإجراءات التي يتم من خلالها استعمال هذه الوسيلة.

1- تقديم طلب المساعدة القضائية المتبادلة:

تتم المساعدة القضائية المتبادلة بطلب تقدمه الدولة الطالبة الراغبة في المساعدة وتسمى الدولة الطالبة إلى الدولة المراد منها تقديم المساعدة وتسمى الدولة متلقية الطلب، ويكون ذلك وفقا للأشكال والإجراءات التي حددتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات[2] شرط أن لا تكون الدولتين مرتبطتين بمعاهدة لتبادل المساعدة القضائية أين تطبق وجوبا الأحكام المقابلة في هذه المعاهدة.

ومن شروط تقديم طلب[3] المساعدة القضائية المتبادلة:

أ- أن يكون قضاء الدولة الطالبة مختصة بالنظر في الجريمة المرتكبة:

حتى تتمكن أي دولة من تقديم طلب المساعدة القضائية يتعين أولا أن تكون مختصة بالنظر في الدعوى العمومية الناشئة عن الجريمة الالكترونية، وهذا شرط بديهيه ومنطقي إذ بدونه لا يمكن اللجوء إلى هذه الوسيلة، ويرجع السبب في اشتراط هذا الشرط من أجل إعمال وسيلة المساعدة القضائية إلى اختلاف الدول فيما بينها حول اعتناق مبدأ عالمية الاختصاص الجزائي الذي يعني أحقية أي دولة في

[1]- أنظر الفصل الرابع من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات .

[2]- أنظر المادة 34 من نفس الاتفاقية.

[3]- الطلب هو الوسيلة التي تحمي مسعى الدولة الطالبة للمساعدة القضائية إلى الدولة المطلوب منها ذلك.

النظر في الجريمة الالكترونية حتى ولو لم تكن هذه الدولة من الدول التي ألقت فيها هذه الجريمة ظلالها، إضافة إلى تعدد معايير الاختصاص القضائي المنتهجة من قبل الدول[1].

ب-أن يقدم الطلب إلى الجهة المختصة لتلقي الطلبات:

بما أن طلب المساعدة القضائية المتبادلة يقدم في شكل رسمي، يجب أن يوجه إلى الجهة المختصة بتلقي الطلبات المتعلقة بهذا النظام في الدولة المطلوب منها المساعدة وذلك احتراما لمبدأ التخصص.

حيث نصت المادة 34 الفقرة الثانية من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على كون السلطة المركزية مسؤولة عن إرسال و إجابات طالبات المساعدة القضائية المتبادلة بعد توجيه الطلب إلى الجهة المختصة بتلقي الطلبات و بالتالي إيصالها إلى الجهات المكلفة بتنفيذها.

هذا و تشترط السلطة مركزية التي تتلقى طلبات المساعدة القضائية المتبادلة أن لا يمس الطلب بحق أي دولة طرف في الاتفاقية العربية للمكافحة جرائم تقنية المعلومات على أن تختار طريقا آخر لتوجيه مثل هذه الطلبات إما عن طريق وزارة العدل أو القنوات الدبلوماسية أو عن طريق المنظمة الدولية للشرطة الجنائية و التي عادة ما يمثلها المكتب الوطني المركزي للانتربول خاصة في حالة الاستعجال وذلك حسب ما تتفق عليه الدولتين المعنيتين بناءا على الاتفاقية الثنائية الموقعة عليها ومثال ذلك اتفاقية التعاون القضائي بين الجزائر وايطاليا التي بينت أن إرسال طلبات المساعدة تتم بواسطة وزارة العدل.

كما أفادت الجزائر بأنَّ سلطاتها قدَّمت عشرة (10) طلبات للتعاون القضائي الدولي في عام 2016 إلى سلطات قضائية أجنبية، استندت أربعة(04) طلبات منها إلى اتفاقية مكافحة الفساد، و استند طلب واحد(01) إلى اتفاقية الأمم المتحدة لمكافحة الجريمة المنظَّمة عبر الوطنية، واستندت خمسة(05) طلبات إلى اتفاقات ثنائية للتعاون القضائي هذا و تخضع أغلب الطلبات التعاون القضائي الدولي الواردة و الصادرة للمتابعة في الجزائر من قبل مكتب التعاون القضائي الجزائي الدولي في وزراة العدل وذلك لغياب آلية معمول بها و نظام إلكتروني من أجل تتبع طلبات التعاون القضائي الدولي .

[1]- فاطمة محمد عطوي، المرجع السابق، ص 239.

ت-أن يكون طلب المساعدة القضائية مكتوبا:

جاء في أغلب الاتفاقيات و المعاهدات الدولية في مجال التبادل القضائي الدولي و من ضمنها الاتفاقية العربية لمكافحة الجرائم الإلكترونية أن تكون طلبات المساعدة القضائية في مجال الحصول على الأدلة الإلكترونية مكتوبا، كما يجوز في الحالات المستعجلة أن يقدم هذا الطلب عبر الفاكس أو البريد الإلكتروني على أن تتضمن هذه الإتصالات القدرة المعقولة اللازمة من الأمن و المرجعية .

ث-محتوى طلب المساعدة القضائية:

حتى يكون طلب المساعدة القضائية مقبولا يشترط اشتماله على البيانات التي تحددها الاتفاقية الثنائية بين البلدين أو الاتفاقية المتعددة الأطراف، وفي هذا الصدد يجب التمييز بين حالتين الحالة العادية وحالة الضرورة، و هو ما نصت عليه المادة 05 من اتفاقية التعاون القضائي في مجال الجزائي بين الجزائر و دولة الكويت و بين الجزائر و دولة روسيا الفيدرالية، بحيث يشمل الطلب البيانات التالية:

- **في الحالات العادية:** يفترض أن يتضمن الطلب في هذه الحالات معلومات عامة تعرف في مجملها الدولة والطالبة والأشخاص محل التحقيق فيتضمن الطلب مايلي:
- اسم السلطة المختصة بمباشرة التحقيقات أو الإجراءات ذات الصلة بموضوع طلب.
- وصف الوقائع موضوع الاتهام مشفوعا بنصوص القوانين ذات الصلة أو بيان عنها.
- غرض الطلب و طبيعة المساعدة القضائية المطلوبة .
- التفاصيل الخاصة بأية إجراءات أو متطلبات محددة ترغب الدولة الطالبة في إتباعها عند التنفيذ.
- طلب الحصول على أدلة أو إجراء تفتيش أو ضبط يرفق بيان يوضح فيه أساس الاعتقاد بأن هذه الأدلة تدخل في نطاق الإختصاص القضائي للدولة المطلوب إليها.
- الحاجة إلى السرية و أسباب ذلك.

- المدة الزمنية المطلوب تنفيذ الطلب خلالها .

- لا ترفض الدولة المطلوب إليها التنفيذ الطلب لمجرد أنه لا يشتمل على كافة المعلومات المنصوص عليها متى كان بإمكانها تنفيذه طبقا لقانونها.

- **حالة الضرورة:** يحتوي الطلب في حالة الاقتضاء و الضرورة و في حدود الإمكان على معلومات أكثر دقة تتعلق بـ:

- الهوية و تاريخ الميلاد و المكان الذي يتواجد فيه الشخص المطلوب شهادته و الذي يجب تبليغه.

- و صف دقيق للمكان الذي ينبغي فيه التفتيش و البحث و كذلك الأشياء و الوثائق التي يجب حجزها

- وصف الإجراءات الخاصة الواجب إتباعها خلال تنفيذ الطلب.

- عند الاقتضاء بيان عن مدى الضرر الناتج عن إركاب الجريمة.

- أية معلومات أخرى تقدم للطرف المطلوب منه لتسهيل تنفيذ طلب المساعدة القضائية.

و كثيرا ما يلزم تقديم الطلب في مهلة إشعار قصيرة و تستلزم المساعدة الفعالة على الرّد على الطلبات مقدمة بالشكل الصحيح من أول مرة لذلك و جب أن تتضمن الطلبات جميع المعلومات اللازمة لتسهيل اتخاذ قرار إيجابي بشأن الطلب و تنفيذه تفاديا لأية مشاكل قانونية قد تقع فيها الدولتين خاصة في ظل اختلاف الأنظمة الداخلية و يلزم تنفيذ هذه الطلبات على وجه السرعة، كون حالات التأخر و التعاون لا تخدم إلا مصلحة المجرمين على حساب العدالة.

2- تنفيذ طلب المساعدة القضائية

في حالة ما إذا كان طلب المساعدة القضائية المتبادلة مقبولا فإنه يتعين على الدولة المطلوب منها أن تنفذ محتوى الطلب ويكون ذلك بضوابط معينة يتعين مراعاتها سواء من قبلها أو قبل الدولة الطالبة :

أ- مدة تنفيذ الطلب:

متى قدم طلب المساعدة القضائية وفقا للقانون و أعراف الدولة المطلوب إليها يجوز تنفيذه بالتالي وفقا للمتطلبات أو الكيفية المحدّدة في الطلب مالم يكن ذلك متعارضا مع قانون الدولة المطلوب إليها، على أن تخطر الدولة المطلوب إليها الدولة الطالبة بناءا على طلب ، بأية ظروف يمكن أن تتسبب في تأخير ملحوظ في تنفيذ الطلب.[1]

غير أن الاتفاقية العربية لمكافحة للجرائم المعلوماتية أجازت للدولة المطلوب منها أن تؤجل المساعدة القضائية لكونها تتعارض مع تحقيقات الملاحقات أو إجراءات قضائية جارية من قبل سلطاتها و في هذه الحالة يتعين عليها قبل التأجيل أن تتشاور مع الدولة الطالبة و تخطرها بسبب التأجيل.[2]

ب-القانون الذي يخضع له تنفيد القانون:

حددت المادة 32 من نفس الاتفاقية القانون الذي يخضع له تنفيذ الطلب بنصها صراحة "إن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة. "

الفرع الثاني: الإنـــــابة القضائية الــدولية

تعرف الإنابة القضائية الدولية بأنها: "قيام سلطة قضائية مختصة تابعة لدولة أجنبية باتخاذ إجراء أو أكثر من إجراءات التحقيق، وذلك لحساب سلطة قضائية مختصة تابعة لدولة أخرى من أجل كشف الحقيقة في دعوى جنائية منظورة أمام محاكم هذه الأخيرة"[3]

---

[1]- القرار الرئاسي رقم 304 بشأن الموافقة على إتفاقية المساعدة القضائية المتبادلة في المواد الجنائية بين حكومتي جمهورية مصر العربية و جمهورية الهند ،بتارخ 2008/01/08،الجريدة الرسمية العدد 21 بتاريخ 21 ماي 2009 ، ص 8.

[2]- انظر المادة 32 الفقرة الرابعة من اتفاقية العربية لمكافحة جرائم تقنية المعلومات.

[3] - عادل يحي، الأحكام العامة للتعاون الدولي لمكافحة الجريمة -ماهيته -صوره-أهميته-، الطبعة الأولى ، دار النهضة العربية، القاهرة، مصر، 2013، ص 65-64.

و تعرف أيضا بأنها: " طلب اتخاذ إجراء قضائي من إجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك في الفصل في مسألة معروضة على السلطة القضائية في الدولة الطالبة ويتعذر عليها القيام به بنفسها"[1]

ووفقا للتعريفين السابقين، فإن الإنابة القضائية الدولية تفترض في المسائل الجنائية وجود علاقة تعاون بين دولتين، وبصورة أكثر تحديدا بين سلطتين قضائيتين في دولتين مستقلتين.

وتهدف الإنابة القضائية إلى تسهيل الإجراءات الجنائية بين الدول بما يكفل إجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة والتغلب على عقبة السيادة الإقليمية التي تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى، كسماع الشهود أو إجراء التفتيش وغيره.[2]

وعادة يتم نقل طلب الإنابة إما بالطرق الدبلوماسية [3] أو بالطريق القضائي[4] المباشر، وذلك وفقا للشروط والأوضاع التي تتحدد غالبا بموجب اتفاقية دولية ثنائية أو إقليمية أو جماعية أو في ضوء ما يحدده القانون الوطني حال وجود نصوص تنظم إجراءات وشروط الإنابة القضائية الدولية. وبموجب هذه الإنابة تقوم السلطة القضائية في الدولة المطلوب منها تنفيذ الإنابة باتخاذ إجراء أو إجراءات من الإجراءات التحقيق، وفقا لقانونها الوطني، لحساب الدولة الطالبة من اجل الوصول إلى كشف الحقيقة أمام محاكم هذه الأخيرة[5].

ورغم ذلك فان ثمّة صعوبات تعترض تنفيذ الإنابة القضائية الدولية في بعض الحالات، وتقلّل من فاعليتها بحيث لا يتحقق الغرض المنشود منها في كثير من الأحيان، كاختلاف النظام الإجرائي في كل من الدولة الطالبة والدولة المنفذة، استحالة إعمال نظام المواجهة بين الشهود أو بين المتهمين، أو

---

[1] - حسين بن سعيد الغافري، المرجع السابق، ص 646-647. وأنظر أيضا: محمد كمال محمود الدسوقي، المرجع السابق، ص 151.

[2] - حسين بن سعيد الغافري، المرجع السابق، ص 647

[3] - بالنسبة للطريق الدبلوماسي تقوم المحكمة القائمة بالنظر الدعوة بإرسال طلب الإنابة إلى وزارة الخارجية، وتقوم هذه الأخيرة بإرسال الطلب ذاته الى ممثلها الدبلوماسي في الدولة المطالبة بتنفيذ طلب الإنابة، ويطلق أحيانا على هذا الطريق (الطريق السياسي)

[4] - عادل يحي، المرجع السابق، ص 65-66

[5] - عادل يحي، المرجع نفسه ، ص 66-65

بين الشهود والمتهمين معا، صعوبة الاعتداء بدليل تم الحصول عليه عن طريق الإنابة القضائية، طول إجراءات الإنابة القضائية وزيادة التكاليف، الاعتبارات الخاصة ببعض المتهمين أو الشهود الموجودين في الخارج والتي تقتضي حمايتهم من خطر الانتقام منهم[1].

وإزاء هذه الصعوبات تبدو أهمية تقنية الاتصال المرئي المسموع[2] كوسيلة إضافية للمساعدة القضائية المتبادلة، ويعد استخدام هذه التقنية في مباشرة إجراءات التحقيق، احد التطبيقات الهامة للتكنولوجيا في هذا المجال.

وعلى الرغم من أن تقنية التحقيق الجنائي عن بعد تعد من أساليب المساعدة القضائية الدولية، وهي بذلك تتلاقى مع الإنابة القضائية، إلا أنها تتميز عن هذه الأخيرة في أن الدولة الطالبة هي التي تباشر إجراءات التحقيق باستخدام هذه التقنية، ويقتصر دور الدولة المطلوب إليها على توفير الماكينات المادية والفنية لتنفيذ هذه الإجراءات، فدورها مادي ولا يمتد كما هو الحال في الإنابة القضائية إلى القيام بعمل قضائي، ولاشك أن هذه التقنية تخفف من الغلو في فكرة السيادة التي قد تعوق التعاون القضائي بين الدول في مكافحه الجرائم[3].

وما تجدر الإشارة إليه أن التشريع الجزائري جاء خاليا من أي تنظيم لمسألة الإنابة القضائية الدولية، ما يعني أنه اكتفى بأحكام الإنابة القضائية الواردة في الاتفاقيات الدولية التي وقعت عليها الجزائر، نذكر منها اتفاقية تبادل الإنابة القضائية الدولية المبرمة بين الجزائر وفرنسا في 28اوت1962 مفادها أن البلدين يتعاونان لتقديم المعونة أو المساعدة القضائية التي تطلبها كل دولة، وتضمنت أيضا شروط تنفيذ الإنابة القضائية، وضوابط المحافظة على النظام العام في الدولة المرسل إليها طلب الإنابة، وكذا الجهة التي تتولى تنفيذ الإنابة، وتتحمل نفقاتها.

[1] -عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 96-97

[2] -اخذ بهذه التقنية التشريع الايطالي بموجب القانون رقم 360 لسنه 1992 كما أخذت بها الولايات المتحدة الأمريكية سواء في إجراءات التحقيق على المستوى الداخلي او في مجال المساعدة القضائية في المسائل الجنائية حاله وجود اتفاقيه دوليه تقتضي بذلك

[3] -عادل عبد العال ابراهيم خراشي، المرجع السابق، ص 97.

الفرع الثالث: التحقيقات المشتركة

هذا النوع من التعاون تفرضه طبيعة الجرائم الإلكترونية، حيث يتطلب التحقيق فيها تشكيل فرق مشتركة بين الجهات المختصة في كل دولة من الدول التي وقعت فيها بها جزء من الجريمة، مثال على ذلك: شاركت أجهزة الشرطة الخاصة بأربعة دول مجتمعة وهي السويد ، الدنمارك، فنلندا والنرويج في جوان 2009، في ضبط مجموعة تطلق على نفسها اسم (محاربي شمال أوروبا الفايكنغ) وهي عبارة عن مجموعة من مجرمي دعارة الأطفال تعمل من خلال الأنترنت، وقد تمكنت هذه المجموعة من إيقاع حوالي 80 شخصا في شباكها، وكانت تقوم هذه المجموعة بتبادل صور جنسية للأطفال على الأنترنت بالإضافة إلى أنهم كانوا يقومون بتصوير عمليات اعتداء جنسي على ضحاياهم[1].

وعلى الرغم مما يحققه التحقيق المشترك من تنسيق أمني بين الدول، من خلال توحيد الخطوط والجهود لتعزيز امن واستقرار الدول المعنية لهذا التحقيق، إلا أن الواقع يثبت بطء الوتيرة التي يسير عليها هذا التعاون، فمثلا في سنة 2011 لم يكن من بين الدول الأطراف المستعرضة لتنفيذ اتفاقية الأمم المتحدة لمكافحة الفساد من خلال مؤتمر الدول الأطراف في هذه الاتفاقية إلاّ ثلاث دول أطراف التي لجأت إلى إبرام اتفاقيات وترتيبات ثنائية أو متعددة الأطراف تجيز إنشاء أجهزة تحقيق مشتركة، بينما ذكرت دولتان طرفان أخريان أن نظامهما القانوني وممارستهما يجيزان طلب تحقيقات مشتركة وإجرائها على أساس كل حالة على حدا، وأكدتا أنهما قامتا بذلك في عدد من الحالات.[2]

وما يمكن قوله في هذا الصدد على أن التحقيق في الجرائم الإلكترونية وكشف غموضها بشكل أكثر سرعة وفعالية يتطلب عناصر بشرية مؤهلة علميا وتقنيا للتحقيق في هذه الجرائم وتحليل أدلتها وحفظها، وهو ما قد يكون غير متاح لإحدى الدول، مما يشكل العقبة أمامها وقد يترتب عليه إفلات الجناة لو قامت بهذا التحقيق منفردة، مما يجعل من تشكيل فرق تحقيق مشتركة مع دول أكثر تقدما في هذا المجال حلا لها.

[1] - محمد كمال محمود الدسوقي، المرجع السابق، ص 150-151

[2] - عباسي حبيب، المرجع السابق، ص 545

و الجدير بالذكر أن تشكيل فرق التحقيق هذه لا يقتصر فقط على الدول، وإنما يمكن أن يتم تشكيل هذه الفرق من أعضاء دولة معينة وأعضاء من المنظمات الدولية أو الإقليمية المتخصصة في مجال مكافحة الجريمة بشكل عام والجريمة الإلكترونية بشكل خاص .

و بطبيعة الحال يتم هذا النوع من التعاون في حدود الاحترام التام لسيادة الدولة الطرف التي سيجرى التحقيق داخل إقليمها.

و أخيرا يمكن القول أن اللجوء إلى التعاون في مجال التحقيقات المشتركة سيساهم في تدعيم التعاون الأمني بين الدول، وبالتالي تعزيز فعالية الخطط المنتهجة من قبل الدول في مجال مكافحة الجريمة الإلكترونية.

خاتمة

خـــاتمـة

في ختام هذا الموضوع والذي يعتبر جهد متواضع لدراسة موضوع التحقيق في الجرائم الإلكترونية، هذه الجرائم التي ظهرت نتيجة التطور العلمي والتكنولوجي السريع، وثورة المعلومات الهائلة، والتي تعتبر بلا أدنى شك من الموضوعات المهمة التي باتت الحاجة إلى دراستها بصورة جيدة ومتأنية من قبل الباحثين والدارسين القانونيين، حيث تشكل هذه الجرائم خطرا يهدد الحفاظ على سيادة القانون في معظم الدول، نظر لكونها في معظم الأحوال ذات أبعاد دولية، وما يشكله ارتفاع وزيادة حجمها، وتنوع صورها وأنماطها من مخاطر تهدد الأمن الفردي والجماعي معا.

وهذه الجريمة إن كانت لا تخرج من نطاق المدلول العام للجريمة، في كونها تمثل القيام بعمل أو الامتناع عن عمل جرمه القانون، ضف إلا أنها تتشابه مع الجريمة التقليدية في أطراف الجريمة من مجرم والدافع لارتكاب الجريمة والضحية الذي قد يكون شخص طبيعي أو شخص اعتباري، إلا أن الاختلاف الحقيقي بينهما يتمثل في الوسيلة المرتكبة بها، حيث غالبا ما يعتمد مرتكبي هذا النوع من الجرائم أو ما يعرف بالمجرم بالمعلوماتي على أداة تقنية عالية وأيضا مكان الجريمة الذي لا يتطلب انتقال الجاني إليه إنتقالا فيزيقيا وإنما تتم عن بعد باستخدام خطوط وشبكات الاتصال بين الجاني ومكان الجريمة، مما يشكل صعوبات في الكشف عنها.

كما تتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن الجرائم الأخرى تجعلها صعبة الإثبات لعدم وجود الآثار المادية التقليدية، مما يؤدي إلى ضرورة البحث عن أدلة أخرى لإثباتها، ودون أدنى شك فإن مسألة الحصول على هذه الأدلة يتطلب منظومة قانونية وقضائية فعالة تتولى مسألة التحقيق في هذا النوع من الجرائم باعتبار أن الدليل فيها ذو طابع معنوي غير مادي يسهل تغييره وتعديله والعبث به دون أن يترك ذلك أثر في أغلب أحواله.

فالتحقيق في الجريمة الإلكترونية يتسم بأنه موضوع مستجد ولم يحض بعد بالاستقرار على النحو الذي حظيت به أنشطة التحقيق في الجرائم التقليدية، إلى جانب أن فعالية إجراءات التحقيق في هذا النمط من الجرائم المرهونة بتوافر الدراية الفنية والقانونية معا لدى جهات مباشرة التحقيق، وهي دراية متخصصة لا تقتضيها فقط سلامة إجراءات التحقيق، بل تتطلبها خطط تفعيل وتطوير أداء الجهة التي تمارسها.

خـــاتمـة

ومن خلال هذه الدراسة تم التوصل إلى العديد من النتائج أهمها:

– صعوبة الإتفاق على مفهوم محدد للجريمة الإلكترونية، بسبب اختلاف المفاهيم والقيم الاجتماعية والأخلاقية بين المجتمعات، وهذا يؤدي إلى تجريم الأفعال في بعض الدول دون أخرى، فبالرغم من الاهتمام المتزايد بهذه الجريمة سواء على المستوى الدولي أو الوطني، إلا أنه مازال يكتنفها بعض الغموض، والدليل على ذلك عدم وجود تعريف جامع ومانع لهذه الجريمة يتلائم والطبيعة الخاصة لها، وفكرة عالمية المعلومات والاتصالات والتطور السريع الذي يلحق بهما.

– الجريمة الإلكترونية تعد من أخطر الجرائم التي بدأ خطرها يتفاقم شيئا فشيئا، تزامنا مع تطور التكنولوجيا، ونمو عصابات الجريمة المنظمة التي تتخذ من هذه الجرائم على تنوعها حرفة لها.

– الجريمة الإلكترونية تتميز عن الجريمة التقليدية بطبيعة خاصة، ويعود ذلك لعدة عوامل أهمها أنها ترتكب في بيئة تقنية المعلومات، مما أضفى عليها وعلى مرتكبيها سمات خاصة وسمي المجرم فيها بالمجرم المعلوماتي، الذي تميز بأنه ذو مهارات فنية وتقنية عالية وقدرة على التعامل معلوماتيا، ولو لم يكونوا على مستوى علمي كبير، فهذه الميزة تجعل تعاملهم مع آثار الجريمة يفوق مقدرة سلطات التحقيق في اكتشاف آثار الجريمة، فضلا عن كونها جريمة عابرة للحدود ومحل الإعتداء فيها غالبا هو المعلومات، والذي يعد أمر جديد على المحقق الجنائي، حيث تم التوصل إلى اعتبار المعلومة ذات قيمة مالية يمكن الإعتداء عليها شأنها شأن القيم المالية الأخرى.

– أن الجريمة الإلكترونية تقع في البيئة الرقمية، أي خارج الواقع المادي الملموس الذي هو البيئة التي تقع فيها الجرائم التقليدية، وينعكس هذا على طبيعة الدليل في الجرائم الإلكترونية، فيتكون هذا الدليل من نبضات إلكترونية تنساب عبر النظام المعلوماتي، الأمر الذي يعني إمكانية نقل الدليل الإلكتروني عبر شبكات الحاسوب، لكي يستقر في بعيد عن الموقع المادي، خصوصا أن استخدام شبكة الأنترنت يسهل بشكل كبير على الجناة إخفاء الأدلة في مواقع توجد في أماكن بعيدة، ومن هذه الناحية يختلف الدليل الإلكتروني عن أدلة الجريمة التقليدية التي تكون في الغالب في مكان بعيد عن مكان ارتكاب الجريمة.

– صعوبة إثبات الجرائم الإلكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها، فقد يكون هذا الدليل غير مرئي ويسهل إخفائه أو تدميره، وقد يكون متصلا بدول أخرى، فتكون هناك صعوبة في الحصول

عليه، نظرا لتمسك كل دولة بسيادتها، كما أن هذا الإثبات يحتاج إلى معرفة علمية وفنية قد لا تتوافر لدى رجال الشرطة والمحققين والقضاة.

- إن التقنيات العلمية الحديثة لعبت دورها الفعال في إمكانية استرجاع الدليل الإلكتروني بعد محوه وإصلاحه بعد إتلافه، وإظهاره بعد خفائه.

- حرص مختلف التشريعات على تطبيق مبدأ مشروعية الدليل الإلكتروني، واعتبار مبدأ حرية الإثبات الجنائي أساس قبول الدليل الإلكتروني.

- الإبقاء على السلطة التقديرية للقاضي الجنائي في تقديره للدليل الإلكتروني، حيث يستطيع هذا الأخير أن يفسر الشك لصالح المتهم، كما يمكنه أن يستبعد الأدلة الإلكترونية التي يتم الحصول عليها بطرق غير مشروعة.

- عدم إشارة المشرع الجزائري لمسألة تقدير قيمة الدليل الالكتروني بين أدلة الإثبات.

- نص المشرع الجزائري صراحة على جواز تفتيش المنظومة المعلوماتية في المادة 5 من القانون 09-04، المؤرخ في 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وبذلك يكون قد قطع الخلاف الفقهي حول جواز تفتيش المكونات المعنوية للحاسب الآلي من عدمه، كما أجاز المشرع الجزائري على غرار بعض التشريعات المقارنة التفتيش ولو عن بعد، وأجاز لقاضي التحقيق أيضا القيام بأية عملية تفتيش أو حجز ليلا أو نهارا، إذا تعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- عزز المشرع الجزائري إجراءات التفتيش بقواعد تتماشى وطبيعة الجريمة الإلكترونية، بإضافته لعملية التفتيش عن بعد والتفتيش في الشبكة، إلا أنه بالغ في احترام سيادة الدول الأخرى من خلال منع التفتيش في الأنظمة المعلوماتية التابعة لإقليمها.

- أضاف المشرع الجزائري محلين للتفتيش هما: المنظومة المعلوماتية أو جزء منها، وكذا المعطيات المخزنة فيها ومنظومة تخزين معلوماتية، وبالتالي يكون قد وضع نهاية جدال فقهي لا تزال العديد من الدول تتخبط فيه، كما نص صراحة على إمكانية التفتيش عن بعد.

خـــاتمـة

– إسناد التحقيق لجهات متخصصة يعتبر من الحلول العملية التي تساعد سلطات التحقيق والعدالة الجنائية في التصدي للجرائم الإلكترونية، وتوفر فرصة لبناء كوادر وظيفية متمكنة وقادرة على التعامل بكفاءة وفاعلية مع هذا النوع من الجرائم، الأمر الذي سيؤدي إلى الاستغناء عن خدمات الخبراء أو تقليل الاعتماد عليهم.

– أفرد المشرع الجزائري دون غيره من التشريعات بوضع قانون إجرائي لمواجهة الجرائم الإلكترونية

– من أهم الاتفاقيات التي عملت على إرساء النصوص موضوعية مفصلة لمكافحة الجرائم الإلكترونية والمعروفة باتفاقية بودابست لمكافحة الجرائم المعلوماتية لسنة 2001، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحررة بالقاهرة بتاريخ 21 ديسمبر 2010، حيث نص هاذين الاتفاقيتين على إجراءات تقليدية لمكافحة الجريمة الإلكترونية تتمثل في التفتيش وضبط البيانات المعلوماتية والتجميع في الوقت الفعلي للبيانات المعلوماتية، وإجراءات جديدة تتمثل في التحفظ العاجل على البيانات المعلوماتية المخزنة والأمر بإنتاج بيانات معلوماتية.

– إن مواجهة الدول العربية للجريمة الإلكترونية لم يكن على نفس المستوى الموجود في الدول الغربية، فمثلا نجد أن دولة الإمارات العربية المتحدة ورغم انضمامها للاتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، والتي عملت على تطوير إجراءات التحقيق والتحري لمكافحة الجريمة الإلكترونية، وألزمت الدول الأطراف فيها بتبني هذه الإجراءات الضرورية في قانونها الداخلي، إلا أنها اعتمدت وسائل الإثبات التقليدية في مكافحة الجريمة الإلكترونية دون التطوير في أحكامها، أما عن المشرع الأردني فقد اكتفى هو الآخر بالنص على إجراء التفتيش وضبط النظم المعلوماتية دون التفصيل في الأحكام المقررة لهما.

بخلاف المشرع الجزائري الذي واكب القوانين الغربية والاتفاقيات الدولية المصادق عليها في مكافحة الجريمة الإلكترونية، حيث قام بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 06–22، المؤرخ في 20 ديسمبر 2006،أضاف بموجبه إجراءات استثنائية من القواعد العامة المنظمة للتفتيش والضبط تخصص جرائم محددة على سبيل الحصر، كما أضاف اعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور وإجراء التسرب، حيث يحق للسلطات القضائية المختصة الإذن بهما إذا اقتضت ضرورات التحري والتحقيق في تلك الجرائم المحددة على سبيل الحصر.

خـــاتمـة

– نظم المشرع الجزائري في القانون رقم 09–04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، مجموعة من الإجراءات الحديثة والمتعلقة بالتحري والتحقيق في الجرائم الإلكترونية كمراقبة الاتصالات الإلكترونية، تفتيش المنظومة المعلوماتية، حجز المعطيات المعلوماتية، كما تضمن هذا القانون إجراءات تمهيدية لجمع البيانات والمعلومات يقوم بها غالبا مقدمي الخدمات من خلال التزاماتهم العامة بهدف مساعدة سلطات التحقيق وحفظ المعطيات المتعلقة بحركة السير، كما استحدث المشرع الجزائري بموجب هذا القانون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، تم تنظيم عملها بموجب المرسوم الرئاسي رقم 19–172، المؤرخ في 6 جوان 2019 بعدما كان تنظيمها خاضعا للمرسوم الرئاسي رقم 15–261، المؤرخ في 8 أكتوبر 2015، كما أصدر مرسوم رئاسي سنة 2020 يتضمن إعادة تشكيلة وتنظيم وسير هذه الهيئة.

– كما أصدر المشرع الجزائري القانون 18–07، المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث تعتبر هذه المعطيات جزء من الحياة الخاصة تستوجب الحماية الجزائية، وتضمن هذا القانون إجراءات صارمة في حالة إساءة استخدامها.

– أنشأ المشرع الجزائري منظومة لأمن أنظمة المعلومات بناء على مرسوم رئاسي رقم 20–05، المؤرخ في 20 يناير 2020، حيث كلفت هذه الأخيرة فيه بإجراء تحقيقات في حالة حدوث هجمات إلكترونية، كما تقوم هذه المنظومة أيضا بتقييم وجمع البيانات والمعلومات وتقديم المشورة للهيئات العمومية، بالإضافة إلى مهام أخرى متعلقة بالأمن الإلكتروني للمؤسسات العمومية.

– إدراك معظم الدول بضرورة التعاون الدولي فيما بينها لمكافحة الجريمة الإلكترونية باعتبارها جريمة عابرة للحدود، من خلال إبرام العديد من الاتفاقيات الثنائية والجماعية، العامة أو الخاصة لمكافحة هذه الجريمة، والتي من شأنها أن تسمح للدول بتوحيد التجريم وتوحيد الإجراءات بين الدول خاصة في مجال الإجراءات الحديثة للتحري والتحقيق.

– نظم المشرع أحكام التعاون والمساعدة القضائية الدولية فيما يخص جمع الأدلة الخاصة في الشكل الإلكتروني في القانون رقم 09–04 والقانون 20–05، مما يعطي دفعة قوية لجهات التحري والتحقيق لمواجهة كل أصناف الجرائم الإلكترونية .

خـــاتـمـة

ونظرا لخطورة الجريمة الالكترونية وصعوبة التحقيق فيها وكذلك إثباتها بسبب تعددها وصعوبة حصرها في دولة معينة نرى بضرورة تقديم بعض التوصيات منها:

– توحيد المفاهيم المتعلقة بالجرائم الإلكترونية وتنسيق الجهود لوضع تصور موحد لها، وتحديد صورها، ومن ثم تعميمها على الدول، حتى لا يحدث اختلاف حول تجريم أفعال في دولة دون أخرى، الأمر الذي يعيق سبل التعاون الدولي في هذا المجال.

– إعادة تسمية القانون رقم 09–04، المؤرخ في 5 أوت2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، بقانون الوقاية من الجرائم الإلكترونية ومكافحتها، وذلك لعدم إدراج مصطلح الإعلام ولا الاتصال في نص القانون.

– إعادة النظر في المادة 5 من القانون رقم 09–04، والمتعلق بتفتيش المنظومة المعلوماتية، وذلك بالتفصيل في طبيعة المعطيات المبحوث عنها والواقعة خارج التراب الوطني، حيث أن المشرع الجزائري لم يفرق بين المعطيات المتاحة للجمهور والمعطيات التابعة للمتهم، والمعطيات التابعة لدولة أجنبية، وكان عليه حصر منع التفتيش خارج الإقليم في المعطيات الموجودة بالخارج، والمملوكة لغير المتهم دون تلك المفتوحة للجمهور.

– على المشرع الجزائري إدراج أعمال الخبرة في مجال الجرائم الالكترونية وكل ما يتعلق بها من إجراءات تبين كيفية الإستعانة بالخبير المعلوماتي عند التحقيق مع الأشخاص ذوي العلاقة بالحاسوب في القانون رقم 09–04.

– الفصل بين إجراء اعتراض المراسلات السلكية واللاسلكية وإجراء تسجيل الأصوات والتقاط الصور وتخصيص كل إجراء بالأحكام المقررة له.

– يتوجب على المشرع الجزائري أن يخصص قانون خاص لمكافحة الجريمة الإلكترونية ينظم فيه كل من النصوص الموضوعية والإجرائية والتنظيمية التي تسهل تلك المكافحة.

– ضرورة صياغة و اعتماد سياسة جزائية حازمة قائمة على خطط واستراتيجيات تنطلق من الوقاية من الجريمة الالكترونية إلى غاية مواجهتها والتصدي لها.

– التفات المشرع الجزائري لضحية الجريمة الإلكترونية، والتكفل به وحماية حقوقه باعتباره الطرف الضعيف في الرابطة الإجرائية الجزائية.

– إدراج الدول العربية الإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، ضمن قوانينها الإجرائية الداخلية تنفيذا لالتزاماتها الدولية من جهة، وتحقيقا للمساعدة القضائية الدولية المتبادلة فيما بينها من جهة أخرى، لأن عدم العمل بذلك سيؤدي حتما إلى عرقلة التحقيقات وجمع الأدلة الإلكترونية في هذه الجريمة لعدم وحدة مجالات المساعدة القضائية، وعدم شرعيتها في هذه الدول لعدم التنصيص عليها، وهذا ما يؤدي إلى إفلات المجرم المعلوماتي من العقاب نظرا لضياع الدليل الإلكتروني المثبت لارتكابه الجريمة.

– الاهتمام بتدريب الخبراء والمحققين والقضاة على التعامل مع الجرائم الإلكترونية ذات الطبيعة الفنية والعلمية المعقدة بحيث يمكن الوصول إلى الحقيقة وإماطة اللثام عن هذه الجرائم تحقيقا لصالح المجتمع وأفراده ولصالح المتهمين أنفسهم لكي لا يدان إلى المسيء.

– سرعة إنجاز التحقيق في الجرائم الإلكترونية، فعندما يكون المحقق ملما بكافة أبعاد الجريمة الإلكترونية، ومدركا بحكم تخصصه لما تمثله من ضرر على المجتمع، فإن ذلك سيساعده على سرعة إنجاز التحقيق.

– ضرورة تدعيم الأجهزة المكلفة بالتحقيق في الجرائم الإلكترونية في كل مرة بآليات وتقنيات ووسائل جديدة تضمن المواجهة الفعالة.

– عقد دورات مكثفة للكوادر البشرية العاملين في حقل التحري والتحقيق، والمحاكمة حول جرائم المساس بأنظمة المعالجة الآلية للمعطيات وتطبيقات الحاسوب، والجرائم المرتبطة بها، والنظر في تضمين مناهج التحقيق الجنائي في كليات، ومعاهد تدريب الشرطة موضوعات عن جرائم الإنترنت.

– ضرورة إنشاء نيابة متخصصة بالتحقيق في الجرائم الإلكترونية، أسوة ببلدان عديدة أجنبية وعربية، والعمل على تعزيز قدرات أعضاء النيابة العامة في الموضوعات المرتبطة بتلك الجرائم وآليات مكافحتها، كيفية البحث والتحقيق فيها، خصوصا في الجانب المتعلق بجمع وسائل الإثبات وتقييم

الأدلة والتأكيد على أهمية عقد دورات تكوينية حول تقنيات التحقيق في، لما لهذا الموضوع من تأثير في مكافحة هذه الجرائم.

– نوصي أن تعمل الجزائر على استحداث أقسام متطورة داخل أجهزة العدالة تعنى بمكافحة الجرائم الإلكترونية والتي من أهم سماتها صعوبة اكتشافها وكذلك ضبطها، مع الأخذ بنظام القضاة الجنائيين في الجريمة الإلكترونية على المستوى العلمي المعرفي والعملي.

– تشجيع الجامعات على تنظيم العديد من الندوات والمؤتمرات التي تعالج تطور الإجرام المعلوماتي وكيفية مكافحة الجريمة الإلكترونية والحد منها.

– ضرورة تحسيس المواطنين بالتبليغ عن الجرائم الالكترونية وهذا من أجل السماح للضبطية القضائية القيام بمهامها بصفة أكثر فعالية وعلى أحسن وجه.

– إن المكافحة والوقاية من الجريمة الإلكترونية لا تعد حكرا على الدولة وحدها بل لابد للمواطن المشاركة والمساهمة في هذه العملية، وذلك عن طريق تنمية ثقافته ووعيه الكافي بما يحيط به وتحسيسه بمخاطر الجريمة وكيفية الحماية منها، وبالتالي نشوء جيل صاعد واعي يتأقلم مع التطور بكل صوره دون الحاجة إلى الخوف من استغلال هذا التطور لخدمة الجريمة.

– إنشاء موقع إلكتروني خاص يكون مفتوحا للجميع للرد على الشكاوى والإستفسارات المتعلقة بالجرائم الالكترونية ونشر كل ما هو جديد في مجال التقنية وتكنولوجيا المعلومات من الناحية الفنية والقانونية .

– ضرورة تفعيل وتثقيف مرتدي وسائل الإعلام الجديدة بالقوانين الخاصة باحترام حقوق الإنسان ومراعاة الخصومة.

– ضرورة تكثيف وتعزيز التعاون والتنسيق الإقليمي والدولي في مجال مكافحة الجرائم الالكترونية بين الدول مع بعضها البعض، وبين الدول والمؤسسات الدولية وخاصة الإنتربول في مجال المساعدة القضائية المتبادلة أو في مجال التدريب والعمل على دراسة ومتابعة المستجدات في هذا المجال .

– تشجيع البحث العلمي التطبيقي المشترك وتبادل الخبرات والتجارب بين دول العالم في مجال نتائج

خـــاتـمـة

البحوث، حتى يتم تطويق الأساليب الإجرامية والقضاء عليها مبكرا قبل انتشارها في كافة الدول باستغلال الفراغ التشريعي.

تمت بعون الله فله الحمد والشكر

قائمة المراجع

قائـمة المراجـع

❶-المراجع باللغة العربية.

أولا: المراجع الشرعية.

-القرآن الكريم.

ثانيا: المعاجم.

1- ابن منظور، لسان العرب، الطبعة الأولى، دار المعارف، القاهرة، مصر.
2- ابن منظور عبد الله العلايلي، لسان العرب ، المحيط ، المجلد الثالث ، الجزء الثاني، دار لسان العرب ، بيروت ، لبنان، بدون سنة نشر.
3- رياض النعمان، المعجم القانوني، الجزء الأول، دار أسامة للنشر والتوزيع، الأردن، 2013.
4- القاموس الجديد للطلاب، علي بن هادية، بن لحسن البليمن، الجيلالي بن حاج يحي، المؤسسة الوطنية للكتاب، الجزائر، بدون سنة.
5- الوسيط الحديث، منجد عربي- عربي، الطبعة الأولى، دار أيوب للمنشورات، باتنة، الجزائر، 2013.

ثانيا: المراجع العامة.

1- أحسن بوسقيعة، الوجيز في القانون الجزائي، الطبعة الثالثة، دار هومة، الجزائر، 2006.
2- أحمد ضياء، الظاهرة الإجرامية بين الفهم والتحليل، دار النهضة العربية، القاهرة، 2001.
3- أحمد عبد الكريم سلامة، قانون حماية البيئة، دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، السعودية، 1997.
4- أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، الطبعة الثالثة، دار هومة، الجزائر، 2011.
5- خالد بن سليمان الغثير ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مركز التأمين لأمن المعلومات، دون بلد النشر، 2009.
6- رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء قواعد القانون الجنائي الداخلي والدولي، الطبعة الأولى، دار الجامعة الجديدة، مصر،2007.

7- رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، الطبعة الثالثة، دار الفكر العربي، القاهرة، بدون سنة النشر.

8- رياض النعمان، المعجم القانوني، الجزء الأول، دار أسامة للنشر والتوزيع، الأردن، 2013.

9- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

10- سهيل حسين الفتلاوي، الدبلوماسية بين النظرية والتطبيق، دار الثقافة، عمان، الأردن، 2006.

11- عادل يحي، الأحكام العامة للتعاون الدولي لمكافحة الجريمة -ماهيته -صوره- أهميته-، الطبعة الأولى ، دار النهضة العربية، القاهرة، مصر، 2013.

12- عامر خضير حميد الكبيسي، التدريب الأمني العربي، واقع وآفاق تطويره، جامعة نايف للعلوم الأمنية، الرياض، 2007 .

13- عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر.

14- عبد الغني بسيوني عبد الله، النظرية العامة في القانون الإداري، منشأة المعارف، الإسكندرية ، 2003.

15- عبد الفتاح عبد اللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن،2011.

16- عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق دار هومة، الجزائر،2004.

17- عبد الله أوهايبية، شرح قانون العقوبات الجزائري الجريمة (القسم العام)، الجزء الأول، الطبعة السادسة، ديوان المطبوعات الجامعية، الجزائر، 2005.

18- عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن، بين النظرية و التطبيق، بدون بلد النشر، بدون سنة النشر.

19- عجة الجيلالي، مدخل للعلوم القانونية، الجزء الأول، برقي للنشر، الجزائر، 2009.

20- عجة الجيلالي، مدخل للعلوم القانونية ، الجزء الثاني، برقي للنشر، بدون سنة النشر.

21- عز الدين عبد الله، القانون الدولي الخاص، الجزء الثاني (تنازع القوانين وتنازع الاختصاص القضائي الدوليين، الطبعة الثامنة، دار النهضة العربية، القاهرة، 1977.

22- علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2006.

23- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان.

24- فاطمة محمد العطوي، الإشكاليات التي يثيرها التعاون الدولي في المواد الجنائية، دار النهضة العربية، القاهرة، 2013.

25- فضيل العيش، شرح قانون الإجراءات الجزائية النظرية والعملي، بدون طبعة ، بدون دار نشر، الجزائر.

26- قادري أعمر، أطر التحقيق، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

27- كامل سعيد، شرح قانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

28- كوركيس يوسف داوود، الجريمة المنظمة، الطبعة الأولى، الدار العلمية الدولية للثقافة والنشر والتوزيع، عمان، الأردن، 2001.

29- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الأولى، دار هومه، الجزائر،2006.

30- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2008.

31- محمد سيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005.

32- محمد صبري السعدي، الواضح في شرح القانون المدني- الإثبات في المواد المدنية والتجارية-، دار الهدى، الجزائر،2009.

33- محمد صغير بعلي، مدخل للعلوم القانونية، دار العلوم، عنابة، 2006.

34- محمود نجيب حسني، شرح قانون العقوبات(العام)، المجلد الأول، الطبعة الثالثة، (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، لبنان، بدون سنة نشر.

35- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية القاهرة، 1995.

36- محمود نجيب حسني، شرح قانون العقوبات اللبناني، المجلد الأول، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، 1988.

37- مختار شبلي، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة، الجزائر، 2013.

38- مراد محمود الشنيكات، الإثبات بالمعاينة والخبرة في القانون المدني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

39- مروك نصر الله، محاضرات في الإثبات الجنائي، الجزء الثاني، دار هومة، الجزائر، 2004.

40- ممدوح خليل بحر، حماية الحياة الخاصّة في القانون الجنائي، مكتبة دار الثقافة للنشر والتوزيع، عمان 1996.

41- منصور رحماني، الوجيز في القانون الجنائي العام، فقه وقضايا، دار العلوم للنشر، الجزائر، 2006.

42- نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017.

43- نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، الطبعة الأولى، دار هومة، الجزائر، 2015، 2016.

44- هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والاجرائية والتعاون الدولي، دار النهضة العربية، 2000.

45- هدى حامد قشقوش، الجريمة المنظمة، الطبعة الأولى، الدار العلمية الدولية ودار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

ثالثا : المراجع المتخصصة.

1- أحمد خليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2000.

2- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، الطبعة الأولى، دار النهضة العربية، القاهرة، 2010.

3- أحمد مهدي، اشرف الشافعي التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها، الطبعة الأولى، دار الكتب القانونية، مصر 2005.

4- أحمد يوسف الطحطاوي، الأدلة الإلكترونية، ودورها في الإثبات الجنائي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2015.

5- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامعي، الإسكندرية، 2011.

6- أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية، دار الفكر الجامعي، الإسكندرية، 2016.

7- أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، بدون دار نشر، بدون بلد، 2003.

8- إيهاب فوزي السقا، الحماية الجنائية والأمنية بطاقات الإئتمان، دار الجامعة الجديدة، الإسكندرية، 2007.

9- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011.

10- توفيق محمد الشاوي، حرمة الأسرار الخاصّة ونظرية عامّة للتفتيش، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006.

11- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية، القاهرة، 2002.

12- حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017.

13- حسن طاهر داوود، جرائم نظم المعلومات، الطبعة الأولى، الرياض، 2000.

14- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنيت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.

15- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنيت، دار الثقافة، عمان، 2011.

16- خالد مختار الفار، إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب، الطبعة الأولى، دار عزّة للنشر والتوزيع، أسيوط، 2010.

17- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

18- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009.

19- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، 2010.

20- خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، بدون بلد نشر، 2012.

21- دليلة جلول، الأسس النفسية للتحقيق الجنائي، دار هومة، الجزائر، 2015.

22- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011.

23- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2003.

24- رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنيت، دار النهضة العربية، القاهرة، 2013.

25- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.

26- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011.

27- سامي حسن الحسيني، النظرية العامّة للتفتيش، الطبعة الأولى، دار النهضة العربية، القاهرة، 1972.

28- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.

29- سراج الدين الروبي، آلية الإنتربول في التعاون الدولي الشرطي، الطبعة الثانية، الدار المصرية اللبنانية للطباعة والنشر، 2001.

30- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

31- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013.

32- سليم علي عبده، التفتيش في ضوء أصول المحاكمات الجزائية الجديدة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، 2006.

33- سهيل محمد العزام، الوجيز في جرائم الأنترنيت، الطبعة الأولى، مكتبة الجامعة الأردنية، 2009.

34- سيف بن الراشد الحوسني، جرائم التجارة الإلكترونية، دراسة مقارنة، السحاب للنشر والتوزيع، سلطنة عمان 2010.

35- صليحة علي صداقة، الإبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية ،2017.

36- ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة والوراقة الوطنية، مراكش، 2011.

37- طارق عفيفي صادق أحمد، الجرائم الإلكترونية، جرائم الهاتف المحمول، الطبعة الأولى المركز القومي للإصدارات القانونية، القاهرة، 2015.

38- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.

39- عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015.

40- عادل عبد العال إبراهيم خراشي، دور الضبطية الإدارية والقضائية، في مكافحة جرائم بطاقات الإئتمان الإلكترونية والتعاون الأمني الدولي حيالها، دار الجامعة الجديدة، الإسكندرية، 2015.

41- عبد الحميد الشواربي، إذن التفتيش في ضوء الفقه والقضاء، منشأة المعارف، الإسكندرية، بدون سنة نشر.

42- عبد الرحيم بن بوعيدة ، ضياء علي أحمد نعمان ، موسوعة التشريعات الإلكترونية المدنية و الجنائية – التشريع المغربي و العربي و الفرنسي الاتفاقيات العربية و الأوروبية و الدولية–، الجزء الأول، الطبعة الأولى، المطبعة و الوراقة الوطنية، مراكش ، 2010.

43- عبد الرحيم بن بوعيدة ، ضياء علي أحمد نعمان ، موسوعة التشريعات الإلكترونية المدنية و الجنائية – التشريع المغربي و العربي و الفرنسي الاتفاقيات العربية و الأوروبية و الدولية–، الجزء الثاني، الطبعة الأولى، المطبعة و الوراقة الوطنية، مراكش ، 2010.

44- عبد الصبور عبد القوي علي مصري، الجريمة الإلكترونية، الطبعة الأولى، دار العلوم للنشر والتوزيع، القاهرة، 2008.

45- عبد العال الديربي، محمد صادق، الجرائم الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.

46- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دار الفكر الجامعي، الإسكندرية، 2006.

47- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007.

48- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2009.

49- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبيعة الأولى، منشأة المعارف، الإسكندرية، 2009.

50- – عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.

51- عبد الله حسين علي محمود، سرقة المعلومات المخزّنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2001.

52- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت(الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

53- عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن- بين النظرية و التطبيق–، بدون بلد النشر، بدون سنة النشر.

54- عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة، دار الجامعة الجديدة، الإسكندرية، 2013.

55- عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنّفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

56- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنيت، الطبعة الأولى، عالم الكتب الحديثة، أربد، الأردن، 2004.

57- علي حسن محمد الطوالبة، الجرائم الإلكترونية، الطبعة الأولى، جامعة العلوم التطبيقية، مملكة البحرين، 2008.

58- علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، الاسكندرية، 2011.

59- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2012.

60- عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات- دراسة مقارنة-، دار النهضة العربية، القاهرة، 2000.

61- عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنيت في مصر والدول العربية، المكتب الجامعي الحديث، مصر، بدون سنة نشر.

62- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان، 2006.

63- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

64- فريد منعم جبور، حماية المستهلك عبر الانترنيت ومكافحة الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010.

65- لحسن ناني، التحقيق في الجرائم المتصلة بتكنلوجية المعلوماتية، بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، بدون بلد النشر، 2017.

66- مجدي عبد الملك، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، الإسكندرية، 2011.

67- محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، الإسكندرية، 2003.

68- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، سنة 1993.

69- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، 2004.

70- محمد حماد مرهج الهيتي ، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006.

71- محمد خليفة، الحماية الجنائية المعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

72- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011.

73- محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، بدون بلد نشر، 2016.

74- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والانترنيت، المكتب العربي الحديث، الإسكندرية، 2007.

75- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت، الطبعة الثانية، دار النهضة العربية، 2009.

76- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية، الطبعة الأولى، دار الفكر والقانون، 2015.

77- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر/ مصر،2012 .

78- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع، مصر، 2010.

79- محمد مصطفى الشقيري، السرية المعلوماتية، ضوابطها وأحكامها الشرعية، الطبعة الأولى، دار البشائر الإسلامية، بيروت، لبنان، 2008.

80- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2004.

81- مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة ،2015.

82- مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، الطبعة الأولى، بدون دار نشر، 2001.

83- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2008.

84- **ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.**

85- منتصر سعيد حمودة، المنظمة الدولية للشرطة الجنائية الإنتربول، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008.

86- منى جاسم الكواري، التفتيش شروطه وحالات بطلانه، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2008.

87- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية ، الطبعة الأولى، منشورات الحلبي، 2005.

88- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

89- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2007.

90- نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017.

91- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية 2008.

92- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان، الأردن، 2008.

93- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994.

94- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.

95- هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.

96- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.

97- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.

98- هلالي عبد اللاه احمد، كيفية المواجهة التشريعية لجرائم المعلوماتية، في النظام البحريني على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، 2011.

99- وضاح محمود الحمود ونشأت مفطي، جرائم الانترنيت، دار المنار للنشر، عمان، 2005.

100- وليد الزيدي، القرصنة على الانترنيت والحاسوب، الطبعة الأولى، دار أسامة للنشر والتوزيع، عمان، الأردن، 2003.

101- يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى، المصدر القومي للإصدارات القانونية، القاهرة، مصر، 2011.

رابعا: الرسائل الجامعية.

أ- رسائل الدكتوراه.

1- إبراهيم إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980.

2- أحمد سعد محمد الحسني، الجوانب الإجرائية الناشئة عن استخدام الشبكات الإلكترونية، أطروحة الدكتورة، كلية الحقوق، قسم القانون الجنائي، عين شمس، مصر، 2012.

3- إسماعيل طواهري، الاقتناع الشخصي للقاضي في المواد الجنائية، أطروحة دكتوراه، كلية الحقوق، فرع القانون العام، جامعة الجزائر 1، 2014/2013.

4- الموسوس عتو، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي والتكنولوجي دراسة مقارنة، رسالة دكتوراه، جامعة سيدي بلعباس،2014-2015.

5- بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض، 2006.

6- حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة دكتوراه في العلوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2017/2016.

7- جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه، تخصص قانون كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018.

8- خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض، 2006.

9- سالم محمد سليمان اوجلي، احكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1997.

10- سامح أحمد بلتاجي موسى، الجوانب الإجرامية للحماية الجنائية لشبكة الانترنيت، رسالة دكتوراه في الحقوق، جامعة الاسكندرية، مصر 2010.

11- شريف نصر أحمد، النظرية العامّة للخبرة في المواد الجنائية، رسالة دكتوراه في الحقوق، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2010.

12- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005.

13- صورية بورباية، قواعد الأمن المعلوماتي، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، بلعباس، 2016-2017.

14- طارق فوزي الفقي، الجوانب الإجرامية في الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية ،2011.

15- عادل فتحي صابر شريف، تفتيش غير المتهم، رسالة للحصول على درجة دكتوراه، كلية الحقوق، جامعة حلوان، مصر، 2010.

16- عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017-2018.

17- علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، رسالة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، 2011.

18- عمارة فوزي، قاضي التحقيق، أطروحة دكتوراه العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة ،2009-2010.

19- غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل شهادة دكتوراه في القانون، الجامعة الاسلامية، كلية الحقوق، لبنان، 2004.

20- فايز محمد راجب غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني أطروحة الدكتوراه، كليه الحقوق، فرع القانون الجنائي و العلوم الجنائية، جامعه الجزائر (1)، 2010-2011.

21- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2012.

22- كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، تخصص علوم قانونية ، كلية الحقوق والعلوم السياسية، فرع العلوم الجنائية، جامعة جيلالي اليابس، سيدي بلعباس، 2014-2015.

23- محمد حسن الكندري، المسؤولية الجنائية عن التلوث البيئي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005.

24- محمد حمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2013.

25- محمد فتحي محمد أنور عزّت، تفتيش شبكة الانترنيت لضبط جرائم الإعتداء على الآداب العامة والشرف والاعتبار التي تقع بواسطتها، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين الشمس، مصر.

26- مريم قسول، مبدأ مشروعية الأدلة العلمية في المواد الجنائية, رسالة دكتوراه, كلية الحقوق والعلوم السياسية, قسم الحقوق, جامعة جيلالي اليابس, سيدي بلعباس, 2015-2016.

27- ممدوح حسن مانع العد، ضمانات المتهم أثناء التحقيق ومدى مراعاة مبادئ القانون الدولي لحقوق الإنسان في المجال الجنائي، رسالة الدكتوراه في القانون، كليه الحقوق، جامعة الإسكندرية.

28- منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.

ب- رسائل الماجيستير.

1- حسيبة محي الدين، ضمانات المشتبه فيه أثناء التحريات الأولية، رسالة الماجستير، كليه الحقوق، جامعه الإسكندرية، مصر، 2010 .

2- خديجة بتقة، السياسة الأمنية الأوربية في مواجهة الهجرة غير الشرعية، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، جامعة محمد خيضر، بسكرة، 2013.

3- عبد الله بن الحسين أل حجراف القحطاني، تطوير مهارات التحقيق الجنائي والادعاء العام، مذكرة ماجستير، كلية الدراسات العليا، الرياض،2014.

4- عبد الله بن عبد العزيز عبد الله الخثعي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

5- عماد أحمد هاشم الشيخ خليل، ضمانات المتهم أثناء مرحلة الاستجواب، مذكرة ماجيستر في القانون الجنائي، كلية الحقوق، جامعة العالم الأمريكية، 2006.

6- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية التخصص قانون جنائي وعلوم جنائية، جامعة الحاج لخضر باتنة ،2011-2012.

7- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية، رسالة ماجستير في العلوم الجنائي، جامعة الحاج لخضر، باتنة، 2012- 2013.

8- هدى أحمد العوضي، استجواب المتهم في مرحلة التحقيق الابتدائي، مذكرة ماجستير في الحقوق، تخصص قانون عام، جامعة المملكة، البحرين، 2009.

9- يوسف صغير، الجريمة المرتكبة عبر الأنترنيت، مذكرة لنيل شهادة الماجستير في القانون، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2013/03/06.

خامسا: المقالات والمداخلات الأكاديمية.

أ- المقالات العلمية.

1- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مجلّة المحلّية العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، 2013.

2- أسامة بن غانم العبيدي، الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية، مجلة جامعة الملك سعود، الحقوق والعلوم السياسية(1)، المجلد الخامس والعشرون، الرياض ، المملكة العربية السعودية، 2013.

3- الحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، مجلة الواحة القانونية، العدد الثاني، 2006.

4- باسم محمد شهاب، عملية التسرّب، الحقيقة التشريعية، مقال منشور في مجلة الحقوق، مجلّة فصلية علمية محكمة، تصدر عن مجلس النشر العلمي، جامعة الكويت، العدد 04، ديسمبر 2013.

5- حسام محمد رمضان ،تطبيقات المحاكاة الحاسوبية في التخطيط والتدريب على إدارة الكوارث، مقال منشور بمجلة البحوث الأمنية ،أكاديمية الملك فهد، المجلد 11، العدد 22، أكتوبر 2002.

6- حسني درويش عبد الحميد ،البحث الجنائي المعاصر ،مقال منشور بمجلة البحوث الأمنية، كلية الملك فهد، المجلد 10، العدد 1522، نوفمبر 2001.

7- دلال مولاي ملياني، التفتيش في جرائم تكنولوجيا الإعلام و الاتصال، مقال منشور بمجلة القانون والعلوم السياسية، العدد 03، ، منشورات معهد الحقوق، المركز الجامعي النعامة، جانفي 2016.

8- راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقني المعلومات، دراسة تطبيقية على إمارة أبوظبي، مقال منشور ضمن مجلة الدراسات الإستراتيجية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الإستراتيجية، العدد 131، 2008.

9- زوزو هدى، التسرّب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلّة دفاتر السياسة والقانون، مجلة جامعية محكمّة في الحقوق والعلوم السياسية، تصدر عن جامعة قاصدي مرباح، ورقلة، العدد الحادي عشر، جوان 2014.

10- سرحان حسن المعيني التحقيق في جرائم تقنيه المعلومات، مجلة الفكر الشرطي، المجلد عشرون، العدد الرابع، الشارقة، الإمارات العربية المتحدة، 2011.

11- عبد الحميد كرود، التسول النصب والاحتيال، عبر الانترنت، مجلة الدركي، العدد 16، 2008.

12- عزيزة رابحي، التفتيش في نظم المعالجة الآلية للمعطيات، مقال منشور بمجلة القانون والعلوم السياسية، العدد03، جانفي 2016، منشورات معهد الحقوق، المركز الجامعي، ولاية النعامة.

13- عصماني ليلى، صهيب سهيب غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، مجلة القانون، المجتمع والسلطة، المجلد 9، العدد 2، جامعة وهران، 2020.

14- علاء الدين عبد الله الحواصنة وبشار طلال المومني، النظام القانوني للصورة الفوتوغرافية، مجلة الشريعة والقانون، العدد 53، جامعة الإمارات العربية المتحدة، 2013.

15- علاوة هوام، التسرّب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلة الفقه والقانون، العدد الثاني، المغرب، 2012.

16- محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، مجلة الفكر الشرطي، المجلد 20، العدد الرابع، الشارقة، الإمارات العربية المتحدة، 2011.

17- محمد محمد درويش، التطلعات المستقبلية نحو استخدام أسلوب المحاكاة في مجال التدريب الأمني بأكاديمية الشرطة، مقال منشور بمجلة الأمن العام المصرية، العدد 46.

18- محمد نور الدين عبد الحكيم، دور نظم المعلومات في المجال الشرطي، مقال منشور بمجلة الفكر الشرطي ،المجلد العاشر، يناير 2002.

19- ناصر بن محمد البقمي، أهمية الأدلة الرقمية في الإثبات الجنائي، دراسة وفق الأنظمة السعودية، الفكر الشرطي، المجلد 20، العدد4، الشارقة، الإمارات العربية المتحدة،2011.

ب- المداخلات العلمية.

1- أشرف صلاح الدين، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة، أعمال مؤتمرات حول مكافحة الجريمة عبر الأنترنيت، المنظمة العربية للتنمية الإدارية، القاهرة، 2010.

2- دلال مولاي ملياني، التفيش في جرائم تكنولوجيا الإعلام و الإتصال، مقال منشور بمجلة القانون والعلوم السياسية، العدد 03، منشورات معهد الحقوق، المركز الجامعي، النعامة، جانفي 2016.

3- شرف الدين وردة، عيساني علي، المساعدة القضائية الدولية المتبادلة في مجال جمع الأدلة الرقمية، وفقا للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مداخلة للمشاركة في فعاليات الملتقى الدولي حول أدلّة الإثبات الجنائية في التشريعات المقارنة المنعقد يومي 25-26 أبريل 2018، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار.

4- رجم جمال، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ، مجلة الجيش، مجلة شهرية للجيش الشعبي الوطني، عدد 599، تصدر عن مؤسسة المنشورات العسكرية، جوان، 2013.

5- رشيدة كابوية، حجية الدليل الرقمي في الإثبات الجنائي، ملتقى دولي حول أدلة الإثبات الجنائية الحديثة في التشريعات المقارنة، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، يومي 26/25 أبريل 2018.

6- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلّة الجنائية والطب الشرعي، الرياض، 2007.

7- عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية، بحث مقدم إلى المؤتمر الإقليمي حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة 26-2008/04/27، مقر جامعة الدول العربية.

8- كريم راشد، بحث إستراتيجية المديرية العامة للأمن الوطني في مكافحة الجريمة المعلوماتية مقدم لليوم الدراسي حول مخاطر الانترنيت وجرائم الإعلام من تنظيم مخبر الدراسات القانونية ومسؤولية المهنيين المنعقد بتاريخ 14 فبراير 2019، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار.

9- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنيت من 1 - 3 ماي هي 2000، المجلد الثالث، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، 2004.

10- محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنيت، بحث مقدم في الحلقة العلمية بعنوان " الأنترنيت والإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، دبي، في الفترة الممتدة ما بين 15 إلى 2008/11/19.

11- محمد عبد الرحيم سلطان العلماء، جرائم الأنترنيت والاحتساب عليها، بحوث مؤتمر القانون و الكمبيوتر و الأنترنيت من 1-3 ماي 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، الطبعة الثالثة، 2004.

12- محمد محمد الألفي، العوامل الفاعلة في إنشاء جرائم الارهاب عبر الأنترنيت، أعمال المؤتمرات حول مكافحة الجريمة عبر الأنترنيت، المنظمة العربية للتنمية الادارية، القاهرة، مصر، 2010.

13- منصف خطابي، ضمانات المشتبه فيه أثناء التحريات الأولية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الدفعة السابعة عشر، الجزائر، 2006-2009.

14- موسى مسعود أرحومة، الاشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا طرابلس، ليبيا خلال الفترة 28-2009/10/29.

15- هدى حامد قشقوش، الإتلاف غير العمدي لبيانات وبرامج الحاسب الإلكتروني، بحوث مؤتمر القانون والكمبيوتر والانترنيت، المجلد الثالث، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، من 01 إلى 03 ماي 2000.

سادسا: الوثائق القانونية الرسمية.

أ- الوثائق القانونية الرسمية العربية:

1- دستور الجمهورية الجزائرية الديمقراطية الشعبية، المعدل سنة 2020، الصادر بالمرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2022، الجريدة الرسمية العدد 82، الصادرة في 30 ديسمبر 2020.

2- دستور الإمارات العربية المتحدة، الجريدة الرسمية ، السنة الأولى، بتاريخ 1971/12/31، المعدل في سنة 2009.

ب-الاتفاقيات الدولية.

1- الإعلان العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة 217 ألف (د-3) المؤرخ في 10 كانون الأول، ديسمبر 1948.

2- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25، الدورة 55، المؤرخة في تشرين الثاني، نوفمبر 2000، وثيقة رقم: A/RES/55/25.

3- ديباجة الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقع بالجزائر في 25 أكتوبر 2003، المصادق عليه بموجب مرسوم رئاسي رقم 07- 375 مؤرخ في 01 ديسمبر 2007، الجريدة الرسمية العدد 77 ، بتاريخ 9 ديسمبر 2007.

4- ديباجة الاتفاقية الجزائرية الديمقراطية الشعبية والمملكة الإسبانية في مجال الأمن ومكافحة الإرهاب والجرام المنظم، الموقعة بالجزائر في 15 جوان 2008، المصادق عليها بموجب المرسوم الرئاسي 08 / 427 المؤرخ في 28 ديسمبر، ج.ر.ج.ج، العدد 05، تاريخ 21 جانفي 2009.

5- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة، بتاريخ 21 ديسمبر 2010، وثيقة متاحة على موقع الشبكة القانونية العربية، إدارة الشؤون القانونية التابعة للأمانة العامة لجامعة الدول العربية، متوفر على الموقع الإلكتروني: www.arablegalnet.org)

ج- القوانين

1- القانون رقم 01/06 المؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، جريدة رسمية للجمهورية الجزائرية، العدد 14، بتاريخ 18 مارس 2006، المعدل والمتمم.
2- القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية.
3- القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، ج.ر.ج.ج رقم 47 ، الصادرة في 2009/08/16.
4- القانون رقم 04/15 المؤرخ في 2015/02/01 المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية العدد 06، الصادر في 2015/12/10.
5- القانون رقم 18-04، المؤرخ في 10 ماي 2018، يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية العدد27، الصادرة بتاريخ 13 ماي 2018.
6- القانون 18- 07 المؤرخ في 10 جوان سنة 2018 و المتعلق بحماية الأشخاص الطبيعيين ذات الطابع الشخصي ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ،العدد 34.
7- القانون 05/20 المؤرخ في 2020/04/28 ،يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر.ج.ج رقم 25 الصادرة في 2020/04/29.

د- الأوامر.

1- الأمر 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية العدد 48 ، الصادرة في 1966/06/10 المعدل والمتمم بالأمر 11/21 الصادر في 2021/08/25، ج.ر.ج.ج رقم65 الصادرة في 2021/08/26.
2- الأمر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات ج.ر.ج.ج رقم 49 الصادرة في 1966/06/11 المعدل والمتمم بالقانون رقم 08/21 الصادر في 2021/06/08، ج.ر.ج.ج رقم 45 الصادرة في 2021/06/09.

3- الأمر 02/15 المؤرخ في 23 يوليو 2015، يعدّل ويتمم الأمر 155/66 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائرية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، السنة الثالثة والأربعون، الصادرة في 24 ديسمبر 2006.

هـ- المراسيم والقرارات الوزارية.

1- المرسوم الرئاسي رقم 183/04، الصادر في 06/26/ 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج رقم41، الصادرة في 27 /2004/06.

2- المرسوم الرئاسي رقم 323/07، الصادر في 2007/10/23، المتضمن التصديق على اتفاقية التعاون القضائي والإعلانات والانابات القضائية وتنفيذ الأحكام و تسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الامارات العربية المتحدة الموقعة بالجزائر بتاريخ 12 اكتوبر 1988، ج.ر.ج.ج رقم ،67 الصادرة في 24 /2007/10 .

3- المرسوم رئاسي رقم 07 –35، مؤرخ في 23 أكتوبر 2007، يتضمن التصديق على اتفاقية التعاون القانوني والقضائي بين حكومة الجهورية الجزائرية الديمقراطية الشعبية وحكومة جمهورية السودان، الموقعة بالجزائر في 24 يناير 2003، الجريدة الرسمية للجمهورية الجزائرية، العدد 68، بتاريخ 28 أكتوبر 2007.

4- المرسوم الرئاسي رقم 151/08، المؤرخ في 26 ماي 2008، يتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، ج.ر.ج.ج رقم 27، الصادرة في 28 /2008/05.

5- المرسوم الرئاسي رقم 143/09، الصادر في 2009/04/27، يتضمن مهام الدرك الوطني وتنظيمه، ج.ر.ج.ج رقم 26، الصادرة في03 /2009/05.

6- المرسوم الرئاسي رقم 252/14 المؤرخ في 8 /2014/09 المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرر بالقاهرة بتاريخ 21ديسمبر 2010، ج.ر.ج.ج رقم 57 الصادرة في 2014/09/28.

7- المرسوم الرئاسي 15-261، المؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة بتاريخ 8 أكتوبر 2015.

8- المرسوم الرئاسي 172/19 الصادر في 06/06/ 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات يسرها، ج.ر.ج.ج رقم37، الصادرة في 09 /2019/06.

9- المرسوم الرئاسي رقم 05/20 الصادر في 2020/01/20، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ج.ر.ج.ج رقم 04 الصادرة في 2020/01/21.

8- المرسوم الرئاسي رقم 20-183، المؤرخ في 13 يوليو 2020،يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 40، الصادرة بتاريخ 18 جويلية 2020.

9- المرسوم التنفيذي رقم 348/06 الصادر في2006/10/05، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج رقم 63، الصادرة في 08 /2006/10.

10- المرسوم التنفيذي رقم 10-322، المؤرخ في 22 ديسمبر 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، جريدة رسمية للجمهورية الجزائرية، العدد78، بتاريخ 26 ديسمبر 2010.

11- القرار الرئاسي رقم 304 بشأن الموافقة على إتفاقية المساعدة القضائية المتبادلة في المواد الجنائية بين حكومتي جمهورية مصر العربية وجمهورية الهند، بتارخ 2008/01/08،الجريدة الرسمية العدد 21 بتاريخ 21 ماي 2009 .

12- القرار الوزاري الصادر في 14 /2007/04 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للأدلّة الجنائية وعلم الإجرام، ج.ر.ج.ج رقم 36، الصادرة في 2007/06/03.

آآ- الوثائق القانونية الرسمية العربية.

1- دستور الإمارات العربية المتحدة، الجريدة الرسمية، السنة الأولى، بتاريخ 1971/12/31.

2- قانون رقم 35 لسنة 1992، والمتعلق بإصدار قانون الإجراءات الجزائية، الجريدة الرسمية لدولة الإمارات -العربية المتحدة، العدد 233مكرر، السنة 22، بتاريخ 1992/01/26.

3- قانون الاتصالات الأردني رقم 13 لسنة 1995 الجريدة الرسمية رقم 4072، بتاريخ 1995/10/01، المعدّل بموجب القانون رقم 21 لسنة 2011 والصادر بالجريدة الرسمية بتاريخ 2011/04/21.

4- قانون الجرائم الإلكترونية الأردني لسنة 2015، الجريدة الرسمية العدد 5631.

5- قرار جمهوري بالقانون رقم 13 لسنة 1994 بشأن الإجراءات الجزائية ،المؤرخ بتاريخ 8 جمادى الأول 1415 الموافق لـ 12 أكتوبر 1994 ،الجريدة الرسمية العدد 19/4 .

سابعا:المواقع الالكترونية.

1- موقع المديرية العامة للأمن الجزائري www.algeriepolice.dz

2- موقع شبكة قوانين الشرق www.eastlaw.com

3- الدستور الأردني، متاح على الموقع الإلكتروني:
http://www.parliament.jo/node/137

4- الدستور المصـري لسنة 2014، مشار إليه على الموقع الإلكتروني:
http://www.youm7.com

5- الموقع الرسمي للأفريبول : www.el-mass.com/dz.

6- قانون رقم 575-2004، المؤرخ في 21 جوان 2004، المتعلق بالثقة في الاقتصاد الوطني، متاح على الموقع الإلكتروني: https:// wipolex.wipo.in

7- حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، متوفر على موقع الالكتروني شبكة القوانين شرق www.eastlaw.com

8- لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، مقال منشور ضمن مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، 2013، مشار إليه في الموقع الإلكتروني:revenue_univ_ourgla.dz

9- محمد معسكر، مقال الكتروني بعنوان تعريف لعملية التحقيق الجنائي الرقمي، متوفر على الموقع الالكتروني: http :www.isecurity.org

10- محمد معسكر، مقال الكتروني بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته متوفر على الموقع الالكتروني: http://www. Isecurity.Org..

11- الدرك الوطني الجزائري، مقال منشور على موقع ويكيبيديا، الموسوعة الحرة، على الرابط الإلكتروني:

12- الدرك-الوطني-الجزائري http :ar.wikipediaorg/wiki/

13- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة، بتاريخ 21 ديسمبر 2010، وثيقة متاحة على موقع الشبكة القانونية العربية، إدارة الشؤون القانونية التابعة للأمانة العامة لجامعة الدول العربية، الموقع الالكتروني: .WWW.ARABLEGALNET.ORG

❷- المراجع باللغة الأجنبية.

A- Les ouvrages.

1- André (Lucas),Jean Droit de l'informatique et de L'internet, édition Dalloz, collection thèmes (droit privé), France, 2001.

2- CLAUDE Soyer ،Droit Pénal et Procédure Pénale ،L.G.D.J ،Paris ، France ،12 éme édit ،1996.

3- DECAUX Emanuel, la protection de la vie privée au regard des données informatiques, droit fanda mentaux, n° 7,janvier 2008-decembre 2009.

4- FREDERIC Deboue ،FRANÇOIS Falletti et EMANUAL Dupic،Précis de droit pénal et de procédure pénal ،PUF ،Paris ،France ،5éme édit mise a jour ،2013.

5- JACQUES Leroy،Procédure Pénale Librairie Général de Droit et de Juris Prudence،L'extenso éd . Paris cedex 2009.

6- Kenneth l'Auden, Manegement Information System managing the digital
firm ", Seventh édition , prentice bhall , inc,new jersey , USA , 2004.

7- LUCAS de Lyssac (Marie Paul),Une Information Seul Est-Elle Susceptible De Vol D'une Autre Atteinte Juridique Aux Bien . Dallozsiery ,1985.

8- Masse (Michel) infaction contre pordre financier, rev , sc , crim, janvier1985 N1.

9- MICHEL Quille, Ouropol, La Criminalité Organisée , Sous La Direction De Marcel , LECLERC, Paris, 1996.

10- Parker (Done B), Fighting computer crime « A new fram work for
protecting information , john wiley and son , 1998.
11- - QUEMENER Myriam ،YVES Charpenel ،Cyber criminalité ، Droit Pénal Appliqué،Economica ،Paris ،2010
12- - Ravanas (J), la protection des personnes contre la réalisation et la publication de leur image ,L.D.J ,Paris ,1978
13- Roden (Adrian), computer crime and the law , CLT .1991. VOL 15.
14- 16- tatty (Richard) and hard castle (Antony) , computer- Related Crime in informations technology and the law, Macmilla publishers, UK, 1986.
15- Thompson (David), currrent trends in computer control crime, computer quarterly, vol 9 N 1, 1991.

B- Textes réglementaires.

1- Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des Etats de l'Union économique Benelux, de la République Fédérale d'Allemagne et de la République Française relatif à la suppression graduelle des contrôles aux frontières communes, convention d'application de l'accord de schengen le 19 juin 1990.

2-Code pénal ,109 e ,édition dalloz2012 ,

3-Code de procédure pénal 54 e, édition dalloz ,2013 France

4-Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

5-Loi n° 72 – 1226 du 29 décembre 1972

6-Cour de cassation : Chambre Criminelle Lecture de 9 Octobre 1978, N° 76 .92.075 publier au bulletin.

Books :

1- Ball (Leslie D) computer Crime in the information technology revolution,
2- CATALA Pierre, Ebouche D'ume Théorie Juridique De L'information, D 1984 .

3- Glough(Brayn) and mango (Paul),approaching Zero :data crime and criminal under world,1992.
4- Michel, D Rostoker and Robert H ; Rimes, computer jurisprudence, Leyel responses to the information révolution, ocona publication.
5- Tiedeman (klaus), frande et autre délits d'affaires commis d'ordinateur électroniques, rev, Dr, Pén, crime and the lawcrim n 7, Bruxelles, 1984.

قائـمة المراجـع

❶-المراجع باللغة العربية.

أولا: المراجع الشرعية.

-القرآن الكريم.

ثانيا: المعاجم.

1- ابن منظور، لسان العرب، الطبعة الأولى، دار المعارف، القاهرة، مصر.
2- ابن منظور عبد الله العلايلي، لسان العرب ، المحيط ، المجلد الثالث ، الجزء الثاني، دار لسان العرب ، بيروت ، لبنان، بدون سنة نشر.
3- رياض النعمان، المعجم القانوني، الجزء الأول، دار أسامة للنشر والتوزيع، الأردن، 2013.
4- القاموس الجديد للطلاب، علي بن هادية، بن لحسن البليمن، الجيلالي بن حاج يحي، المؤسسة الوطنية للكتاب، الجزائر، بدون سنة.
5- الوسيط الحديث، منجد عربي- عربي، الطبعة الأولى، دار أيوب للمنشورات، باتنة، الجزائر، 2013.

ثانيا: المراجع العامة.

1- أحسن بوسقيعة، الوجيز في القانون الجزائي، الطبعة الثالثة، دار هومة، الجزائر، 2006.
2- أحمد ضياء، الظاهرة الإجرامية بين الفهم والتحليل، دار النهضة العربية، القاهرة، 2001.
3- أحمد عبد الكريم سلامة، قانون حماية البيئة، دراسة تأصيلية في الأنظمة الوطنية والاتفاقية، الطبعة الأولى، منشورات جامعة الملك سعود، السعودية، 1997.
4- أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، الطبعة الثالثة، دار هومة، الجزائر، 2011.
5- خالد بن سليمان الغثير ومحمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، الطبعة الأولى، مركز التأمين لأمن المعلومات، دون بلد النشر، 2009.
6- رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء قواعد القانون الجنائي الداخلي والدولي، الطبعة الأولى، دار الجامعة الجديدة، مصر،2007.

7- رؤوف عبيد ، مبادئ القسم العام من التشريع العقابي، الطبعة الثالثة، دار الفكر العربي، القاهرة، بدون سنة النشر.

8- رياض النعمان، المعجم القانوني، الجزء الأول، دار أسامة للنشر والتوزيع، الأردن، 2013.

9- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

10- سهيل حسين الفتلاوي، الدبلوماسية بين النظرية والتطبيق، دار الثقافة، عمان، الأردن، 2006.

11- عادل يحي، الأحكام العامة للتعاون الدولي لمكافحة الجريمة -ماهيته -صوره- أهميته-، الطبعة الأولى ، دار النهضة العربية، القاهرة، مصر، 2013.

12- عامر خضير حميد الكبيسي، التدريب الأمني العربي، واقع وآفاق تطويره، جامعة نايف للعلوم الأمنية، الرياض، 2007 .

13- عبد الرحمن خلفي، محاضرات في قانون الإجراءات الجزائية، دار الهدى، الجزائر.

14- عبد الغني بسيوني عبد الله، النظرية العامة في القانون الإداري، منشأة المعارف، الإسكندرية ، 2003.

15- عبد الفتاح عبد اللطيف الجبارة، إجراءات المعاينة الفنية لمسرح الجريمة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن،2011.

16- عبد الله أوهابية، شرح قانون الإجراءات الجزائية الجزائري، التحري والتحقيق دار هومة، الجزائر،2004.

17- عبد الله أوهايبية، شرح قانون العقوبات الجزائري الجريمة (القسم العام)، الجزء الأول، الطبعة السادسة، ديوان المطبوعات الجامعية، الجزائر، 2005.

18- عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن، بين النظرية و التطبيق، بدون بلد النشر، بدون سنة النشر.

19- عجة الجيلالي، مدخل للعلوم القانونية، الجزء الأول، برقي للنشر، الجزائر، 2009.

20- عجة الجيلالي، مدخل للعلوم القانونية ، الجزء الثاني، برقي للنشر، بدون سنة النشر.

21- عز الدين عبد الله، القانون الدولي الخاص، الجزء الثاني (تنازع القوانين وتنازع الاختصاص القضائي الدوليين، الطبعة الثامنة، دار النهضة العربية، القاهرة، 1977.

22- علي أحمد عبد الزعبي، حق الخصوصية في القانون الجنائي، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، 2006.

23- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان.

24- فاطمة محمد العطوي، الإشكاليات التي يثيرها التعاون الدولي في المواد الجنائية، دار النهضة العربية، القاهرة، 2013.

25- فضيل العيش، شرح قانون الإجراءات الجزائية النظرية والعملي، بدون طبعة ، بدون دار نشر، الجزائر.

26- قادري أعمر، أطر التحقيق، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2013.

27- كامل سعيد، شرح قانون أصول المحاكمات الجزائية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2005.

28- كوركيس يوسف داوود، الجريمة المنظمة، الطبعة الأولى، الدار العلمية الدولية للثقافة والنشر والتوزيع، عمان، الأردن، 2001.

29- محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، الطبعة الأولى، دار هومه، الجزائر،2006.

30- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، دار هومة، الجزائر، 2008.

31- محمد سيد عرفة، تدريب رجال العدالة وأثره في تحقيق العدالة، جامعة نايف العربية للعلوم الأمنية، الرياض، 2005.

32- محمد صبري السعدي، الواضح في شرح القانون المدني- الإثبات في المواد المدنية والتجارية-، دار الهدى، الجزائر،2009.

33- محمد صغير بعلي، مدخل للعلوم القانونية، دار العلوم، عنابة، 2006.

34- محمود نجيب حسني، شرح قانون العقوبات(العام)، المجلد الأول، الطبعة الثالثة، (معدلة ومنقحة)، منشورات الحلبي الحقوقية، بيروت، لبنان، بدون سنة نشر.

35- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثالثة، دار النهضة العربية القاهرة، 1995.

36- محمود نجيب حسني، شرح قانون العقوبات اللبناني، المجلد الأول، الطبعة الثالثة، منشورات الحلبي الحقوقية، بيروت، 1988.

37- مختار شبلي، الجهاز العالمي لمكافحة الجريمة المنظمة، دار هومة، الجزائر، 2013.

38- مراد محمود الشنيكات، الإثبات بالمعاينة والخبرة في القانون المدني، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2008.

39- مروك نصر الله، محاضرات في الإثبات الجنائي، الجزء الثاني، دار هومة، الجزائر، 2004.

40- ممدوح خليل بحر، حماية الحياة الخاصّة في القانون الجنائي، مكتبة دار الثقافة للنشر والتوزيع، عمان 1996.

41- منصور رحماني، الوجيز في القانون الجنائي العام، فقه وقضايا، دار العلوم للنشر، الجزائر، 2006.

42- نادية دردار، الجهود الدولية لمكافحة الجريمة، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2017.

43- نجيمي جمال، قانون الإجراءات الجزائية الجزائري على ضوء الاجتهاد القضائي، الجزء الأول، الطبعة الأولى، دار هومة، الجزائر، 2015، 2016.

44- هدى حامد قشقوش، الجريمة المنظمة، القواعد الموضوعية والاجرائية والتعاون الدولي، دار النهضة العربية، 2000.

45- هدى حامد قشقوش، الجريمة المنظمة، الطبعة الأولى، الدار العلمية الدولية ودار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

ثالثا : المراجع المتخصصة.

1- أحمد خليفة الملط، الجريمة المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2000.

2- أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، الطبعة الأولى، دار النهضة العربية، القاهرة، 2010.

3- أحمد مهدي، اشرف الشافعي التحقيق الجنائي الابتدائي وضمانات المتهم وحمايتها، الطبعة الأولى، دار الكتب القانونية، مصر 2005.

4- أحمد يوسف الطحطاوي، الأدلة الإلكترونية، ودورها في الإثبات الجنائي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2015.

5- الشحات إبراهيم محمد منصور، الجرائم الإلكترونية في الشريعة الإسلامية والقوانين الوضعية، دار الفكر الجامعي، الإسكندرية، 2011.

6- أنيس حسيب السيد المحلاوي، الخبرة القضائية في الجرائم المعلوماتية والرقمية، دار الفكر الجامعي، الإسكندرية، 2016.

7- أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة جرائم استخدام الحاسب الآلي، بدون دار نشر، بدون بلد، 2003.

8- إيهاب فوزي السقا، الحماية الجنائية والأمنية بطاقات الإئتمان، دار الجامعة الجديدة، الإسكندرية، 2007.

9- بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011.

10- توفيق محمد الشاوي، حرمة الأسرار الخاصّة ونظرية عامّة للتفتيش، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006.

11- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالأنترنيت، دار النهضة العربية، القاهرة، 2002.

12- حازم محمد حنفي، الدليل الالكتروني ودوره في المجال الجنائي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2017.

13- حسن طاهر داوود، جرائم نظم المعلومات، الطبعة الأولى، الرياض، 2000.

14- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الانترنيت، دراسة مقارنة، دار النهضة العربية، القاهرة، 2009.

15- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنيت، دار الثقافة، عمان، 2011.

16- خالد مختار الفار، إسماعيل بابكر محمد، التحقيق الجنائي في جرائم الحاسوب، الطبعة الأولى، دار عزّة للنشر والتوزيع، أسيوط، 2010.

17- خالد ممدوح ابراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، الإسكندرية، 2009.

18- خالد ممدوح إبراهيم، الجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2009.

19- خثير مسعود، الحماية الجنائية لبرامج الكمبيوتر، دار الهدى، الجزائر، 2010.

20- خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، بدون بلد نشر، 2012.

21- دليلة جلول، الأسس النفسية للتحقيق الجنائي، دار هومة، الجزائر، 2015.

22- رامي متولي القاضي، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الإتفاقيات والمواثيق الدولية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2011.

23- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية، 2003.

24- رشدي محمد علي محمد عيد، الحماية الجنائية الموضوعية للمعلومات عبر شبكة الانترنيت، دار النهضة العربية، القاهرة، 2013.

25- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2012.

26- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية ودار شتات للنشر والبرمجيات، مصر، 2011.

27- سامي حسن الحسيني، النظرية العامّة للتفتيش، الطبعة الأولى، دار النهضة العربية، القاهرة، 1972.

28- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، 2006.

29- سراج الدين الروبي، آلية الإنتربول في التعاون الدولي الشرطي، الطبعة الثانية، الدار المصرية اللبنانية للطباعة والنشر، 2001.

30- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى، دار النهضة العربية، القاهرة، 1999.

31- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013.

32- سليم علي عبده، التفتيش في ضوء أصول المحاكمات الجزائية الجديدة، الطبعة الأولى، منشورات زين الحقوقية، بيروت، لبنان، 2006.

33- سهيل محمد العزام، الوجيز في جرائم الأنترنيت، الطبعة الأولى، مكتبة الجامعة الأردنية، 2009.

34- سيف بن الراشد الحوسني، جرائم التجارة الإلكترونية، دراسة مقارنة، السحاب للنشر والتوزيع، سلطنة عمان 2010.

35- صليحة علي صداقة، الإبعاد القانوني والأخلاقي للمعلوماتية الصحية، دار المطبوعات الجامعية، الإسكندرية ،2017.

36- ضياء علي أحمد نعمان، الغش المعلوماتي الظاهرة والتطبيقات، الطبعة الأولى، المطبعة والوراقة الوطنية، مراكش، 2011.

37- طارق عفيفي صادق أحمد، الجرائم الإلكترونية، جرائم الهاتف المحمول، الطبعة الأولى المركز القومي للإصدارات القانونية، القاهرة، 2015.

38- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، دار الجامعة الجديدة، الإسكندرية، 2010.

39- عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015.

40- عادل عبد العال إبراهيم خراشي، دور الضبطية الإدارية والقضائية، في مكافحة جرائم بطاقات الإئتمان الإلكترونية والتعاون الأمني الدولي حيالها، دار الجامعة الجديدة، الإسكندرية، 2015.

41- عبد الحميد الشواربي، إذن التفتيش في ضوء الفقه والقضاء، منشأة المعارف، الإسكندرية، بدون سنة نشر.

42- عبد الرحيم بن بوعيدة ، ضياء علي أحمد نعمان ، موسوعة التشريعات الإلكترونية المدنية و الجنائية – التشريع المغربي و العربي و الفرنسي الاتفاقيات العربية و الأوروبية و الدولية–، الجزء الأول، الطبعة الأولى، المطبعة و الوراقة الوطنية، مراكش ، 2010.

43- عبد الرحيم بن بوعيدة ، ضياء علي أحمد نعمان ، موسوعة التشريعات الإلكترونية المدنية و الجنائية – التشريع المغربي و العربي و الفرنسي الاتفاقيات العربية و الأوروبية و الدولية–، الجزء الثاني، الطبعة الأولى، المطبعة و الوراقة الوطنية، مراكش ، 2010.

44- عبد الصبور عبد القوي علي مصري، الجريمة الإلكترونية، الطبعة الأولى، دار العلوم للنشر والتوزيع، القاهرة، 2008.

45- عبد العال الديربي، محمد صادق، الجرائم الإلكترونية، الطبعة الأولى، المركز القومي للإصدارات القانونية، القاهرة، 2012.

46- عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنيت، دار الفكر الجامعي، الإسكندرية، 2006.

47- عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر والانترنيت في القانون العربي النموذجي، دار الكتب القانونية، القاهرة، 2007.

48- عبد الفتاح بيومي حجازي، الجوانب الإجرائية لأعمال التحقيق الابتدائي في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 2009.

49- عبد الفتاح بيومي حجازي، نحو صياغة نظرية عامة في علم الجريمة والمجرم المعلوماتي، الطبيعة الأولى، منشأة المعارف، الإسكندرية، 2009.

50- – عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.

51- عبد الله حسين علي محمود، سرقة المعلومات المخزّنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2001.

52- عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والانترنيت(الجرائم الإلكترونية)، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

53- عبد الواحد إمام مرسي، التحقيق الجنائي علم وفن- بين النظرية و التطبيق–، بدون بلد النشر، بدون سنة النشر.

54- عكروم عادل، المنظمة الدولية للشرطة الجنائية والجريمة المنظمة كآلية لمكافحة الجريمة المنظمة، دار الجامعة الجديدة، الإسكندرية، 2013.

55- عفيفي كامل عفيفي، جرائم الكمبيوتر، وحقوق المؤلف والمصنّفات الفنية ودور الشرطة والقانون، الطبعة الثانية، منشورات الحلبي الحقوقية، بيروت، لبنان، 2007.

56- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والانترنيت، الطبعة الأولى، عالم الكتب الحديثة، أربد، الأردن، 2004.

57- علي حسن محمد الطوالبة، الجرائم الإلكترونية، الطبعة الأولى، جامعة العلوم التطبيقية، مملكة البحرين، 2008.

58- علي عدنان الفيل، الإجرام الإلكتروني، الطبعة الأولى، منشورات زين الحقوقية، الاسكندرية، 2011.

59- علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، المكتب الجامعي الحديث، الاسكندرية، 2012.

60- عمرو أحمد حسبو، حماية الحريات في مواجهة نظم المعلومات- دراسة مقارنة-، دار النهضة العربية، القاهرة، 2000.

61- عمرو عيسى الفقي، الجرائم المعلوماتية، جرائم الحاسب الآلي والانترنيت في مصر والدول العربية، المكتب الجامعي الحديث، مصر، بدون سنة نشر.

62- فاضل زيدان محمد، سلطة القاضي الجنائي في تقدير الأدلة، الطبعة الأولى، دار الثقافة، عمان، 2006.

63- فتوح الشاذلي، عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي الحقوقية، بيروت، لبنان، 2003.

64- فريد منعم جبور، حماية المستهلك عبر الانترنيت ومكافحة الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010.

65- لحسن ناني، التحقيق في الجرائم المتصلة بتكنلوجية المعلوماتية، بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، بدون بلد النشر، 2017.

66- مجدي عبد الملك، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، الإسكندرية، 2011.

67- محمد أمين الرومي، جرائم الكمبيوتر والانترنيت، دار المطبوعات الجامعية، الإسكندرية، 2003.

68- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، سنة 1993.

69- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، عمان، 2004.

70- محمد حماد مرهج الهيتي ، جرائم الحاسوب، ماهيتها، موضوعها، أهم صورها، والصعوبات التي تواجهها، الطبعة الأولى، دار المناهج للنشر والتوزيع، عمان، 2006.

71- محمد خليفة، الحماية الجنائية المعطيات الحاسب الآلي، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

72- محمد طارق عبد الرؤوف الخن، جريمة الاحتيال عبر الانترنت، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2011.

73- محمد عبد الله إبراهيم، المواجهة الأمنية لجرائم شبكة المعلومات الدولية، بدون بلد نشر، 2016.

74- محمد عبد الله أبو بكر سلامة، جرائم الكمبيوتر والانترنيت، المكتب العربي الحديث، الإسكندرية، 2007.

75- محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنيت، الطبعة الثانية، دار النهضة العربية، 2009.

76- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الالكترونية، الطبعة الأولى، دار الفكر والقانون، 2015.

77- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر/ مصر،2012 .

78- محمد محمود المكاوي، الجوانب الأخلاقية والاجتماعية والمهنية للحماية من الجرائم المعلوماتية، الطبعة الأولى، المكتبة العصرية للنشر والتوزيع، مصر، 2010.

79- محمد مصطفى الشقيري، السرية المعلوماتية، ضوابطها وأحكامها الشرعية، الطبعة الأولى، دار البشائر الإسلامية، بيروت، لبنان، 2008.

80- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة للنشر والتوزيع، عمان، 2004.

81- مدحت محمد عبد العزيز إبراهيم، الجرائم المعلوماتية الواقعة على النظام المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة ،2015.

82- مصطفى محمد موسى، الجهاز الإلكتروني لمكافحة الجريمة، الطبعة الأولى، بدون دار نشر، 2001.

83- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، الطبعة الأولى، مطابع الشرطة، القاهرة، 2008.

84- **ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، مصر، 2006.**

85- منتصر سعيد حمودة، المنظمة الدولية للشرطة الجنائية الإنتربول، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008.

86- منى جاسم الكواري، التفتيش شروطه وحالات بطلانه، الطبعة الأولى، منشورات الحلبي الحقوقية، لبنان، 2008.

87- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية ، الطبعة الأولى، منشورات الحلبي، 2005.

88- ناير نبيل عمر، الحماية الجنائية للمحل الإلكتروني في جرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2012.

89- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الانترنيت في مرحلة جمع الاستدلالات، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية،2007.

90- نجاة بن مكي، السياسة الجنائية لمكافحة جرائم المعلوماتية، منشورات دار الخلدونية، الجزائر، 2017.

91- نسرين عبد الحميد نبيه، الجريمة المعلوماتية والمجرم المعلوماتي، منشأة المعارف، الإسكندرية 2008.

92- نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة، عمان، الأردن، 2008.

93- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، 1994.

94- هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.

95- هلالي عبد اللاه أحمد، إلتزام الشاهد بالإعلام في الجرائم المعلوماتية، الطبعة الأولى، دار النهضة العربية، القاهرة، 1997.

96- هلالي عبد اللاه أحمد، حجية المخرجات الكمبيوترية في المواد الجنائية، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.

97- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.

98- هلالي عبد اللاه احمد، كيفية المواجهة التشريعية لجرائم المعلوماتية، في النظام البحريني على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، 2011.

99- وضاح محمود الحمود ونشأت مفطي، جرائم الانترنيت، دار المنار للنشر، عمان، 2005.

100- وليد الزيدي، القرصنة على الانترنيت والحاسوب، الطبعة الأولى، دار أسامة للنشر والتوزيع، عمان، الأردن، 2003.

101- يوسف حسن يوسف، الجرائم الدولية للأنترنت، الطبعة الأولى، المصدر القومي للإصدارات القانونية، القاهرة، مصر، 2011.

رابعا: الرسائل الجامعية.

أ- رسائل الدكتوراه.

1- إبراهيم إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980.

2- أحمد سعد محمد الحسني، الجوانب الإجرائية الناشئة عن استخدام الشبكات الإلكترونية، أطروحة الدكتورة، كلية الحقوق، قسم القانون الجنائي، عين شمس، مصر، 2012.

3- إسماعيل طواهري، الاقتناع الشخصي للقاضي في المواد الجنائية، أطروحة دكتوراه، كلية الحقوق، فرع القانون العام، جامعة الجزائر 1، 2014/2013.

4- الموسوس عتو، حماية الحق في الخصوصية في القانون الجزائري في ظل التطور العلمي والتكنولوجي دراسة مقارنة، رسالة دكتوراه، جامعة سيدي بلعباس،2014-2015.

5- بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض، 2006.

6- حبيب عباسي، الجريمة المنظمة العابرة للحدود، أطروحة دكتوراه في العلوم، تخصص القانون العام، جامعة أبي بكر بلقايد، تلمسان، 2017/2016.

7- جمال براهيمي، التحقيق الجنائي في الجرائم الالكترونية، أطروحة دكتوراه، تخصص قانون كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2018.

8- خالد بن مبارك القريوي القحطاني، التعاون الأمني الدولي في مواجهة الجريمة المنظمة عبر الوطنية، رسالة دكتوراه في الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية، الرياض، 2006.

9- سالم محمد سليمان اوجلي، احكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 1997.

10- سامح أحمد بلتاجي موسى، الجوانب الإجرامية للحماية الجنائية لشبكة الانترنيت، رسالة دكتوراه في الحقوق، جامعة الاسكندرية، مصر 2010.

11- شريف نصر أحمد، النظرية العامّة للخبرة في المواد الجنائية، رسالة دكتوراه في الحقوق، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2010.

12- شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الإلكترونية، رسالة دكتوراه، كلية الحقوق، جامعة المنصورة، 2005.

13- صورية بورباية، قواعد الأمن المعلوماتي، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، بلعباس، 2016-2017.

14- طارق فوزي الفقي، الجوانب الإجرامية في الجرائم المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة المنوفية ،2011.

15- عادل فتحي صابر شريف، تفتيش غير المتهم، رسالة للحصول على درجة دكتوراه، كلية الحقوق، جامعة حلوان، مصر، 2010.

16- عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة أبو بكر بلقايد، تلمسان، 2017-2018.

17- علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، رسالة دكتوراه في الحقوق، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، 2011.

18- عمارة فوزي، قاضي التحقيق، أطروحة دكتوراه العلوم، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة ،2009-2010.

19- غازي عبد الرحمن هيان الرشيد، الحماية القانونية من الجرائم المعلوماتية، أطروحة أعدت لنيل شهادة دكتوراه في القانون، الجامعة الاسلامية، كلية الحقوق، لبنان، 2004.

20- فايز محمد راجب غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني أطروحة الدكتوراه، كليه الحقوق، فرع القانون الجنائي و العلوم الجنائية، جامعه الجزائر (1)، 2010-2011.

21- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، مصر، 2012.

22- كمال حطاب، الحماية الجزائية للتجارة الإلكترونية، أطروحة دكتوراه في العلوم، تخصص علوم قانونية ، كلية الحقوق والعلوم السياسية، فرع العلوم الجنائية، جامعة جيلالي اليابس، سيدي بلعباس، 2014-2015.

23- محمد حسن الكندري، المسؤولية الجنائية عن التلوث البيئي، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2005.

24- محمد حمد عمر الغياثين، الجرائم المعلوماتية عابرة الحدود، رسالة دكتوراه في القانون الجنائي، كلية الحقوق، قسم القانون الجنائي، جامعة القاهرة، 2013.

25- محمد فتحي محمد أنور عزّت، تفتيش شبكة الانترنيت لضبط جرائم الإعتداء على الآداب العامة والشرف والاعتبار التي تقع بواسطتها، رسالة دكتوراه في القانون، كلية الحقوق، جامعة عين الشمس، مصر.

26- مريم قسول، مبدأ مشروعية الأدلة العلمية في المواد الجنائية, رسالة دكتوراه, كلية الحقوق والعلوم السياسية, قسم الحقوق, جامعة جيلالي اليابس, سيدي بلعباس, 2015-2016.

27- ممدوح حسن مانع العد، ضمانات المتهم أثناء التحقيق ومدى مراعاة مبادئ القانون الدولي لحقوق الإنسان في المجال الجنائي، رسالة الدكتوراه في القانون، كليه الحقوق، جامعة الإسكندرية.

28- منى فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات صورها ومشاكل إثباتها، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.

ب- رسائل الماجيستير.

1- حسيبة محي الدين، ضمانات المشتبه فيه أثناء التحريات الأولية، رسالة الماجستير، كليه الحقوق، جامعه الإسكندرية، مصر، 2010 .

2- خديجة بتقة، السياسة الأمنية الأوربية في مواجهة الهجرة غير الشرعية، مذكرة مقدمة لنيل شهادة الماجستير، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية والعلاقات الدولية، جامعة محمد خيضر، بسكرة، 2013.

3- عبد الله بن الحسين أل حجراف القحطاني، تطوير مهارات التحقيق الجنائي والادعاء العام، مذكرة ماجستير، كلية الدراسات العليا، الرياض،2014.

4- عبد الله بن عبد العزيز عبد الله الخثعي، التفتيش في الجرائم المعلوماتية في النظام السعودي دراسة تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

5- عماد أحمد هاشم الشيخ خليل، ضمانات المتهم أثناء مرحلة الاستجواب، مذكرة ماجيستر في القانون الجنائي، كلية الحقوق، جامعة العالم الأمريكية، 2006.

6- معتوق عبد اللطيف، الإطار القانوني لمكافحة جرائم المعلوماتية في التشريع الجزائري والتشريع المقارن، مذكرة ماجستير في العلوم القانونية التخصص قانون جنائي وعلوم جنائية، جامعة الحاج لخضر باتنة ،2011-2012.

7- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية، رسالة ماجستير في العلوم الجنائي، جامعة الحاج لخضر، باتنة، 2012- 2013.

8- هدى أحمد العوضي، استجواب المتهم في مرحلة التحقيق الابتدائي، مذكرة ماجستير في الحقوق، تخصص قانون عام، جامعة المملكة، البحرين، 2009.

9- يوسف صغير، الجريمة المرتكبة عبر الأنترنيت، مذكرة لنيل شهادة الماجستير في القانون، قسم الحقوق، جامعة مولود معمري، تيزي وزو، 2013/03/06.

خامسا: المقالات والمداخلات الأكاديمية.

أ- المقالات العلمية.

1- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، مجلّة المحلّية العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، 2013.

2- أسامة بن غانم العبيدي، الإثبات بالدليل الإلكتروني في الجرائم المعلوماتية، مجلة جامعة الملك سعود، الحقوق والعلوم السياسية(1)، المجلد الخامس والعشرون، الرياض ، المملكة العربية السعودية، 2013.

3- الحسن بيهي، الجريمة الإلكترونية مقاربة قانونية وقضائية، مجلة الواحة القانونية، العدد الثاني، 2006.

4- باسم محمد شهاب، عملية التسرّب، الحقيقة التشريعية، مقال منشور في مجلة الحقوق، مجلّة فصلية علمية محكمة، تصدر عن مجلس النشر العلمي، جامعة الكويت، العدد 04، ديسمبر 2013.

5- حسام محمد رمضان ،تطبيقات المحاكاة الحاسوبية في التخطيط والتدريب على إدارة الكوارث، مقال منشور بمجلة البحوث الأمنية ،أكاديمية الملك فهد، المجلد 11، العدد 22، أكتوبر 2002.

6- حسني درويش عبد الحميد ،البحث الجنائي المعاصر ،مقال منشور بمجلة البحوث الأمنية، كلية الملك فهد، المجلد 10، العدد 1522، نوفمبر 2001.

7- دلال مولاي ملياني، التفتيش في جرائم تكنولوجيا الإعلام و الاتصال، مقال منشور بمجلة القانون والعلوم السياسية، العدد 03، ، منشورات معهد الحقوق، المركز الجامعي النعامة، جانفي 2016.

8- راشد بشير إبراهيم، التحقيق الجنائي في جرائم تقني المعلومات، دراسة تطبيقية على إمارة أبوظبي، مقال منشور ضمن مجلة الدراسات الإستراتيجية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الإستراتيجية، العدد 131، 2008.

9- زوزو هدى، التسرّب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلّة دفاتر السياسة والقانون، مجلة جامعية محكمّة في الحقوق والعلوم السياسية، تصدر عن جامعة قاصدي مرباح، ورقلة، العدد الحادي عشر، جوان 2014.

10- سرحان حسن المعيني التحقيق في جرائم تقنيه المعلومات، مجلة الفكر الشرطي، المجلد عشرون، العدد الرابع، الشارقة، الإمارات العربية المتحدة، 2011.

11- عبد الحميد كرود، التسول النصب والاحتيال، عبر الانترنت، مجلة الدركي، العدد 16، 2008.

12- عزيزة رابحي، التفتيش في نظم المعالجة الآلية للمعطيات، مقال منشور بمجلة القانون والعلوم السياسية، العدد03، جانفي 2016، منشورات معهد الحقوق، المركز الجامعي، ولاية النعامة.

13- عصماني ليلى، صهيب سهيب غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، مجلة القانون، المجتمع والسلطة، المجلد 9، العدد 2، جامعة وهران، 2020.

14- علاء الدين عبد الله الحواصنة وبشار طلال المومني، النظام القانوني للصورة الفوتوغرافية، مجلة الشريعة والقانون، العدد 53، جامعة الإمارات العربية المتحدة، 2013.

15- علاوة هوام، التسرّب كآلية للكشف عن الجرائم في قانون الإجراءات الجزائية الجزائري، مقال منشور ضمن مجلة الفقه والقانون، العدد الثاني، المغرب، 2012.

16- محمد حسن السراء، الأساليب الحديثة والمهارات المتقدمة في تحقيق الجرائم الالكترونية، مجلة الفكر الشرطي، المجلد 20، العدد الرابع، الشارقة، الإمارات العربية المتحدة، 2011.

17- محمد محمد درويش، التطلعات المستقبلية نحو استخدام أسلوب المحاكاة في مجال التدريب الأمني بأكاديمية الشرطة، مقال منشور بمجلة الأمن العام المصرية، العدد 46.

18- محمد نور الدين عبد الحكيم، دور نظم المعلومات في المجال الشرطي، مقال منشور بمجلة الفكر الشرطي ،المجلد العاشر، يناير 2002.

19- ناصر بن محمد البقمي، أهمية الأدلة الرقمية في الإثبات الجنائي، دراسة وفق الأنظمة السعودية، الفكر الشرطي، المجلد 20، العدد4، الشارقة، الإمارات العربية المتحدة،2011.

ب- المداخلات العلمية.

1- أشرف صلاح الدين، طرق الحماية التكنولوجية بأنواعها وأشكالها المختلفة، أعمال مؤتمرات حول مكافحة الجريمة عبر الأنترنيت، المنظمة العربية للتنمية الإدارية، القاهرة، 2010.

2- دلال مولاي ملياني، التفيش في جرائم تكنولوجيا الإعلام و الإتصال، مقال منشور بمجلة القانون والعلوم السياسية، العدد 03، منشورات معهد الحقوق، المركز الجامعي، النعامة، جانفي 2016.

3- شرف الدين وردة، عيساني علي، المساعدة القضائية الدولية المتبادلة في مجال جمع الأدلة الرقمية، وفقا للإتفاقية العربية لمكافحة جرائم تقنية المعلومات لسنة 2010، مداخلة للمشاركة في فعاليات الملتقى الدولي حول أدلّة الإثبات الجنائية في التشريعات المقارنة المنعقد يومي 25-26 أبريل 2018، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار.

4- رجم جمال، مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ، مجلة الجيش، مجلة شهرية للجيش الشعبي الوطني، عدد 599، تصدر عن مؤسسة المنشورات العسكرية، جوان، 2013.

5- رشيدة كابوية، حجية الدليل الرقمي في الإثبات الجنائي، ملتقى دولي حول أدلة الإثبات الجنائية الحديثة في التشريعات المقارنة، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار، يومي 26/25 أبريل 2018.

6- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف سعيد المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث مقدم إلى المؤتمر العربي الأول لعلوم الأدلّة الجنائية والطب الشرعي، الرياض، 2007.

7- عمرو حسين عباس، أدلة الإثبات الجنائي والجرائم الإلكترونية، بحث مقدم إلى المؤتمر الإقليمي حول تحديات تطبيق الملكية الفكرية في الوطن العربي، خلال الفترة 26-2008/04/27، مقر جامعة الدول العربية.

8- كريم راشد، بحث إستراتيجية المديرية العامة للأمن الوطني في مكافحة الجريمة المعلوماتية مقدم لليوم الدراسي حول مخاطر الانترنيت وجرائم الإعلام من تنظيم مخبر الدراسات القانونية ومسؤولية المهنيين المنعقد بتاريخ 14 فبراير 2019، كلية الحقوق والعلوم السياسية، جامعة طاهري محمد، بشار.

9- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنيت من 1 - 3 ماي هي 2000، المجلد الثالث، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الامارات العربية المتحدة، 2004.

10- محمد الأمين البشري، تأهيل المحققين في جرائم الحاسب الآلي وشبكات الانترنيت، بحث مقدم في الحلقة العلمية بعنوان " الأنترنيت والإرهاب"، المنظمة من طرف جامعة نايف العربية للعلوم الأمنية بالتعاون مع جامعة عين شمس، دبي، في الفترة الممتدة ما بين 15 إلى 2008/11/19.

11- محمد عبد الرحيم سلطان العلماء، جرائم الأنترنيت والاحتساب عليها، بحوث مؤتمر القانون و الكمبيوتر و الأنترنيت من 1-3 ماي 2000، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، المجلد الثالث، الطبعة الثالثة، 2004.

12- محمد محمد الألفي، العوامل الفاعلة في إنشاء جرائم الارهاب عبر الأنترنيت، أعمال المؤتمرات حول مكافحة الجريمة عبر الأنترنيت، المنظمة العربية للتنمية الادارية، القاهرة، مصر، 2010.

13- منصف خطابي، ضمانات المشتبه فيه أثناء التحريات الأولية، مذكرة تخرج لنيل إجازة المدرسة العليا للقضاء، الدفعة السابعة عشر، الجزائر، 2006-2009.

14- موسى مسعود أرحومة، الاشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون الذي تنظمه أكاديمية الدراسات العليا طرابلس، ليبيا خلال الفترة 28-2009/10/29.

15- هدى حامد قشقوش، الإتلاف غير العمدي لبيانات وبرامج الحاسب الإلكتروني، بحوث مؤتمر القانون والكمبيوتر والانترنيت، المجلد الثالث، الطبعة الثالثة، جامعة الإمارات العربية المتحدة، كلية الشريعة والقانون، من 01 إلى 03 ماي 2000.

سادسا: الوثائق القانونية الرسمية.

أ- الوثائق القانونية الرسمية العربية:

1- دستور الجمهورية الجزائرية الديمقراطية الشعبية، المعدل سنة 2020، الصادر بالمرسوم الرئاسي رقم 20-442، المؤرخ في 30 ديسمبر 2022، الجريدة الرسمية العدد 82، الصادرة في 30 ديسمبر 2020.

2- دستور الإمارات العربية المتحدة، الجريدة الرسمية ، السنة الأولى، بتاريخ 1971/12/31، المعدل في سنة 2009.

ب-الاتفاقيات الدولية.

1- الإعلان العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة 217 ألف (د-3) المؤرخ في 10 كانون الأول، ديسمبر 1948.

2- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، اعتمدت وعرضت للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة رقم 25، الدورة 55، المؤرخة في تشرين الثاني، نوفمبر 2000، وثيقة رقم: A/RES/55/25.

3- ديباجة الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الجمهورية الفرنسية المتعلق بالتعاون في مجال الأمن ومكافحة الإجرام المنظم، الموقع بالجزائر في 25 أكتوبر 2003، المصادق عليه بموجب مرسوم رئاسي رقم 07- 375 مؤرخ في 01 ديسمبر 2007، الجريدة الرسمية العدد 77 ، بتاريخ 9 ديسمبر 2007.

4- ديباجة الاتفاقية الجزائرية الديمقراطية الشعبية والمملكة الإسبانية في مجال الأمن ومكافحة الإرهاب والجرام المنظم، الموقعة بالجزائر في 15 جوان 2008، المصادق عليها بموجب المرسوم الرئاسي 08 / 427 المؤرخ في 28 ديسمبر، ج.ر.ج.ج، العدد 05، تاريخ 21 جانفي 2009.

5- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة، بتاريخ 21 ديسمبر 2010، وثيقة متاحة على موقع الشبكة القانونية العربية، إدارة الشؤون القانونية التابعة للأمانة العامة لجامعة الدول العربية، متوفر على الموقع الإلكتروني: www.arablegalnet.org)

ج- القوانين

1- القانون رقم 01/06 المؤرخ في 20 فبراير 2006، يتعلق بالوقاية من الفساد ومكافحته، جريدة رسمية للجمهورية الجزائرية، العدد 14، بتاريخ 18 مارس 2006، المعدل والمتمم.
2- القانون رقم 22/06 المؤرخ في 20 ديسمبر 2006، يعدل ويتمم الأمر رقم 155/66 المؤرخ في 8 يونيو 1966 والمتضمن قانون الإجراءات الجزائية.
3- القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والاتصال، ج.ر.ج.ج رقم 47 ، الصادرة في 2009/08/16.
4- القانون رقم 04/15 المؤرخ في 2015/02/01 المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية العدد 06، الصادر في 2015/12/10.
5- القانون رقم 18-04، المؤرخ في 10 ماي 2018، يحدد القواعد المتعلقة بالبريد والاتصالات الإلكترونية، الجريدة الرسمية العدد27، الصادرة بتاريخ 13 ماي 2018.
6- القانون 18- 07 المؤرخ في 10 جوان سنة 2018 و المتعلق بحماية الأشخاص الطبيعيين ذات الطابع الشخصي ،الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ،العدد 34.
7- القانون 05/20 المؤرخ في 2020/04/28 ،يتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتها، ج.ر.ج.ج رقم 25 الصادرة في 2020/04/29.

د- الأوامر.

1- الأمر 155/66 المؤرخ في 1966/06/08 المتضمن قانون الإجراءات الجزائية الجريدة الرسمية العدد 48 ، الصادرة في 1966/06/10 المعدل والمتمم بالأمر 11/21 الصادر في 2021/08/25، ج.ر.ج.ج رقم65 الصادرة في 2021/08/26.
2- الأمر 156/66 المؤرخ في 1966/06/08 المتضمن قانون العقوبات ج.ر.ج.ج رقم 49 الصادرة في 1966/06/11 المعدل والمتمم بالقانون رقم 08/21 الصادر في 2021/06/08، ج.ر.ج.ج رقم 45 الصادرة في 2021/06/09.

3- الأمر 02/15 المؤرخ في 23 يوليو 2015، يعدّل ويتمم الأمر 155/66 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائرية، الجريدة الرسمية للجمهورية الجزائرية، العدد 84، السنة الثالثة والأربعون، الصادرة في 24 ديسمبر 2006.

هـ- المراسيم والقرارات الوزارية.

1- المرسوم الرئاسي رقم 183/04، الصادر في 06/26/ 2004، يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، ج.ر.ج.ج رقم41، الصادرة في 27 /2004/06.

2- المرسوم الرئاسي رقم 323/07، الصادر في 2007/10/23، المتضمن التصديق على اتفاقية التعاون القضائي والإعلانات والانابات القضائية وتنفيذ الأحكام و تسليم المجرمين بين الجمهورية الجزائرية الديمقراطية الشعبية ودولة الامارات العربية المتحدة الموقعة بالجزائر بتاريخ 12 اكتوبر 1988، ج.ر.ج.ج رقم ،67 الصادرة في 24 /2007/10 .

3- المرسوم رئاسي رقم 07 –35، مؤرخ في 23 أكتوبر 2007، يتضمن التصديق على اتفاقية التعاون القانوني والقضائي بين حكومة الجهورية الجزائرية الديمقراطية الشعبية وحكومة جمهورية السودان، الموقعة بالجزائر في 24 يناير 2003، الجريدة الرسمية للجمهورية الجزائرية، العدد 68، بتاريخ 28 أكتوبر 2007.

4- المرسوم الرئاسي رقم 151/08، المؤرخ في 26 ماي 2008، يتضمن إحداث مدرسة للشرطة القضائية تابعة للدرك الوطني، ج.ر.ج.ج رقم 27، الصادرة في 28 /2008/05.

5- المرسوم الرئاسي رقم 143/09، الصادر في 2009/04/27، يتضمن مهام الدرك الوطني وتنظيمه، ج.ر.ج.ج رقم 26، الصادرة في03 /2009/05.

6- المرسوم الرئاسي رقم 252/14 المؤرخ في 8 /2014/09 المتضمن التصديق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرر بالقاهرة بتاريخ 21ديسمبر 2010، ج.ر.ج.ج رقم 57 الصادرة في 2014/09/28.

7- المرسوم الرئاسي 15-261، المؤرخ في 8 أكتوبر 2015، يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53، الصادرة بتاريخ 8 أكتوبر 2015.

8- المرسوم الرئاسي 172/19 الصادر في 06/06/ 2019، يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنظيمها وكيفيات يسرها، ج.ر.ج.ج رقم37، الصادرة في 09 /2019/06.

9- المرسوم الرئاسي رقم 05/20 الصادر في 2020/01/20، يتعلق بوضع منظومة وطنية لأمن الأنظمة المعلوماتية ج.ر.ج.ج رقم 04 الصادرة في 2020/01/21.

8- المرسوم الرئاسي رقم 20-183، المؤرخ في 13 يوليو 2020،يتضمن تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 40، الصادرة بتاريخ 18 جويلية 2020.

9- المرسوم التنفيذي رقم 348/06 الصادر في2006/10/05، يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، ج.ر.ج.ج رقم 63، الصادرة في 08 /2006/10.

10- المرسوم التنفيذي رقم 10-322، المؤرخ في 22 ديسمبر 2010، المتضمن القانون الأساسي الخاص بالموظفين المنتمين للأسلاك الخاصة بالأمن الوطني، جريدة رسمية للجمهورية الجزائرية، العدد78، بتاريخ 26 ديسمبر 2010.

11- القرار الرئاسي رقم 304 بشأن الموافقة على إتفاقية المساعدة القضائية المتبادلة في المواد الجنائية بين حكومتي جمهورية مصر العربية وجمهورية الهند، بتارخ 2008/01/08،الجريدة الرسمية العدد 21 بتاريخ 21 ماي 2009 .

12- القرار الوزاري الصادر في 14 /2007/04 يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للأدلّة الجنائية وعلم الإجرام، ج.ر.ج.ج رقم 36، الصادرة في 2007/06/03.

آآ- الوثائق القانونية الرسمية العربية.

1- دستور الإمارات العربية المتحدة، الجريدة الرسمية، السنة الأولى، بتاريخ 1971/12/31.

2- قانون رقم 35 لسنة 1992، والمتعلق بإصدار قانون الإجراءات الجزائية، الجريدة الرسمية لدولة الإمارات -العربية المتحدة، العدد 233مكرر، السنة 22، بتاريخ 1992/01/26.

3- قانون الاتصالات الأردني رقم 13 لسنة 1995 الجريدة الرسمية رقم 4072، بتاريخ 1995/10/01، المعدّل بموجب القانون رقم 21 لسنة 2011 والصادر بالجريدة الرسمية بتاريخ 2011/04/21.

4- قانون الجرائم الإلكترونية الأردني لسنة 2015، الجريدة الرسمية العدد 5631.

5- قرار جمهوري بالقانون رقم 13 لسنة 1994 بشأن الإجراءات الجزائية ،المؤرخ بتاريخ 8 جمادى الأول 1415 الموافق لـ 12 أكتوبر 1994 ،الجريدة الرسمية العدد 19/4 .

سابعا:المواقع الالكترونية.

1- موقع المديرية العامة للأمن الجزائري www.algeriepolice.dz

2- موقع شبكة قوانين الشرق www.eastlaw.com

3- الدستور الأردني، متاح على الموقع الإلكتروني:
http://www.parliament.jo/node/137

4- الدستور المصـري لسنة 2014، مشار إليه على الموقع الإلكتروني:
http://www.youm7.com

5- الموقع الرسمي للأفريبول : www.el-mass.com/dz.

6- قانون رقم 575-2004، المؤرخ في 21 جوان 2004، المتعلق بالثقة في الاقتصاد الوطني، متاح على الموقع الإلكتروني: https:// wipolex.wipo.in

7- حسين بن سعيد الغافري، التحقيق وجمع الأدلة في الجرائم المتعلقة بشبكة الحاسوب، متوفر على موقع الالكتروني شبكة القوانين شرق www.eastlaw.com

8- لموسخ محمد، تنازع الاختصاص في الجرائم الإلكترونية، مقال منشور ضمن مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، 2013، مشار إليه في الموقع الإلكتروني:revenue_univ_ourgla.dz

9- محمد معسكر، مقال الكتروني بعنوان تعريف لعملية التحقيق الجنائي الرقمي، متوفر على الموقع الالكتروني: http :www.isecurity.org

10- محمد معسكر، مقال الكتروني بعنوان مقدمة لمراحل التحقيق الجنائي وخطواته متوفر على الموقع الالكتروني: http://www. Isecurity.Org..

11- الدرك الوطني الجزائري، مقال منشور على موقع ويكيبيديا، الموسوعة الحرة، على الرابط الإلكتروني:

12- الدرك-الوطني-الجزائري http :ar.wikipediaorg/wiki/

13- الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، المحررة بالقاهرة، بتاريخ 21 ديسمبر 2010، وثيقة متاحة على موقع الشبكة القانونية العربية، إدارة الشؤون القانونية التابعة للأمانة العامة لجامعة الدول العربية، الموقع الالكتروني: .WWW.ARABLEGALNET.ORG

❷- المراجع باللغة الأجنبية.

A- Les ouvrages.

1- André (Lucas),Jean Droit de l'informatique et de L'internet, édition Dalloz, collection thèmes (droit privé), France, 2001.

2- CLAUDE Soyer ،Droit Pénal et Procédure Pénale ،L.G.D.J ،Paris ، France ،12 éme édit ،1996.

3- DECAUX Emanuel, la protection de la vie privée au regard des données informatiques, droit fanda mentaux, n° 7,janvier 2008-decembre 2009.

4- FREDERIC Deboue ،FRANÇOIS Falletti et EMANUAL Dupic،Précis de droit pénal et de procédure pénal ،PUF ،Paris ،France ،5éme édit mise a jour ،2013.

5- JACQUES Leroy،Procédure Pénale Librairie Général de Droit et de Juris Prudence،L'extenso éd . Paris cedex 2009.

6- Kenneth l'Auden, Manegement Information System managing the digital
firm ", Seventh édition , prentice bhall , inc,new jersey , USA , 2004.

7- LUCAS de Lyssac (Marie Paul),Une Information Seul Est-Elle Susceptible De Vol D'une Autre Atteinte Juridique Aux Bien . Dallozsiery ,1985.

8- Masse (Michel) infaction contre pordre financier, rev , sc , crim, janvier1985 N1.

9- MICHEL Quille, Ouropol, La Criminalité Organisée , Sous La Direction De Marcel , LECLERC, Paris, 1996.

10- Parker (Done B), Fighting computer crime « A new fram work for protecting information , john wiley and son , 1998.
11- - QUEMENER Myriam ،YVES Charpenel ،Cyber criminalité ، Droit Pénal Appliqué،Economica ،Paris ،2010.
12- - Ravanas (J), la protection des personnes contre la réalisation et la publication de leur image ,L.D.J ,Paris ,1978.
13- Roden (Adrian), computer crime and the law , CLT .1991. VOL 15.
14- 16- tatty (Richard) and hard castle (Antony) , computer- Related Crime in informations technology and the law, Macmilla publishers, UK, 1986.
15- Thompson (David), currrent trends in computer control crime, computer quarterly, vol 9 N 1, 1991.

B- Textes réglementaires.

1- Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des Etats de l'Union économique Benelux, de la République Fédérale d'Allemagne et de la République Française relatif à la suppression graduelle des contrôles aux frontières communes, convention d'application de l'accord de schengen le 19 juin 1990.

2-Code pénal ,109 e ,édition dalloz2012 ,

3-Code de procédure pénal 54 e, édition dalloz ,2013 France.

4-Loi nº 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

5-Loi n° 72 – 1226 du 29 décembre 1972.

6-Cour de cassation : Chambre Criminelle Lecture de 9 Octobre 1978, N° 76 .92.075 publier au bulletin.

Books :

1- Ball (Leslie D) computer Crime in the information technology revolution,
2- CATALA Pierre, Ebouche D'ume Théorie Juridique De L'information, D 1984 .

3- Glough(Brayn) and mango (Paul),approaching Zero :data crime and criminal under world,1992.
4- Michel, D Rostoker and Robert H ; Rimes, computer jurisprudence, Leyel responses to the information révolution, ocona publication.
5- Tiedeman (klaus), frande et autre délits d'affaires commis d'ordinateur électroniques, rev, Dr, Pén, crime and the lawcrim n 7, Bruxelles, 1984.

الفهرس

الفهرس

الملخص.

تعد الجرائم الإلكترونية من أكبر التحديات الأمنية التي تواجه المجتمع الدولي فهي جرائم معقدة ترتكب بوسائل تقنية حديثة ومتطورة، من قبل مجرمين على مستوى عال من الذكاء مما جعل التحقيق والإثبات فيها صعب.

فرض ظهور هذا النوع من الجرائم على جهات التحقيق تحديات كبيرة لم يسبق لها مثيل، لما تتميز به من سهولة وسرعة فائقة في التنفيذ وانعدام الآثار المادية لها وكذا غياب الدليل المرئي فيها، وصعوبة الوصول إليه بالوسائل التقليدية وكذا سهولة إتلاف الدليل المادي في وقت قياسي، كل هذه العوامل استدعت إعادة النظر في وسائل المكافحة التقليدية للجريمة وأساليبها وطرق الوقاية منها، فأصبح من الضروري وضع البرامج الإستراتيجية لتحديث أجهزة العدالة وتطويرها من حيث بنيتها المؤسسية وكوادرها البشرية لتصبح قادرة من الناحية التقنية على التصدي لهذا النوع من الجرائم وضبط مرتكبيها وتقديمهم للعدالة.

الكلمات المفتاحية:

الجريمة الإلكترونية، التحقيق الإلكتروني، الدليل الإلكتروني، تكنولوجيا الإعلام.

résumé :

La cybercriminalité est l'un des grands défis de sécurité auxquels la communauté internationale est confrontée, il s'agit de crimes complexes commis, par des criminels dotés d'une intelligence supérieure, avec des moyens techniques modernes et développés ce qui rend l'enquête criminelle et l'établissement des preuves difficiles.

La parution de ce genre de crime a imposé aux juridictions d'instruction, des défis considérables et sans précédent, en raison de la facilité de son exécution, de sa rapidité, de l'absence de traces matérielles, de l'absence de preuves visuelles et même la difficulté de les avoir par les méthodes classiques, ainsi que la facilité de les effacés en un temps record. Tous ces facteurs nécessitent la reconsidération des méthodes classiques de lutte contre la criminalité ainsi que les moyens de préventions, donc il est devenu nécessaire d'élaborer des plans stratégiques pour moderniser et développer les organes judiciaires en termes de structure institutionnelle et en terme de personne pour devenir techniquement capables d'affronter ce type de crime, arrêter les auteurs et les presenter en justice.

Mots Clés :

Cybercriminalité, instruction électronique, preuve électronique , technologies de l'information.

Abstract:

Cybercrime is one of the biggest security challenges facing the international community, as it is complex crime committed by modern and advanced technical means, by criminals with a high level of intelligence, which made investigation and proof difficult,

The emergence of this type of crime poses unprecedented challenges to the investigation authorities, due to its ease and speed of execution, the absence of material effects, as well as the absence of visual evidence in it.

The difficulty is of accessing it by traditional means, as well as the ease of destroying physical evidence in a record time. All these factors called for a review of the traditional means of combating crime and its methods of prevention. It became necessary to develop strategic programs to modernize and develop justice agencies in terms of their institutional structure and human cadres to become capable of the technical aspect is to confront this type of crime, apprehend the perpetrators and bring them to justice.

Keywords:

Cybercrime, electronic investigation, Electronique evidence, information technologies.