بسم الله الرحمن الرحيم

﴿وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ وَحَمَلْنَاهُمْ فِي الْبَرِّ وَالْبَحْرِ وَرَزَقْنَاهُم مِّنَ الطَّيِّبَاتِ وَفَضَّلْنَاهُمْ عَلَىٰ كَثِيرٍ مِّمَّنْ خَلَقْنَا تَفْضِيلًا﴾[1] صدق الله العظيم

[1] (الآية 70 من سورة الإسراء)

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة أبي بكر بلقايد – تلمسان –

كلية الحقوق والعلوم السياسية

قسم الحقوق

التحقيق الجنائي في الجرائم الإلكترونية

أطروحة لنيل شهادة الدكتوراه علوم في القانون الخاص

إعداد الطالب: بن يحي إسماعيل

إشراف الأستاذ: بن عمار محمد

أعضاء لجنة المناقشة

كحلولة محمد	أستاذ	جامعة تلمسان	رئيسا
بن عمار محمد	أستاذ	جامعة تلمسان	مشرفا مقررا
هديلي أحمد	أستاذ محاضر أ	جامعة سيدي بلعباس	عضوا مناقشا
زعزوعة فاطمة	أستاذة محاضرة أ	المركز الجامعي عين تموشنت	عضوا مناقشا

السنة الجامعية 2021/2020

الإهداء

إلى كل من يحمل هذا الوطن في قلبه

إلى كل ذي قلب مخلص ينبض حبا لهذا الوطن

إلى كل من يعتصر قلبه ألما على هذا الوطن

إلى كل الشرفاء في هذا الوطن

أهدي هذا العمل المتواضع

"إنِّي رأيتُ أنَّه لا يكتُبُ إنسانٌ كتابًا في يومِه؛ إلاَّ قالَ في غَدِهِ: لو غُيِّرَ هذا لكان أحسنَ، ولو زِيدَ كذا لكان يُستَحسَنُ، ولو قُدِّمَ هذا لكان أفضلَ، ولو تُرِكَ هذا لكان أجملَ. هذا مِنْ أعظَمِ العِبَرِ، وهو دليلٌ علَى استيلاءِ النَّقصِ علَى جُملةِ البَشَرِ"

(العسقلاني)[1]

[1] تُنسب هذه المقولة إلى القاضي الفاضل عبر الرحيم بن علي البيساني العسقلاني (526 هـ – 596 هـ) وعُرف بالعسقلاني نسبة إلى مسقط رأسه "عسقلان" وهي مدينة تقع بشمال غزة بفلسطين.

شكر وامتنان

الحمد لله المعين الذي أعانني ووفقني على إنجاز هذه الرسالة، فله الحمد والشكر والثناء.

كما أتقدم بخالص شكري للأستاذ بن عمار محمد الذي تكرّم بقبول الإشراف على هذه الأطروحة، وأشكره على صبره وطيبته وسعة صدره وعلى نصحه وكل ما قدمه طيلة هذه السنوات. كما أتقدم بالشكر للأساتذة أعضاء لجنة المناقشة على قبولهم وتحملهم عناء قراءة ومناقشة هذه الرسالة.

وأتوجه بشكري لكل من شجعني على المضي قدما –ولو بكلمة–من أجل إتمام هذه الرسالة.

مقدمة

مقدمة:

الجريمة ظاهرة اجتماعية متصلة بما هو سائد داخل المجتمع من قيم وعادات وتقاليد، كما أنها تتأثر بتلك التغييرات والتطورات المستمرة التي يشهدها هذا المجتمع. وبدوره فإن التحقيق في الجريمة كان محل تأثر وتطور هو الآخر، فانتقل من نهج بدائي طغت عليه أساليب يغلب عليها الجهل والخرافة والعنف (الدجل، السحر، التعذيب...الخ)، ثم بدأ الاعتماد على تصريحات وأقوال الناس بحيث اتخذ من شهاداتهم وسيلة لإثبات الجرائم رغم ما يعاب على ذلك كون هذه الشهادات كانت في كثير من الأحيان تتخذ كوسيلة للانتقام والابتزاز من خلال شهود زور.

رويدا رويدا وبتطور المجتمعات ظهر التحقيق الجنائي كعلم وأخذ هذا العلم في التطور مستفيدا ومتأثرا بالتطورات الحاصلة بباقي العلوم الأخرى (الطب، الكيمياء، ...الخ)، وبالتالي تطورت أساليبه فظهرت المخابر العلمية وبدأ الاعتماد على الخبرة العلمية لدى فحص مسرح الجريمة (بقع الدم وبصمات الأصابع، الأسلحة والذخيرة المستعملة، ...الخ). ولاحقا ظهرت مخابر تعنى بفحص الحمض النووي (من خلال استخلاصه من خصلات الشعر أو اللعاب أو الأظافر وأجزاء أخرى من الجسم) كجزء من إجراءات التحقيق الجنائي، إلى غير ذلك من الأساليب العلمية المتطورة والتي انعكست على القانون الجنائي بشقيه الموضوعي والإجرائي.

نجم عن التطور المتسارع لوسائل الاتصالات بالموازاة مع القفزة الهائلة التي عرفها العالم في المجال التقني والتكنولوجي الغير مسبوق، ظهور أجهزة الكمبيوتر والهواتف المحمولة وتطور الوضع أكثر بتطور الأقمار الاصطناعية وما أصبحت تقدمه من خدمات. غير أن الحدث الأبرز كان ظهور "الإنترنت" واتساع شبكتها حيث أضحت تربط جميع مختلف أرجاء الكرة الأرضية بعضها ببعض وصاحبها التنافس والتسابق المحموم بين كبرى الشركات العالمية في مجال الصناعات المرتبطة بتكنولوجيا الاتصالات الحديثة، فظهرت لاحقا أجهزة الكمبيوتر المحمول والهواتف الذكية والألواح الذكية وكلها مزودة بتقنية تتيح الارتباط بشبكة الإنترنت والتي تزايدت سرعة تدفقها. هذا وشهدت أنظمة الاتصالات

اللاسلكية تطورا مذهلا بلغت الجيل الرابع (G4) ويتحدثون حاليا في سنة 2020 عن تجارب لشبكة الجيل الخامس (G5) بلغت سرعتها 1 جيجابايت (Giga byte) في الثانية وقد تصل أو تفوق سرعتها لاحقا 8 جيجابايت حسب التقديرات مما يعني المقدرة على نقل كم هائل من المعلومات لا يمكن تصوره، وذلك في ظرف وجيز جدا.

وبما أن الجريمة تتطور بالتطورات الحاصلة بالمجتمع ما كان للإجرام أن يتأخر في الاستفادة من أشكال ووسائل هذا التطور التكنولوجي الحاصل، ونتيجة لذلك ظهرت "الجريمة الإلكترونية" وتعقدت معها أكثر فأكثر مهمة التحقيق الجنائي ذلك أن التشريعات الجنائية السائدة لم تعد بمقدرتها مجاراة الإجرام الإلكتروني لا من حيث كونه يشكل في حد ذاته نمطا وصنفا جديدا من الجرائم، ولا من حيث تلك السرعة الفائقة التي تنفذ بها هذه الجرائم.

وأمام هذا الوضع كان لزاما على المشرع التحرك وإعادة النظر في التشريعات الجنائية سواء في شقها الموضوعي أو في جوانبها الإجرائية، وكان لابد من حصول تغييرات وحدوث تطور من شأنه أن يمنح لجهات التحقيق الجنائي الدعم الذي تحتاجه في مواجهة الجريمة الإلكترونية على المستويين الوطني والدولي خاصة وأن الجريمة الإلكترونية جريمة ألغت مفهوم الحدود كونها جريمة عابرة للقارات.

وعلى ذكر جهود التشريعات الجنائية المقارنة، فلقد اختلفت هذه الأخيرة ومنذ بداياتها، وتجلى هذا الاختلاف في ظهور تباين حول إعطاء تعريف موحد للجريمة الإلكترونية وامتد هذا الاختلاف كذلك للفقه المقارن، كما أن هذا التباين لم يبق محصورا فقط في مسألة إيجاد تعريف جامع ومانع للجريمة الإلكترونية بل تعداه ليشمل تسمية هذه الجريمة في حد ذاتها فتعددت التسميات كالجريمة الإلكترونية، الجريمة المعلوماتية، جرائم الإنترنت، جرائم الحاسب الآلي، جرائم التقنية الحديثة، جرائم أنظمة المعالجة الآلية للبيانات ...الخ.

وبما أن الجريمة الإلكترونية تستهدف البيانات وما تمثله هذه الأخيرة من معلومات، نجد بأن التشريعات المقارنة والفقه المقارن اهتما كذلك بإعطاء تعريف للمعلومات وتحديد تلك

الشروط التي كلما توافرت في المعلومة منحتها حماية قانونية بما فيها الحماية ضد الجريمة الإلكترونية.

يخضع التحقيق الجنائي في الجريمة الإلكترونية لمعايير وقواعد الاختصاص القضائي، لذلك كان لابد من تحديد الجهة المناط مباشرة مهمة التحقيق ورسم حدود اختصاصها القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية سواء على المستوى الوطني أو المستوى الدولي، وهذا الأمر وإن كان لا يطرح إشكالات على المستوى الوطني إلا أن الوضع على المستوى الدولي ليس بتلك البساطة.

لقد أجبرت الجريمة الإلكترونية التشريعات الوطنية والدولية على ضرورة تطوير تلك الأجهزة القضائية المكلفة بالتحقيق الابتدائي في الجريمة الإلكترونية وكذا استحداث هيئات أخرى لمساعدتها، لذلك كان من البديهي أن يمتد تأثير الجريمة الإلكترونية إلى جهاز الضبطية القضائية لما له من صلة بجهات القضاء المختصة بالتحقيق الابتدائي في الجريمة الإلكترونية، بحيث شهد جهاز الضبطية القضائية بدوره تطورات عديدة سواء على المستوى الوطني والإقليمي والدولي وذلك استجابة للتحولات التي فرضتها طبيعة الجريمة الإلكترونية.

اصطدمت جهود جهات التحقيق الرامية إلى جمع تلك الأدلة المرتبطة بالجريمة الإلكترونية بجملة من الصعوبات منها ما هو مرتبط بالعامل البشري ومنها ما هو مرتبط بالدليل الإلكتروني في حد ذاته، كما تبرز الخصوصية المعلوماتية كموضوع حساس زاد من صعوبات جهات التحقيق.

وبما أن إجراءات جمع الدليل الإلكتروني تعتمد في كثير من الأحيان على تعاون الدول فيما بينها، شهد موضوع التعاون الدولي في مجال التحقيق الجنائي في الجريمة الإلكترونية إشكاليات عديدة ثبطت من عزيمة جهات التحقيق.

بدورها عرفت عملية جمع الدليل الإلكتروني تعقيدات كبيرة بداية من الانتقال إلى مسرح الجريمة الإلكترونية ومعاينته وصولا إلى موضوع الشاهد المعلوماتي، وذلك بعد المرور بإجراءات التفتيش والضبط والخبرة المتعلقة بالدليل الإلكتروني. كما أن هناك إجراءات

أخرى تستهدف الوصول إلى الدليل الإلكتروني ونقصد بها التسرب ومراقبة الاتصالات الإلكترونية وحفظ المعلومات، أبانت كلها عن جملة من الإشكالات تقف كشاهد على مدى تأثر التحقيق الجنائي (الابتدائي) بالجريمة الإلكترونية.

أسباب اختيار الموضوع:

من خصائص البحث العلمي أنه تجديدي، وبالرغم من مرور أكثر من عقد أو عقدين على بداية اتساع رقعة الجريمة الإلكترونية بفعل انتشار وسائل الاتصالات الإلكترونية (الهواتف الذكية، الألواح الإلكترونية، أجهزة الكمبيوتر ...الخ) وكذلك بسبب السرعة غير المسبوقة التي بلغتها الاتصالات نتيجة التدفق العالي للأنترنت عبر كل أرجاء المعمورة والتي أضحت كل أطرافها مرتبطة بالأنترنت، فرغم كل هذا وذاك يبقى موضوع التحقيق الجنائي في الجريمة الإلكترونية موضوعا حديثا وخصبا للبحث. وهذا بحد ذاته يعتبر سببا كافيا لوحده يبرر اختياري لهذا الموضوع.

يضاف إلى ما سبق، أن اختياري لهذا الموضوع كان كذلك من أجل الإسهام في إعداد وثيقة يمكن لغيري من طلبة وباحثين الاعتماد عليها مستقبلا. ويبقى أملي وبكل تواضع، من أن تتمكن هذه الدراسة من إضافة ــ ولو القدر اليسير ــ مما يمكنه أن يشكل مرجعا يلبي حاجة المهتمين بموضوع التحقيق الجنائي في الجريمة الإلكترونية.

أهداف الدراسة:

تهدف هذه الدراسة إلى التعريف بالجوانب الإجرائية المتعلقة بجمع الأدلة في الجريمة الإلكترونية، مع وجوب التنويه في هذا المقام إلى أنه لا يمكن حصر كل تلك الإجراءات والوسائل المعتمدة نظرا لكون الجريمة الإلكترونية جريمة متطورة وبشكل مستمر ومتواصل، وتبعا لذلك تظل كذلك وسائل وإجراءات جمع الأدلة في هذا النوع من الجرائم متطورة باستمرار.

ومن أهداف هذه الدراسة كذلك، تسليط الضوء على حجم التغييرات التي شهدها التحقيق الجنائي (التحقيق الابتدائي) في مجال الجريمة الإلكترونية سواء في جانبه الهيكلي أو في جوانبه الإجرائية نتيجة التحديات التي فرضتها عليه طبيعة الجريمة الإلكترونية. فالجانب

الهيكلي يتضمن تلك الأجهزة والهيئات التي تم إنشائها على المستوى الوطني والإقليمي والدولي. بحيث تهدف هذه الدراسة إلى إظهار تلك الحاجة التي أدت إلى إنشاء واستحداث هيئات جديدة توكل إليها مهمة التحقيق، وكذا الوقوف على التحديات التي فرضتها الجريمة الإلكترونية على الدول من خلال حثها ودفعها نحو ضرورة تطوير آليات للتعاون الدولي في مجال التحقيق في الجرائم الإلكترونية.

أما بخصوص الجوانب الإجرائية، فتهدف هذه الدراسة إلى إبراز مدى حاجة جهات التحقيق في الجريمة الإلكترونية إلى دعم من طرف المشرعين على كافة المستويات (الوطني والإقليمي والدولي) من خلال إقرار وسن نصوص تشريعية خاصة في الجوانب الإجرائية، وذلك من أجل وضع جهات التحقيق في وضع يساعدها ويسهل عليها جمع الأدلة في الجريمة الإلكترونية. وهذا راجع إلى قصور وعجز النصوص القانونية التقليدية (المتعلقة بالجريمة بمفهومها التقليدي المادي) في مجاراة طبيعة الجريمة الإلكترونية وفي قدرتها على توفير الدعم اللازم لجهات التحقيق والمساهمة بالتحقيق في الجريمة الإلكترونية.

ويدخل ضمن الجوانب الإجرائية التي تسعى وتهدف هذه الدراسة إلى استعراضها مجموعة الإجراءات التي جاءت بها التشريعات المقارنة في مجال الإجراءات الجنائية، يضاف إليها تلك التي تضمنتها الاتفاقيات الإقليمية والدولية من أجل دعم جهات التحقيق.

ونظرا لكون الجريمة الإلكترونية جريمة عابرة للقارات ولا تعترف بالحدود، كان لهذه الدراسة أن تتخذ جزءا من أهدافها عرضا لمدى حاجة الدول للتعاون فيما بينها من خلال إدراجنا لصور التعاون الدولي في مجال التحقيق الجنائي في الجرائم الإلكترونية.

أهمية موضوع الدراسة:

تبرز أهمية هذه الدراسة في كون أن مرحلة التحقيق (والمراد به التحقيق الابتدائي في هذا البحث) تعد من أهم مراحل الدعوى الجنائية، ذلك أنه من أجل محاكمة الجاني وتوقيع العقاب عليه لابد أولا من أن تقام ضده تلك الأدلة التي تدينه، وبدوره فإن الحصول على الأدلة التي من شأنها إثبات الجريمة وإدانة الجاني يستوجب إجراء تحقيق يفضي إلى

جمع هذه الأدلة. لذلك تعد هذه الدراسة ذات أهمية كونها تناقش وتتناول أهم مراحل الدعوى الجنائية المتعلقة بالجريمة الإلكترونية، ألا وهي مرحلة التحقيق الابتدائي في الجريمة الإلكترونية.

كما تبرز أهمية هذا الموضوع في كون الجريمة الإلكترونية أضحت مشكلة عويصة تؤرق كافة الدول دون استثناء، لذلك نجد أن العديد من الاتفاقيات تناولت أمر مكافحة هذه الجريمة وسبل التحقيق فيها من أجل جمع الأدلة المتعلقة بها. وفي هذا الصدد أتت هذه الدراسة من أجل تسليط الضوء على تلك الصعوبات التي تعيق المجتمع الدولي في مواجهته للجريمة الإلكترونية وتحثه في نفس الوقت على ضرورة الاستمرار في تطوير سبل التعاون في إطار التحقيق الجنائي في الجريمة الإلكترونية.

كما أن أهمية هذه الدراسة تعود كذلك إلى التطور المستمر للجريمة الإلكترونية، وهو الأمر الذي يتحتم معه العمل على تطوير وسائل وأساليب التحقيق الجنائي لمواجهة هذه الجريمة التي لم تستثن أي قطاع من القطاعات (المالية، التجارية، الصحية، العسكرية، التربوية، السياسية، الدينية، الاقتصادية ...) فاستهدفت الأفراد والجماعات والحكومات والدول على حد سواء، أشخاصا طبيعيون كانوا أم معنويون، فلا يوجد حدود للإجرام الإلكتروني. كل هذا دون أن ننسى ذلك البعد الاجتماعي التي تخلفه الجريمة الإلكترونية وتلك الآثار النفسية التي تتركها على الأفراد حين يتم استهداف بياناتهم الشخصية، وما لذلك من تداعيات على الخصوصية المعلوماتية للأفراد. فلهذه الدراسة أهمية أيضا في كونها تضعنا أمام حقيقة يؤكدها الواقع ومفادها أنه لا يمكن بأي حال من الأحوال مواجهة كل الأخطار والتهديدات الناجمة عن الجريمة الإلكترونية إلا من خلال أجهزة قضائية قوية تقود التحقيق بالاعتماد على إجراءات قانونية فعالة ووسائل تقنية جد متطورة وعنصر بشري كفء، وهذه مكونات لا مناص منها وذلك بغية الكشف عن الجناة في مجال الجريمة الإلكترونية وردعهم.

ونضيف إلى ما سبق، أن موضوع هذه الدراسة يستمد أهميته كذلك من كونه يخوض ويبحث في مسألة شائكة وهي تلك المتعلقة بمسألة الاختصاص القضائي بالتحقيق في الجرائم الإلكترونية وما تثيره من تعقيدات ومشكلات قانونية متعلقة بالسيادة وما يترتب

عن ذلك من تنازع سلبي أو تنازع إيجابي من شأنه أن يعيق في كثير من الأحيان جهود جهات التحقيق الجنائي في الجريمة الإلكترونية، وهذا ما يصب في مصلحة الجناة بكل تأكيد.

نطاق الدراسة (حدود الدراسة):

التحقيق في الجريمة قد يكون أوليا، ابتدائيا أو نهائيا. ويقصد بالتحقيق الأولي تلك الإجراءات التي تمارسها جهة غير قضائية ممثلة في الضبطية القضائية بحيث تقوم بالبحث والتحري وجمع الاستدلالات. أما التحقيق النهائي فهو ذلك التحقيق القضائي الذي يتم أثناء جلسة المحاكمة وتقوم به تلك الجهة القضائية التي تترأس التشكيلة المناط بها محاكمة المتهم. وهذين الصنفين من التحقيق لا يدخلان في نطاق دراستنا.

أما التحقيق الابتدائي والذي يعد مرحلة وسطى بين التحقيق الأولي والتحقيق النهائي، فهو تحقيق قضائي تمارسه سلطة قضائية مختصة حددها القانون، ونعني بها هنا قاض التحقيق وهذا هو الوضع في الجزائر (وإن كان للنيابة كذلك بعض صلاحيات المتعلقة بالتحقيق).

فالتحقيق الذي تعنى به دراستنا الحالية هو ذلك التحقيق الابتدائي الذي تمارسه السلطة المخولة قانونا بذلك، مع الأخذ بعين الاعتبار أن التشريعات الجنائية المقارنة اختلفت في تحديد هذه الجهة ومرد هذا الاختلاف يعود إلى التباين الحاصل بين الدول ففي الوقت الذي أخذت دول بمبدأ الجمع بين سلطتي الاتهام والتحقيق، فضلت دول أخرى تبني مبدأ الفصل بين سلطتي الاتهام والتحقيق كما هو الحال في الجزائر والتي يتولى فيها قاض التحقيق مهمة وصلاحية التحقيق الابتدائي.

يمارس قاض التحقيق مهمة التحقيق الابتدائي من خلال صورتين، صورة أولى باعتباره "محقق" وهي الصورة التي يباشر من خلالها الإجراءات المتعلقة بجمع الأدلة. أما الصورة الثانية فيظهر من خلالها على أنه "قاض للتحقيق" وهذه الصورة يمارس بموجبها تلك الإجراءات المعبر عنها عادة بتسمية "الإجراءات الاحتياطية ضد المتهم" فيقوم من خلالها بالتصرف في ملف القضية.

إذن فمراعاة منا للدقة والتي تعد من خصائص العلم، وحرصا منا على رسم حدود لموضوع بحثنا كان لزاما علينا التوضيح بأن محتوى دراستنا الحالية سوف يقتصر على الصورة الأولى المتعلقة بجمع الأدلة في الجريمة الإلكترونية أو ما يسمى بالتحقيق بمفهومه الضيق. ويمكننا تبرير ذلك لسببين أساسيين هما:

السبب الأول: أن الإجراءات الاحتياطية أو الاحترازية ضد المتهم المتابع في جريمة من الجرائم التقليدية هي نفسها تلك الإجراءات التي يخضع لها المتهم المتابع في جريمة من الجرائم الإلكترونية (الاستدعاء، الأمر بالقبض، الأمر بالإيداع، الأمر بالإفراج المؤقت، الأمر بالوضع تحت الرقابة القضائية ...) ونفس الشيء يقال بشأن أوامر التصرف في ملف التحقيق (الأمر بألا وجه للمتابعة، الأمر بالإحالة، الأمر بإرسال الملف ...) فالخوض في هذه المسائل في نظرنا غير مجد، وكان سيعتبر مجرد تكرار لمواضيع عالجتها العديد من الدراسات التي خاضت في مهام قاض التحقيق بخصوص الجرائم التقليدية إلى درجة أنها أضحت إلى حد كبير أمور مُستهلكة فالتطرق لها لا يقدم جديدا بل لا يعدو مجرد تكرار، بل وأكثر من ذلك سوف يُنظر إليه على أنه بمثابة "حشو" لتضخيم حجم الرسالة وهي أمور تتنافى مع قيمة البحث العلمي.

السبب الثاني: أن الدليل في الجريمة الإلكترونية بمسماه الجديد " الدليل الإلكتروني" وما يحمله من خصائص لا مادية كان سببا رئيسيا في خلق صعوبات غير مسبوقة أمام جهات التحقيق على المستوى الوطني والدولي، فكان منطقيا أن يكون محور بحثنا التركيز على الجوانب الإجرائية المتعلقة بجمع الدليل الإلكتروني كون هذا الموضوع تتوافر فيه "الجِدة" ذلك أنه من خصائص البحث العلمي أنه تجديدي، يضاف إلى ذلك أن الجريمة الإلكترونية في تطور مستمر، ما يعني بأن إجراءات جمع الدليل الإلكتروني محكوم عليها هي الأخرى بالتطور المستمر من أجل مجاراة تطور الإجرام الإلكتروني.

ونتيجة لذلك سوف نركز في بحثنا هذا على تلك السلطات التي أوكلها القانون مهمة التحقيق الابتدائي في الجريمة الإلكترونية، وكذلك على الجوانب الإجرائية والتي يراد بها ما تمارسه هذه السلطات من إجراءات متعلقة بجمع الدليل الإلكتروني سواء على المستوى

الوطني أو الدولي، لذلك سوف لن تقتصر الدراسة الحالية على الوضع في الجزائر فقط بل يتخللها عرض للأوضاع في التشريعات المقارنة كذلك.

وهذا دون إغفال للدور الذي تقوم به الضبطية القضائية والذي له صلة وعلاقة وطيدة بالتحقيق الابتدائي، لا سيما تلك الصلاحيات المخولة لها من الجهات المختصة بالتحقيق الابتدائي في إطار ما يسمى بالندب القضائي (الإنابة القضائية) على سبيل المثال. فالضبطية القضائية من هذه الزاوية شهدت هي الأخرى تحولات في عصر الجريمة الإلكترونية سواء في جانبها الهيكلي أو الإجرائي المتصل بالتحقيق الابتدائي في الجريمة الإلكترونية.

مجال الدراسة:

لقد تأثرت مختلف فروع القانون بعصر المعلوماتية ونتيجة لذلك ظهرت فروع جديدة مستحدثة، والقانون الجنائي لم يبق بمنأى عن هذه التحولات فتأثر بدوره بالجريمة الإلكترونية وشهد تغيرات في شقه الموضوعي أو الإجرائي على حد سواء. والتشريعات الإلكترونية التي ألقت بظلالها على القانون الجنائي أفرزت لنا ما يسمى بقانون العقوبات الإلكتروني وقانون الإجراءات الجنائية الإلكتروني (وإن كان المشرع الجزائري إلى غاية تحرير هذه الرسالة لم يفرد تقنينا خاصا بالعقوبات والإجراءات الجزائية في مجال الجريمة الإلكترونية).

بخصوص هذه الدراسة، نعتقد بأنه يمكن وضعها وتصنيفها ضمن القانون الجنائي الإلكتروني، وبصورة أدق فالموضوع الحالي له صلة وطيدة بقانون الإجراءات الجنائية الإلكتروني.

مشكلة الدراسة:

أدت الخصائص التي تتميز بها الجريمة الإلكترونية إلى تسهيل ارتكابها وبالمقابل صعبت على جهات التحقيق أمر جمع الأدلة بشأنها والتحقيق فيها، وهذا الوضع تولدت عنه جملة من المشاكل فمنها تلك المتعلقة بالجوانب الإجرائية لجمع الدليل الإلكتروني في

إطار التحقيق الجنائي في الجريمة الإلكترونية، ومنها تلك المرتبطة بالأجهزة في حد ذاتها أي الهيئات أو الجهات المناط بها مهمة التحقيق الجنائي.

فبالإضافة إلى السرعة والسهولة وغيرهما من الميزات التي يستفيد منها المجرم الإلكتروني لدى ارتكابه للجرائم الإلكترونية، فإنه يتمتع كذلك بالمقدرة على طمس الأدلة والتلاعب بها وإخفائها، لذلك فإن جهات التحقيق تواجه مشاكل جمة منها ما هو مرتبط بالدليل الإلكتروني في حد ذاته والذي هو بمثابة بيانات غير مادية، ومنها ما هو متصل بإجراءات الحصول على هذا الدليل كالانتقال إلى مسرح الجريمة الإلكترونية ومعاينته، وتفتيش المنظومة المعلوماتية وضبط الأدلة بها ...الخ. كل هذه جملة من المشاكل تثيرها هذه الدراسة.

وبالنظر لكل ما سبق فإن التساؤل الرئيسي الذي تدور حوله إشكالية البحث أو الدراسة الحالية يمكن صياغته في صورة السؤال التالي:

هل بإمكان أجهزة التحقيق الابتدائي في الجريمة التقليدية المادية – وبما يتوافر لديها من إمكانيات وإجراءات– أن تتولى التحقيق الابتدائي في الجرائم الإلكترونية ؟ وهل هذه الإجراءات وهذه الأجهزة كافية وكفيلة لوحدها بضمان التحقيق الابتدائي في الجرائم الإلكترونية ؟

هذا التساؤل الجوهري تتفرع عنه عدة تساؤلات فرعية يتشكل منها البحث، ومن أبرزها:

1. كيف أثرت الجريمة الإلكترونية –بما تحمله من خصائص–على الجهات المناط بها التحقيق الابتدائي في الجرائم؟ وماهي أبرز صور ومظاهر هذا التأثر، سواء في الجانب الهيكلي أو في الجوانب الإجرائية؟ وسواء على المستوى الوطني وكذلك على المستوى الإقليمي والدولي؟
2. ما مدى جدوى إجراءات جمع الأدلة في الجريمة التقليدية وما مدى فعاليتها في التنقيب عن الأدلة في الجريمة الإلكترونية واستخلاصها ؟

3. هل وفقت جهات التحقيق في الحصول على الأدلة الإلكترونية دون المساس بالخصوصية المعلوماتية؟ وكيف شكلت المحافظة على الخصوصية المعلوماتية وصونها عائقا أما جهات التحقيق؟
4. ما مدى حاجة الدول إلى التعاون فيما بينها في مجال التحقيق في الجريمة الإلكترونية؟ وما هي مبررات وصور هذا التعاون؟ وكيف تتعارض مصالح الدول وسيادتها مع الجهود الرامية إلى تعزيز التعاون الدولي بخصوص مكافحة الجريمة الإلكترونية؟ ألا تتناقض تصرفات ومواقف بعض الدول مع ما هو معلن عنه من ضرورة التعاون الدولي الهادف إلى دعم جهود التحقيق في الجريمة الإلكترونية؟

منهج الدراسة:

اعتمدنا في بحثنا هذا على كل من المنهج الوصفي والمنهج التحليلي وكذا المنهج المقارن. حيث استخدمنا المنهج الوصفي في وصفنا للجريمة الإلكترونية وخصائصها واعتمدنا ذات المنهج لدى تقديمينا وصفا لتلك الجهات المناط بها مهمة التحقيق، سواء تعلق الأمر بتلك الجهات على المستوى الوطني أو الإقليمي أو الدولي. هذا ولقد استندنا على نفس المنهج الوصفي في وصفنا لكل إجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية، وتناولنا كل هذه النقاط بشيء من التحليل لإبراز مدى ملائمة النصوص القانونية المعتمدة في مجال التحقيق الجنائي في الجريمة الإلكترونية ومدى كفايتها وفعاليتها في التنقيب عن الأدلة وكشف الجناة من جهة، ومن جهة أخرى للخوض في تلك الخلافات والإشكالات التي أثيرت بشأنها والوقوف على العوائق التي تواجهها. هذا ولقد حرصنا قدر الإمكان أن نتناول كل ما سبق مع مراعاة موقف التشريعات المقارنة والفقه المقارن.

الجانب الهيكلي للدراسة (خطة البحث):

بعد المفاضلة بين الكثير من التقسيمات المختلفة للبحث، قررنا تقسيم دراستنا هذه إلى بابين بحيث خصصنا الباب الأول لعرض تلك الجهات المناط بها التحقيق الابتدائي في الجريمة الإلكترونية، في حين تناولنا بالباب الثاني الجوانب الإجرائية المتعلقة بجمع الدليل

في الجريمة الإلكترونية. وقد أدرجنا قبل هذين البابين فصلا تمهيديا سلطنا من خلاله الضوء على مفهوم الجريمة الإلكترونية والتي ينصب عليها موضوع التحقيق الجنائي. هذا وقد أنهينا بحثنا بخاتمة تضمنت أبرز النتائج التي توصلنا إليها في دراستنا هاته.

الفصل التمهيدي: ماهية الجريمة الإلكترونية

يعد التعرف على ماهية الجريمة الإلكترونية وكذا إدراك أخطارها وما تكتسيه من طبيعة خاصة شرطا أساسيا لمواجهة هذا الصنف المستحدث من الجرائم الذي أصبح يشكل ظاهرة صاحبت التطور التكنولوجي في مجال الاتصالات وارتبطت بالبيئة التقنية لنظم المعالجة الآلية، كما استفادت من شبكة الإنترنت.

فجهات التحري والتحقيق وقبل سعيها إلى جمع الدليل المتعلق بالجريمة الجريمة الإلكترونية، وجب عليها بادئ ذي بدء الإحاطة بماهية الجريمة محل التحري والتحقيق، والتعرف على كافة جوانبها نظرا لاختلاف طبيعتها عن الجريمة التقليدية.

سنحاول من خلال هذا الفصل التمهيدي التطرق إلى مفهوم الجريمة الإلكترونية وذلك بإعطائها تعريف، وكذا النظر في خصائصها وأشكالها وأخطارها. وبعد ذلك ننتقل إلى التعرف على كل من المجرم الإلكتروني والضحية في الجريمة الإلكترونية، لننهي هذا الفصل بإلقاء نظرة على نقطة ذات صلة وثيقة بالجريمة الإلكترونية ألا وهي المعلومات باعتبارها محلا للجريمة الإلكترونية. وعليه سوف نقسم هذا الفصل التمهيدي إلى ثلاثة مباحث كالآتي:

المبحث الأول، ونقدم من خلاله مفهوما للجريمة الإلكترونية.

المبحث الثاني، نتعرف من خلاله على طرفي الجريمة الإلكترونية.

أما المبحث الثالث والأخير نخصصه للتعرف على المعلومات بوصفها محلا للجريمة الإلكترونية.

الفصل التمهيدي: ماهية الجريمة الإلكترونية

المبحث الأول: مفهوم الجريمة الإلكترونية

المبحث الثاني: طرفي الجريمة الإلكترونية

المبحث الثالث: التعريف بالمعلومات بوصفها محلا للجريمة الإلكترونية

تُعرف الجريمة عموما بأنها سلوك غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيرا احترازيا وهذا التعريف يحدد أركان الجريمة، من سلوك غير مشروع وإرادة جنائية والعقوبة أو التدبير الاحترازي الذي يفرضه القانون، كل ذلك من شأنه أن يوفر وصفا دقيقة للجريمة[1].

أما بخصوص الجريمة الإلكترونية، فلقد تعددت وتنوعت تلك التعريفات التي أعطيت للجريمة الإلكترونية، غير أن الفقهاء لم يفلحو في إيجاد تعريف جامع ومانع لها، إذ تفرقوا إلى عدة اتجاهات أفرزت تعريفات مختلفة تضيق تارة وتتسع تارة أخرى. ومرد ذلك هو اختلاف تلك المعايير التي لجأ إليها هذا الاتجاه أو ذاك في تعريف الجريمة الإلكترونية.

وإجمالا يمكن تلخيص تلك المعايير التي اعتمدها الفقهاء في تعريفهم للجريمة الإلكترونية إلى معيار الأداة أو الوسيلة التي استعملت لارتكاب الجريمة، معيار محل أو موضوع الجريمة، معيار مدى إلمام الجاني ومعرفته بتقنيات الحاسب الآلي، إلى غير ذلك من المعايير. كما أن هناك من اعتمد أكثر من معيار في تعريفه للجريمة الإلكترونية.

لذلك سوف نستعرض عينة من تلك التعريفات التي أخذت بهذا المعيار أو ذاك.

الفرع الأول: تعريف الجريمة الإلكترونية وفق معيار محل الجريمة

حيث يعتبر جانب من الفقه أن الجريمة يمكن وصفها بكونها جريمة إلكترونية إذا كان موضوعها الحاسب الآلي أو أي نظام معلوماتي.

ومن التعريفات التي أخذت بهذا المعيار نجد ذلك التعريف الذي جاء به الفقيه ROSENBLATT الذي عرف هذا النوع من الجرائم على أنه " نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب أو التي تُحوَلُ عن طريقه"[2]

---

[1] غايب محروس نصار، الجريمة المعلوماتية، مجلة كلية التراث الجامعية، العدد السابع عشر المجلد 24 الإصدار التاسع، 2011، ص4. أشار إليه: محمد عبد الرحمن عنانزة، القصد الجرمي في الجرائم الإلكترونية، الطبعة الأولى، دار الأيام، عمان، الأردن، 2017، ص61.

[2] Michael D. Rostoker, Robert H. Rines, Computer jurisprudence: legal responses to the information revolution, New York, N.Y. : Oceana Publications, P 104,1986. =

=أشار إليه:

Mohamed Chawki, Essai sur la notion de cybercriminalité, p 27, 2006.

فيعرفها القاضي والفقيه النرويجي Stein SCHJOLBERG على أنها " الجرائم التي يتطلب إلماما خاصا بتقنيات الحاسب ونظم المعلومات، لارتكابها أو التحقيق فيها ومقاضاة فاعليها"[1]

علاوة على التعريفات السابقة والتي تقيدت بمعيار واحد لدى تعريفها للجريمة الإلكترونية، نجد بأن هناك تعريفات أخرى مزجت بين معيارين على الأقل فتبنت بذلك أكثر من معيار واحد عند تعريفها للجريمة الإلكترونية. ولعل أبرز مثال في هذا الصدد ذلك التعريف الذي قدمته منظمة الأمم المتحدة، وكان ذلك خلال المؤتمر الذي عقد بعاصمة النمسا فيينا في الفترة الممتدة ما بين (10-17 أبريل 2000) والمتعلق بمنع الجريمة ومعاقبة المجرمين. حيث عرفت الجريمة الإلكترونية على أنها "أية جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل تلك الجريمة جميع الجرائم التي يمكن ارتكابها في بيئة إلكترونية"[2]. ويلاحظ بأن هذا التعريف قد جمع بين معيار الوسيلة المستخدمة في الجريمة وكذا معيار محل الجريمة.

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بعدة خصائص جعلت منها جريمة مختلفة عن الجريمة بمفهومها التقليدي، سواء تعلق الأمر بمرتكبيها أو بالوسيلة المستعملة فيها أو البيئة المرتكبة فيها، أو حتى بالنتائج والآثار المترتبة عنها.

ونظرا لكثرة تلك الخصائص فلا يمكننا حصرها جميعا، لذلك سنتطرق إلى أهم الخصائص التي جعلت من الجريمة الإلكترونية جريمة مختلفة عن الجريمة بمفهومها التقليدي.

---

[1] Stein SCHJOLBERG, Computers and Penal Legislation – A Study of the Legal Politics of a New Technology, CompLex 2/83, Universitetsforlaget, Oslo, 1983, p40.

أشار إليه أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة، الإسكندرية، 2007، ص 89.

[2] " tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes d'information et des données qu'ils traitent".

Dixième Congrès des Nations Unies, "la prévention du crime et le traitement des délinquants", Vienne, 10 –17 avril 2000.

https://www.unodc.org/documents/congress//Previous_Congresses/10th_Congress_2000/017_ACONF.187.10_Crimes_Related_to_Computer_Networks_F.pdf

أنظر في هذا المعنى: أسامة أحمد المناعسة، جرائم الحاسب الآلي والأنترنت، الطبعة الأولى، دار وائل للطباعة والنشر، عمان، الأردن، 2001، ص77.

الفرع الأول: الجريمة الإلكترونية تقع في بيئة افتراضية

فالجريمة الإلكترونية تتخذ من العالم اللامادي والافتراضي بيئة لها ذلك أنها ترتكب في بيئة إلكترونية غير مادية تكون في شكل نبضات إلكترونية، وهذه الخاصية تعتبر في نفس الوقت مشكلا يعيق جهات التحقيق وهذا أمر سنتحدث عنه عند تطرقنا للمشاكل والمعوقات التي أفرزتها الجريمة الإلكترونية.

الفرع الثاني: الجريمة الإلكترونية عابرة للدول ولا تعترف بالحدود الجغرافية

لقد ساهمت شبكة الأنترنت في اتساع مسرح الجريمة الإلكترونية، فأصبح بإمكان الجاني ارتكاب عدة جرائم في عدة دول مختلفة وفي قارات مختلفة، كل ذلك وهو جالس في بيته دون الحاجة إلى التنقل وهذا من خلال استغلال العالم الافتراضي الذي يمتد إلى مختلف بقاع الأرض. فالحدود الجغرافية لا وجود لها في مفهوم الجريمة الإلكترونية.

ولهذا فإن جرائم الحاسوب تشترك مع غيرها من الجرائم في أنها تتخطى حدود الدول، كتجارة المخدرات وغسيل الأموال، إلا أنها تتميز عن الأخيرة حيث يمكن ارتكابها دون مغادرة المقعد المقابل للحاسب الآلي بعكس جرائم المخدرات التي تتطلب حركة بين الدول[1].

الفرع الثالث: الجريمة الإلكترونية جريمة يصعب اكتشافها

ومرد ذلك كون الجاني يرتكب جريمته من خلال نبضات إلكترونية خفية وغير مرئية، فلا يمكن للضحية الشعور بها، لذلك فغالبا لا يمكن اكتشافها أثناء تنفيذها أو بعد ارتكابها بفترة وجيزة. فلا يكتشف الضحية ذلك إطلاقا، أما إذا تم ذلك فيكون بعد مضي مدة معتبرة من الزمن على تاريخ ارتكابها.

ومن بين العوامل التي تساهم في صعوبة اكتشاف الجريمة الإلكترونية أنها تتم في وقت قصير فلا يستغرق تنفيذها سوى مدة زمنية وجيزة قد لا تتعدى في بعض الأحيان دقائق معدودة أو حتى أقل من دقيقة.

[1] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009، ص34

الفرع الرابع: الجريمة الإلكترونية جريمة ناعمة تعتمد على الذكاء

فالمجرم الإلكتروني لا يحتاج إلى جهد عضلي لتنفيذ جريمته الإلكترونية، بل يعتمد على ذكائه وقدراته العقلية ومدى إلمامه باستخدام الوسائل التقنية الحديثة، وكذا التحكم في البرمجيات والتمكن من الاستغلال الأمثل لشبكات الأنترنت وتطويعها خدمة لتسهيل ارتكاب جرائمه. فهو بذلك لا يلجأ إلى كسر الأقفال والأبواب ولا إلى التسلق والمواجهة والالتحام الجسدي والتشابك بالأيدي، بل يستخدم ذكائه لكسر شفرات المرور والكلمات السرية، والولوج إلى البيانات المحمية من خلال التفوق على وسائل الحماية التي يلجأ إليها الأشخاص سواء كانوا طبيعيين أم معنويين.

الفرع الخامس: الجريمة الإلكترونية جريمة ذات أضرار جسيمة

فالخسائر التي تتسبب فيها الجريمة الإلكترونية باهظة، سواء تعلق الأمر بالخسائر المعنوية المرتبطة بالحياة الشخصية للأفراد والمتعلقة بعامل الثقة بين الأفراد والشركات، كما أن الأضرار المادية التي تنجم عن الجريمة الإلكترونية غالبا ما تكون مرتفعة جدا كتلك التي تلحق بالمؤسسات المالية والاقتصادية بل وحتى المؤسسات العسكرية والمؤسسات الصحية كالمستشفيات والمؤسسات الإعلامية كالقنوات التلفزيونية. فالتجسس الإلكتروني وسرقة التكنولوجيا المعلوماتية وإذاعة الأسرار يكلف الدول والمؤسسات وحتى الأفراد أضرارا بليغة على المستوى المادي والمعنوي.

إضافة إلى هذه الخصائص، هناك عدة ميزات أخرى للجريمة الإلكترونية يمكن اختصارها فيما يلي:

- تعدد المجني عليهم وتعدد مسرح الجريمة كذلك.
- في أغلب الأحيان تستغرق الجريمة الإلكترونية وقت قصير لارتكابها فيسهل تنفيذها دون حاجة الجاني إلى مساعدة أشخاص آخرين.
- تحدث أضرار جسيمة لا سيما تلك المتعلقة بالجانب الاقتصادي، فهي تتسبب في أضرار بالغة التكلفة مقارنة بالجريمة التقليدية.
- لا تترك أثارا مادية الأمر الذي يصعب التحقيق بخصوصها وإثباتها.
- يسهل إتلاف الأدلة المتعلقة بها وإعاقة الوصول إليها من خلال تشفيرها مثلا.

– تعتمد على الوسائل التقنية في ارتكابها كما أنها تتخذ من شبكة الأنترنت بيئة لها.

بالإضافة إلى عدة ميزات أخرى تصب في صالح الجناة وبالمقابل خلقت الكثير من الصعاب وعقبات جمة أمام جهات التحري والتحقيق.

المطلب الثالث: صور الجريمة الإلكترونية

للجريمة الإلكترونية عدة أشكال وصور شأنها في ذلك شأن الجرائم التقليدية، فهناك من يصنف الجريمة الإلكترونية إلى ثلاث مجموعات وذلك بحسب كونها تقع على الأفراد أو على الأموال أو على نظم المعالجة الآلية للبيانات.

كما أن هناك محاولات فقهية سعت لوضع أشكال للجريمة الإلكترونية داخل تصنيفات اعتمدتها بعض الهيئات. وعلى كل حال فإن تصنيف الجرائم الإلكترونية يختلف باختلاف تلك الزاوية التي ينظر من خلالها إلى الجريمة وهذا ما أدى إلى ظهور عدة تصنيفات متباينة من حيث معيار التفرقة والتمييز بين مختلف صور وأشكال الجرائم الإلكترونية غير أن مضمونها متشابه إلى حد ما.

من خلال هذا المطلب سوف نستعرض بعض التصنيفات التي تناولت أشكال الجريمة الإلكترونية، وهذا بحسب التقسيم الآتي:

الفرع الأول: التصنيف الفقهي للجرائم الإلكترونية.

الفرع الثاني: التقسيم الثلاثي للجرائم الإلكترونية (جرائم الأشخاص والأموال والنظم)

الفرع الثالث: التصنيف المعتمد من طرف بعض الهيئات.

الفرع الأول: التصنيف الفقهي للجرائم الإلكترونية

حيث سنتطرق من خلال هذا الجزء إلى كل من ذلك التصنيف الذي اعتمده الفقيه أولرتش سيبر ULRICH Sieber وكذلك تصنيف الفقيه مارتن فاسك Martin Wasik.

أولا: تصنيف الفقيه أولرتش للجرائم الإلكترونية

بحسب الفقيه ULRICH Sieber[1] فإن الجرائم الإلكترونية تضم ثلاث مجموعات أو أصناف مقسمة كما يلي:

[1] Ulrich Sieber, "The international Handbook on Computer Crime "Computer related Economic crime and infringements of privacy", John Wiley & Sons, 1986, PP 03-27.

أ–الجرائم الإلكترونية الماسة بحرمة الحياة الخاصة: وتضم كل تلك الجرائم الإلكترونية التي تستهدف انتهاك البيانات الشخصية سواء عن طريق جمعها وتخزينها ونشرها وتعديلها ومحوها أو أي فعل آخر صادر عن جهة غير مرخصة قانونا باستخدام تلك البيانات الشخصية، أو من خلال تجاوز تلك الحدود التي نص عليها القانون.

ب–الجرائم الإلكترونية الماسة بالجوانب الاقتصادية: وتضم كل تلك الجرائم المتعلقة بالقرصنة والتجسس والاحتيال والتي تستهدف قطاع الأعمال بغية الحصول على أموال أو خدمات بغير حق، أو تدمير وإتلاف النظم المعلوماتية المتعلقة بالجوانب الاقتصادية سواء تعلق الأمر بالمكونات المادية أو المعنوية.

ج–الجرائم الإلكترونية الماسة بالمصالح العليا للدولة وسلامة الأشخاص: وتتضمن تلك الجرائم التي تمثل اعتداءات على الأنظمة الدفاعية للدولة وكذا أنظمة النقل الجوي بما يمس بسلامة الأفراد.

ثانيا: تصنيف الفقيه مارتن للجرائم الإلكترونية:

يقسم الفقيه مارتن فاسك Martin Wasik[1] هو الآخر الجرائم الإلكترونية إلى ثلاثة أقسام أو مجموعات على النحو التالي:

أ–الجرائم الإلكترونية باستعمال الحاسب الآلي: وتضم هذه الفئة كل تلك الجرائم التي تتم من خلال الحاسب الآلي مستهدفة الأنظمة المعلوماتية للحواسيب بمكوناتها المادية والمعنوية أو تستهدف الاعتداء على الأفراد من خلال التهديد والابتزاز.

كما تشمل هذه الفئة تلك الأفعال التي قد تساعد في الجرائم السابقة كإعداد الفيروسات وكل أنواع البرامج الخبيثة والأدوات التي تساهم في تخريب وإتلاف الحاسب الآلي سواء تعلق الأمر بمكوناته المادية أو المعنوية.

أشار إليه: مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، المجلد 3، العدد 1، 2014، ص 358.

تم التحميل من موقع (المجلات الأكاديمية العلمية العراقية) من خلال الرابط (متاح بتاريخ 2019/09/12):

https://www.iasj.net/iasj/download/a8e379f16a4e5871

[1] Martin Wasik, "Crime and the computer", Oxford University press, USA, 1991, P 42

أشار إليه: مشتاق طالب وهيب، المرجع نفسه، ص 359.

ب-الجرائم الإلكترونية المتعلقة بالولوج والاستعمال غير المشروع للنظام المعلوماتي: حيث تضم هذه الفئة جرائم الولوج أو الدخول غير المصرح به للنظام المعلوماتي سواء تبعه ارتكاب جرائم أخرى أم لا، كما تضم كل تلك الأفعال التي تستهدف البيانات الشخصية.

ج-الجرائم الإلكترونية المرتبطة بالاحتيال المعلوماتي: وتشمل كل تلك الجرائم التي يتم فيها التزوير والتلاعب بالمعلومات المعالجة آليا وكذا الأفعال التي تشمل القرصنة والسرقة قصد تحقيق أرباح مادية.

الفرع الثاني: تقسيم الجرائم الإلكترونية إلى جرائم أشخاص وأموال ونظم المعالجة الآلية للمعلومات

دأبت العديد من التشريعات المقارنة على تقسيم الجرائم التقليدية تقسيما يطغى عليه تواجد الصنفين الأول والثاني والمقصود بهما جرائم الأشخاص وجرائم الأموال، في حين تتراوح باقي التقسيمات بين جرائم تمس مؤسسات الدولة ومصالحها الاستراتيجية كجرائم النقد والصرف والمخدرات والتهريب وغيرها من الجرائم الاقتصادية.

وفي موضوع الجريمة الإلكترونية يمكن تقسيم وتصنيف الجرائم الإلكترونية تقسيما ثلاثيا نحتفظ من خلاله بصنفين سائدين في الجرائم التقليدية ويقصد بهما هنا الجرائم الواقعة على الأشخاص وتلك المتعلقة بالأموال، أما الصنف الثالث فنخصصه لتلك الجرائم المتصلة بنظم المعالجة الآلية للبيانات. وعليه، سوف نقدم شرح موجز لهذه التصنيفات كالآتي:

أولا: الجرائم الإلكترونية الواقعة على الأشخاص:

بصفة عامة، يقصد بالجرائم التي تستهدف الأشخاص جملة الأفعال التي تشكل تعديا على السلامة الجسدية للأفراد أو على اعتبارهم وشرفهم وكرامتهم وكذا حياتهم الخاصة. فالقتل والضرب والجرح جرائم تمس السلامة الجسدية للأفراد، في حين أن السب والشتم والقذف هي عينة من تلك الجرائم التي تمس اعتبار الأشخاص فتلحق بهم أضرارا معنوية ونفسية، على أن هناك صنف من الجرائم يجتمع فيه الاعتداء الجسدي والمعنوي والنفسي كهتك العرض والاغتصاب.

يعتبر نشر وإذاعة أخبار تخص الحياة الشخصية للأفراد انتهاكا وتعديا على حرمة حياتهم الخاصة كالمراسلات الخاصة على سبيل المثال.

هذه الجرائم السابقة الذكر، وإن كان يمكن تصور حدوثها كلها في العالم المادي الحقيقي وهي الجرائم التي نطلق عليها عادة تسمية الجرائم التقليدية، غير أنه وبالمقابل لا يمكن تحقق بعضها في العالم الافتراضي الذي يأوي الجريمة الإلكترونية. فجرائم الضرب والاغتصاب وهتك العرض على سبيل المثال لا يمكن تصور حدوثها كجرائم إلكترونية، غير أنه يمكن تصور القيام بالتحريض على ارتكابها عبر وسائل الاتصال الحديثة كالهواتف الذكية والحواسيب الآلية المرتبطة بشبكة الأنترنت.

غير أن جرائم أخرى كالسب والتهديد والابتزاز والجرائم المتعلقة بالآداب وتلك الماسة بحرمة الحياة الخاصة للأفراد يمكن تصور ارتكابها باعتبارها جرائم إلكترونية. وحتى لا نخوض في عرض كل تلك الجرائم الإلكترونية المتعلقة بالأشخاص . مادام أنه ليس موضوع بحثنا. نكتفي فقط بهذا القدر الذي نظنه كاف لتوضيح هذا المطلب المتعلق بصور وأشكال الجرائم الإلكترونية.

ثانيا: الجرائم الإلكترونية الواقعة على الأموال

تعتبر السرقة وتبييض الأموال وكذا التزوير وكل تلك الجرائم المرتبطة بالنقد والصرف من الجرائم التقليدية الشائعة التي تكون الأموال محلا لها. ولقد أدى التطور التكنولوجي في مجال الاتصالات، وما توفره شبكة الأنترنت من تسهيلات إلى توسيع مجال النشاط الإجرامي لا سيما ما انصب منه على الأموال.

فالسرقة وإن كانت في صورتها التقليدية ممتدة إلى كافة المنقولات، غير أنها كجريمة من الجرائم الإلكترونية تتقلص لتشمل فقط ما يسمى بالنقود الإلكترونية كسرقة بطاقات الائتمان على سبيل المثال.

لقد أدى الإقبال على التسوق الإلكتروني نتيجة لظهور ما يسمى التجارة الإلكترونية إلى انتشار استخدام الأفراد لبطاقات الائتمان، وبالتالي إتاحة بياناتهم ومعلوماتهم الشخصية لأولئك المترصدين لها من مجرمي الأنترنت والذين يتخذون من هذه البيانات لاحقا وسيلة يعتمدون عليها من أجل قرصنة البطاقات الإلكترونية التي تمكنهم من سرقة الأموال.

علاوة على السرقة، فلقد ساعدت شبكة الأنترنت كثيرا وساهمت بشكل كبير في تسهيل غسيل الأموال، إذ مكنت المجرين من تسريع وتيرة تبييض الأموال مستفيدين في ذلك من السرعة التي منحتها إياهم شبكة الأنترنت في ظل انعدام الحواجز والحدود الجغرافية وإمكانية تشفير بياناتهم عند تحويل الأموال من بلد لآخر أو من قارة لأخرى.

تعتبر جريمتي سرقة البطاقات الإلكترونية وكذا تبييض الأموال عبر الأنترنت من أبرز صور الجرائم الإلكترونية المنصبة على الأموال رغم تعدد تلك الصور وتنوعها.

ثالثا: الجرائم الإلكترونية الواقعة على نظم المعالجة الآلية للبيانات

بعد عرضنا لتلك الجرائم الإلكترونية التي تقع على الأشخاص وكذا الأموال، نصل إلى آخر صورة يتضمنها التقسيم الثلاثي للجرائم الإلكترونية ويتعلق الأمر هنا بالجرائم الإلكترونية التي تستهدف نظم المعالجة الآلية للبيانات، ونشير هنا إلى عدم وجود تعريف دقيق ومتفق عليه لنظم المعالجة الآلية للبيانات أو المعلومات.

المشرع الفرنسي لم يضع تعريفا لنظم المعالجة الآلية للمعطيات، في حين أن المشرع الجزائري وبموجب القانون 09-04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] تناول هذا المصطلح وذلك بمحتوى المادة الثانية بالفقرة (ب) التي عرفت المنظومة المعلوماتية بكونها " أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

يعتبر مصطلح نظام المعالجة الآلية للبيانات أو المعطيات تعبير فني صعب كما أنه تعبير متطور يخضع لتطورات البيئة التقنية التي يمثلها، أما في الحقل القانوني فهو مصطلح ينطبق على " أي نظام مهما كان مسماه يتوافر على عدة عناصر مرتبطة

[1] القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 47 الصادرة في 25 شعبان 1430 الموافق 16 غشت 2009.

ببعضها بعدد من الروابط لتحقيق المعالجة الآلية للمعلومات من تجميعها وتخزينها ومعالجتها ونقلها وتبادلها...إلخ"[1].

ونكتفي بهذا القدر حتى لا نسترسل في عرض كافة المحاولات التشريعية والفقهية التي تناولت تعريف نظم المعالجة الآلية للبيانات مادام أنه ليس موضوع بحثنا.

فالجرائم الإلكترونية تستهدف نظم المعالجة الآلية للبيانات وذلك من خلال إعداد برامج خبيثة أو ما يسمى بالفيروسات والتي يتمكن بواسطتها المجرم الإلكتروني من الولوج إلى الأنظمة المعلوماتية التي يتم تخزين البيانات بداخلها.

أما عن الغاية من استهداف البيانات فهي متعددة ومتنوعة تماشيا مع تنوع وتعدد الأهداف التي يسعى المجرم الإلكتروني إلى تحقيقها. فقد يعمد المجرم الإلكتروني إلى إتلاف وتدمير البيانات، أو يقوم بتعديلها، أو يكتفي فقط بأخذ نسخ منها أو الاطلاع عليها. كما قد يقوم بزرع برامج تتيح له ربط اتصال مباشر بالجهة المستهدفة بحيث يمكنه اعتراض والتقاط أية بيانات أو التنصت، أي أنه وبصفة عامة يصبح قادرا على مراقبة الجهة المستهدفة سواء كانت شخصا طبيعيا أو معنويا.

تجدر الإشارة إلى أن البيانات المستهدفة قد تتواجد بحاسب آلي أو بهاتف ذكي أو تلفاز ذكي، كما قد تكون تلك البيانات على شبكة الأنترنت.

المطلب الرابع: الأخطار المترتبة عن الجريمة الإلكترونية

سواء تعلق الأمر بالجرائم الإلكترونية أو بالجرائم في صورتها التقليدية، فجميعها تحدث أثرا على المجتمع. قد يقتصر هذا الأثر على فرد معين أو أفراد معينين، كما قد تمتد آثار الجريمة لتشمل شريحة كبيرة من المجتمع. علما بأن الجرائم الإلكترونية قد تحدث آثارا عديدة وفي أماكن متفرقة من العالم وفي فترة وجيزة، مستفيدة في ذلك من تلك الميزات التي أفرزتها شبكة الأنترنت، هذه الأخيرة منحت المجرم الإلكتروني قدرات هائلة لم تكن متاحة في ظل الجريمة التقليدية ولعل من أبرزها إلغاء مفهوم الحدود الجغرافية داخل البيئة الافتراضية.

[1] رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012، ص55-56.

ثانيا: المساهمة في الانحلال الأخلاقي والشذوذ الجنسي بكافة أنواعه ومن أبرز صوره جعل الأطفال موضوع لمواد إباحية داخل المجتمع من خلال نشر وبث صور وأفلام الاعتداء الجنسي على الأطفال وتشجيع الإقبال على ذلك من خلال عرضهم كسلعة لنزوات المرضى والمنحرفين.

ثالثا: إفشاء المعلومات السرية والبيانات الشخصية المرتبطة بالحياة الخاصة للأفراد أو ما يسمى بالخصوصية المعلوماتية، من خلال اختراق أجهزتهم الشخصية أو سرقة بياناتهم المتواجدة لدى جهات أخرى كشركات التأمين والمستشفيات والمحامين والفنادق...إلخ، أو أجهزة تخزين البيانات الخاصة بمواقع التواصل الاجتماعي عبر شبكة الإنترنت.

إلى غير ذلك من المخاطر الاجتماعية التي لا يمكن حصرها.

الفرع الثاني: المخاطر الاقتصادية للجريمة الإلكترونية

تعتبر المخاطر الاقتصادية للجريمة الإلكترونية على درجة بالغة من الخطورة نظرا لوقوعها في معظم الأحوال على معلومات وبرامج ذات قيمة اقتصادية عالية، سواء في ذاتها أو لارتباطها بأموال قيمة، مما يؤدي في الغالب إلى خسائر مالية فادحة، إذ أنه وبمجرد حصول المجرم المعلوماتي على الوقت والوسيلة الكافيتين لتنفيذ جريمته فإنه قد لا يتردد في القضاء على أكبر المؤسسات الاقتصادية في العالم[1].

وفي مقال[2] ورد بالجريدة الفرنسية Les échos في نسختها الإلكترونية بتاريخ 2019/02/21 وتحت عنوان (الجريمة الإلكترونية تكلف 600 مليار دولار سنويا) تشرح صاحبة المقال كيف أن الجريمة الإلكترونية تكبد العالم خسائر سنوية تقدر ب 600 مليار دولار أي ما يعادل 0.8% من إجمالي الناتج الخام المحلي لدول العالم وهذا بحسب تقرير صادر سنة 2018 عن الشركة المتخصصة في الأمن الإلكتروني McAfee وكذا مركز الدراسات الاستراتيجية والدولية CSiS، الأمر الذي يؤثر على

[1] محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004، ص155.

[2] مقال للصحفية Leïla Marchand منشور بتاريخ 2018/02/21 على الساعة 19:39 على الموقع الإلكتروني لجريدة Les échos، تم الاطلاع عليه بتاريخ 2018/04/14 على الساعة 09:25 على الرابط التالي:
https://www.lesechos.fr/2018/02/la-cybercriminalite-coute-600-milliards-de-dollars-par-an-984995

النمو الاقتصادي والاستثمارات وسوق العمل. وتبقى البنوك الهدف المفضل للمجرمين الإلكترونيين، وبحسب التقرير تبقى روسيا أكبر راعي لهذا النوع من المجرمين.

وفي مقال[1] آخر بجريدة Le Parisien أشار إلى أن ربع المؤسسات الاقتصادية الفرنسية تعرضت سنة 2018 إلى أكثر من 10 هجمات إلكترونية أو محاولات احتيال عبر الأنترنت، كما اعتبرت 78% من المؤسسات الاقتصادية الفرنسية أن حدة الهجمات الإلكترونية في تزايد مستمر. وجاء في تقرير المؤشر السنوي لكل من شركة التأمين Euler Hermes والجمعية الوطنية للمدراء الماليين ورقابة التسيير (DFCG)* أن كل من شركة أيربيس Airbus وفيسبوك وسلسلة فنادق ماريوت ومخابر Bayer ...إلخ كانت هدفا لهجمات إلكترونية وعمليات احتيال خلال الأشهر الأربعة الأولى من سنة 2019، وأبرز هذه الهجمات الإلكترونية تلك التي كانت تتم من خلال الولوج أو الدخول غير المشروع إلى نظام معالجة المعلومات أو البيانات وإعاقته عن الخدمة بواسطة فيروس **ransomware، وبعد ذلك يطالب قراصنة الأنترنت بفدية من أجل إعادة نظام معالجة المعلومات إلى العمل مجددا. ثم تطور الأمر لاحقا فأصبح قراصنة الأنترنت لا يهدفون

[1] مقال للصحفي Marc Lomazzi منشور بتاريخ 2019/04/18 على الساعة 05:55 وتم تعديله على الساعة 12:44 من نفس اليوم على الموقع الإلكتروني لجريدة Le Parisien، تم الاطلاع عليه بتاريخ 2019/04/25 على الساعة 12:09 على الرابط التالي:

https://www.leparisien.fr/economie/cybercriminalite-les-entreprises-francaises-de-plus-en-plus-attaquees-18-04-2019-8055717.php

* Directeurs Financiers et de Contrôle de Gestion.

** فيروس الفدية (ransomware) هو نوع خبيث من البرامج يقفل أجهزة الحاسوب الشخصي أو اللوحي أو الهواتف الذكية – أو يضع تشفيراً على ملفاتك ثم يطلب منك فدية مقابل إعادتها إليك في حالة سليمة؛ هناك نوعان أساسيان من فيروسات الفدية. النوع الأول هو فيروسات التشفير، أي: التي تضع شفرة على الملفات بحيث لا يمكن الوصول إليها؛ ويتطلب فك تشفير الملفات امتلاك المفتاح الذي تم استخدامه في تشفيرها – وهذا هو ما تدفع مبلغ الفدية للحصول عليه. النوع الثاني هو فيروسات الحجب، التي ببساطة تحجب الكمبيوتر أو الأجهزة الأخرى مما يجعلها غير صالحة للعمل. وفي الواقع، تُعد حالات فيروسات الحجب أفضل من فيروسات التشفير، ففرص الضحايا في إزالة الحجب واستعادة إمكانية الوصول أفضل من فك الملفات المشفرة. لمزيد من المعلومات حول هذا الفيروس راجع موقع كاسبرسكي (Kaspersky) على الرابط (متاح بتاريخ 2018/03/25):

https://noransom.kaspersky.com/ar/faq/

ويضاف إلى قائمة الجرائم الإلكترونية الماسة بالأمن القومي الجريمة المنظمة والجرائم المرتبطة بغسيل الأموال وإضعاف العملة المحلية للدولة وكذا المتاجرة بالمخدرات، كل هذا دفع بالعديد من الدول عبر العالم إلى إنفاق ملايين الدولارات على تكنولوجيا الأمن الإلكتروني.

الفرع الرابع: المخاطر السياسية للجريمة الإلكترونية:

لا يمكننا سرد كل تلك المخاطر السياسية الناجمة عن الجريمة الإلكترونية، وإما سنذكر أبرزها فقط وهي:

أولا: ويتجسد ذلك في صورة اختراق أجهزة المسؤولين السامين في الدولة، أو نشر البيانات الشخصية للمناضلين في الأحزاب السياسية والنقابات، أو تلك الخاصة بالمعارضين السياسيين.

ثانيا: كذلك التشهير برؤساء ومسؤولي الدول ورموزها السياسية والقيادية، وذلك من خلال نشر أقوال وإشاعات بذيئة ومسيئة لسمعتهم، أو نشر صور مشينة لهم سواء أكانت هذه الصور حقيقية أم مزيفة، وذلك من أجل إضعاف ثقة مواطني دولهم بهم، وإضعاف نفوذهم على الصعيد الوطني والدولي[1]، ويتم ذلك عادة من خلال ما أصبح يعرف ب"الذباب الإلكتروني".

ثالثا: العبث بقاعدة البيانات المستخدمة من طرف الهيئات الانتخابية في هذا البلد أو ذاك، وتوجيهها من أجل ترجيح كفة حزب معين أو مترشح معين من خلال التلاعب بأصوات الناخبين خاصة في تلك الدول التي تلجأ لما يعرف بالتصويت الإلكتروني، أو الحيلولة دون تحقيق الخصوم لمكاسب سياسية.

المبحث الثاني: طرفي الجريمة الإلكترونية

إن ارتكاب أية جريمة بصفة عامة يتطلب وجود جهة أو طرف يقوم بالنشاط الإجرامي يسمى المجرم، تقابله الجهة الأخرى التي يستهدفها المجرم من خلال نشاطه الإجرامي تسمى الضحية. والأمر نفسه ينطبق على الجريمة الإلكترونية حيث نجد ما يسمى

[1] منير محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص34.

بالمجرم الإلكتروني وكذا الضحية في الجريمة الإلكترونية واللذان يشكلان طرفي الجريمة الإلكترونية.

من خلال هذا المبحث سنسعى إلى التعرف على طرفي الجريمة الإلكترونية.

المطلب الأول: المجرم الإلكتروني

انطلاقا من فكرة أن الجريمة في تطور مستمر وأن الإجرام ليس له حدود، فإن التطور التكنولوجي في مجال الاتصالات والمعلوماتية أفرز لنا صنفا جديدا من المجرمين ونقصد به هنا "المجرم الإلكتروني" والذي يتميز عن المجرم التقليدي أو المجرم في الجرائم بصورتها التقليدية من حيث صفاته وخصائصه وكذا من حيث دوافعه.

سنحاول التعرف على المجرم الإلكتروني وذلك بعرض ما يتمتع به من صفات وما يحركه من دوافع لارتكاب جرائمه.

الفرع الأول: ميزات المجرم الإلكتروني

يتمتع المجرم الإلكتروني بعدة ميزات يستخدمها من أجل ارتكاب الجريمة الإلكترونية، هذه الميزات تتنوع وتتعدد باختلاف درجة ومستوى المجرم الإلكتروني إن كان مبتدئا أو محترفا للإجرام الإلكتروني. ومن أبرز هذه السمات نذكر:

أولا: التمتع بالذكاء المعلوماتي، إذ تعد هذه الخاصية الأبرز والتي تميز المجرم الإلكتروني عن المجرم التقليدي.

فالمجرم الإلكتروني يمتلك معرفة بالأنظمة المعلوماتية وكيفية استخدام تكنولوجيا الاتصالات والوسائل الإلكترونية، فيستغل بذلك هذه القدرات الذهنية في تنفيذ مختلف العمليات التي يمكنه من خلالها بلوغ أهدافه. ونشير هنا إلى أن هذه القدرات تتفاوت من مجرم الإلكتروني لآخر ذلك أن نسبة المهارة وكذا رصيد الخبرة ومستوى المعرفة والإحاطة بالنظام المعلوماتي هي مؤهلات تلعب دورا في تحديد مستوى الإجرام الإلكتروني. وهذه كلها أمور يتم اكتسابها من خلال الدراسة وتبادل الخبرات مع باقي المجرمين.

ثانيا: المجرم الإلكتروني هو مجرم متخصص في ميدان الإجرام الإلكتروني، فغالبا ما يقتصر السلوك والنشاط الإجرامي للمجرم الإلكتروني فقط على الجرائم الإلكترونية دون أن

تكون له نزعة أو ميول إجرامي خارج إطار النظم المعلوماتية بما فيها تقنيات الاتصال وشبكة الأنترنت.

ثالثا: المجرم الإلكتروني حريص على الاستمرار في تطوير قدراته خاصة إذا علمنا بأن الجهات المستهدفة بدورها تلجأ إلى تطوير وسائل الأمان كتطوير أساليب التشفير مثلا، لذلك يستمر المجرم الإلكتروني في صقل مواهبه ورفع مستواه المعرفي مواكبة للتطور الحاصل في مجال مواجهة الجريمة الإلكترونية. وفي هذا الصدد فإن أكثر ما يخشاه المجرم الإلكتروني هو أن يتم الكشف عن هويته، لذلك فهو يلجأ باستمرار إلى تحصين نفسه من خلال مواصلة الحصول على أفضل التقنيات والبرامج والخدع التي تبقيه متخفيا يصعب رصده وتحديد هويته الحقيقية.

الفرع الثاني: دوافع المجرم الإلكتروني

سنستعرض فيما يلي أهم الدوافع التي تؤدي بالمجرم الإلكتروني إلى ارتكاب نشاطه الإجرامي:

أولا: الدافع المادي، أو السعي إلى الحصول على الأموال وتحقيق الثراء. فالكثير من الجرائم الإلكترونية يكون الدافع من ورائها تحقيق الكسب المادي وهو دافع تشترك فيه الجريمة الإلكترونية مع بعض أصناف نظيرتها الجريمة التقليدية.

ثانيا: دوافع انتقامية، وقد تستهدف أشخاصا طبيعيين أو معنويين. فقد يعبث المجرم الإلكتروني بالنظام المعلوماتي للجهة المستهدفة وذلك انتقاما منها على تصرف ما بدر منها، كتلك الحالة التي يقوم فيها رب العمل باتخاذ إجراءات عقابية ضد الموظف أو أن يقوم بتسريحه من العمل، كما قد يكون الانتقام كرد فعل على تعرضه لتصرف مهين من شخص ما.

ثالثا: السعي إلى التفوق، إذ يعتبر التغلب على النظام المعلوماتي وقهر أساليب الحماية صورة من صور إثبات الذات والتفوق العلمي، كما قد يكون شكل من أشكال التباهي خاصة إذا أصبح حدثا تتداوله وسائل الإعلام بشكل واسع.

رابعا: الابتزاز، إذ يعمد المجرم الإلكتروني في هذه الحالة إلى ابتزاز الضحايا وذلك بعد تلاعبه بالنظام المعلوماتي، كحصوله على شفرات سرية لأحدى المؤسسات أو على

ملفات تتعلق بالحياة الخاصة لبعض الأشخاص، ليستغل ذلك لاحقا في ابتزازهم من أجل إجبارهم على القيام بأمور ما لصالحه.

خامسا: الدوافع السياسية، وذلك بغرض الإساءة لدولة ما أو تشويه سمعة حزب منافس أو فضح تصرفات مسؤول حكومي أو بغرض مناهضة نظام حكم لدولة معينة.

إضافة إلى العديد من الدوافع الأخرى كالتسلية أو الدوافع الإيديولوجية بهدف إيصال فكرة ما أو للتعبير عن رفض قرارات معينة كتلك ردود الأفعال التي تصدر عن المنظمات غير الحكومية المدافعة عن البيئة أو المناهضة للعولمة.

كما قد يتخذ البعض من الدين وسيلة أو هدفا لنشاطه الإجرامي، إلى غير ذلك من الدوافع التي تشكل باعثا للمجرم الإلكتروني.

المطلب الثاني: الضحية في الجريمة الإلكترونية

بعد تطرقنا للمجرم الإلكتروني كأحد طرفي الجريمة الإلكترونية، نسعى من خلال هذا المطلب إلى التعرف على الطرف الآخر ونعني به الضحية في الجريمة الإلكترونية. وما ينبغي التوقف عنده هنا، هو أن صفة الضحية لا تقتصر فقط على المجني عليه وإنما تمتد لتشمل كل متضرر من الجريمة الإلكترونية.

قد يقع ضحية لجريمة إلكترونية أشخاصا طبيعيون كما قد يكون الأشخاص المعنويون ضحية للإجرام الإلكتروني وذلك في صورة المؤسسات والشركات سواء أكانت حكومية أم خاصة. وعلى هذا الأساس سوف نقسم هذا الجزء المخصص للتعرف على الضحية في الجريمة الإلكترونية.

الفرع الأول: الشخص الطبيعي كضحية في الجريمة الإلكترونية

لقد أدى اتساع استخدام الأفراد للحاسب الآلي والهواتف الذكية إلى ارتفاع حالات الاعتداءات نتيجة للجريمة الإلكترونية، خصوصا في ظل الإقبال المتزايد على الخدمات التي توفرها شبكة الأنترنت، والذي يبلغ أحيانا إلى حد الإدمان. فالمجرم الإلكتروني أصبح لا يجد عناء كبيرا في اصطياد ضحاياه، إذ يستهدفهم مباشرة من خلال قرصنة حواسيبهم أو هواتفهم أو من خلال اختراق بريدهم الإلكتروني أو تلك الحسابات التي ينشئها الأفراد داخل العالم الافتراضي لا سيما بمناسبة إقبالهم على شبكات التواصل الاجتماعي والتي

أضحت ملاذا للقرصنة وما يتبعها من تشهير بالأفراد من خلال نشر صورهم وإتاحتها للجمهور، أو من خلال الابتزاز للضحايا عن طرق التهديد بنشرها مقابل الحصول على فوائد معينة قد تكون في أغلب الحالات مالية.

والملاحظ أنه في كثير من الحالات لا يبادر الضحايا إلى الإبلاغ عن هذه الجرائم خشية على سمعتهم داخل الأسرة والمجتمع، الأمر الذي لا يساعد على مكافحة الجريمة الإلكترونية ويجعل الجناة في منأى عن المتابعة، بل أن عزوف الضحايا عن التبليغ يشجع الجناة على مواصلة نشاطهم الإجرامي من خلال استمرارهم ومواصلتهم في تصيد الضحايا.

كما أنه وفي بعض الأحيان، وبعد تردد قد يبادر بعض الإفراد إلى التبليغ عن هذه الجرائم لكن بشكل متأخر، وهذا ما يعيق جهات التحقيق من تتبع الجاني خاصة وأن الجرائم الإلكترونية تتطلب سرعة اتخاذ الإجراءات نظرا لطبيعتها ولما تتميز به من خاصيات تشكل عقبات أمام جهات التحري والتحقيق.

الفرع الثاني: الشخص المعنوي كضحية في الجريمة الإلكترونية

تشكل الجرائم الإلكترونية التي تستهدف الأشخاص المعنوية خطرا كبيرا، سواء تعلق الأمر بالأشخاص المعنوية الحكومية أو الخاصة، ذلك أنها تستهدف عددا كبيرا من الضحايا دفعة واحدة أو تمس بمصلحة من المصالح الحيوية للدولة إذا ما تعلق الأمر بمنشآت حساسة كتلك المتعلقة بالدفاع والأمن القومي.

لقد أثبت الواقع بأن الأشخاص المعنوية، العامة منها أو الخاصة ليست بمنأى عن الجريمة الإلكترونية سواء تعلق الأمر بالوزارات، المستشفيات، الفنادق، المؤسسات الإعلامية، المنشآت العسكرية والنووية، المؤسسات المالية...الخ، فكلها أضحت مستهدفة ومتاحة أمام المجرم الإلكتروني.

إن ما ذكرناه سابقا بخصوص إحجام الأفراد أو الأشخاص الطبيعيين عن التبليغ لدى وقوعهم ضحايا لجريمة إلكترونية ما، فإنه ينطبق كذلك على تلك الحالات التي يكون فيها الضحايا من الأشخاص المعنويين، حيث تبرز في هذا السياق المؤسسات المالية والبنوك كأكثر الأشخاص المعنوية عزوفا عن الإبلاغ عن تلك الجرائم الإلكترونية التي تكون

ضحايا لها وذلك خشية فقدان ثقة العملاء والزبائن بها فتفقد بالتالي سمعتها وقيمتها بين المنافسين، لذلك تعمد الكثير من البنوك إلى التستر على تلك العمليات التي تتعرض لها أنظمتها المعلوماتية من قرصنة وإتلاف وتجسس وغيرها من الجرائم الإلكترونية.

المبحث الثالث: المعلومات بوصفها محلا للجريمة الإلكترونية

انطلاقا من التعريف المبسط للجريمة على اعتبار أنها فعل غير مشروع يشكل اعتداء على مصلحة يحميها القانون، فإنه وفي موضوع الجريمة الإلكترونية نجد أن المجرم الإلكتروني يستهدف تلك المعطيات المخزنة بالوسائل التقنية الحديثة التي شاع استخدامها في العالم حاليا، ونقصد بها خاصة الحواسيب الآلية والهواتف الذكية والتي يمكن بواسطتها استغلال ما توفره شبكة الأنترنت.

هذه المعطيات تشكل معلومات ذات أهمية بالغة سواء بالنسبة للأفراد أو المؤسسات وتستوجب حمايتها نظرا لكونها أضحت محلا للجريمة الإلكترونية. وهنا يبرز تساؤل بخصوص المقصود بالمعلومات أو المعلومة، لذلك ومن أجل التعرف عن معنى المعلومة سوف نقسم هذا المبحث إلى الأجزاء التالية:

المطلب الأول: تعريف المعلومة.

المطلب الثاني: خصائص المعلومات.

المطلب الثالث: شروط إضفاء الحماية القانونية على المعلومة.

المطلب الرابع: الطبيعة القانونية للمعلومات.

المطلب الأول: تعريف المعلومات

لغة فإن المعلومات مشتقة من كلمة علم. ويقصد بها المعرفة أو جملة المعارف التي يمكن للإنسان اكتسابها ونقلها للغير. والمعلومات جمع معلومة، وبتصفح معجم المعاني الجامع[1] نجد أن المقصود بالمعلومات الأخبار والتحقيقات أو كل ما يؤدي إلى كشف الحقائق وإيضاح الأمور واتخاذ القرارات المعلومات، كما يقصد بالمعلومات مجموعة الأخبار والأفكار المخزنة أو المنسقة بواسطة الكومبيوتر.

[1] عمر أحمد مختار، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، 2008، ص 1544.

أن المشرع السوري استعمل عبارة "...لها معنى قابل للإدراك مرتبط بسياق محدد" وهي عبارة وردت على إطلاقها فلا يمكننا القول إنها تناولت مضمون المعلومات بشكل واضح.
المشرع البحريني وبموجب المادة الأولى من القانون رقم 28 الصادر سنة 2002 والمتعلق بالمعاملات الإلكترونية[1]،عرف المعلومات على أنها "البيانات والنصوص والصور والأشكال والأصوات والرموز وبرامج الحاسب والبرمجيات وقواعد البيانات والكلام وما شابه"
في حين أن المشرع الأردني عرف المعلومات بموجب المادة الثانية من القانون رقم 27 الصادر سنة 2015 والمتعلق بالجرائم الإلكترونية على أنها "البيانات التي تمت معالجتها وأصبح لها دلالة"[2] ويلاحظ بأن هذا التعريف لا يقدم لنا معنى محدد للمعلومات، فيقال بشأنه ما قد قيل بخصوص التعريفات السابقة.
بالنسبة للمشرع الجزائري وبعد مراجعتنا للقانون 09-04[3] وكذا المرسوم الرئاسي 15-261 الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[4] لم نجد أي تعريف للمعلومات، ولو أن كلمة "معلومات" استعملها المشرع الجزائري في كثير من المواضع داخل النصوص القانونية التي تضمنها كل من القانون والمرسوم الرئاسي سابقة الذكر.

---

[1] القانون رقم 28 الصادر بتاريخ 08/18/ 2002 والمتعلق بالمعاملات الإلكترونية المنشور بالجريدة الرسمية لمملكة البحرين تحت رقم 2548. راجع موقع هيئة التشريع والرأي القانوني لمملكة البحرين من خلال الرابط (متاح بتاريخ 2018/08/02): https://www.legalaffairs.gov.bh/Media/LegalPDF/L2802.pdf

[2] القانون رقم 27/ 2015 الصادر بتاريخ 2015/01/06 والمنشور بالصفحة 631 للجريدة الرسمية العدد 5343 والمتضمن قانون الجرائم الإلكترونية. راجع موقع ديوان التشريع والرأي للمملكة الأردنية الهاشمية من خلال الرابط (متاح بتاريخ 2018/08/17):
http://www.lob.jo/?v=1.11&url=ar/LegislationDetails?LegislationID:3184,LegislationType:2,isMod:false

[3] القانون رقم 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المرجع السابق.

[4] المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 الصادرة في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015.

الفرع الثاني: التعريف الفقهي للمعلومات

هناك عدة تعريفات فقهية قيلت بشأن المعلومات، فتارة تتشابه وتارة تختلف، ونذكر منها على سبيل المثال التعريفات التالية:

تعرف المعلومة بأنها " مجموعة رموز نستخلص منها معنى معين في مجال محدد ويتمتع بالتحديد والابتكار والسرية والاستئثار"[1]

ويلاحظ بأن هذا التعريف أصبغ على المعلومات صفة السرية وهي صفة تجعل المعلومات من قبيل الخصوصية وهذا ما يبرر إحاطتها بالحماية الجنائية صونا لحرمة الحياة الخاصة، وهذا بدوره أدى إلى ظهور مصطلح " الخصوصية المعلوماتية".

كما تعرف المعلومات بأنها " كل مادة معرفة قابلة لأن تتمثل في إشارات متعارف عليها من أجل حفظها أو معالجتها أو بثها "[2]. وقد عرف الفقيه Pierre Catala المعلومات بأنها " رسالة معبر عنها بشكل يجعلها قابلة للنقل أو الإبلاغ للغير"[3].

وتعرف المعلومات كذلك بأنها " شيء أولي له قيمة نابعة عما يتميز به هذا الشي من خصوصية من حيث مصدره أو بسبب طبيعته. وتتم. حمايته في إطار البيئة التي يوجد فيها، أو بوصفه لصيقا بشخص أو بوصفه عنصرا في الذمة المالية"[4]

كما عرفت المعلومات على أنها " مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير والتأويل أو للمعالجة سواء بواسطة الأفراد أو الأنظمة الإلكترونية"[5]

كما تعرف المعلومات على أنها " رسالة ما معبر عنها في شكل يجعلها قابلة للنقل أو الإبلاغ للغير"[6]

---

[1] أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006، ص47.

[2] علي كحلون، المسؤولية المعلوماتية، مركز النشر الجامعي، 2005، ص36.

[3] Pierre CATALA, Ébauche d'une théorie juridique de l'information, Dalloz, 1984, chron, p97. cité par: VIVANT, Michel. "La privatisation de l'information par la propriété intellectuelle. Revue internationale de droit économique, no 4 ,2006, P 363. Article téléchargé depuis le lien (disponible 12/04/2018): https://www.cairn.info/load_pdf.php?ID_ARTICLE=RIDE_204_0361&download=1

[4] Alain Madec ; Pierre Leclercq, Les flux transfrontières de données : vers une économie internationale de l'information, La Documentation française, Paris 1982, p122.

[5] Parker Donn, Fighting computer crime - A new framework for protecting information-, John Wiley and Sons Inc., New York, 1998, p22.

[6] محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994، ص173.

الفرع الثاني: المعلومة قابلة للتداول والحيازة المشتركة

حيث أن قابلية المعلومة للتداول أكسبها قيمة اقتصادية أدت إلى ظهور ما يسمى ب " سوق المعلومات" خاصة في ظل التطور التكنولوجي الذي أتاح تداول المعلومات على مستوى عالمي بواسطة وسائل الاتصال الحديثة وشبكة الأنترنت.

كما أن المعلومة قابلة للحيازة من طرف أكثر من شخص واحد وفي الوقت نفسه، وهذا عكس الأشياء ذات الطبيعة المادية والتي لا يمكن أن يحوزها ويستأثر بها سوى شخص واحد أو يحوزها عدة أشخاص بعد تداولها، فلا يمكن أن يستأثر بها عدة أشخاص في نفس الوقت عكس المعلومة.

الفرع الثالث: المعلومة غير قابلة للنفاد

على الرغم من التداول غير المحدود للمعلومة أو امتلاكها من طرف عدة أشخاص في نفس الوقت وفي مناطق متباعدة، غير أن المعلومة لا يمكن استنفادها.

المطلب الثالث: شروط إضفاء الحماية القانونية على المعلومة

إن الخصائص التي سبق ذكرها والتي تتميز بها المعلومة لا تكسب هذه الأخيرة الحماية القانونية إذ لابد أن تقترن بشروط تكفل لها الحماية القانونية في حالة الاعتداء عليها.

المعلومات صنفين أو نوعين، معلومات عامة متاحة لعامة الناس أو الجمهور فيمكن لأي شخص الحصول عليها دون قيد. أما الصنف الثاني فيتمثل في تلك المعلومات التي ترد عليها قيود، إذ يتطلب الوصول أو الحصول عليها ضرورة احترام إجراءات معينة، فتعتبر بذلك معلومات خاصة تحظى بالحماية القانونية في حالة الاعتداء عليها. وهنا يطرح تساؤل حول تلك الشروط الواجب توافرها في المعلومة حتى تستفيد من الحماية القانونية لها وبالتالي يترتب جزاء على كل من يعتدي عليها.

يمكن تلخيص وإيجاز هذه الشروط في التحديد والابتكار، ثم السرية وكذا الاستئثار.

الفرع الأول: شرط التحديد

تتطلب إحاطة المعلومة بالحماية القانونية أن تكون هذه المعلومة محددة، أي يمكن حصرها في نطاق معين وذلك لأن الاعتداء يقع على شيء محدد فلا يمكن شمول المعلومة بحماية قانونية دون تحديد هذه المعلومة[1].

الفرع الثاني: شرط الابتكار

ويقصد بالابتكار الإنتاج الذهني الذي يتميز بقدر من الجدة، والأصالة في طريقة العرض، أو التعبير، أو في أحدهما، والذي من شأنه أن يبرز شخصية معينة لصاحبه[2].

فالمعلومة إذن يجب أن تكون مبتكرة وغير شائعة بين الناس، فترتبط بشخص محدد يمتلكها وتبرز من خلالها شخصيته.

الفرع الثالث: شرط السرية

وتعرف سرية المعلومة على أنها واقعة أو صفة ينحصر نطاق العلم بها في عدد محدود من الناس، إذا كانت ثمة مصلحة يعترف بها القانون لشخص أو لأكثر في أن يظل العلم بها محصورا في ذلك النطاق[3].

فتلك المعلومات التي تعتبر بطبيعتها معلومات شائعة ولا يمكن حيازتها، فهي معلومات فاقدة للسرية كتلك المعلومات المتعلقة بالطقس والأحوال الجوية فهي معلومات يسهل تداولها.

فالمعلومة التي يحظر الاطلاع عليها تتسم بالسرية إذ أن المعلومة التي لا تتسم بالسرية هي معلومة مكشوفة ومجال حركتها غير محدد بمجموعة من الأشخاص وتكون قابلة للتداول، فلا يمكن الحديث عندئذ عن الاعتداء عليها بسرقتها أو الاطلاع عليها بدون وجه حق لأنها بمنأى عن أي حيازة[4].

[1] محمد سامي الشوا، مرجع سابق، ص175.

[2] رشا مصطفى أبو الغيط، تطور الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، 2006، ص115.

[3] سهيل محمد العزام، الوجيز في جرائم الإنترنت، الطبعة الأولى، دائرة المكتبة الوطنية، عمان، 2009، ص99.

[4] نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، 2005، ص109.

فالبيانات التي لا تتم إحاطتها بالسرية والخصوصية فهي غير محمية كونها متاحة لعامة الجمهور. فمستخدم الإنترنت، الذي يقوم بزيارة موقع من المواقع على شبكة الإنترنت به بيانات مكشوفة ومتاحة للعامة، ويمكن لمستخدمي الإنترنت الوصول إليها بطريقة بسيطة؛ هذا المستخدم لا يمكن متابعته قانونيا كون هذه البيانات ليست أصلا محمية ولم يصدر بشأنها أي سلوك يفيد بوقوع تعدي أو انتهاك بأي شكل من أشكال. فهي معلومات لم يتم تحديد نطاق السرية بشأنها وبالتالي فهي غير محاطة بالحماية القانونية.

في المجال القضائي، هناك قضية بارزة عالجت حالة ذات صلة بموضوع السرية والحماية القانونية للمعلومة، ونعني بها تلك القضية التي كانا طرفاها كل من النيابة العامة و شركة (Tati) من جهة، والمدعو (Antoine CHAMPAGNE "Kitetoa")[1] من جهة أخرى. ولقد صدر بشأنها قرار يعتبر من قبيل الاجتهاد القضائي، ونعني به هنا القرار الصادر عن محكمة الاستئناف بباريس سنة 2002.

الفرع الرابع: شرط الاستئثار

يعد الاستئثار أمر ضروري لأن الجرائم التي تنطوي على اعتداء قانوني على القيم، يستأثر الجاني بسلطة تخص الغير وعلى نحو مطلق، والاستئثار في مجال المعلومات يمكن أن يرد على الدخول في المعلومة والمخصص لمجموعة محددة من الأشخاص، لذا فإن الاستئثار ينظر إلى المعلومة بوصفها من قبيل الأسرار ويمكن أن يرد الاستئثار

[1] CA Paris 12ème ch, section A Arrêt du 30 octobre 2002, disponible via le lien (consulté le 20/12/2018 à 19:10):
https://www.legalis.net/jurisprudences/cour-dappel-de-paris-12eme-chambre-section-a-arret-du-30-octobre-2002/

راجع بخصوص هذا المعنى كل من:

- Mohamed KAHLOULA, LE DELIT D'ACCES OU DE MAINTIEN FRAUDULEUX DANS UN SYSTEME DE TRAITEMENT AUTOMATISE DE DONNEES (S.T.A.D), Revue des Sciences Juridiques, Administratives et Politiques, N° 12, la faculté de Droit et des sciences politiques, université Abou- Bekr Belkaid, Tlemcen, 2011, p 94-96.

- Elie Stella. L'adaptation du droit pénal aux réseaux sociaux en ligne. Droit. Université de Lorraine,2019, p109. Consultation et téléchargement disponible via le lien (consulté le 09/12/2020):
https://hal.univ-lorraine.fr/tel-02985468/document

لقد ثار تساؤل حول طبيعة المعلومة خارج دعامتها المادية، فهل يمكن اعتبار المعلومة ـ وهي خارج دعامتها المادية ـ ذات قيمة مادية تستوجب الحماية القانونية في حالة ما إذا تم الاعتداء عليها.

انقسم الفقه في إجابته على هذا التساؤل إلى اتجاهين، اتجاه أول يعرف بالاتجاه التقليدي وهو ينفي صفة القيمة المادية على المعلومة المستقلة بذاتها خارج دعامتها. أما الاتجاه الثاني والذي يعرف بالاتجاه الحديث يعتبر بأن المعلومة بذاتها تعتبر من القيم المستحدثة وأضفى عليها الحماية القانونية. وسنحاول شرح مضمون كلا الاتجاهين فيما يلي:

الفرع الأول: الاتجاه التقليدي

يرى أنصار هذا الاتجاه بأن المعلومة المستقلة بذاتها خارج دعامتها المادية تعتبر فقط ذات طبيعة معنوية وتفقد قيمتها المادية، وبالتالي لا يمكن أن تكون محلا للحماية القانونية. ويبررون موقفهم هذا بكون الأشياء ذات القيمة المادية هي فقط تلك الأشياء التي تقبل الاستحواذ عليها والاستئثار بها، في حين أن المعلومة غير القابلة للاستحواذ عليها والاستئثار بها إلا عن طريق الملكية الأدبية والفكرية أو الصناعية. فالمعلومة المخزنة والتي لا تنتمي إلى حق من هذه الحقوق لا يمكن إدراجها ضمن القيم المحمية، وبالتالي فهي لا تصلح بأن تكون محلا للحماية القانونية[1].

ورغم أن هذا الاتجاه يعترف بالقيمة الاقتصادية للمعلومات ولا ينكرها، غير أنه وبالمقابل ينفي عنها القيمة المالية ويستبعدها من طائفة الأموال. ويبرر ذلك من خلال إدراج المعلومات ضمن الخدمات والمنافع حيث تكون المعلومة وهي خارج دعامتها المادية متاحة للجميع، فيمكنهم الانتفاع بها ما دام أنها غير قابلة للاستحواذ[2].

ويواصلون تبرير موقفهم هذا بعدم جواز الخلط بين القيمة الاقتصادية للمعلومة ـ والتي يعترفون بها ـ والقول بأنها مال يمكن الاعتداء عليه، بحيث ينفون عليها صفة المال. فالمعلومات بحسب رأيهم ليست مالا كونها غير قابلة للقياس والتحريز في ظل عدم وجود قوام مادي لها بذاتها مستقل عن دعامتها المادية (أسطوانة، شريط، صورة ...الخ)

[1] أنظر في هذا المعنى محمد عبد الله أبوبكر، مرجع سابق، ص83.

[2] أنظر في هذا المعنى أحمد خليفة الملط، مرجع سابق، ص104 ومحمد سامي الشوا، مرجع سابق، ص176.

وبالتالي فهي لا تحظى بالحماية القانونية التي تحظى بها الأموال ذات الطبيعة المادية الملموسة[1].

الفرع الثاني: الاتجاه الحديث

على نقيض الاتجاه التقليدي، يرى أنصار الاتجاه الحديث بأن المعلومة تشكل مجموعة من القيم المستحدثة كما أنها تعد من قبيل الأموال وبالتالي فهي جديرة بأن تكون محلا للحماية القانونية من أي اعتداء يطالها.

إذ يرى الفقيه الفرنسي CATALA بأن المعلومة المستقلة عن دعائمها المادية لها قيمة قابلة للاستحواذ وذلك لأنها تقوم وفقا لسعر السوق متى كانت غير محظورة تجاريا، وهذا ما يعبر عنه بالقيمة الاقتصادية للمعلومة. كما يرى بأن هناك علاقة تبعية بين المعلومة ومؤلفها شبيهة بتلك العلاقة القانونية التي تربط المالك بالشيء المملوك. وعلى هذا الأساس يخلص الأستاذ CATALA إلى أن المعلومات تخول لصاحبها ميزتين أساسيتين تتمثل الأولى في حقه بضمان سرية المعلومة والثانية في طلب التعويض عن الأضرار التي تترتب على أي عمل غير مشروع يتعلق بها، مما يجعل المعلومة ذات قيمة قابلة للتملك، وذلك لما لها من قيمة اقتصادية؛ وعليه يمكن أن تعد المعلومة محلا للاعتداء والاستغلال والتملك على أساس قيمتها الاقتصادية[2].

[1] عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، بدون ناشر، 1990، ص102. وكذلك محمد أمين الرومي، المستند الإلكتروني، الطبعة الأولى، دار الفكر الجامعي، 2007، ص117. أشار إليه محمد عبد الرحمن عنانزة، مرجع سابق، ص87. في هذا السياق نذكر كمثال ما ذهب إليه القضاء الفنلندي حيث رفض إضفاء وصف السرقة في الحصول غير المشروع على المعلومات منفصلة عن إطارها المادي وذلك في قضية قيام مبرمج بإحدى شركات التأمين بنقل بيانات خاصة بالعملاء على أسطوانات ممغنطة= =مملوكة للشركة التي يعمل بها بشكل غير مشروع، وقضت محكمة أول درجة بأن التهمة تنحصر في سرقة الأسطوانات الممغنطة دون المعلومات التي تم تسجيلها عليها، هذا ولقد أيدت محكمة الاستئناف هذا الحكم موضحة بأنه في حالة الحصول غير المشروع على المعلومات ينبغي أن ينصرف إلى الإطار أو الوسيط المادي الذي يحتوي على المعلومات، إما إذا انفصلت المعلومات عن إطارها المادي فإنه لا محل لتطبيق جريمة السرقة. وأيدت المحكمة العليا كذلك الحكم السابق. أنظر محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، الإسكندرية، 2018، ص82-83.

[2] Pierre CATALA, «La «propriété» de l'information», Mél. Raynaud, Paris, Dalloz-Sirey, 1985, p 97-98. Cité par: Caroline Cochez. La participation du droit des biens au mouvement de socialisation du droit.= = =

أما عن كون المعلومة غير قابلة للقياس كما ذهب إلى ذلك الاتجاه التقليدي، فإن أنصار الاتجاه الحديث يردون على ذلك بالبحث عن تعريف المادة في العلوم الطبيعية، فالمادة هي كل ما يشغل حيزا ماديا في فراغ معين، وبتطبيق تعريف المادة على الكيانات المنطقية أو البرامج نجد بأنها تشغل حيزا ماديا في ذاكرة الحاسب الآلي يمكن قياسها بمقياس معين هو البايت Byte، والكيلوبايت Kilo byte، والميجابايت Mega byte، والجيجابايت Giga byte وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسب بعدد الحروف التي يمكن تخزينها بها، كما أن هذه البيانات تأخذ شكل نبضات إلكترونية تمثل الرقمين صفر وواحد وهي تشبه التيار الكهربائي الذي اعتبره الفقه والقضاء في مصر وفرنسا من قبيل الأشياء المادية[1].

أما الأستاذ Michel VIVANT فإنه يبرر جدارة المعلومة بالحماية القانونية من خلال الاستناد على فكرة مفادها أن الشيء أو القيمة لها صورة معنوية ذات طابع اقتصادي جديرة بالحماية القانونية[2]. وفي الحقيقة فإن هذا الرأي سبق وأن عبر عنه كل من الأستاذين Marcel PLANIOL و Georges RIPERT[3]. هذا من جهة، ومن جهة أخرى يرى الأستاذ Michel VIVANT بأن الأشياء المملوكة للغير ملكية معنوية ويعترف بها القانون ترتكز على الاعتراف بأن للمعلومة قيمة عندما تكون بصدد براءة اختراع أو

=Université du Droit et de la Santé - Lille II, France, 2013, p 239, p 333. Thèse téléchargée depuis le lien (disponible 14/04/2018): https://tel.archives-ouvertes.fr/tel-01143298/document

أنظر في هذا المعنى كذلك كل من: نائلة عادل محمد فريد قورة، مرجع سابق، ص120 وناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2008، ص18. أشار إليهما كل من محمد عبد الرحمن عنانزة، مرجع سابق، ص88 وسامي جلال فقي حسين، مرجع سابق، ص46.

[1] عبد اللاه أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008، ص87 وما بعدها.

[2] M. Vivant, A propos des " biens informationnels ", JCP 1984, I, n° 3132. Cité par: Étienne MONTERO, La responsabilité civile du fait des bases de données (Travaux de la Faculté de droit de Namur,21), Presses universitaires de Namur, 1998, p 187-188.

[3] M. PLANIOL, G. RIPERT, Traité pratique de droit civil français, t. III, Paris, LGDJ, 2e éd., 1952, p.57, n°50. Cité par: Aurélien DUPEND, L'argument jusnaturaliste en droit privé patrimonial français, thèse droit, Université de Bordeaux, 20 juin 2014, p 195. Téléchargée depuis le lien (disponible 25/12/2018): http://www.theses.fr/2014BORD0148/abes

الباب الأول:

الجهات المتصلة بالتحقيق الابتدائي في الجريمة الإلكترونية

الفصل الأول: الجهة المناط بها التحقيق الابتدائي في الجريمة الإلكترونية

الفصل الثاني: الضبطية القضائية جهة ذات صلة بالتحقيق الابتدائي

حاولنا من خلال هذا الفصل التمهيدي البحث في ماهية الجريمة الإلكترونية وذلك بالخوض أولا في تلك المحاولات الفقهية العديدة التي تناولت موضوع تعريف الجريمة الإلكترونية وذلك بالاعتماد على عدة معايير، غير أن كل هذه المحاولات أكدت عدم إمكانية إيجاد تعريف موحد للجريمة الإلكترونية بل حتى الخلاف طال التسمية في حد ذاتها فنالت بدورها حظها من الاختلاف.

بعد ذلك استعرضنا خصائص الجريمة الإلكترونية والتي جعلت منها جريمة تختلف عن الجريمة بمفهومها التقليدي، سواء من حيث البيئة التي ترتكب فيها أو من حيث كونها جريمة عابرة للحدود ويصعب اكتشافها، كما أنها ذات أضرار جسيمة... إلى غير ذلك من الخصائص التي تفردت بها. وبعد هذا انتقلنا إلى التعرف على صور الجريمة الإلكترونية من خلال تلك التصنيفات الفقهية، كما ألقينا نظرة على مخاطر الجريمة الإلكترونية.

المحطة الثانية لهذا الفصل التمهيدي قادتنا إلى التعرف على طرفي الجريمة الإلكترونية والمتمثلان في المجرم الإلكتروني والضحية في الجريمة الإلكترونية، حيث تعرفنا على ميزات المجرم الإلكتروني ودوافعه من جهة، ومن جهة أخرى أبرزنا بأن الضحية في الجريمة الإلكترونية قد يكون شخصا طبيعيا كما أنه قد يكون شخصا معنويا.

وخصصنا النقطة الثالثة والأخيرة في هذا الفصل التمهيدي للتعريف بالمعلومة كونها مستهدفة في الجريمة الإلكترونية، فاستعرضنا جملة التعريفات الفقيهة والتشريعية التي تناولت تعريف المعلومات ثم تطرقنا لكل من خصائص المعلومات ولتلك الشروط الواجب إضفائها على المعلومة حتى تستفيد هذه الأخيرة من الحماية القانونية لها. لنختم هذا الفصل التمهيدي بالحديث عن الطبيعة القانونية للمعلومات.

تمهيد وتقسيم:

إن الحديث عن التحقيق الابتدائي المتعلق بالجريمة الإلكترونية يقودنا إلى النظر في تلك الجهات المكلفة بمهمة التحقيق الإبتدائي، ونقصد بها هنا ذلك الجهاز الذي منحه القانون صلاحية القيام بإجراءات التحقيق الإبتدائي كجهة أصيلة. هذا الأمر يقودنا بدوره إلى ضرورة التعريف بالتحقيق الإبتدائي وعرض الأهمية التي يكتسيها وكذا الضمانات التي أحاطها به المشرع، هذا من جهة.

ومن جهة أخرى، فإنه وبمناسبة الخوض في موضوع التحقيق الإبتدائي، يتحتم علينا التطرق إلى ذلك الجهاز الذي له صلة وعلاقة وطيدة بالتحقيق الابتدائي بل وقد تسند له مهمة القيام ومباشرة إجراءات هي من صميم التحقيق الابتدائي ونقصد بهذا الجهاز في هذا المقام جهاز الضبطية القضائية أو الشرطة القضائية. فالشرطة القضائية على المستوى الوطني (في الجزائر) قد تسند لها مهام هي من صميم إجراءات التحقيق الإبتدائي، وهذا ما يبرر إدراجنا لهذه النقطة في دراستنا الحالية. يضاف إلى ذلك عرض لما أصبح الوضع عليه بأجهزة الشرطة على المستوى الوطني لبعض الدول، دون أن ننسى الامتداد الدولي للجريمة الإلكترونية والذي اثر على الأجهزة الأمنية بصفة عامة وجهاز الشرطة بصفة خاصة وذلك على المستويين الإقليمي والدولي كذلك.

ونتيجة لما سبق، فلقد قسمنا الباب الأول إلى فصلين بحيث خصصنا الفصل الأول منه للتفصيل في الجهة المناط بها التحقيق الابتدائي في الجريمة الإلكترونية، في حين أفردنا الفصل الثاني للحديث عن الضبطية القضائية باعتبارها جهة ذات صلة بالتحقيق الابتدائي في الجريمة الإلكترونية.

الفصل الأول: الجهة المناط بها التحقيق الابتدائي في الجريمة الإلكترونية

من خلال هذا الفصل سنسعى إلى التعرف على تلك الجهة التي تؤول لها سلطة التحقيق الابتدائي في الجريمة الإلكترونية، لكن قبل ذلك سنتعرف على مفهوم التحقيق الابتدائي وكذا التطرق إلى موضوع الاختصاص القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية.

المبحث الأول: مفهوم التحقيق الابتدائي

كلما وقعت جريمة داخل المجتمع وجدت السلطات القضائية نفسها أمام واجب يفرض عليها مسؤولية إيجاد الجاني ومعاقبته. فالدعوى العمومية أو الجنائية كما تميل إلى تسميتها بعض التشريعات المقارنة، تمر بمرحلة الاتهام، ثم التحقيق، فالمحاكمة.

تعتبر مرحلة التحقيق الابتدائي مرحلة على قدر كبير من الأهمية، وذلك لدورها في البحث عن الأدلة التي تساعد في كشف الحقيقة.

للتعرف على مفهوم التحقيق الابتدائي، قسمنا هذا المبحث إلى ثلاثة أقسام نتطرق من خلالها لتعريف التحقيق الابتدائي، ثم نوضح أهميته، ونختم هذا المبحث بالنظر في الضمانات المرتبطة بالتحقيق الابتدائي.

المطلب الأول: تعريف التحقيق الابتدائي

إن التحقيق الابتدائي باعتباره عملا قضائيا يخول لسلطات التحقيق القيام بإجراءات تسبق المحاكمة. ولقد تعددت تلك التعريفات التي قيلت بشأن التحقيق الابتدائي.

فهناك من يعتبر التحقيق الابتدائي بأنه "مجموعة الإجراءات التي تباشرها السلطة المختصة بتحقيق الدعوى عن جريمة ارتكبت لكشف الحقيقة وذلك بالبحث والتنقيب عن

الأدلة وتجميعها وتقديرها لإثبات حدوث الجريمة ونسبتها إلى المتهم، لتحديد مدى كفايتها لإحالة المتهم للمحاكمة أو لنفي الاتهام كأساس للأمر بالأوجه لإقامة الدعوى"[1].

وهناك من يعرف التحقيق الابتدائي على أنه " مجموعة من الإجراءات تستهدف التنقيب عن الأدلة في شأن جريمة ارتكبت وتجميعها ثم تقديرها لتحديد مدى كفايتها لإحالة المتهم إلى المحاكمة[2]"

وعلى كل، ومهما كثرت التعريفات التي تناولت موضوع التحقيق الابتدائي، فإننا نميل إلى تلك التي تضمنت المعيارين الموضوعي والشخصي في تعريفها للتحقيق الابتدائي، أي أنها تطرقت إلى الإجراءات المتخذة بمناسبة التحقيق الابتدائي، وفي نفس الوقت أشارت إلى تلك الجهة التي منحها المشرع سلطة التحقيق الابتدائي.

المطلب الثاني: أهمية التحقيق الابتدائي

تكتسي مرحلة التحقيق الابتدائي أهمية كبيرة تتجسد من خلال إسهامها في تهيئة الدعوى لقضاة الحكم، فالتحقيق الابتدائي باعتباره مرحلة تحضيرية تسبق المحاكمة فهو لا يستهدف الفصل في القضية، وإنما يعمل على تهيئتها لجهة المحاكمة.

وعلى خلاف ما هو عليه الأمر في مرحلة التحقيق الأولي (مرحلة جمع الاستدلالات) فإن التحقيق الابتدائي يتيح لقاض التحقيق سماع المتهم في عدة جلسات (الحضور الأول، السماع في الموضوع) وكذا مواجهته بالضحية أو بقية المتهمين.

فمرحلة التحقيق الابتدائي من شأنها البحث والتنقيب عن الأدلة وجمعها واستظهار قيمتها واستبعاد الأدلة الضعيفة واستخلاص رأي مبدئي بشأنها، ومن ثم تستطيع المحكمة أن تنظر الدعوى وقد اتضحت عناصرها وتكشفت ملامحها، فيدعم ذلك أن يأتي حكمها

[1] سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الأولى، دار النهضة العربية، 1999، ص133.

[2] محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 1995، ص501.

أقرب إلى الحقيقة والعدالة، وبالتالي فلمرحلة التحقيق الابتدائي أهمية بالغة سواء في تحقيق المصلحة العامة أو في اعتبارها ضمانة للحرية الشخصية[1].

المطلب الثالث: ضمانات التحقيق الابتدائي

إن التحقيق الابتدائي باعتباره يهدف إلى التنقيب عن الأدلة وكشف الحقيقة، كان لزاما أن تحاط إجراءاته بسياج من الضمانات تكفل له السير الحسن. هذه الضمانات يمكن إيجازها فيما يلي:

الفرع الأول: سرية التحقيق الابتدائي

السرية والتي هي نقيض العلانية، يقصد بها عدم السماح للجمهور بالدخول للأمكنة التي يجري بها التحقيق فلا يجوز لهم الحضور أثناء التحقيق، كما لا يصرح لهم بالاطلاع على محاضر التحقيق، فيحضر على وسائل الإعلام نشر وإذاعة مضمون محاضر التحقيق.

غير أن هذه السرية ليست مطلقة وإنما نسبية، ذلك أنها لا تشمل من هم أطرافا في الدعوى ولا محاميهم أو وكلائهم، وإنما السرية تعتبر موجهة لعموم الناس. فالتحقيق الابتدائي تلازمه السرية عكس المحاكمة التي تكون علنية وبإمكان جمهور الناس حضورها.

ويجد مبدأ السرية ما يبرره وذلك من خلال ضرورة حماية حقوق المتهم وصيانة سمعته ومنع التشهير به، خاصة إذا اتضح فيما بعد زور وزيف الاتهامات التي وجهت إليه، وهذا ما يعبر عنه من الناحية القانونية بضرورة احترام قرينة البراءة، فالمتهم برئ حتى تثبت إدانته.

علاوة على ذلك، فإن سرية التحقيق تبقي جهة التحقيق في منأى عن الضغط ومحاولات التأثير على سير التحقيق. كما أن سرية التحقيق بإمكانها المساهمة في تعاون الشهود،

[1] محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية تنقيح فوزية عبد الستار، دار النهضة العربية، الجزء الأول، الطبعة الرابعة، 2011، ص550.

ذلك أن العلانية قد تبعث في نفوسهم الخوف والذعر فيمتنعون عن سرد كل الحقائق التي يعرفونها خشية على سلامتهم أو سلامة ذويهم.

وأخيرا تجدر الإشارة إلى أن جهات التحقيق قد تضطر أحيانا إلى القيام بإجراء من إجراءات التحقيق دون حضور المتهم أو أحد أطراف الدعوى، في حالة ما إذا دعت الضرورة إلى ذلك، كالخشية على زوال آثار الجريمة أو ضياع شهادة لشاهد مهم في القضية يكون على وشك مفارقة الحياة مثلا، وذلك ما نصت عليه المادة 101 من قانون الإجراءات الجزائية الجزائري[1] 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 وشك الاختفاء.

ويجب أن تذكر في المحضر دواعي الاستعجال".

غير أن اتخاذ بعض إجراءات التحقيق في غير مواجهة الخصوم لا يحول دون حق الخصوم في الاطلاع على كافة الإجراءات المدونة بمحضر التحقيق والتي اتخذت في غيابهم، كما أن المقصود باتخاذ إجراء من إجراءات التحقيق في غير مواجهة الخصوم مجرد جواز القيام بالتحقيق في غيبتهم، فإذا حضر أحدهم بشكل تلقائي فلا يجوز منعه من الحضور[2].

الفرع الثاني: تدوين التحقيق

ويقصد بالتدوين قيام الجهة المكلفة بالتحقيق الابتدائي بإثبات كل الإجراءات المتخذة خلال التحقيق، وذلك بكتابتها في محاضر وفق الشكل الذي حدده القانون.

[1] الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 المتضمن قانون الإجراءات الجزائية الصادر بالجريدة الرسمية رقم 48 بتاريخ 20 صفر عام 1386 الموافق 10 يونيو 1966.

[2] سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، الطبعة الثانية، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 1999، ص520.

للتدوين أهمية بالغة من خلاله مساهمته في الحفاظ على كل تلك الإجراءات التي قام بها قاض التحقيق مع كافة الأطراف سواء كانوا متهمين أو ضحايا أو شهود، فالتدوين حجة لكل الأطراف، لهم وعليهم.

وتتجلى أهمية التدوين كذلك في كونه يعد بمثابة ضمان لحقوق المتهم، ذلك أن القيام بكتابة كل ما صرح به المتهم من أقوال أثناء التحقيق وتثبيتها كتابيا في محاضر دون زيادة أو نقصان يكرس نزاهة التحقيق.

فالمحاضر المكتوبة تمكن لاحقا قاض الموضوع من تقدير قيمة وصحة الأدلة المستمدة من محاضر التحقيق الابتدائي والتي بإمكانه الاستناد والاعتماد عليها في تكوين حكمه.

وعلاوة على شرط الكتابة، نجد أن مختلف التشريعات أوجبت أن يتم التدوين بواسطة كاتب مختص وذلك تحت طائلة البطلان. والعلة من ذلك هي تمكين قاض التحقيق من التفرغ للقيام بعمله الفني المتمثل في التفكير واستعمال قدراته الذهنية في إيجاد الأسئلة التي تفيد التحقيق فيطرحها ويركز على ما يقدمه المتهم أو الشهود وأطراف الدعوى من إجابات، لذلك كان من غير اللائق إثقال كاهل قاض التحقيق من خلال إلزامه بكتابة وتدوين التحقيق.

يضاف إلى ذلك، أن وجود كاتب مختص من أجل كتابة المحاضر يبعد الشبهة عن قاض التحقيق فيما لو قام هذا الأخير بتدوين المحاضر شخصيا دون الاستعانة بكاتب، فوجود كاتب مختص يضفي صفة الصحة على الإجراء وإلا نتج عن ذلك بطلان المحاضر أو اعتبارها محاضر استدلال فقط وليست محاضر تحقيق.

المبحث الثاني: السلطة المختصة بالتحقيق الابتدائي في الجريمة الإلكترونية

اختلفت التشريعات المقارنة حول الجهة المختصة بالتحقيق الابتدائي، ومرد هذا الاختلاف يعود إلى أخذ التشريعات في بعض الدول بمبدأ الجمع بين سلطتي الاتهام والتحقيق، في حين فضلت دول أخرى تبني مبدأ الفصل بين سلطتي الاتهام والتحقيق.

الفرع الأول: الوضع في الجزائر

المشرع الجزائري وعلى غرار العديد من نظرائه في التشريع المقارن، لا سيما المشرع الفرنسي، فقد أخذ بمبدأ الفصل بين سلطة الاتهام وسلطة التحقيق، فترك الاتهام للنيابة العامة في حين أسند مهمة التحقيق الابتدائي لقاض التحقيق.

إن التحقيق الابتدائي كمرحلة من مراحل الدعوى الجنائية أو الدعوى العمومية، فهي تأتي بعد مرحلة جمع الاستدلالات التي يقوم بها رجال الضبطية القضائية وتسمى عادة بمرحلة التحقيق الأولي أو التمهيدي، كما أن مرحلة التحقيق الابتدائي تكون سابقة لمرحلة ثالثة هي مرحلة التحقيق النهائي الذي يتم أثناء المحاكمة من طرف قضاة الحكم.

ولابد من الإشارة في هذا المقام إلى أن المشرع الجزائري كان قد استعمل – عن طريق الخطأ–تسمية التحقيق الابتدائي لدى حديثه عن التحقيق الأولي أو مرحلة جمع الاستدلالات والتي تقوم بها الضبطية القضائية، وذلك في الفصل الثاني من الباب الثاني من قانون الإجراءات الجزائية. وعلى سبيل المثال نذكر ما جاء بالمادة 63 من قانون الإجراءات الجزائية[1] التي نصت على أنه " يقوم ضباط الشرطة القضائية، وتحت رقابتهم أعوان الشرطة القضائية، بالتحقيقات الابتدائية ..." غير أنه استعمل وبنفس المادة باللغة الفرنسية عبارة "...des enquêtes préliminaires..." والتي يقابلها في اللغة العربية عبارة "التحريات الأولية". وكما يبدو جليا فإن المشرع الجزائري خانه سوء الترجمة من اللغة الفرنسية إلى اللغة العربية.

وحتى لا نسهب ونسترسل في الحديث عن أخطاء الترجمة التي يحتوي عليها قانون الإجراءات الجزائية، نكتفي بالتأكيد فقط على أن التحقيق الابتدائي هو من اختصاص قاض التحقيق وهذا ما عبرت عنه المادة 66 من الباب الثالث للفصل الأول من قانون

[1] القانون رقم 06–22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر لسنة 2006 والصادر بالجريدة الرسمية العدد 84 المؤرخة في 24 ديسمبر 2006 يعدل ويتمم الأمر رقم 66–155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

نصت المادة 199 من قانون الإجراءات الجنائية[1] المصري على أنه " فيما عدا الجرائم التي يختص قاضي التحقيق بتحقيقها وفقا لأحكام المادة 64 تباشر النيابة العامة التحقيق في مواد الجنح والجنايات طبقا للأحكام المقررة لقاضي التحقيق".

فقاض التحقيق بمصر قد يسند له القيام بإجراء من إجراءات التحقيق لكن ليس بوصفه سلطة صاحبة اختصاص أصيل وإنما يقوم بذلك كمنتدب في إطار الندب القضائي.

الفرع الرابع: الوضع في الأردن

أخذ المشرع في المملكة الأردنية الهاشمية بمبدأ الجمع بين سلطتي الاتهام والتحقيق، فجعل سلطة أو وظيفة التحقيق الابتدائي بيد النيابة العامة، وهذا ما نص عليه قانون أصول المحاكمات الجزائية الأردني[2] في الفصل الرابع المتضمن وظائف المدعي العام لا سيما بالمادة 42 التي نصت على أنه " يتولى المدعي العام التحقيق...".

المطلب الثاني: ضرورة استحداث جهات مختصة بالتحقيق الابتدائي في الجريمة الإلكترونية

إن الجريمة الإلكترونية وبما تتميز به من خصائص مختلفة عن تلك الخاصة بالجريمة بمفهومها التقليدي، أجبرت التشريعات الجنائية بشقيها الموضوعي والإجرائي على ضرورة استحداث نصوص جديدة من أجل مسايرة ومواجهة هذا النمط الجديد من الجرائم. غير أن الواقع أثبت بأن مجرد الاكتفاء بتعديل النصوص القانونية القائمة بهدف منح صلاحيات أوسع للسلطة الأصيلة بالتحقيق الابتدائي لتشمل الجرائم الإلكترونية، ليس كافيا ولا يمنح الدعم اللازم لسلطات التحقيق من أجل ملاحقة الجناة داخل العالم

[1] قانون الإجراءات الجنائية رقم 150 لسنة 1950 الصادر بتاريخ 20 ذي القعدة 1369 هجرية الموافق 03 سبتمبر 1950 الصادر بالجريدة الرسمية العدد 90 (عدد غير اعتيادي) الصادرة يوم الاثنين 14 محرم 1371 هجرية الموافق 15 أكتوبر 1951. المعدل بموجب القانون رقم 107 لسنة 1962 الصادر بتاريخ 7 محرم 1382 هجرية الموافق 11 يونيو 1962 الصادر بالجريدة الرسمية العدد 136 بتاريخ 17 يونيو 1962.

[2] القانون رقم 1961/09 الصادر بتاريخ 1961/01/01 والمنشور بالصفحة 311 للجريدة الرسمية العدد 1539 والمتضمن قانون أصول المحاكمات الجزائية. راجع موقع ديوان التشريع والرأي للمملكة الأردنية الهاشمية من خلال الرابط (متاح بتاريخ 2018/08/18):

http://www.lob.jo/?v=1.11&url=ar/LegislationDetails?LegislationID:1729,LegislationType:2

الفرع الأول: الوضع في الولايات المتحدة الأمريكية

أشرنا سابقا إلى أن النظام الأنجلو- أمريكي أسند مهمة التحقيق لجهاز الشرطة، لذلك ومن أجل أكثر فعالية فيما يخص التحقيق في الجريمة الإلكترونية لجأ المشرع الأمريكي إلى استحداث جهة مختصة بالتحقيق تابعة لجهاز الشرطة بحد ذاته، وذلك من خلال إنشاء قسم جرائم الحاسوب. غير أنه وبعد وصول الرئيس باراك أوباما إلى سدة الحكم في الولايات المتحدة الأمريكية وبعد سلسلة الهجمات الإلكترونية التي أتهم من خلالها الروس باختراق وقرصنة البريد الإلكتروني للعديد من الشخصيات المهمة بالولايات المتحدة الأمريكية، قرر[1] الرئيس باراك أوباما بتاريخ 2016/08/26 إسناد مهمة التحقيقات المرتبطة بالجريمة الإلكترونية إلى مكتب التحقيقات الفيديرالي.

الفرع الثاني: الوضع في فرنسا

بالإضافة لقاض التحقيق باعتباره جهة أصيلة للتحقيق الابتدائي في كل الجرائم بما فيها الجريمة الإلكترونية، أنشأ المشرع الفرنسي اللجنة الوطنية للمعلوماتية والحريات Commission nationale de l'informatique et des libertés والمعبر عنها اختصارا ب (CNIL)، ومنحها صلاحيات التحقيق بموجب القانون[2] الصادر سنة 1978 تحت رقم 78-17. لاسيما بموجب المادتين 11 و 39 من نفس القانون.

[1] راجع القرار تحت رقم 41 ضمن أرشيف قرارات الرئيس باراك أوباما بالبيت الأبيض بالرابط التالي (متاح بتاريخ 2018/08/25):

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

[2] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés JORF du 7 janvier 1978. Modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.Journal officiel, JORF n°0141 du 21 juin 2018. peut être consulté depuis le lien internet suivant (disponible le 29/09/2019):

https://www.legifrance.gouv.fr/download/secure/file/3N2RZHPpYGgeuyQfEBPX

Article 11. "La commission peut demander aux premiers présidents de la cour d'appel ou aux présidents de tribunaux administratifs de déléguer un magistrat de leur ressort, éventuellement assisté d'experts, pour des missions d'investigation et de contrôle effectuées sous sa direction".

Article 39. "En ce qui concerne les traitements intéressants la sûreté de l'Etat, la défense et la sécurité publique, la demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des compte pour mener toutes investigations

وبرمجيات تساعد في إجراءات التحقيق، وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الأدلة[1].

الفرع الرابع: الوضع في مصر

المشرع المصري لم ينشأ جهازا خاصا بالتحقيق الابتدائي في الجريمة الإلكترونية، لذلك ومن خلال استقراء النصوص التي تضمنها قانون الإجراءات الجنائية المصري لا سيما ما جاء بنص المادة 199 من قانون الإجراءات الجنائية المصري[2]، يمكننا القول بسريان القواعد العامة بخصوص تحديد الجهة المناط بها التحقيق الابتدائي في الجريمة الإلكترونية والمتمثلة في النيابة العامة. كما أنه لم يقم باستحداث جهات لمساعدة السلطة الأصيلة بالتحقيق الابتدائي في الجريمة الإلكترونية.

غير أنه ـ وضمنياـ ومن خلال محتوى المادة 1584 من التعليمات القضائية للنيابة العامة[3] والتي نصت على أنه " يجوز إنشاء نيابات تختص بالتحقيق والتصرف في أنواع معينة من الجرائم، ويصدر بإنشاء هذه النيابات قرار من وزير العدل أو النائب العام"، يمكن أن يفهم بأن المشرع المصري ترك الباب مفتوحا لإمكانية إنشاء نيابات مستقبلا تكون مختصة بالتحقيق في الجرائم الإلكترونية[4]. إذن ومجاراة للتشريعات المقارنة تبدو الحاجة ملحة إلى ضرورة إسراع المشرع المصري في إنشاء نيابة مختصة بالتحقيق الابتدائي في الجريمة الإلكترونية.

---

[1] وضاح محمود الحمود ونشأت مفضي المجالي، جرائم الإنترنت، دار المنار للنشر والتوزيع، عمان، 2005، ص120.

[2] قانون الإجراءات الجنائية رقم 150 لسنة 1950، المرجع السابق.

[3] التعليمات القضائية للنيابة العامة (وزارة العدل/ النيابة العامة)، الكتاب الأول (التعليمات القضائية)، القسم الأول (في المسائل الجنائية)، الباب السابع عشر(النيابات المتخصصة)،الطبعة السادسة، 2007، ص 520. يمكن الاطلاع على المحتوى الكامل للتعليمات القضائية للنيابة العامة المصرية على الرابط (متاح بتاريخ 219/02/20):
https://www.academia.edu/38963540/التعليمات_القضائية_كاملة_فهرس_كامل

[4] أنظر في هذا المعنى: أشرف توفيق شمس الدين، شرح قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، الطبعة الأولى، 2009، ص 396.

المبحث الثالث: الاختصاص القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية

يقصد بالاختصاص القضائي تلك السلطة التي منحها القانون لقاض معين أو جهة قضائية معينة، وبمقتضاها تخول لهذا القاضي أو الجهة القضائية حق الفصل في القضايا وفق تلك الحدود التي رسمها القانون.

فالسلطات التحقيقية التي تباشر مهمة التحقيق الابتدائي تعد من السلطات القضائية، لأنها تقوم بدور مزدوج، فهي (كقاض محقق) تجمع الأدلة المتعلقة بالجريمة الواقعة وتتثبت منها، كما وأنها (كقاض لها سلطة التقرير) تتخذ القرارات اللازمة للبت في الطلبات والدفوع المقدمة إليها. وبالإضافة إلى ذلك فإن الإجراءات التي تتخذها هذه السلطات في إجراءات ذات طبيعة قضائية، لأنها تتصف بالحيدة، وتتخذ في ظل التقويم القانوني للأدلة.[1]

من بين المشاكل والتعقيدات الكثيرة التي أفرزتها الطبيعة الخاصة للجريمة الإلكترونية، مشكلة تحديد الاختصاص القضائي. ذلك أن الجريمة الإلكترونية باعتبارها جريمة عابرة للقارات فقد ألغت مفهوم الحدود، وهو الأمر الذي أربك السلطات القضائية خاصة في المسائل الإجرائية وما تعلق منها بتحديد الجهة التي يؤول لها الاختصاص القضائي من أجل التحقيق الابتدائي في الجريمة الإلكترونية.

إن مسألة تحديد نطاق اختصاص قاض التحقيق داخل إقليم الدولة فيما يخص الجريمة الإلكترونية هو أمر تم حسمه والتغلب عليه، غير أن المشكل الحقيقي يكمن في البث في المدى الذي يبلغه الاختصاص المكاني لجهات التحقيق في تلك الجرائم الإلكترونية التي تتعدى حدود إقليم الدولة. وعليه سنتناول مسألة الاختصاص المحلي لقاض التحقيق على المستوى الوطني، ثم نتعرض لقضية الاختصاص المكاني على المستوى الدولي.

لكن وقبل التفصيل في ذلك، هناك ما يستوجب ـ بحسب تقديرينا ـ الوقوف عنده وتوضيحه، فالحديث عن الاختصاص القضائي قد يترك انطباعا بأن هذا الأمر له علاقة

[1] حسن الجوخدار، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008، ص13 و14. أشار إليه رشاد خالد عمر، مرجع سابق، ص96.

أكثر بالجوانب الموضوعية وليس الإجرائية، إلا أننا توصلنا إلى أن هناك تداخل بين القواعد الموضوعية والإجرائية عند الحديث الاختصاص القضائي لجهات التحقيق الابتدائي. لذلك سوف نأخذ فقط ما يخدم بحثنا من الناحية الإجرائية.

المطلب الأول: الاختصاص القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية على المستوى الوطني (في التشريع الجزائري)

لقد أرسى المشرع الجزائري قواعد تنظم سلطة قاض التحقيق بصفته قائما بالتحقيق الابتدائي، هذه القواعد حددت نطاق اختصاص قاض التحقيق بإجراء أي تحقيق من خلال ثلاثة معايير متمثلة في الاختصاص الشخصي، الاختصاص النوعي، والاختصاص المحلي والذي يعبر عنه عادة بالاختصاص الإقليمي.

وأن كنا سنركز في هذا الجزء من البحث على الاختصاص المحلي فقط دون الاختصاصين الشخصي والنوعي، فإن ذلك يجد مبررا له في كون هذين الاختصاصين الأخيرين لا يطرحان إشكالا بعكس الاختصاص المحلي الذي يفضي في كثير من الحالات إلى قضايا تنازع، ويصبح الأمر أكثر تعقيدا في الجريمة الإلكترونية نظرا لطبيعتها الخاصة التي تمتاز بالسرعة وبتعدد آثارها داخل وخارج الدولة بحيث تكتسي في كثير من الحالات طابعا دوليا.

فالاختصاص النوعي يحدد نوع تلك الجرائم التي يمكن لقاض التحقيق إجراء تحقيق بشأنها متى طلب منه ذلك من طرف وكيل الجمهورية أو من خلال شكوى مصحوبة بادعاء مدني، ويحدد نوع الجريمة بمعيار الجسامة فقد تكون جناية أو جنحة أو مخالفة.

في موضوع التحقيق الإبتدائي دائما، فإنه يمكن وطبقا للمادة 66 من قانون الإجراءات الجزائية الجزائري[1] أن يجري قاض التحقيق تحقيقا في كل من الجنايات (وجوبي) والجنح (اختياري إلا في حالة وجود نص ينص صراحة على ذلك) والمخالفات (جوازي في حال كان بطلب من وكيل الجمهورية)، في حين إذا كان بناء على شكوى المدعي المدني طبقا

[1] الأمر رقم 66-155، المرجع السابق.

للمادة 72 من قانون الإجراءات الجزائية[1] الجزائري فالتحقيق في هذه الحالة يشمل فقط نوعين من الجرائم هما الجنايات والجنح دون المخالفات.

أما بالنسبة للاختصاص الشخصي فإنه وبكل بساطة يحظر على قاض التحقيق أن يحقق مع أشخاص معينين في حالة إحالتهم على التحقيق. فإذا كانت القاعدة العامة تقضي بأن يكون قاض التحقيق مختصا بالتحقيق مع أي شخص طلبت النيابة فتح تحقيق بشأنه أو ورد اسمه في شكوى المدعي المدني، إلا أن القانون استثنى وبموجب المادة 573 من القانون[2] 90-24 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري بعض الأشخاص وهم أعضاء الحكومة، قضاة المحكمة العليا، الولاة، رؤساء المجالس القضائية والنواب العامون للمجالس القضائية، فهؤلاء يتم تحديد جهة أخرى تحقق معهم وذلك خروجا عن القاعدة العامة بالنظر للوظائف التي يشغلونها.

هذا بخصوص الاختصاصين النوعي والشخصي واللذان ـ كما أشرنا سابقا ـ لا يثيرا إشكالا، كما أنهما لا يبرزان علاقة مباشرة بموضوع الدراسة والمتمثل في التحقيق الابتدائي في الجريمة الإلكترونية.

نصل الآن إلى الاختصاص المحلي لقاضي التحقيق والذي سنتناوله بنوع من التفصيل مقارنة بالمعيارين السابقين.

الفرع الوحيد: الاختصاص المحلي لقاضي التحقيق

نصت المادة 40 من القانون[3] 04-14 المعدل والمتمم لقانون الإجراءات الجزائية الجزائري على ما يلي "يتحدد اختصاص قاضي التحقيق محليا بمكان وقوع الجريمة أو

[1] القانون رقم 06-22، المرجع السابق.

[2] القانون 90-24 المؤرخ في 27 محرم عام 1411 الموافق 18 غشت 1990 الصادر بالجريدة الرسمية رقم 36 بتاريخ أول صفر عام 1411 الموافق 22 غشت سنة 1990 المعدل والمتمم لقانون الإجراءات الجزائية.

[3] القانون 04-14 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر 2004 الصادر بالجريدة الرسمية رقم 71 المعدل والمتمم لقانون الإجراءات الجزائية.

محل إقامة أحد الأشخاص المشتبه في مساهمتهم في اقترافها أو بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا القبض قد حصل لسبب آخر.

يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، 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".

والمقصود بكلمة "التنظيم" التي ورد ذكرها في الفقرة الثانية من المادة أعلاه ورد بموجب المرسوم التنفيذي[1] رقم 06-348 لسنة 2006 والذي أنشأ ما يعرف بالأقطاب أو ما يسميه البعض بالجهات القضائية ذات الاختصاص الموسع والذي من خلاله تم تمديد الاختصاص المحلي لمحاكم: سيدي امحمد بالجزائر العاصمة، قسنطينة، ورقلة ووهران. وكذا تمديد الاختصاص المحلي لوكلاء الجمهورية وقضاة التحقيق بهذه المحاكم إلى محاكم مجالس قضائية أخرى كالآتي:

1- محكمة سيدي محمد بالجزائر العاصمة تشمل جميع محاكم المجالس القضائية التالي : الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدنية، المسيلة، بومرداس، تيبازة، عين الدفلى.

2- محكمة قسنطينة يمتد اختصاصها المحلي ولوكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس التالية : قسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق أهراس، ميلة.

3-محكمة ورقلة يمتد اختصاصها المحلي كذلك وكذا كل من وكيل الجمهورية وقاضي التحقيق بها إلى محاكم المجالس التالية:

[1] المرسوم التنفيذي رقم 06-348 المؤرخ في 12 رمضان 1427 الموافق 05 أكتوبر سنة 2006 الصادر بالجريدة الرسمية رقم 63 بتاريخ 15 رمضان عام 1427 الموافق 08 أكتوبر سنة 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

أولا: معيار مكان وقوع الجريمة

يعتبر مكان وقوع الجريمة من أهم المعايير وذلك باعتباره مكان مسرح الجريمة، حيث يسهل جمع الأدلة بالنسبة لجهة التحقيق. غير أنه وبالنظر لطبيعة الجريمة الإلكترونية فإنه من الصعب تحديد مكان وقوعها.

بالنسبة للمشرع الجزائري فإنه وطبقا للمادة 40 من قانون الإجراءات الجزائية والمرسومين السابقين، تم تمديد الاختصاص المحلي لقاض التحقيق لكل من محكمة سيدي امحمد بالعاصمة، قسنطينة، ورقلة ووهران. ففي حالة وقوع جريمة من الجرائم الإلكترونية بدائرة اختصاص هذه المحاكم أو دائرة المحاكم الأخرى فإن الاختصاص بالتحقيق يؤول دائما لقاض التحقيق بالمحاكم السابقة ذات الاختصاص الموسع (محكمة سيدي امحمد بالعاصمة، قسنطينة، ورقلة ووهران).

هذا ولقد أخذت العديد من تشريعات دول العالم بمعيار مكان وقوع الجريمة، من بينها المشرع الفرنسي وذلك بموجب المادة 52[1] من قانون الإجراءات الجزائية الفرنسي، وكذا المشرع الأمريكي بنص المادة 3232 من قانون الجرائم والإجراءات الجنائية الأمريكي[2]. أما بالنسبة للمشرع المصري فجاء بالمادة 217 من قانون الإجراءات الجنائية[3] أنه "يتعين الاختصاص بالمكان الذي وقعت فيه الجريمة..."

[1] L'article 52 " Sont compétents le juge d'instruction du lieu de l'infraction …"
Codifié par la loi n° 57-1426 du 31 décembre 1957 instituant un code de procédure pénale JORF du 8 janvier 1958. Modifié par la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale JORF n°0129 du 4 juin 2016. peut être consulté depuis le lien internet suivant (disponible le 29/09/2019) :
https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032654809

[2] "Proceedings to be in district and division in which offense committed"
18 USC 3232: District of offense-(Rule) Text contains those laws in effect on June 18, 2018
From Title 18-CRIMES AND CRIMINAL PROCEDURE PART II-CRIMINAL PROCEDURECHAPTER 211-JURISDICTION AND VENUE (June 25, 1948, ch. 645, 62 Stat. 826).
The link below allows you to download the file from the Internet (Available 18/06/2018)
https://uscode.house.gov/download/releasepoints/us/pl/116/344/pdf_usc18@116-344.zip

[3] قانون الإجراءات الجنائية رقم 150 لسنة 1950، المرجع السابق.

ثانيا: معيار مكان إقامة المتهم

طبقا لهذا المعيار فإن الاختصاص بالتحقيق ينعقد لقاض التحقيق الذي يقيم بدائرة اختصاصه المتهم، أي المحكمة التي يتواجد بدائرة اختصاصها مكان إقامة المتهم.

بالنسبة للمشرع الجزائري فإن مكان إقامة المتهم بالجريمة الإلكترونية هو من يحدد أي قاض للتحقيق يكون مختصا محليا بالتحقيق في الجريمة الإلكترونية، وبحسب ما قيل في المعيار السابق فإن الاختصاص لن يخرج عن أحد قضاة التحقيق بالمحاكم ذات الاختصاص الموسع المشار إليهم آنفا (محكمة سيدي امحمد بالعاصمة، قسنطينة، ورقلة ووهران).

ولقد أخذ بهذا المعيار المشرع في العديد من الدول كما هو حال كل من المشرع الفرنسي[1] وكذلك المشرع المصري طبقا لما ورد بمحتوى نص المادة 217 من قانون الإجراءات الجنائية[2] "يتعين الاختصاص بالمكان ..... أو الذي يقيم فيه المتهم ...." على سبيل المثال.

تبرز أهمية هذا المعيار في حالة ما إذا لم يكن بالإمكان تحديد مكان وقوع الجريمة وهو أمر وارد جدا بخصوص الجريمة الإلكترونية. ففي حالة تعدد المتهمون وكانوا يقيمون بأماكن مختلفة، فإنه وإعمالا بمبدأ وحدة الدعوى الجزائية فإن الاختصاص بالتحقيق في هذه الحالة يؤول وبالنسبة لسائر المتهمين إلى قاض التحقيق الذي يقيم بدائرة اختصاصه المحلي أحد المتهمين.

ثالثا: معيار مكان القبض المتهم

بالرجوع إلى نص المادة 40 من قانون الإجراءات الجزائية[3] "يتحدد اختصاص قاضي التحقيق محليا ..... بمحل القبض على أحد هؤلاء الأشخاص حتى ولو كان هذا

[1] L'article 52 " Sont compétents le juge d'instruction ……. celui de la résidence de l'une des personnes soupçonnées d'avoir participé à l'infraction …". Op.cit.

[2] قانون الإجراءات الجنائية رقم 150 لسنة 1950، المرجع السابق.

[3] القانون 04-14، المرجع السابق.

القبض قد حصل لسبب آخر...." كما نصت الفقرة الثانية من نفس المادة أعلاه "....يجوز تمديد الاختصاص المحلي لقاضي التحقيق إلى دائرة اختصاص محاكم أخرى، 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".

وعليه، فبمقتضى هذا المعيار فإن الاختصاص بالتحقيق يؤول لجهة التحقيق الذي يتم إلقاء القبض على المتهم بدائرة اختصاصه. فإذا لم يتم تحديد مكان وقوع الجريمة الإلكترونية، ولم يكن للمتهم محل إقامة معروف فإن معيار مكان القبض على المتهم يفيدنا في تحديد الجهة المختصة بالتحقيق. فمكان إلقاء القبض على المتهم بالجريمة الإلكترونية هو من يحدد أي قاض للتحقيق يكون مختصا محليا بالتحقيق في الجريمة الإلكترونية، وبحسب ما قيل في المعيارين السابقين فإن الاختصاص لن يخرج عن أحد قضاة التحقيق بالمحاكم ذات الاختصاص الموسع المشار إليهم آنفا (محكمة سيدي امحمد بالعاصمة، قسنطينة، ورقلة ووهران).

أما في حالة تعدد المتهمين، فإن قاض التحقيق الذي ألقي القبض على أحد المتهمين بدائرة اختصاصه يعتبر مختصا بالتحقيق مع سائر المتهمين الآخرين.

المشرع المصري أخذ هو الآخر بهذا المعيار بنص المادة 217 من قانون الإجراءات الجنائية[1] أنه "يتعين الاختصاص بالمكان ..... أو الذي يقبض عليه فيه...."

إن تعدد معايير تحديد الاختصاص المحلي لقاض التحقيق قد يضع جهات التحقيق أمام مشكلة وذلك في حالة ما إذا وقعت الجريمة الإلكترونية بدائرة اختصاص قاض تحقيق أول، وكان محل إقامة المتهم يقع بدائرة اختصاص قاض تحقيق ثان، وألقي القبض على المتهم بدائرة اختصاص قاض ثالث. فهذا الأمر قد يجعلنا أما تنازع إيجابي أو سلبي أي أن كل قاض تحقيق قام بدائرة اختصاصه معيار من المعايير الثلاثة فله إما أن يتمسك بأحقيته بالتحقيق أو أن يصدر أمرا بالتخلي.

[1] قانون الإجراءات الجنائية رقم 150 لسنة 1950، المرجع السابق.

الأصل أنه لا توجد أفضلية لقاضي تحقيق على قاض تحقيق آخر، ففي هذه الحالة يعتبر مختصا بالتحقيق ذاك القاضي الذي رفعت الدعوى بدائرة اختصاصه قبل الآخرين فهذا أمر يحدد لنا أي جهة تحقيق لها الأسبقية.

المطلب الثاني: الاختصاص القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية على المستوى الدولي

يعتمد قانون العقوبات أو ما يسمى بالقانون الجنائي بشقه الموضوعي، عند تطبيقه على قانون الإجراءات الجزائية أو ما يسمى بالقانون الجنائي في شقه الإجرائي. فقانون الإجراءات الجزائية هو من بيث الحركة في النصوص الموضوعية لقانون العقوبات والتي تكون في حالة ركود وسكون.

إن مواجهة الجريمة الإلكترونية يتم من خلال تطبيق النصوص التي جرمت تلك الأفعال التي تنتمي لفئة ما يسمى بالجرائم الإلكترونية وحددت عقوبات لها. هذه الجرائم قد ترتكب داخل إقليم الدولة أو خارجه، وهذا ما يجعلنا أمام ما يسمى بسريان القانون الجنائي من حيث المكان والذي يواجه على المستوى الدولي إشكالية تحديد الجهة المختصة قضائيا بالتحقيق على المستوى الدولي.

بما أن الجريمة الإلكترونية هي جريمة لا تعترف بالحدود الجغرافية، فإن السلوك الإجرامي قد يرتكب في دولة ما في حين أن النتيجة تتحقق في دولة أخرى وبالتالي قد تتضمن ما يسمى بالعنصر الأجنبي والذي يعد سببا في إثارة وبروز التنازع في الاختصاص.

سنحاول من خلال هذا المطلب الحديث عن تلك الحالات التي ينعقد فيها الاختصاص وتكون فيها سلطة التحقيق للقضاء الوطني في كل دولة دون القضاء الأجنبي وذلك من أجل التحقيق في تلك الجرائم الإلكترونية وذلك من خلال تلك المبادئ التي اعتمدت عليها التشريعات الجنائية المقارنة ونقصد بهذه المبادئ مبدأ الإقليمية، ومبدأ الشخصية، ومبدأ العينية وكذا مبدأ العالمية، حيث يعتبر مبدأ الإقليمية كمبدأ أصلي في حين تعد بقية المبادئ الثلاثة الأخرى بمثابة استثناءات ترد على مبدأ الإقليمية.

الفرع الأول: الاختصاص القضائي بالتحقيق وفقا لمبدأ الإقليمية

يقصد بمبدأ الإقليمية تطبيق القانون الجنائي للدولة على كافة الجرائم التي ترتكب داخل إقليمها وذلك بغض النظر عن جنسية مرتكب الجريمة سواء كان مواطنا يحمل جنسية هذه الدولة أم أجنبيا.

بخصوص الوضع في الجزائر فقد نص المشرع الجزائري في المادة الثالثة من قانون العقوبات[1] على أنه "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية" . إذن فوفقا لمبدأ الإقليمية فإن الاختصاص القضائي بالتحقيق في الجريمة الإلكترونية يكون من اختصاص القضاء الجزائري متى ارتكبت الجريمة فوق الإقليم الجزائري ومهما كانت جنسية مرتكب الجريمة.

معلوم بأن الركن المادي للجريمة يتكون من سلوك إجرامي متمثل في ذلك الفعل الذي يقوم به الجاني، وكذا من النتيجة التي تتحقق بعد ذلك، وتربط بينهما العلاقة السببية. فإذا تمت كل عناصر الركن المادي للجريمة الإلكترونية فوق نفس الإقليم فهنا لا يثار إشكال بخصوص تحديد مكان الجريمة، وبالتالي فلا يثار أيضا مشكل في تحديد قضاء الدولة المختص بالتحقيق في الجريمة الإلكترونية.

غير أن الإشكال يثار في تلك الحالة التي يقع فيها السلوك الإجرامي في دولة معينة، في حين تتحقق النتيجة في إقليم دولة أخرى، فأي الدولتين تختص قضائيا بالتحقيق في الجريمة الإلكترونية؟ نجد بأن مختلف التشريعات الجنائية المقارنة لاسيما الإجرائية منها قد وضعت حلا لهذا الاحتمال رغم اختلافها من حيث الأخذ بعين الاعتبار إما المكان الذي وقع به السلوك الإجرامي، أو المكان الذي تحققت فيه النتيجة، أو الأخذ بهما معا، فلا يهم إن كان إقليم الدولة قد ارتكب فيه السلوك الإجرامي فقط أو تحققت فيه النتيجة فقط، لأنه في كلتا الحالتين ينعقد الاختصاص للجهة القضائية لهذه الدولة.

[1] الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يوينو سنة 1966 الصادر بالجريدة الرسمية رقم 49 بتاريخ 21 صفر عام 1386 الموافق 11 يونيو سنة 1966 المتضمن قانون العقوبات.

لدى المشرع العراقي نجد المادة السادسة من قانون العقوبات العراقي[1] التي نصت على أنه: " تسري أحكام هذا القانون على جميع الجرائم التي ترتكب في العراق وتعتبر الجريمة مرتكبة في العراق إذا وقع فيه فعل من الأفعال المكونة لها أو إذا تحققت فيه نتيجتها أو كان يراد أن تتحقق فيه ..."

أما المشرع الجزائري وبموجب المادة 586 من قانون الإجراءات الجزائية[2] نص على أنه " تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر" وهو تقريبا نفس محتوى المادة 113-2 من قانون العقوبات الفرنسي[3] والتي جاءت في الصيغة التالية " يطبق القانون الفرنسي على الجرائم المرتكبة فوق إقليم الجمهورية.

وتعتبر الجريمة قد ارتكبت فوق إقليم الجمهورية إذا كان أحد عناصر المكون لها قد وقعت فوق هذا الإقليم ".

علاوة على ذلك، فالمشرع الفرنسي وفي سعيه إلى تحديث وتقوية تشريعاته لمواجهة الجريمة الإلكترونية، سن تشريعا جديد متمثلا في القانون المتعلق بتعزيز مكافحة الجريمة المنظمة والإرهاب وتمويله[4]، وتحسين فعالية وضمانات الإجراءات الجنائية، هذا الأخير جاء بمادة جديدة ألحقها بقانون العقوبات الفرنسي[5] تحت الرقم 113-2-1 ونصت على أنه "يطبق القانون الفرنسي على الجرائم المرتكبة على إقليم الجمهورية وتعتبر الجريمة قد ارتكبت على إقليم الجمهورية إذا كان أحد عناصر الجريمة قد وقعت على هذا الإقليم"[6].

---

[1] قانون العقوبات العراقي رقم 111 لسنة 1969 الصادر بتاريخ 1969/12/15 بجريدة الوقائع العراقية (الجريدة الرسمية لجمهورية العراق) العدد 1778 يمكن الاطلاع عليه من خلال موقع (قاعدة التشريعات العراقية) عبر الرابط (متاح بتاريخ 2019/11/23): http://iraqld.hjc.iq/LoadLawBook.aspx?SC=120120012516407

أو من خلال صفحة جريدة الوقائع العراقية على موقع وزارة العدل لجمهورية العراق عبر الصفحة (متاح بتاريخ 2019/11/23): https://www.moj.gov.iq/iraqmag

[2] الأمر رقم 66-155، المرجع السابق.

[3] Article 113-2 " La loi pénale française est applicable aux infractions commises sur le territoire de la République.

L'infraction est réputée commise sur le territoire de la République dès lors qu'un de ses faits constitutifs a eu lieu sur ce territoire". La loi n°92-683 du 22 juillet 1992 portant réforme des dispositions générales du code pénal . JORF n°169 du 23 juillet 1992.

[4] La loi n° 2016-731, Op.cit.

[5] La loi n°92-683 du 22 juillet 1992 portant réforme des dispositions générales du code pénal . JORF n°169 du 23 juillet 1992.

[6] "Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne

أما بالنسبة للجرائم التي ترتكب على متن الطائرات فقد نصت المادة 591 من قانون الإجراءات الجزائية الجزائري[1] على أنه "تختص الجهات القضائية الجزائرية بالنظر في الجنايات والجنح التي ترتكب على متن الطائرات الجزائرية أيا كانت جنسية مرتكب الجريمة.

كما أنها تختص أيضا بنظر الجنايات أو الجنح التي ترتكب على متن الطائرات الأجنبية إذا كان الجاني أو المجني عليه جزائري الجنسية أو إذا هبطت الطائرة بالجزائر بعد وقوع الجناية أو الجنحة.

وتختص بنظرها المحاكم التي وقع بدائرتها هبوط الطائرة في حالة القبض على الجاني وقت هبوطها، أو مكان القبض على الجاني في حالة ما إذا كان مرتكب الجريمة قد قبض عليه بالجزائر فيما بعد".

من خلال المادتين السابقتين يتضح بأن المشرع الجزائري اعتبر السفن والطائرات امتداد للإقليم الجزائري إذا كانت جزائرية أي تحمل العلم الجزائري وذلك بغض النظر عن جنسية الجاني، وفي هذه الحالة فإن الاختصاص القضائي يتجاوز المياه الإقليمية إذا ارتكبت الجرائم على ظهر السفن الجزائرية ليمتد إلى المياه الدولية أو عرض البحر.

ويلاحظ كذلك من خلال المادة 591 أعلاه أن القضاء الجزائري يكون مختصا حتى ولو كانت الطائرة أجنبية والجاني والمجني عليه أجنبيين لكن بشرط أن تهبط الطائرة بالجزائر بعد وقوع الجريمة.

بخصوص التشريعات المقارنة، فلقد حثث الاتفاقية الأوربية للجريمة الإلكترونية بودابست[2] 2001 الدول الأطراف فيها على اتخاذ ما يلزمها من تدابير تشريعية تخص الاختصاص القضائي بشأن الجرائم التي ترتكب بإقليم دولة طرف بالاتفاقية، على متن السفن التي ترفع علم الدولة الطرف بالاتفاقية، على متن الطائرات المسجلة بموجب قوانين تلك الدولة

[1] المرجع نفسه.

[2] Convention de Budapest du 21 novembre 2001 sur la cybercriminalité
.تفاصيل أكثر بخصوص هذه الاتفاقية موجودة على الموقع الرسمي بالرابط التالي: (متاح وتمت زيارته بتاريخ 2017/12/09 الساعة 19:00) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

القضائي بالتحقيق خارج الإقليم البلجيكي حين تجد جهات التحقيق نفسها مضطرة إلى البحث عن الأدلة المتعلقة بالجريمة الإلكترونية بأنظمة معلوماتية متواجدة خارج إقليم بلجيكا. وهذا دون اشتراط الحصول على إذن من تلك الدولة التي يوجد بها النظام المعلوماتي محل البحث عن الأدلة الإلكترونية وذلك في حالة وجود ضرورة ملحة لذلك أو خشية من ضياع الأدلة.

كان هذا فيما يتعلق بمبدأ الإقليمية والذي قلنا بشأنه سابقا على أنه يعتبر الأصل الذي ترد عليه الاستثناءات المتمثلة في بقية المبادئ الأخرى ونقصد بها مبدأ الشخصية، مبدأ العينية ومبدأ العالمية.

الفرع الثاني: الاختصاص القضائي بالتحقيق وفقا لمبدأ الشخصية

بمقتضى مبدأ الشخصية يسري النص الجنائي للدولة ويطبق على كل مواطن يحمل جنسيتها سواء كان هو الجاني أو المجني عليه، حتى ولو ارتكبت الجريمة خارج إقليم الدولة.

ولمبدأ الشخصية وجهان، أحدهما إيجابي ويقصد به سريان النص الجنائي للدولة على تلك الجرائم التي يرتكبها كل مواطن يحمل جنسيتها وحتى لو ارتكبت بالخارج، وفي هذه الصورة يكون هذا المواطن هو الجاني.

" Lorsque le juge d'instruction ordonne une recherche dans un système informatique ou une partie de celui-ci,
cette recherche peut être étendue vers un système informatique ou une partie de celui-ci qui se trouve dans
un autre lieu que celui où la recherche est effectuée :
- si cette extension est nécessaire pour la manifestation de la vérité à l'égard de l'infraction qui fait l'objet de
la recherche, et
- si d'autres mesures seraient disproportionnées, ou s'il existe un risque que, sans cette extension, des éléments de preuve soient perdus…..".La loi du 28 novembre 2000 relative à la criminalité informatique, publication : 03-02-2001, n°: 2001009035, p 02909. Dossier N°: 2000-11-28/34,
Entrée en vigueur : 13-02-2001.

يمكن الاطلاع عليه من خلال الرابط (متاح بتاريخ 2020/08/15 على 09:15):

https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2000112834

أو تحميله على الرابط (متاح بنفس التاريخ):

https://www.ejustice.just.fgov.be/mopdf/2001/02/03_1.pdf#Page1

أما الوجه الثاني أو ما يسمى بالوجه بالسلبي لمبدأ الشخصية فيراد به سريان النص الجنائي للدولة على تلك الجرائم التي يكون فيها مواطن هذه الدولة هو المجني عليه، وحتى لو ارتكبت الجريمة بالخارج وكان الجاني أجنبيا.

في التشريعات المقارنة هناك دول أخذت بمبدأ الشخصية في وجهه الإيجابي فقط، في حين أن هناك دولا أخرى أخذت بمبدأ الشخصية بوجهيه الإيجابي والسلبي معا، ويعبر عن هذه الحالة (الأخذ بمبدأ الشخصية بالوجهين معا) بمبدأ الحماية لكون الدولة تهدف من خلال تبني كلا الصورتين أو الوجهين لمبدأ الشخصية إلى حماية حقوق مواطنيها سواء كانوا جناة أم مجني عليهم.

المشرع الجزائري أخذ بمبدأ الشخصية في صورته الإيجابية وكذا السلبية. ففي حالة الصورة الإيجابية فإن المشرع الجزائري يفرق بين حالتين، الأولى هي حالة ارتكاب المواطن جناية، أما الثانية هي تلك الحالة التي تكون فيها الجريمة المقترفة تحمل وصف جنحة ولكن بشروط حددتها كل من المادتين 582 و583 من قانون الإجراءات الجزائية الجزائري[1].

ففي حالة كانت الجريمة المرتكبة عبارة عن جناية، نصت المادة 582 من قانون الإجراءات الجزائية الجزائري على أنه:

"كل واقعة موصوفة بأنها جناية معاقب عليها من القانون الجزائري ارتكبها جزائري خارج إقليم الجمهورية يجوز أن يتابع ويحاكم عليها في الجزائر.

غير أنه لا يجوز أن تجري المحاكمة والمتابعة إلا إذا عاد الجاني إلى الجزائر ولم يثبت أنه حكم عليه في الخارج وأن يثبت في حالة الحكم بالإدانة أنه قضى العقوبة أو سقطت عنه بالتقادم أو حصل على العفو عنها".

يتضح من خلال مضمون المادة بأن المشرع قيد هذه الحالة بشروط هي:

– أن تأخذ الواقعة وصف الجناية بحسب قانون العقوبات الجزائري.

[1] الأمر رقم 66–155، المرجع السابق.

– أن ترتكب الجناية خارج الجزائر، لأنه في حالة ما إذا ارتكبت فوق الإقليم الجزائري تسري عليها قواعد الاختصاص المحلي.

– عودة الجاني إلى أرض الجزائر، وهذا يلغي إمكانية محاكمته غيابيا.

– ألا يكون الجاني قد حوكم في الخارج وقضى العقوبة بعد إدانته أو تم العفو عنه، أو أن العقوبة تقادمت. أما إذا ثبت بأنه حوكم في الخارج، أو أنه قضى العقوبة بعد إدانته، أو تم العفو عنه أو تقادمت العقوبة، فلا يمكن إعادة محاكمته مرة ثانية بعد عودته إلى أرض الوطن.

– أضافت المادة 584 من قانون الإجراءات الجزائية[1] شرطا آخر وهو أن يكون الجاني جزائريا وقت ارتكاب الجناية، أو أن يكتسب الجنسية الجزائرية بعد ارتكابه للجناية. والحكمة من وراء ذلك هي الحيلولة بألا يتحول اكتساب الجنسية الجزائرية إلى مطية للإفلات من العقاب. إذ نصت المادة 584 من قانون الإجراءات الجزائري على أنه: "يجوز أن تجري المتابعة أو يصدر الحكم في الحالات المنصوص عليها آنفا في المادتين 582 و583 حتى ولو لم يكن المتهم قد اكتسب الجنسية الجزائرية إلا بعد ارتكاب الجريمة أو الجنحة "

أما بخصوص الحالة الثانية التي نص عليها المشرع الجزائري لدى أخذه بمبدأ الشخصية في صورته الإيجابية هي تلك الحالة التي تكون فيها الجريمة المقترفة من طرف الجاني تحمل وصف جنحة وهي الحالة التي تناولتها المادة 583 من قانون الإجراءات الجزائية[2] والتي نصت على أنه "كل واقعة موصوفة بأنها جنحة سواء في نظر القانون الجزائري أم في نظر تشريع القطر الذي ارتكبت فيه يجوز المتابعة من أجلها والحكم عليها في الجزائر إذا كان مرتكبها جزائريا.

ولا يجوز أن تجري المحاكمة أو يصدر الحكم إلا بالشروط المنصوص عليها في الفقرة الثانية من المادة 582.

[1] الأمر رقم 66–155، المرجع السابق.

[2] المرجع السابق.

وعلاوة على ذلك فلا يجوز أن تجري المتابعة في حالة ما إذا كانت الجنحة مرتكبة ضد أحد الأفراد إلا بناء على طلب النيابة العامة بعد إخطارها بشكوى من الشخص المضرور أو ببلاغ من سلطات القطر الذي ارتكبت الجريمة فيه"

وكما يبدو جليا من مضمون المادة، فهذه الحالة هي الأخرى قيدها المشرع الجزائري بشروط تتمثل في:

– أن توصف الجريمة بأنها جنحة في كل من القانون الجزائري وكذا قانون تلك الدولة التي ارتكبت فوق إقليمها، فإذا كان الفعل مباحا وغير معاقب عليه طبقا قانون الدولة الأجنبية فلا تجوز متابعة الشخص في الجزائر من أجل فعل مباح في إقليم تلك الدولة الأجنبية التي ارتكب فيها الجزائري جنحة معاقب عليها فقط في القانون الجزائري دون قانون تلك الدولة الأجنبية.

أما إذا كان الفعل معاقبا عليه فقط في تلك الدولة الأجنبية دون الجزائر فلا يمكن إذن متابعة هذا الشخص في الجزائر لأن ذلك سيؤدي إلى تطبيق قانون دولة أجنبية فوق التراب والإقليم الوطني دون أن يكون معاقبا عليها في الجزائر.

– أن يكون الجاني جزائريا، سواء كان يتمتع بالجنسية الجزائرية قبل ارتكاب الجنحة أو اكتسبها بعد ارتكابه للجنحة، وهذا الشرط سبقت الإشارة إليه سابقا بمناسبة وروده بنص المادة 584 من قانون الإجراءات الجزائية[1] التي تطرقنا لها عند حديثنا عن الحالة الأولى الخاصة بالجناية.

– أن ترتكب الجنحة بالخارج.

– عودة الجاني إلى أرض الوطن فلا تجوز محاكمته غيابيا.

– ألا يكون قد حوكم في الخارج أو قضى عقوبة في حالة إدانته أو تم العفو عنه أو تقادمت العقوبة.

[1] المرجع السابق.

– لا تجوز متابعة الشخص ومحاكمته إلا بناء على طلب من النيابة العامة بعد إخطارها بشكوى من طرف الشخص المتضرر أي المجني عليه أو الطرف المدني أو بواسطة بلاغ من سلطات الدولة التي ارتكبت الجنحة فوق أراضيها. والملاحظ هنا أن المشرع ربط وقيد هذا الشرط بوجوب أن تكون الجنحة مرتكبة ضد أحد الأفراد، فهل حصرها فقط في الأشخاص الطبيعيين؟ وماذا لو كان الطرف المتضرر شخصا معنويا، وهذا أمر وارد جدا في حالة الجرائم الإلكترونية.

أما بخصوص الصورة الثانية لمبدأ الشخصية ونقصد بها الصورة السلبية، نصت المادة 588 من قانون الإجراءات الجزائية[1] على أنه "تجوز متابعة ومحاكمة كل أجنبي وفقا لأحكام القانون الجزائري، إذا ارتكب خارج الإقليم الجزائري بصفة فاعل 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 بالجزائر أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري". فالعبارة التي وردت بآخر هذه المادة "...أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري..." تفيد أخذ المشرع الجزائري بالوجه السلبي لمبدأ الشخصية.

مما سبق ذكره يتضح بأن السلطات الجزائرية ينعقد لها الاختصاص القضائي بالتحقيق متى كانت الجريمة الإلكترونية عبارة عن جناية أو جنحة وذلك ضمن الأوضاع والشروط التي سبق ذكرها.

بحسب تقديرينا فإن المشرع الجزائري قد أحسن ووفق حينما أخذ بمبدأ "الحماية" فجمع بين صورتي مبدأ الشخصية، ولم يكتف فقط بالأخذ بالوجه الإيجابي لمبدأ الشخصية دون الوجه السلبي، ذلك أنه وفي كثير من الأحيان يكون الجزائريون ضحايا في الخارج لعدة جرائم معاقب عليها كذلك بموجب القانون الجزائري، ولا يقتصر الأمر فقط على الأشخاص الطبيعيين بل يمتد ذلك حتى إلى الأشخاص المعنوية خصوصا إذا ما تعلق الأمر بالجرائم الإلكترونية. وبهذا تكون جهات التحقيق الجزائرية مختصة في حالة ما إذا

[1] الأمر رقم 15–02 المؤرخ في 7 شوال 1436 الموافق 23 يوليو سنة 2015 الصادر بالجريدة الرسمية رقم 40 المعدل والمتمم لقانون الإجراءات الجزائية.

كان الضحية في الخارج جزائري الجنسية. فقد يكون ضحية لجريمة إلكترونية شخص في الخارج يحمل الجنسية الجزائرية، ويستوي أن يكون شخصا طبيعيا أو معنويا.

كما أن جمع المشرع الجزائري للوجهين الإيجابي والسلبي لمبدأ الشخصية، لا يترك مجالا للمجرم لكيلا يفلت من العقاب في حالة ما إذا كان قانون الإقليم الذي ارتكبت فيه الجريمة لا يعاقب عليها، ويجد هذا الأمر أهميته أكثر في حالة الجريمة الإلكترونية إذا كان المجني عليه سواء شخص طبيعي أو معنوي ضحية جريمة إلكترونية في الخارج.

المشرع الفرنسي هو الآخر أخذ بمبدأ الشخصية في كلتا صورتيه الإيجابية والسلبية. فأما الصورة الإيجابية، فلقد جاءت بنص المادة 6/113 من قانون العقوبات الفرنسي[1] فنصت على أنه: "يطبق قانون العقوبات الفرنسي على كل جناية يرتكبها فرنسي خارج أراضي الجمهورية. كما يطبق أيضا على الجنح المرتكبة من الفرنسيين خارج أراضي الجمهورية إذا كانت الوقائع يعاقب عليها تشريع الدولة التي ارتكبت فيها. كذلك تطبق على انتهاكات لائحة المفوضية الأوروبية رقم 561\2006 للبرلمان الأوروبي ومجلس 15 مارس 2006 الخاص بتنسيق بعض التشريعات الاجتماعية الخاصة بالنقل البري، المرتكبة داخل دولة أخرى عضوه في الاتحاد الأوروبي وسجلت في فرنسا مع مراعاة أحكام المادة 692من قانون الإجراءات الجنائية ".

[1] L'article 113-6: "La loi pénale française est applicable à tout crime commis par un Français hors du territoire de la République.

Elle est applicable aux délits commis par des Français hors du territoire de la République si les faits sont punis par la législation du pays où ils ont été commis.

Elle est applicable aux infractions aux dispositions du règlement (CE) n° 561/2006 du Parlement européen et du Conseil du 15 mars 2006 relatif à l'harmonisation de certaines dispositions de la législation sociale dans le domaine des transports par route, commises dans un autre Etat membre de l'Union européenne et constatées en France, sous réserve des dispositions de l'article 692 du code de procédure pénale ou de la justification d'une sanction administrative qui a été exécutée ou ne peut plus être mise à exécution.

Il est fait application du présent article lors même que le prévenu aurait acquis la nationalité française postérieurement au fait qui lui est imputé. ", la loi n°92-683, Op.cit. Modifié par la loi n° 2009-1503 du 8 décembre 2009 relative à l'organisation et à la régulation des transports ferroviaires et portant diverses dispositions relatives aux transports, JORF n°0285 du 9 décembre 2009.

" 1-يسري هذا القانون على كل من ارتكب في الخارج من موظفي الجمهورية أو المكلفين بخدمة عامة لها أثناء تأدية أعمالهم أو بسببها جناية أو جنحة مما نص عليه في هذا القانون.

2-ويسري كذلك على من ارتكب في الخارج من موظفي السلك الدبلوماسي العراقي جناية أو جنحة مما نص عليه في هذا القانون ما تمتعوا بالحصانة التي يخولها إياها القانون الدولي العام".

وبحسب رأينا المتواضع فإن المشرع في كل من جمهورية العراق وجمهورية مصر لم يوفق حينما اكتفى فقط بالأخذ بالوجه الإيجابي لمبدأ الشخصية دون الوجه السلبي، ذلك أنه وفي كثير من الأحيان يكون رعايا هذين البلدين ضحايا في الخارج لعدة جرائم معاقب عليها كذلك بموجب القانون في كلا البلدين، ولا يقتصر الأمر فقط على الأشخاص الطبيعيين بل يمتد ذلك حتى إلى الأشخاص المعنوية خصوصا إذا ما تعلق الأمر بالجرائم الإلكترونية. وهذا الموقف لا يساهم في توفير الحماية القانونية لرعايا هذين ذلك أن الاكتفاء بالوجه الإيجابي لمبدأ الشخصية دون الوجه السلبي يجعل من جهات التحقيق في البلدين غير مختصة في حالة ما إذا كان الضحية في الخارج عراقي أو مصري الجنسية ويستوي أن يكون شخصا طبيعيا أو معنويا.

الفرع الثالث: الاختصاص القضائي بالتحقيق وفقا لمبدأ العينية

يعني هذا المبدأ تتبع التشريع العقابي الوطني جرائم محدده بعينها تمس مصالح الدولة الجوهرية وأمنها، ولو وقعت خارج إقليم الدولة ، لذلك يجد مبدأ العينية أساسه في فكرة الخطر الاجتماعي الذي يحدثه المجرم بفعله ضد مصالح الدولة، إذ قد لا تعنى الدولة التي ارتكبت الجريمة على إقليمها بملاحقتها ، مما يشجع على ارتكاب تلك الجرائم فكان من اللازم أن يتقرر للدولة حق ملاحقة تلك الجرائم وعلى الرغم من عدم وقوعها على الإقليم الوطني وبصرف النظر عن جنسية مرتكبيها فالعبرة بطبيعة الجريمة لا بمكان وقوعها وذلك للحفاظ على أمنها ومصالحها[1].

[1] محمد كمال شاهين، مرجع سابق، ص194-195.

ومصالح الدولة لا يمكننا حصرها، ذلك أنها تختلف وتتباين من دولة لأخرى. فالدولة المعنية هي المناط بها تحديد ما تعتبره مصالح أساسية تجب حمايتها وفق مبدأ العينية. المشرع الجزائري وبموجب المادة 588 من قانون الإجراءات الجزائية[1] حدد تلك المصالح في: (سلامة الدولة الجزائرية، تزييف النقود أو الأوراق المصرفية المتداولة قانونا بالجزائر)، إذ نصت هذه المادة على أنه "تجوز متابعة ومحاكمة كل أجنبي وفقا لأحكام القانون الجزائري، إذا ارتكب خارج الإقليم الجزائري بصفة فاعل 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 بالجزائر أو أي جناية أو جنحة ترتكب إضرارا بمواطن جزائري".

غير أنه وخلافا للمبدئين السابقين ونعني بهما مبدأ الإقليمية ومبدأ الشخصية، نجد بأن المشرع الجزائري لم يكتف بالقواعد العامة المنصوص عليها في قانون الإجراءات الجزائية عند تبنيه لمبدأ العينية وإنما أضاف مادة أخرى بموجب قانون آخر خص بها الجريمة الإلكترونية وهي المادة 15 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، والتي نصت على أنه "زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية ، تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبيا و تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني".

ويلاحظ بأن المشرع الجزائري أدرك مدى خطورة الجريمة الإلكترونية، فالمساس بمصالح الدولة لا يقتصر على الجريمة التقليدية، لذلك وبموجب المادة 15 أعلاه نجده وسع من مجال مبدأ العينية ليشمل كذلك تلك الجرائم الإلكترونية التي تستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني، وحسن ما فعل. وبالتالي فإن القضاء الجزائري يعتبر مختصا بالتحقيق في تلك الجرائم الإلكترونية التي

[1] الأمر رقم 15-02، المرجع السابق.

[2] القانون رقم 09-04، المرجع السابق.

المشرع الفرنسي أخذ بمبدأ العينية بموجب المادة 10/113 من قانون العقوبات الفرنسي[1] إذا نصت على أنه " يطبق قانون العقوبات الفرنسي على الجنايات والجنح التي تأثر على المصالح الأساسية للوطن والمجرمة بالعنوان الأول بالكتاب الرابع، للتزوير وتقليد ختم الدولة، ولقطع النقد والعملات الورقية أو ذات الأثر العام والمجرمة بالمواد 442-1، 442-2، 442-5، 442-15، 443-1 و444-1 وعلى كل جناية أو جنحة ترتكب ضد الموظفين أو المباني الدبلوماسية أو القنصلية الفرنسية، خارج أراضي الجمهورية".

والملاحظ بأن المشرع الفرنسي لم يحدد إذا ما كان مرتكب هذه الجرائم فرنسي الجنسية أم أجنبي ما يفهم منه أن مضمون المادة جاء بصيغة عامة فيستوي أن يكون الجاني فرنسيا أو أجنبيا ارتكب الأفعال المشار إليها أعلاه خارج فرنسا. كما يلاحظ بأن المشرع الفرنسي لم يدرج الجريمة الإلكترونية بمضمون المادة 10/113 من قانون العقوبات الفرنسي[2] لذلك يمكننا القول بأن اكتفى بالقواعد العامة في تحديد الأخذ بمبدأ العينية في حالة ما إذا ارتكبت إحدى الأفعال المشار إليها بنص المادة أعلاه من خلال استعمال وسائل الاتصالات الإلكترونية، وهو عكس ما نص عليه عند تطرقه لمبدأ الإقليمية حيث نص بصريح العبارة على الجنايات والجنح التي ترتكب من خلال شبكة الاتصالات الإلكترونية.

وهو نفس ما ذهب إليه المشرع المصري عند أخذه بمبدأ العينية، إذ نصت المادة الثانية بالفقرة الثانية وما يليها من قانون العقوبات المصري[3]على أنه " تسري أحكام هذا القانون..... على كل من ارتكب في خارج القطر جريمة من الجرائم الآتية:

أ-جناية مخلة بأمن الحكومة مما نص عليه في البابين الأول والثاني من الكتاب الثاني من هذا القانون.

---

[1] Article 113-10 " La loi pénale française s'applique aux crimes et délits qualifiés d'atteintes aux intérêts fondamentaux de la nation et réprimés par le titre Ier du livre IV, à la falsification et à la contrefaçon du sceau de l'Etat, de pièces de monnaie, de billets de banque ou d'effets publics réprimées par les articles 442-1, 442-2, 442-5, 442-15, 443-1 et 444-1 et à tout crime ou délit contre les agents ou les locaux diplomatiques ou consulaires français, commis hors du territoire de la République." .La loi n°92-683, Op.cit. Modifié par la loi n° 2001-1168 du 11 décembre 2001 portant mesures urgentes de réformes à caractère économique et financier JORF n°288 du 12 décembre 2001.

[2] Ibid.

[3] القانون رقم 1937/58، المرجع السابق.

ب-جناية تزوير مما نص عليه في المادة 206 من هذا القانون.

ج-جناية تقليد أو تزيف أو تزوير عمله ورقية أو معدنية مما نص عليه في المادة 202 أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلى مصر أو إخراجها منها أو ترويجها أو حيازتها بقصد الترويج أو التعامل بها مما نص عليه في المادة 203 بشرط أن تكون العملة متداولة قانونا في مصر".

فالاختصاص بالتحقيق إذا ما تعلق الأمر بجريمة إلكترونية، يكون بتطبيق القواعد العامة للاختصاص وفقا لمبدأ العينية المشار إليه بنص المادة أعلاه.

الفرع الرابع: الاختصاص القضائي بالتحقيق وفقا لمبدأ العالمية

يقصد بمبدأ العالمية أن يكون لكل دولة ولاية القضاء في أي جريمة، بصرف النظر عن مكان وقوعها أو مساسها بمصالحها أو جنسية مرتكبها[1]. ويقصد به كذلك صلاحية تقررت للقضاء الوطني في ملاحقة ومحاكمة وعقاب مرتكب أنواع معينة من الجرائم التي يحددها التشريع الوطني دون النظر لمكان ارتكابها أو ضحاياها وأيا ما كانت جنسية مرتكبيها أو ضحاياها[2]. ولمبدأ العالمية أو ما يعبر عنه بمبدأ عالمية القانون الجنائي وجهان أو صورتان، وجه إلزامي ووجه جوازي أو اختياري.

فأما الوجه الإلزامي، بمقتضاه يقع على عاتق الدولة الالتزام بالنص في قانونها الجنائي على إخضاع جرائم معينة لقانونها الجنائي فيما إذا تواجد مرتكبها أو أحد مرتكبيها في إقليمها بغض النظر عن جنسية الجاني والمجني عليه وبغض النظر عن مكان وقوع الجريمة، وذلك تطبيقا لاتفاقيات دولية صادقت عليها أو كانت طرفا فيها. وأما الوجه الاختياري فبموجبه يحق لكل دولة إخضاع بعض الجرائم المرتكبة في الخارج إلى قانونها الجنائي، باعتبارها جرائم خطيرة في نظرها وذلك في حال تواجد مرتكبها في إقليمها

[1] جلال ثروت، نظم القسم العام في قانون العقوبات، دار الهدى للمطبوعات، الإسكندرية، 1999، ص104.

[2] طارق سرور، الاختصاص الجنائي العالمي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006، ص25.

وبغض النظر عن جنسية الأخير وصفته أو جنسية المجني عليه، على أن لا يكون هناك طلب مسبق أو قول مسبق بتسليمه من أو إلى الدولة التي وقعت فيها الجريمة[1].

بخصوص المشرع الجزائري، ولدى مراجعة مواد قانون الإجراءات الجزائية لا سيما تلك المتعلقة بالجنايات والجنح التي ترتكب بالخارج والتي ورد ذكرها في الباب التاسع من الكتاب الخامس بموجب المواد من 582 إلى 598، لم نجد ما له علاقة بمبدأ العالمية بخصوص سريان النص الجنائي، اللهم إلا إذا عمد المشرع الجزائري على عدم إدراج الجرائم التي تضمنتها تلك المعاهدات والاتفاقيات الدولية التي كانت الجزائر طرفا فيها بقانون الإجراءات الجزائية، ونعني بها هنا تلك الجرائم التي تعهدت الجزائر بمحاربتها والتي كانت موضوع اتفاقيات دولية.

وعلى عكس المشرع الجزائري، نجد بأن المشرع الفرنسي قد نص على مبدأ العالمية في تشريعاته ولم يكتف بذلك فحسب بل أخذ بكلا الوجهين لمبدأ العالمية، الوجه الإلزامي وكذا الاختياري. وظهر ذلك من خلال نص المادة 1/689 من قانون الإجراءات الجزائية الفرنسي[2] وما يليها، إذ نصت المادة سالفة الذكر على أنه "وفقا للاتفاقيات الدولية المشار إليها أدناه، يمكن ملاحقة أي شخص أدين خارج أراضي الجمهورية بجريمة من الجرائم المذكورة في هذه المواد ومحاكمته أمام المحاكم الفرنسية إذا كان موجودا في فرنسا. وتسري أحكام هذه المادة على الشروع في تلك الجرائم، إذا كان القانون يعاقب عليها". وهذا ما يدخل ضمن الصورة الإلزامية لمبدأ العالمية.

[1] عباس توفيق البستاني نافطة، مبدأ الاختصاص العالمي في القانون العقابي، الطبعة الأولى، مطبعة آراس، أربيل، 2009، ص 60 و100. أشار إليه رشاد خالد عمر، المرجع السابق، ص103 و105.

[2] Article 689-1 "En application des conventions internationales visées aux articles suivants, peut être poursuivie et jugée par les juridictions françaises, si elle se trouve en France, toute personne qui s'est rendue coupable hors du territoire de la République de l'une des infractions énumérées par ces articles. Les dispositions du présent article sont applicables à la tentative de ces infractions, chaque fois que celle-ci est punissable.", Ordonnance n° 58-1296 du 23 décembre 1958 modifiant et complétant le code de procédure pénale JORF n°0300 du 24 décembre 1958 .Modifié par la Loi n°99-515 du 23 juin 1999 renforçant l'efficacité de la procédure pénale. JORF n°144 du 24 juin 1999.

في حين أن الوجه الاختياري جاءت به المادة 113-8-2 من قانون العقوبات الفرنسي[1] حيث نصت على أنه "مع عدم الإخلال بتطبيق المواد من 113-6 إلى 113-8، يطبق القانون الجنائي الفرنسي أيضاً على أي جريمة أو جنحة يعاقب عليها بالسجن خمس سنوات على الأقل ارتكبت خارج أراضي الجمهورية من قبل شخص أجنبي ترفض السلطات الفرنسية تسليمه إلى الدولة الطالبة إما على أساس كون الجرم الذي يلتمس بشأنه التسليم يعاقب عليه بعقوبة أو يطبق بشأنه إجراء أمني كلاهما مخالف للنظام العام الفرنسي، أو لكون محاكمة الشخص المطلوب ستُجرى في تلك الدولة من قبل محكمة لا توفر الضمانات الإجرائية الأساسية وحماية حقوق الدفاع، أو لكون الجرم المعني يكتسي صبغة جريمة سياسية. أو أن تسليم الشخص المطلوب قد تكون له عواقب خطيرة لا سيما بسبب سنه أو حالته الصحية.

ولا يمكن متابعة الجرائم المنصوص عليها في الفقرة الأولى إلا بطلب من المدعي العام"

فيما يخص الجريمة الإلكترونية باعتبارها جريمة عابرة للحدود، يبدو للوهلة الأولى بأن مبدأ العالمية يبرز على أنه المبدأ الأكثر ملائمة وأهمية من حيث تطبيقه على الجريمة الإلكترونية مقارنة ببقية المبادئ الثلاثة السابقة ونقصد بها مبدأ الإقليمية ومبدأ الشخصية ومبدأ العينية. ذلك أن الجريمة الإلكترونية قد يتم التخطيط له وتنفيذها في دول مختلفة وتتحقق نتائجها في دول أخرى، وحتى أنه قد يتم القبض على المجرم في دولة غير تلك التي خطط فيها للجريمة ولا تلك التي نفذت فيها ولا التي تحققت فيها النتيجة، أو أن الدولة التي ارتكبت الجريمة بإقليمها إما تكون متواطئة مع المجرم أو أنها تتقاعس عن متابعته أو أن يكون ذو نفوذ فلا يمكن لسلطات ذاك البلد متابعته قضائيا.

[1] Article 133-8-2 "Sans préjudice de l'application des articles 113-6 à 113-8, la loi pénale française est également applicable à tout crime ou à tout délit puni d'au moins cinq ans d'emprisonnement commis hors du territoire de la République par un étranger dont l'extradition ou la remise a été refusée à l'Etat requérant par les autorités françaises aux motifs, soit que le fait à raison duquel l'extradition avait été demandée est puni d'une peine ou d'une mesure de sûreté contraire à l'ordre public français, soit que la personne réclamée aurait été jugée dans ledit Etat par un tribunal n'assurant pas les garanties fondamentales de procédure et de protection des droits de la défense, soit que le fait considéré revêt le caractère d'infraction politique, soit que l'extradition ou la remise serait susceptible d'avoir, pour la personne réclamée, des conséquences d'une gravité exceptionnelle en raison, notamment, de son âge ou de son état de santé.

La poursuite des infractions mentionnées au premier alinéa ne peut être exercée qu'à la requête du ministère public.". Crée par la loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée. JORF n°0312 du 26 décembre 2020.

الباب الأول: الجهات المتصلة بالتحقيق الابتدائي في الجريمة الإلكترونية

وهناك حالات تكون فيها أجهزة وإدارات رسمية داخل الدولة وراء ارتكاب جريمة من الجرائم الإلكترونية باختلاف أشكالها، وهذا موضوع سنتناوله بالتفصيل في الباب الثاني من هذه الدراسة.

غير أن تطبيق مبدأ عالمية النص الجنائي بما في ذلك النص الإجرائي، قد تعترضه عوائق، فعلى سبيل المثال إذا ما تم إلقاء القبض على شخص ما داخل دولة ما وكان قد ارتكب جريمة من الجرائم الإلكترونية، ففي حالة ما إذا قررت هذه الدولة متابعة هذا الشخص قضائيا فإنها ستواجه صعوبات جمة في جمع الأدلة الكافية التي تدينه خاصة بالنظر إلى طبيعة الدليل الإلكتروني، ذلك أن الجريمة ارتكبت فوق إقليم دولة أخرى. ضف إلى ذلك مسألة تنازع الاختصاص التي قد تثيرها العديد من الدول مستندة في ذلك إلى مبدأ العينية أو مبدأ الإقليمية.

في الأخير، يبقى وحده التعاون الدولي كفيل بتجسيد فعالية مبدأ العالمية كمبدأ يبدو الأقرب والأنسب لنجاعة مواجهة الجريمة الإلكترونية لا سيما من حيث تسهيل مهام جهات التحقيق، وذلك مقارنة بالمبادئ الثلاثة الأخرى. وتجدر الإشارة إلى أن موضوع التعاون الدولي هو الآخر يشهد عدة معوقات سوف نتطرق لها في الباب الأخير من هذا البحث.

الفصل الثاني: الضبطية القضائية جهة ذات صلة بالتحقيق الابتدائي في الجريمة الإلكترونية

تمهيد وتقسيم:

يرجع أصل كلمة "الضبط" إلى اللغة اليونانية "politis"، ويقصد بها الحكومة الداخلية للدولة، وقد اكتسبت معاني جديدة بعد انتقالها إلى عدة لغات (اللغة اللاتينية واللغات الغربية الأخرى)، وإن كانت كلها تصب في ذات الهدف، ففي البداية كانت تعني مجموعة القواعد التي يلتزم بها الأفراد في سبيل تحقيق الخير العام لهم. وفي مرحلة لاحقة أصبحت تعني مجموعة الأشخاص المنوط بهم تحقيق الغرض السابق، إلى أن استقر المعني كما هو عليه الآن، وهو وظيفة ضرورية من وظائف السلطة العامة، تهدف إلى وقاية النظام العام في المجتمع بوسائل معينة في ظل القانون.[1]

وهناك نوعان من الضبط، ضبط إداري وضبط قضائي. فالأول هدفه وقائي يسعى للحيلولة دون الإخلال بالنظام العام ووقوع جرائم، أما الثاني فهو علاجي يأتي كرد فعل على ذلك الإخلال الذي أصاب النظام العام جراء ارتكاب الجريمة.

ويقول في هذا الشأن أحد الرؤساء الفرنسيين السابقين، والأمر يتعلق بالرئيس الأسبق "جيسكار ديستان" في مؤلفه "الديمقراطية الفرنسية" مشيرا إلى مدى أهمية كل من وظيفة الضبط القضائي والإداري: "لمواجهة أي إخلال بالأمن العام يجب استخدام أسلوبين مكملين لبعضهما، وهما منع وقوع هذا الإخلال ومعاقبة الجاني بعد ارتكابه واقعة الإخلال بالعقاب الرادع"[2]

[1] نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007، ص83.

[2] ممدوح إبراهيم السبكي، حدود سلطات مأمور الضبط القضائي في التحقيق، دار النهضة العربية، القاهرة، 1998، ص04.

لقد شرحنا في مقدمة هذا الباب علاقة الضبطية القضائية بالتحقيق الابتدائي بصفة عامة وكذا الجريمة الإلكترونية بصفة خاصة، واعتبرنا بأن ذلك يعد سببا كافيا يبرر تطرقنا للضبطية القضائية من حين لآخر وذلك بكل مختلف أجزاء هذه الدراسة.

من خلال هذا الفصل سنحاول تقديم نظرة موجزة لجهاز الضبطية بصفة عامة، وكذا حاجة المشرع الجزائري والتشريعات المقارنة إلى ضرورة إيلاء الضبطية بعناية فرضتها طبيعة الجريمة الإلكترونية. وذلك من خلال تحديث تلك النصوص المتعلقة بطبيعة عمل هذا الجهاز تجعل منه سندا لجهات التحقيق في الجريمة الإلكترونية، وذلك في خضم سعيها إلى ملاحقة الجناة وجمع الأدلة بغية كشف الحقيقة.

لقد قسمنا هذا الفصل إلى مبحثين، حيث سنتطرق في المبحث الأول للضبطية الإدارية في مجال الجريمة الإلكترونية، أما الثاني نخصصه للضبطية القضائية في مجال الجريمة الإلكترونية.

المبحث الأول: الضبطية الإدارية في مجال الجريمة الإلكترونية

قبل الحديث عن جهات الضبط الإداري في الجريمة الإلكترونية وكذا عن طبيعة عملها، لابد من التعرَف أولا عن المقصود بالضبط الإداري.

المطلب الأول: تعريف الضبط الإداري

كثيرة هي ومتنوعة تلك التعريفات التي أعطيت للضبط الإداري. فيمكن إعطاء تعريفات متنوعة للضبط الإداري من زوايا متعددة. غير أنها لا تخرج عن معيارين للتعريف بالضبط الإداري هما المعيار العضوي والمعيار الموضوعي.

فتبعا للمعيار العضوي يمكن تعريف الضبط الإداري على أنه مجموعة من الأجهزة والهيئات التي تتولى القيام بالتصرفات والإجراءات التي تهدف إلى المحافظة على النظام

العام. ومن منطلق المعيار الموضوعي يمكن تعريف الضبط الإداري على أنه مجموعة الإجراءات والتدابير التي تقوم بها الهيئات العامة حفاظا على النظام العام[1].

وبصفة عامة يمكن تعريف الضبط الإداري بأنه "حق الإدارة في أن تفرض على الأفراد قيود تحد بها من حرياتهم بقصد حماية النظام العام"[2].

ويعد الضبط الإداري أو البوليس الإداري من أهم وظائف الإدارة، ويهدف إلى المحافظة على النظام العام في الأماكن العامة عن طريق إصدار القرارات اللائحية والفردية واستخدام القوة المادية، مع ما يستتبع ذلك من فرض قيود على الحريات الفردية، يستلزمها انتظام أمر الحياة في المجتمع[3].

المطلب الثاني: الضبط الإداري المتعلق بالجريمة الإلكترونية

أشرنا سابقا أن الهدف من تلك الإجراءات المتخذة في إطار الضبط الإداري هو هدف وقائي يحول دون الإخلال بالنظام العام وذلك من خلال المحافظة على الأمن العام والصحة العامة والسكينة العامة، وهذا هو المثلث الذي يشكل ما يعرف ب "النظام العام".

إن الأخطار التي تهدد النظام العام لم تعد محصورة في تلك المتعلقة بعالمنا المادي فقط، ذلك أن التطور التكنولوجي خلق لنا ما يسمى بالعالم الافتراضي الذي أصبح بدوره يشكل مرتعا لكافة أنواع الجرائم. وبالتالي وجدت جهات الضبط الإداري نفسها أمام تحد آخر، وهو السعي إلى الحفاظ على النظام العام داخل العالم الافتراضي، وذلك من خلال اتخاذ جملة من الصلاحيات التي خولها إياها القانون.

[1] طعيمة الجرف، القانون الإداري والمبادئ العامة في تنظيم نشاط السلطات الإدارية، دار النهضة العربية، القاهرة، 1978، ص291.

[2] سليمان محمد الطماوي، الوجيز في القانون الإداري، دار الفكر العربي، 1997، ص574.

[3] ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، 1994، ص 471.

سنقسم هذا المطلب إلى فرعين نتعرف من خلالهما على صفة أولئك الأشخاص المكلفين بالضبط الإداري داخل العالم الافتراضي، وعن تلك الإجراءات المخول لهم القيام بها كإجراء وقائي للمحافظة على النظام العام.

الفرع الأول: الجهة القائمة بالضبط الإداري في العالم الافتراضي

الأصل أن كل شخص ينتمي إلى الضبطية القضائية فهو بالضرورة يحمل كذلك صفة الضبط الإداري. ذلك أن صفة الضبط القضائي أشمل من صفة الضبط الإداري؛ فكل عضو من أعضاء الضبطية القضائية هو بالضرورة عضو من أعضاء الضبط الإداري. غير أن العكس ليس دائما صحيحا، فليس كل الأشخاص الذين ينتمون إلى الضبطية الإدارية هم بالضرورة يتمتعون بصفة الضبطية القضائية. ومرد ذلك هي تلك الشروط التي تضعها التشريعات وتمنح من خلالها صفة الضبطية القضائية لأشخاص محددين دون سواهم، وهذا ما سنناقشه في المبحث الثاني من هذا الفصل والمخصص للضبطية القضائية في مجال الجريمة الإلكترونية.

إذن ومن خلال ما قيل سابقا، فهناك إمكانية بأن يكون الشخص القائم بالضبط الإداري جامعا لصفتي الضبط الإداري وكذا الضبط القضائي.

في مجال الجريمة الإلكترونية يختص بالضبط الإداري في الجريمة الإلكترونية مأمورو الضبط القضائي حين قيامهم بحفظ النظام – أي بوظيفة الضبط الإداري – كما تمنح تلك الصفة لبعض العاملين في مجال الاتصالات الإلكترونية كمزودي الخدمات عبر الإنترنت، فضلا عن بعض موظفي الاتصالات، وذلك لكون القانون يمنحهم حق الرقابة المعتادة لأعمال الشبكات ومدى التزام المشتركين بأحكام القانون ولنظام الاشتراك في الخدمة، فإذا اكتشف مزودو الخدمة إحدى الجرائم عن طريق ممارسة عمله فليس له سوى التحفظ على أدلة الجريمة لحين حضور مأمور الضبط القضائي[1].

[1] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004، ص808 وما بعدها.

الفرع الثاني: بعض صور الضبط الإداري في مجال الجريمة الإلكترونية

الضبطية الإدارية، ومن خلال عملها تسعى إلى الوقاية من الجريمة وذلك عن طريق اتخاذ إجراءات لمنع وقوع الجريمة، والحفاظ بالتالي على النظام العام. وكذلك هو الشأن بالنسبة للضبط الإداري في العالم الافتراضي.

من بين تلك الإجراءات المتخذة إجراء يتضمن القيام بدوريات في كل وقت، ليلا ونهارا، وذلك داخل العالم الافتراضي عبر شبكة الإنترنت. فعلى سبيل المثال، قد يدخل أحد رجال الشرطة إلى مواقع التواصل الاجتماعي المنتشرة عبر شبكة الإنترنت من أجل رصد ذلك السلوك أو تلك التصرفات التي من شأنها تهديد النظام العام، كالتحريض على الكراهية والعنصرية، أو تلك التي تهدف إلى الابتزاز والتشهير أو غير ذلك. كما أنه بإمكان رجال الضبطية الإدارية التواصل – دون الكشف عن هوياتهم-مع أولئك الأشخاص المتواجدين بغرف الدردشة عبر شبكة الإنترنت، وذلك لرصد إن كان هناك من بينهم مجرمين كمثل الذين يتبادلون الملفات ذات المضمون الإباحي كصور القصر أو الذين يتخذون من فضاء الإنترنت وسيلة لترويج الممنوعات كالمخدرات مثلا.

هذا، وقد تقوم الشرطة الإدارية كذلك بدوريات لمراقبة مقاهي الإنترنت للوقوف على عدم ارتكاب أية أفعال تدخل ضمن الجرائم الإلكترونية من طرف أصحاب هذه المحلات، كنسخ وبيع برمجيات ومؤلفات إلكترونية محمية بحقوق المؤلف، أو السماح للقصر بالولوج للمواقع الإباحية، أو تحميل الملفات ذات المحتوى المجرَّم طبقا للقوانين واللوائح التي تنظم سير هذه الأماكن.

ففي حالة وقوف الشرطة الإدارية على ارتكاب جريمة إلكترونية يتحول عملهم حينئذ من الضبط الإداري إلى الضبط القضائي إذا كان القانون قد منحهم سلفا صفة الضبط القضائي.

المبحث الثاني: الضبطية القضائية في مجال الجريمة الإلكترونية

الضبطية القضائية جهاز يضم مجموعة من الأشخاص منحهم القانون صفة الضبط القضائي، وحدد لهم مهام يمارسونها من خلال هذه الصفة.

لقد نتج عن ظهور ما يعرف بالجريمة الإلكترونية تبني نصوص قانونية تتيح وتخول للضبطية القضائية ممارسة مهامها بشكل يمتد إلى العالم الافتراضي وذلك في إطار ما يسمى الشرعية أو المشروعية الإجرائية.

من خلال هذا المبحث سنلقي نظرة على الضبط القضائي بصفة عامة، وعلى أولئك الأشخاص الذين منحهم المشرع صفة الضبطية القضائية وذلك بمختلف الفئات التي ينتمون إليها. كما وسنتطرق إلى تلك التطورات التي مست هذا الجهاز في سبيل مواجهة الجريمة الإلكترونية، لاسيما باعتباره كجهة لها صلة بالتحقيق الابتدائي المتعلق بالجريمة الإلكترونية.

المطلب الأول: الضبط القضائي بصفة عامة

خصص المشرع الجزائري للضبط القضائي الفصل الأول من الكتاب الأول من قانون الإجراءات الجزائية الجزائري، وذلك ابتداء من المادة 12. حيث بيّن تلك المهام التي يتضمنها الضبط القضائي، كما حدد أولئك الأشخاص الذين أكسبهم وأصبغ عليهم صفة الضبطية القضائية.

لذا سنقسم هذا المطلب إلى فرعين، بحيث نتطرق في الفرع الأول للأشخاص الذين يتمتعون بصفة الضبطية القضائية، أما الفرع الثاني نتناول فيه طبيعة المهام التي أوكلها المشرع للضبطية القضائية.

الفرع الأول: الأشخاص القائمون بالضبطية القضائية

ويقصد بهم أولئك الأشخاص الذين منحهم المشرع صفة الضبط القضائي، إذ عمدت مختلف التشريعات المقارنة إلى تحديد هذه الفئة استنادا على معايير معينة. هذا ونشير إلى اختلاف التشريعات المقارنة حول التسمية التي تم منحها لهذه الفئة، ففي لبنان مثلا

يطلق عليهم اسم الضبطية العدلية في حين يحملون في مصر تسمية مأموري الضبط القضائي.

المشرع الجزائري ومن خلال المادة 14 من قانون الإجراءات الجزائية الجزائري[1] حدد أولئك الأشخاص القائمين بالضبط القضائي وهم: ضباط الشرطة القضائية، أعوان الضبط القضائي وكذا الموظفين والأعوان المنوط بهم قانونا بعض مهام الضبط القضائي.

وحتى لا نسهب في التطرق إلى الضبطية القضائية بالتفصيل، سنكتفي فقط بما يخدم دراستنا وذلك من خلال الاقتصار على أولئك الأشخاص الذين لهم علاقة بالتحقيق الابتدائي، سواء من خلال الندب القضائي أو ما يعرف بالإنابة القضائية من جهة، ومن جهة أخرى بناء على تلك الصلاحيات التي خولهم إياها القانون وذلك في حالة التلبس. هذا دون أن ننسى تلك القوانين المستحدثة والتي أشارت إليهم في إطار مكافحة الجريمة الإلكترونية.

لذلك فإن حديثنا عن الأشخاص القائمون بالضبطية القضائية سوف يقتصر فقط على ضباط الشرطة القضائية وكذا أعوان الضبط القضائي، وسنلقي نظرة على كل منهم كالآتي:

أولا: ضباط الشرطة القضائية

حددت المادة 15 من قانون الإجراءات الجزائية الجزائري[2] الأشخاص الذين يتصفون ب"ضباط الشرطة القضائية" حيث نصت على ما يلي " يتمتع بصفة ضابط الشرطة القضائية:

1-رؤساء المجالس الشعبية البلدية.

2-ضباط الدرك الوطني.

[1] الأمر رقم 66-155، المرجع السابق.

[2] الأمر رقم 15-02، المرجع السابق.

3-الموظفون التابعون للأسلاك الخاصة للمراقبين، ومحافظي وضباط الشرطة للأمن الوطني.

4-ذوو الرتب في الدرك، ورجال الدرك الذين امضوا في سلك الدرك الوطني ثلاث (3) سنوات على الأقل والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني، بعد موافقة لجنة خاصة.

5-الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين امضوا ثلاث (3) سنوات على الأقل بهذه الصفة والذين تم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية والجماعات المحلية، بعد موافقة لجنة خاصة.

6-ضباط وضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل.

يحدد تكوين اللجنة المنصوص عليها في هذه المادة وتسييرها بموجب مرسوم."

من خلال نص المادة أعلاه يمكن تقسيم ضباط الشرطة القضائية إلى صنفين أو فئتين هما:

أ-الفئة الأولى:

تضم أولئك الأشخاص المشار إليهم في الفقرات 1 و2 و3 من المادة 15 أعلاه، فهؤلاء يكتسبون صفة ضباط الشرطة القضائية من خلال الوظائف التي يشغلونها أو الرتب التي تحصلوا عليها بمجرد تعيينهم في مناصبهم وذلك بقوة القانون ودون أي شرط آخر.

ب-الفئة الثانية:

وتضم الأشخاص المبينين في الفقرات 5 و6 و7 من المادة 15 أعلاه، فهؤلاء يكتسبون صفة ضباط الشرطة القضائية بموجب تعيينهم بقرار مشترك بين وزيري العدل والدفاع بالنسبة للدرك الوطني والأمن العسكري؛ وقرار مشترك بين وزيري العدل والداخلية والجماعات المحلية فيما يتعلق بالمفتشين وحفاظ وأعوان الشرطة للأمن الوطني.

ثانيا: أعوان الضبط القضائي

حددت المادة 19 من قانون الإجراءات الجزائية الجزائري[1] أعوان الضبط القضائي، ويقصد بهم أولئك الأشخاص الذين لهم صفة ضباط الشرطة القضائية.

حيث نصت المادة 19 أعلاه على أنه "يعد من أعوان الضبط القضائي موظفو مصالح الشرطة وذوو الرتب في الدرك الوطني، ورجال الدرك ومستخدمو الأمن العسكري الذين ليست لهم صفة ضباط الشرطة القضائية".

إذا وبحسب نص المادة أعلاه يعتبر من أعوان الضبط القضائي، والذين يتمتعون بصفة ضباط الشرطة القضائية:

- موظفو مصالح الشرطة.
- ذوو الرتب في الدرك الوطني.
- رجال الدرك الوطني.
- مستخدمو مصالح الأمن العسكري.

الفرع الثاني: مهام الضبطية القضائية

جاء بالفقرة الثالثة من المادة 12 من قانون الإجراءات الجزائية الجزائري[2] أنه "... ويناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات وجمع الأدلة عنها والبحث عن مرتكبيها ما دام لم يبدأ فيها تحقيق قضائي...".

كما نصت المادة 13 من قانون الإجراءات الجزائية[3] " إذا ما افتتح التحقيق فإن على الضبط القضائي تنفيذ تفويضات جهات التحقيق وتلبية طلباتها".

[1] الأمر رقم 95-10 مؤرخ في 25 رمضان عام 1415 الموافق 25 فبراير سنة 1995 الصادر بالجريدة الرسمية رقم 11 بتاريخ 29 رمضان 1415 الموافق 01 مارس سنة 1995 المعدل والمتمم لقانون الإجراءات الجزائية.

[2] القانون رقم 17-07 مؤرخ في 28 جمادى الثانية عام 1438 الموافق 27 مارس سنة 2017 الصادر بالجريدة الرسمية رقم 20 بتاريخ أول رجب 1438 الموافق 29 مارس سنة 2017 المعدل والمتمم لقانون الإجراءات الجزائية.

[3] الأمر رقم 66-155، المرجع السابق.

من خلال محتوى المادتين أعلاه يتضح لنا أن مهمة الضبطية القضائية تشمل البحث والتحري عن كافة الجرائم، وكذا جمع الأدلة والبحث عن مرتكبيها مادام لم يفتتح تحقيق قضائي في هذه الجرائم. وأنه بمجرد أن يفتتح تحقيق قضائي فإن مهام الضبطية القضائية في هذه المرحلة تتمثل في تنفيذ وتلبية طلبات جهات التحقيق.

يمكن تقسيم اختصاصات الشرطة القضائية إلى نوعين، وذلك بحسب المرحلة التي تمارس من خلالها هذه الاختصاصات. فهناك اختصاصات تمارسها الشرطة القضائية قبل فتح تحقيق قضائي، وأخرى تمارس بعد فتح تحقيق قضائي.

أولا: اختصاصات الشرطة القضائية قبل فتح تحقيق قضائي

حيث تمارس الشرطة القضائية مهام عادية وأخرى استثنائية، وذلك من خلال هذه المرحلة التي تسبق افتتاح تحقيق قضائي أي تسبق تحريك الدعوى العمومية. وتسمى هذه المرحلة بمرحلة جمع الاستدلالات أو كما يسميها البعض بمرحلة التحقيق الأولي أو التحريات الأولية.

أ-في الحالات العادية:

في الحالة التي لاتزال فيها الجريمة غامضة، فإن الضبطية القضائية تقوم بكل ما من شأنه الكشف عنها وذلك من خلال التحريات إذ تتلقى الضبطية في هذه المرحلة البلاغات والشكاوى، وتنتهي هذه المرحلة بتحرير محاضر.

رغم أهمية مرحلة جمع الاستدلالات، إلا أنها تبقى ذات طبيعة إدارية وليست قضائية. كما أن المحاضر التي يتم تحريرها لا تعتبر ملزمة للجهات القضائية.

ب-في حالة التلبس:

في حالة التلبس أو ما يسمى بالجرم المشهود، فإن الضبطية القضائية تمارس صلاحيات تعتبر استثنائية مادام أنه لم يكن بإمكانها أن تمارسها في ظل الحالات العادية، ومن بينها القبض وتفتيش المساكن على سبيل المثال. فحالة التلبس، ونظرا لما تتطلبه من سرعة،

منحت للضبطية صلاحية القيام ببعض الإجراءات هي في الأصل من اختصاص السلطات القضائية.

وعلى عكس المحاضر التي يتم تحريرها في الحالات العادية خارج التلبس، والتي تعتبر محاضر استدلالية، فإن المحاضر التي يتم تحريرها بمناسبة التلبس لها قوة من حيث الإثبات.

ثانيا: اختصاصات الشرطة القضائية بعد فتح تحقيق قضائي

الأصل أن إجراءات التحقيق هي من اختصاص قاض التحقيق، غير أنه ونظرا لكثرة انشغال قضاة التحقيق من جهة، وكذا من أجل إضفاء مرونة على أعمال التحقيق ومراعاة السرعة التي يتطلبها التحقيق من جهة أخرى، أجاز القانون لقاض التحقيق تفويض أحد ضباط الشرطة القضائية من أجل القيام بإجراء أو أكثر من إجراءات التحقيق، وهذا ما يسمى بالإنابة القضائية أو الندب القضائي.

الإنابة القضائية هي عبارة عن تفويض كتابي صادر من قاض التحقيق، يكلف من خلاله ضباط الشرطة القضائية من أجل القيام ببعض المهام التي تعتبر في الأصل من ضمن سلطة التحقيق.

إضافة إلى هذه الاختصاصات المناطة بالضبطية القضائية قبل وبعد فتح تحقيق قضائي، هناك اختصاصات أخرى متعلقة بفئة الأحداث، وهي تلك الحالات التي يكون فيها القصر ضحايا أو ارتكبوا جريمة ما. ونظرا لحساسية هذه الشريحة من المجتمع، خص المشرع الضبطية القضائية كذلك بصلاحيات وإجراءات خاصة تستوجب مراعاتها لدى التعامل مع الحدث أو القاصر.

الفرع الثالث: نطاق اختصاص الضبطية القضائية

ويقصد بنطاق الاختصاص، تلك الحدود التي وضعها المشرع، والتي على الضبطية القضائية احترامها. سواء ما تعلق منها بالمجال الإقليمي، والذي تقوم الضبطية القضائية

بمهامها داخله، وهو ما يعبر عنه بالاختصاص الإقليمي. أو بنوع تلك الجرائم التي يمكن ضبطها، وهو ما يسمى بالاختصاص النوعي.

أولا: الاختصاص الإقليمي (المكاني)

يخضع تحديد الاختصاص المكاني الذي يمارس فيه أعضاء الضبطية القضائية مهامهم إلى المعايير الثلاثة وهي: مكان وقوع الجريمة، محل إقامة المشتبه فيه، وكذا مكان إلقاء القبض عليه.

نصت المادة 16 من قانون الإجراءات الجزائية الجزائري[1] على أنه "يمارس ضباط الشرطة القضائية اختصاصهم المحلي في الحدود التي يباشرون ضمنها وظائفهم المعتادة.

إلا أنه يجوز لهم –في حالة الاستعجال –أن يباشروا مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به.

ويجوز لهم أيضا –في حالة الاستعجال أن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا ويجب أن يساعدهم ضابط الشرطة القضائية الذي يمارس وظائفه في المجموعة السكنية المعنية.

وفي الحالات المنصوص عليها في الفقرتين السابقتين يتعين عليهم أن يخبروا مسبقا وكيل الجمهورية الذي يباشرون مهمتهم في دائرة اختصاصه.

وفي كل مجموعة سكنية عمرانية، مقسمة إلى دوائر للشرطة فإن اختصاص محافظي وضباط الشرطة الذين يمارسون وظائفهم في إحداها يشمل كافة المجموعة السكنية.

لا تطبق أحكام الفقرات الثانية والثالثة والرابعة والخامسة من هذه المادة على ضباط الشرطة القضائية التابعين لمصالح الأمن العسكري الذين لهم الاختصاص على كافة الإقليم الوطني.

[1] القانون رقم 06-22، المرجع السابق.

غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني.

ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات".

إذن وبحسب الفقرة الأولى من المادة 16 من قانون الإجراءات الجزائية[1]، فإن ضباط الشرطة القضائية يمارسون مهامهم داخل نطاق اختصاصهم المحلي والذي يتمثل في تلك الحدود أو الحيز الجغرافي الذي يمارسون ضمنه وظائفهم المعتادة.

غير أنه وبحسب نفس المادة 16 أعلاه يمكن تمديد اختصاص الشرطة القضائية ضمن الحالات والشروط التالية:

أ-تمديد الاختصاص المحلي ليشمل كل المجلس القضائي:

حيث نصت الفقرة الثانية من المادة 16 من قانون الإجراءات الجزائية الجزائري[2] على أنه "...إلا أنه يجوز لهم في حالة الاستعجال أن يباشروا مهمتهم في كافة دائرة اختصاص المجلس القضائي الملحقين به ...".

فالمشرع الجزائري إذن أجاز تمديد الاختصاص المحلي لضباط الشرطة القضائية ليشمل كل دائرة اختصاص المجلس القضائي الذي يباشرون مهامهم به، وذلك في حالة الاستعجال.

[1] المرجع نفسه.

[2] المرجع نفسه.

ب-تمديد الاختصاص المكاني ليشمل كافة الإقليم الوطني:

نصت الفقرة الثالثة من المادة 16 من قانون الإجراءات الجزائية الجزائري[1] على أنه "... ويجوز لهم أيضا في حالة الاستعجال أن يباشروا مهمتهم في كافة الإقليم الوطني إذا طلب منهم أداء ذلك من القاضي المختص قانونا ويجب أن يساعدهم ضابط الشرطة القضائية الذي يمارس وظائفهم في المجموعة السكنية المعنية...".

فبالإضافة لحالة الاستعجال، فإن هذا التمديد يحدث إذا طلب القاضي المختص قانونا ذلك من ضباط الشرطة القضائية، وبشرط أن يساعدهم في ذلك ضابط الشرطة القضائية الذي يمارس وظيفته في المجموعة السكنية المعنية.

بالنسبة لحالتي التمديد المذكورتين أعلاه، فلقد أضافت لهما الفقرة الرابعة من المادة 16 من قانون الإجراءات الجزائية الجزائري شرطا آخرا يتعين بموجبه على ضباط الشرطة القضائية أن يخبروا مسبقا وكيل الجمهورية الذي سوف يمارسون مهامهم داخل دائرة اختصاصه، فنصت على أنه "... وفي الحالات المنصوص عليها في الفقرتين السابقتين يتعين عليهم أن يخبروا مسبقا وكيل الجمهورية الذي يباشرون مهمتهم في دائرة اختصاصه...".

غير أنه وإذا تعلق الأمر بتلك الجرائم المذكورة بالفقرة السابعة من المادة 16 أعلاه، فإن اختصاص ضباط الشرطة القضائية يمتد إلى كافة الإقليم الوطني، حيث نصت الفقرة أعلاه على أنه "...غير أنه فيما يتعلق ببحث ومعاينة جرائم المخدرات والجريمة المنظمة عبر الحدود الوطنية والجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب والجرائم المتعلقة بالتشريع الخاص بالصرف يمتد اختصاص ضباط الشرطة القضائية إلى كامل الإقليم الوطني...".

ويتم ذلك تحت إشراف النائب العام للمجلس القضائي المختص إقليميا، مع ضرورة القيام بإعلام وكيل الجمهورية الذي سيباشرون مهامهم داخل دائرته، وذلك ما جاء بالفقرة

[1] المرجع نفسه.

الأخيرة من المادة 16 من قانون الإجراءات الجزائية الجزائري[1] التي نصت على أنه "... ويعمل هؤلاء تحت إشراف النائب العام لدى المجلس القضائي المختص إقليميا ويعلم وكيل الجمهورية المختص إقليميا بذلك في جميع الحالات...".

وأخيرا يجب الإشارة إلى أن الاختصاص المكاني لضباط الشرطة القضائية التابعين للأمن العسكري يمتد عبر كامل التراب الوطني دون الخضوع لتلك الأحكام الواردة بالفقرات 2 و3 و4 و5 من المادة 16 من قانون الإجراءات الجزائية الجزائري، وهذا ما نصت عليه الفقرة السادسة من المادة 16 من قانون الإجراءات الجزائية الجزائري بقولها "... لا تطبق أحكام الفقرات الثانية والثالثة والرابعة والخامسة من هذه المادة على ضباط الشرطة القضائية التابعين لمصالح الأمن العسكري الذين لهم الاختصاص على كافة الإقليم الوطني...".

المشرع الفرنسي تناول الأحكام المتعلقة بهذا الشق من الضبطية القضائية بالمواد من 20 إلى 29 من قانون الإجراءات الجزائية الفرنسي[2]، في حين تطرق إليها نظيره المصري بالمادتين 22 و23 وما يليهما من قانون الإجراءات الجنائية المصري[3].

ثانيا: الاختصاص النوعي

ويقصد به نوع الجرائم التي تدخل ضمن اختصاص أعضاء الضبطية القضائية، فيمكنهم ضبطها.

ينقسم هذا الاختصاص إلى صنفين، اختصاص نوعي عام وآخر خاص.

[1] المرجع نفسه.

[2] la loi n° 57-1426 instituant un code de procédure pénale, Op.cit. Modifié et complété.

[3] القانون رقم 150 لسنة 1950، المرجع السابق.

أ-الاختصاص النوعي العام:

ومن خلاله يمكن لضباط الشرطة القضائية مباشرة البحث والتحري في كافة أنواع الجرائم مهما كان وصفها، فيمكنهم جمع الأدلة بشأنها واتخاذ تلك الإجراءات الواجب اتخاذها إذا تعلق الأمر بحالة تلبس.

ب-الاختصاص النوعي الخاص:

عكس الاختصاص النوعي العام، فإنه وفي حالة الاختصاص النوعي الخاص لا يمكن لأعضاء الضبطية القضائية ضبط سوى نوع معين من الجرائم محدد وفق القوانين. ونجد بأن الفئة المقيدة بهذا النوع من الاختصاص النوعي هي فئة محددة، ونذكر منها على سبيل المثال أعوان الجمارك ومفتشو العمل وأعوان الشرطة العمرانية، فهم معنيون بضبط نوع محدد من الجرائم تحددها قوانين تلك الوظائف التي ينتمون إليها عادة.

المطلب الثاني: الضبط القضائي المختص بالجريمة الإلكترونية

إن الجريمة الإلكترونية، وبما تحمله من ميزات تختلف عن الجريمة بمفهومها التقليدي، شكلت صعوبات جمة ألقت بظلالها على الجوانب القانونية لاسيما الإجرائية منها. وليس هذا فحسب، بل أن الجهات المختصة بالبحث والتحري وجمع الأدلة، وجدت نفسها عاجزة أمام الطابع اللامادي للجريمة الإلكترونية، مع ما يحمله ذلك من معوقات متعلقة بصعوبة الكشف عن الجاني الذي بإمكانه تنفيذ جريمته دون ترك آثار.

كما أن الأدلة يصعب جمعها داخل البيئة الافتراضية، أضف إلى ذلك ميزة السرعة في ارتكاب الجرائم الإلكترونية، هذه الأخيرة التي لا تعترف بالحدود الجغرافية للدول، فأصبح بإمكان أي مجرم إلكتروني وفي أية بقعة من العالم ارتكاب جريمة تكون الضحية أو الضحايا فيها على بعد آلاف الكيلومترات.

كل هذه الأسباب وضعت الدول أمام ضرورة إيجاد السبل لمواجهة الجريمة الإلكترونية، فكان لابد من تطوير تلك الأجهزة والسلطات المختصة بالضبط القضائي بشكل يجعلها

قادرة على مجاراة الإجرام الإلكتروني الذي وظف تلك التقنيات الحديثة واستغل التطور التكنولوجي في مجال الاتصالات من أجل تطوير أسلوبه الإجرامي.

لقد بادرت العديد من الدول إلى إنشاء سلطات مختصة، وإعداد قوات من شأنها التعامل مع الجريمة الإلكترونية بما في ذلك تطوير أجهزة الضبط القضائي من خلال إنشاء وحدات مختصة بالتحري وجمع الأدلة بخصوص الجريمة الإلكترونية، الأمر الذي يتطلب توفير إمكانيات بشرية متمثلة في رجال ضبطية قضائية يكونون على قدر عال من الكفاءة لمواجهة الجريمة الإلكترونية، هذه الكفاءة التي يمكن اكتسابها وبلوغها من خلال الإعداد والتدريب والتكوين المنصب على وسائل الاتصال الحديثة والتحكم في التقنيات الحديثة، بما فيها الحاسب الآلي وشبكات الإنترنت والهواتف الذكية وكل تلك الأدوات والوسائل التكنولوجية التي قد يستخدمها المجرم الإلكتروني لتنفيذ جرائمه.

من أجل ذلك تم إنشاء شرطة متخصصة لمواجهة هذا الإجرام المستحدث أطلق عليها مصطلحات مختلفة ولكنها متقاربة: "كشرطة الإنترنت (Cyber police) "أو (Police de net) أو" درك الإنترنت (Cyber Gendarme)" أو" دورية شرطة الإنترنت-Cyber) " (patrouille أو" متحري الإنترنت (Cyber detective) " أي أصبح هناك وجود للشرطة بالعالم الافتراضي الإنترنت، بحيث تمارس مهامها من خلال ضبطية قضائية مختلفة تماما عن تلك التي تقوم بالكشف عن الجرائم التقليدية، لكونها لا تعتمد على التدريبات المادية أو الفيزيولوجية التي يتلقاها رجال الشرطة للوصول إلى هذه المرتبة، وإنما تعتمد على قوة تكوين البناء العلمي والتكنولوجي لأفرادها. وهي تتولى في ذلك مهمة مباشرة جمع الاستدلالات والتحري في العالم الافتراضي، من أجل كشف النقاب عن هذا النوع المتميز من الإجرام. كما يمكنها أن تطارد الهكرة ومخترقي الأنظمة على كافة المستويات[1].

من خلال هذا المطلب سنحاول التعرف على ردة فعل الدول إزاء الجريمة الإلكترونية، وذلك فيما يخص الجانب المتعلق بالضبطية القضائية والأجهزة المكلفة بالبحث والتحري

[1] نبيلة هبة هروال، مرجع سابق، ص99 و100.

ومساعدة جهات التحقيق من أجل جمع الأدلة وكشف الحقيقة من خلال التوصل إلى الجناة.

من أجل ذلك، سوف نبحث في هذا الموضوع من خلال شقين أو قسمين، الأول نخصصه للضبطية القضائية المختصة بالجريمة الإلكترونية على المستوى الوطني، في حين يكون القسم الثاني للنظر في الضبطية القضائية المختصة بالجريمة الإلكترونية على المستوى الإقليمي والدولي.

الفرع الأول: الضبطية القضائية المختصة بالجريمة الإلكترونية على المستوى الوطني

قررت العديد من الدول إنشاء أجهزة تتولى البحث والتحري وجمع الاستدلالات فيما يتعلق بالجريمة الإلكترونية، بحيث تكون بمثابة عون وسند لجهات التحقيق في الجريمة الإلكترونية. وكمثال على تلك الدول التي بادرت بإنشاء هذه السلطات على المستوى الوطني نذكر كل من الولايات المتحدة الأمريكية وفرنسا، كما سنتطرق لما هو عليه الوضع في كل من الجزائر ومصر.

أولا: الوضع في الولايات المتحدة الأمريكية

إن الولايات المتحدة الأمريكية باعتبارها الدولة الأكثر تطورا من حيث التكنولوجيا لاسيما في مجال الاتصالات، ونظرا لكونها كانت السباقة في استعمال شبكة الإنترنت كونها تعتبر مهد هذه التقنية والتكنولوجيا المتطورة في عالم الاتصالات، فإنه من المنطقي أن تكون من أول الدول التي واجهت الجريمة الإلكترونية.

كل هذا، دفع المشرع الأمريكي إلى استحداث أكثر من جهاز من أجل مواجهة الجرائم الإلكترونية لاسيما ما تعلق منها بالبحث والتحري ومساعدة جهات التحقيق، ونعني بها كل ما يعد من ضمن أعمال الضبطية القضائية.

ففي سنة 1991 تم إنشاء وحدة لمكافحة جرائم الحاسوب وجرائم حقوق الملكية الفكرية التابعة لوزارة العدل الأمريكية، وتطورت تلك الوحدة في وقت لاحق وتحديدا عام 1996

هذا ولقد تم إنشاء قسم لمتابعة الجرائم الإلكترونية ويعتبر واحد من ضمن عدة أقسام يضمها مكتب التحقيقات الفيدرالي (FBI) الذي يأتي في مقدمة الأجهزة المعنية بمحاربة الإرهاب الإلكتروني أو الإرهاب عبر الإنترنت.

إلى جانب هذه الأجهزة تم إنشاء مركز يختص بتلقي الشكاوى المتعلقة بجرائم الاحتيال عبر الإنترنت (IFCC) أو (Internet Fraud Complaint Center) والذي تم تعديل تسميته لاحقا في أكتوبر 2003 ليصبح (IC3) وهي اختصار للعبارة (Internet Crime Complaint Center) أي مركز معالجة الشكاوى المرتبطة بجرائم الإنترنت (IC3) والذي من اختصاصاته تلقي تلك الشكاوى التي تصله وتحليلها لتحديد نوع ودرجة ذلك الإجرام، أو بمعنى آخر للتأكد من ذلك الإجرام وتقييمه، لإرساله بعد ذلك إلى السلطات القضائية المختصة بالبحث والتحري. هذا إلى جانب المركز الوطني لجرائم الياقات البيضاء (NW3C) يهتم كذلك بمحاربة الاحتيال عبر الإنترنت بحيث يمكن للضحايا تقديم شكاويهم من خلال الموقع الإلكتروني (www.ic3.gov)[1].

ثانيا: الوضع في فرنسا

أنشأت فرنسا عدة وحدات ومراكز متخصصة ضمن الشرطة والدرك الوطني لمكافحة الإجرام الإلكتروني بجميع صوره، مما يعد استجابة لما دعت إليه الاتفاقية الأوربية للجرائم الإلكترونية[2] المنعقدة ببودابست 2001 والتي انضمت إليها فرنسا ضمن ثلاثة وأربعين دولة أوربية الأعضاء في المجلس الأوربي[3].

[1] لمزيد من المعلومات حول هذه الأجهزة، يمكن الاطلاع أو تحميل الوثيقة بالرابط (متاح بتاريخ 2019/08/04):
https://www.ic3.gov/Media/PDF/AnnualReport/2011_IC3Report.pdf

والرابط:

https://www.hstoday.us/subject-matter-areas/cybersecurity/the-fbis-internet-crime-complaint-center-ic3-marks-its-20th-year/

كما يمكن الاطلاع عليها عبر موقع (Wikipedia) على الرابط (متاح بتاريخ 2019/12/14):
https://en.wikipedia.org/wiki/Internet_Crime_Complaint_Center

[2] Convention de Budapest du 21 novembre 2001, Op.cit.

[3] عمر محمد أبو بكر بن يونس، الاتفاقية الأوربية حول الجريمة الافتراضية، المذكرة التفسيرية، بدون ناشر، 2005، ص4.

المذكور أعلاه، قيامها بعمليات المتابعة الفنية للجرائم الإلكترونية والتحري عنها وعن الجرائم التي تبلغ إليها سواء من الأشخاص أو من الإدارات الأخرى، وكذا مكافحة وضبط الجرائم التي تقع باستخدام الحاسبات وعلى نظم شبكات المعلومات وقواعد البيانات، كبث الفيروسات وعمليات الاختراق للأنظمة وللشبكات، واتخاذ الإجراءات القانونية حيالها[1].

الفرع الثاني: الضبطية القضائية المختصة بالجريمة الإلكترونية على المستوى الإقليمي

إلى جانب تلك الجهود المبذولة من طرف الدول على المستوى الداخلي لكل دولة، من خلال إنشاء أجهزة لمكافحة الإجرام الإلكتروني ومنح هذه الأجهزة سلطات للضبط القضائي، تماشيا مع طبيعة الجريمة الإلكترونية، فهناك مجموعة أخرى من الدول لم تكتف بتقوية السلطات الداخلية لها وإنما قامت كذلك بتوحيد جهودها من خلال إنشاء أجهزة إقليمية إدراكا منها لمخاطر الجريمة الإلكترونية بوصفها جريمة عابرة للحدود.

ولعل أبرز مثال لتلك التجمعات على المستوى الأوربي يتمثل في جهازين وهما مركز الشرطة الأوربية (الأوروبول–Europol) منظمة التعاون القضائي للاتحاد الأوروبي (الأورجست – Eurojust). أما على المستوى الإفريقي نجد آلية الاتحاد الإفريقي للتعاون الشرطي (أفريبول – Afripol) كما نجد على المستوى الأسيوي رابطة دول جنوب شرق أسيا (الأسيانابول – ASEANAPOL) إلى غير ذلك من التجمعات على المستوى الإقليمي والتي سوف نستعرضها كالآتي:

أولا: مكتب الشرطة الأوربية (الأوروبول– Europol)

يعتبر المستشار الألماني (Helmut Kohl)* أول من أطلق فكرة إنشاء مكتب الشرطة الأوروبي سنة 1991، ثم جاءت بعد ذلك معاهدة الاتحاد الأوربي والمعروفة كذلك بمعاهدة (Maastricht)[2] والتي نصت صراحة على إنشاء هذا الجهاز. حيث تمت الموافقة

[1] لمزيد من المعلومات حول هذا الهيئة وأعمالها راجع: محمد كمال شاهين، مرجع سابق، ص152 و153.

* معلومات أكثر حول هذه الشخصية على الرابط (متاح بتاريخ 2018/09/29 الساعة 22:15):
https://en.wikipedia.org/wiki/Helmut_Kohl

كما يعمل هذا الجهاز على تسهيل تبادل المعلومات المتعلقة بالأنشطة الإجرامية عن طريق تزويد المحققين بتحاليل عملية واستراتيجية وتزويدهم بمساعدات التقنية وبالتالي يكون للأوربول دور فعال في مكافحة الإجرام الإلكتروني، ومساعدة سلطات التحقيق للقيام بعملها بإمدادها بالمعلومات والبيانات اللازمة لذلك[1].

ثانيا: منظمة التعاون القضائي للاتحاد الأوروبي (الأورجست – Eurojust)

تم إنشاء منظمة التعاون القضائي للاتحاد الأوروبي **(Eurojust)** من طرف مجلس الاتحاد الأوربي وذلك بموجب القرار[2] الصادر بتاريخ 2002/02/28، وقد لعبت المبادرة الألمانية دورا بارزا في نشأة هذه المنظمة وذلك من خلال الاقتراح الذي تقدمت به والذي يهدف أساسا إلى إنشاء جهاز يسمح للهيئات الوطنية المكلفة بالتحقيقات من الحصول على المعلومات ذات الصلة بالتحقيقات الجارية. ومن أبرز الأهداف التي تسعى إليها هذه المنظمة تقوية التعاون في مواجهة كافة الأشكال الخطيرة للجريمة المنظمة وتنسيق جهود جهات التحقيق الجنائي في مختلف الجرائم بما في ذلك الجرائم الإلكترونية.

ثالثا الأسيانابول:

(رابطة رؤساء أجهزة الشرطة التابعة لرابطة أمم جنوب شرق آسيا–ASEANAPOL)

بتاريخ 1967/08/08 تم تأسيس رابطة دول جنوب شرق أسيا[3] والتي تسمى اختصار بالآسيانا أو ASEANA (The Association of Southeast Asian Nations) وتضم

---

[1] أنظر كذلك في هذا الصدد كل من: جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002، ص 79. شريف سيد كامل، الجريمة المنظمة في القانون المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001، ص 72 وما بعدها. أشارت إليه نبيلة هبه هروال، المرجع السابق، ص 158.

[2] Décision du Conseil 2002/187/JAI du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JOCE N° L 63/1, 06/03/2002.(modifiée par le règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil).

معلومات أكثر بالموقع الرسمي الخاص بتشريعات الاتحاد الأوربي بالروابط التالية:

- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=LEGISSUM%3Al33188
- https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32018R1727&qid=1606932541304

[3] تم ذلك بالعاصمة التايلاندية بانكوك، ولهذا يطلق عليه كذلك تسمية "إعلان بانكوك". حيث ضم آنذاك الدول الخمس المؤسسة له (تايلند، اندونيسيا، الفلبين، ماليزيا، سنغافورة) ثم انضمت لاحقا كل من بروناي سنة 1984، فيتنام سنة 1995، لاوس وميانمار سنة 1997، وأخيرا كمبوديا سنة 1999. مزيد من المعلومات حول نشأة وأهداف الآسيانا

وفي هذا الاتجاه دائما، وسعيا منها إلى تكثيف التعاون الإقليمي فيما بينها وتطوير قدراتها من أجل مكافحة الجريمة الإلكترونية لاسيما في موضوع التحقيقات عمدت رابطة دول جنوب شرق أسيا إلى تقييم قدرات كل دول طرف في الرابطة على كشف الجريمة الإلكترونية والتحقيق فيها، ليتم فيما بعد التركيز على تقديم تدريب متخصص يتعلق بشبكة الإنترنت وتحليل البرمجيات الخبيثة لما له من أهمية في موضوع التحقيق في الجرائم الإلكترونية، وتم تتويج ذلك بتبادل للمعلومات المتعلقة بالتحقيقات السيبرانية وذلك من خلال ورشات عمل[1] ركزت على آليات تحديد الأدلة الرقمية والحصول عليها بشكل قانوني وكذا الإجراءات المتعلقة بجمعها وحفظها.

رابعا: آلية الاتحاد الافريقي للتعاون الشرطي (أفريبول –Afripol):

تعتبر الأفريبول مؤسسة تقنية شرطية وتهدف هذه الهيئة الإقليمية في المقام الأول إلى تعزيز وترقية التعاون بين أجهزة الشرطة للدول الأعضاء بالاتحاد الإفريقي، وذلك من أجل مكافحة الجريمة بكافة أشكالها بما فيها الجريمة الإلكترونية. تعود فكرة إنشاء آلية الاتحاد الإفريقي للتعاون الشرطي أو ما يعرف بالأفريبول (Afripol) إلى المبادرة التي طرحتها الجزائر بمناسبة احتضانها للمؤتمر الإفريقي الإقليمي الثاني والعشرون للمنظمة الدولية للشرطة الجنائية وذلك في الفترة الممتدة ما بين 10 و12 سبتمبر 2013 بمدينة وهران. وبتاريخ 30 يناير 2017 تجسدت هذه الفكرة على أرض الواقع من خلال إقرار النظام الأساسي الخاص بآلية الاتحاد الإفريقي للتعاون الشرطي، وفي شهر ماي من العام ذاته انعقدت الجمعية العامة الأولى للأفريبول وتم انتخاب الجزائر لرئاسة هذه المنظمة

[1] سنة 2017 تم تنظيم حلقة عمل موجهة إلى أجهزة إنفاذ القانون والسلطات القضائية بشأن الحصول على معلومات تتعلق بالتحقيقات في الجرائم السيبرية في العديد من البلدان. وجمعت حوالي 30 مشاركا لبحث آليات تحديد الأدلة الرقمية والحصول عليها بشكل قانوني وفعال، والنظر في الصعوبات المتصلة بذلك. وقد أسهم مدربون من وزارة العدل في الولايات المتحدة في حلقة العمل هذه. كما نظمت حلقة عمل سنة 2018 شملت تمرينا بالمحاكاة يستند إلى سيناريوهات تتعلق بالتحديات التي تعترض بلدان متعددة وتبادل الاطلاع على أفضل الممارسات. وجرى توسيع نطاق حلقة العمل هذه أيضا ليشمل مشاركين من 12 بلدا من أمريكا الجنوبية وأفريقيا وآسيا والمحيط الهادئ، الأمر الذي أتاح فرصة فريدة للإلمام= =بالتحديات وأفضل الممارسات من خارج منطقة ASEAN. وأسهم مدربون من قوات الشرطة في هونغ كونغ وسنغافورة في هذا التمرين.

راجع الرابط التالي (متاح بتاريخ 2018/10/23 الساعة 22:35) https://www.interpol.int/ar/4/6/3/1

المؤتمر[1] العربي السادس عشر لرؤساء أجهزة المباحث والأدلة الجنائية من خلال دعوته للدول الأعضاء في المجلس إلى:

- القيام بالتحديث المستمر للتشريعات الوطنية الخاصة بالجرائم الإلكترونية من خلال لجان قانونية وفنية متخصصة، بما يضمن مواكبة المستجدات في عالم الجريمة الإلكترونية.
- تفعيل تطبيق بنود الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وخاصة فيما يتعلق بتكثيف التعاون وتبادل الخبرات بين الأجهزة المختصة في مجال مكافحة الجرائم الإلكترونية، وتكثيف عقد المؤتمرات وورش العمل لمواكبة التطورات في هذا المجال.
- تعزيز تبادل الخبرات والمعارف بشكل دائم بين الأجهزة الأمنية المعنية والقطاع الخاص المختص في مجال الجريمة الإلكترونية، ومع الشركات المقدمة لخدمات الاتصال، وشبكات التواصل الاجتماعي بهدف المساعدة في الحد من إساءة استخدامها في ارتكاب الجرائم الإلكترونية، وكذلك الأمر مع كافة المنظمات والمؤسسات الدولية المعنية بمواجهة الجرائم الإلكترونية.
- ضرورة زيادة مستوى الدعم المقدم إلى الأجهزة المعنية بمكافحة الجريمة الإلكترونية لتطوير تجهيزاتها ورفع قدرات عناصرها للارتقاء بمستوى مكافحة الجريمة والتصدي لها.

[1] بيان صادر عن الأمانة العامة لمجلس وزراء الداخلية العرب بمناسبة اختتام أعمال المؤتمر العربي السادس عشر لرؤساء أجهزة المباحث والأدلة الجنائية المنعقد بتونس بتاريخ 2017/05/18. منشور بالموقع الرسمي لمجلس وزراء الداخلية العرب بالصفحة الخاصة بأخبار الأمانة العامة على الرابط: (متاح بتاريخ 2018/08/02 الساعة 07:30) https://www.aim-council.org/news/secretariat-news/1023/

* كما وافق المؤتمر على تشكيل فريق خبراء عرب من المختصين في المجالات الأمنية والقانونية والفنية وسائر الجهات المعنية لمواجهة الجرائم الإلكترونية. وطلب المؤتمر من الأمانة العامة للمجلس إصدار نشرة دورية بالمواقع والحسابات الإلكترونية التي ثبت تورطها في جرائم إلكترونية وفي ممارسة الاحتيال الإلكتروني، أو الاستغلال الجنسي أو الإيقاع بمستخدمي الإنترنت لابتزازهم، أو غيرها من المواقع التي تمارس الإجرام الإلكتروني بمختلف أشكاله. وذلك بهدف التوعية بخطورة هذه المواقع واتخاذ الإجراءات اللازمة لحجبها، ووضع الدول التي تمارس هذه الأنشطة الإجرامية الإلكترونية على أراضيها أمام مسؤولياتها في ضبطها والتصدي لها.

- رفع مستوى التوعية بالاستخدام الآمن لوسائل تقنية المعلومات والإنترنت بين كافة شرائح المجتمع وصولا إلى "أمن معلوماتي عربي شامل"

كما أوصى المؤتمر بإنشاء:

- آلية للتواصل بين الوحدات المعنية بمكافحة الجرائم الإلكترونية على المستوى العربي بما يحقق التواصل المباشر فيما بينها ويضمن انسيابية تبادل المعلومات والخبرات ورصد هذه الجرائم والمستجد منها لمحاصرتها بفاعلية أكبر وملاحقة مرتكبيها، وإصدار التحذيرات اللازمة بشأن الهجمات الإلكترونية الوشيكة والتوعية بأساليب الوقاية منها.
- مركز عربي متخصص للبحوث العلمية الرقمية بهدف تحليل الفيروسات والتصدي لها، وإجراء الدراسات اللازمة لمواجهة المد المتنامي من الجرائم والهجمات الإلكترونية في المنطقة العربية.

ونشير في الأخير إلى أن مجلس وزراء الداخلية العرب يواصل باستمرار التنسيق مع الهيئات الإقليمية الأخرى وكذلك مع المنظمة الدولية للشرطة الجنائية "الإنتربول".

وكأمثلة على ذلك نذكر[1]:

- اجتماع رؤساء أجهزة الشرطة في منطقة الشرق الأوسط وشمال إفريقيا بمدينة ليون الفرنسية بتاريخ 2017/11/21، والذي انعقد بمقر المنظمة الدولية للشرطة الجنائية "الإنتربول". وذلك في إطار تعزيز الجهود التي يبذلها الإنتربول من خلال توفير معلومات محدثة عن القدرات الشرطية العالمية للإنتربول في إطار كل برنامج من

[1] من صفحة الأخبار للأمانة العامة بمجلس وزراء الداخلية العرب على الرابطين: (متاحين بتاريخ 2018/08/02 الساعة 09:45)

- https://www.aim-council.org/news/secretariat-news/1095/
- https://www.aim-council.org/news/secretariat-news/1041/

يضاف إلى ما سبق، ما تضمنه مقترح استراتيجية دول المجلس لمكافحة الجريمة الإلكترونية (2015-2024) والذي يهدف إلى تشكيل فرق متخصصة تضم ضباط خبراء في تشخيص وتصنيف الهجمات المتعلقة بالجرائم الإلكترونية. كما يعمل المجلس على تزويد الأجهزة الضبطية بالإمكانيات المادية والبشرية (الخبرات، التدريب، التقنيات والوسائل العلمية الحديثة الكافية) من أجل تمكينها من أداء مهامها بفاعلية. كما تسعى وفي إطار التعاون الإقليمي والدولي إلى تنسيق الجهود والتعاون مع المؤسسات العالمية المهتمة بالجريمة الإلكترونية كمركز "مايكروسوفت لمكافحة الجرائم الإلكترونية" وهو مركز متخصص يعمل على تطوير أساليب مواجهة الجرائم الإلكترونية، ويضم خبراء من شركة مايكروسوفت في المجالات القانونية والتقنية، بالإضافة إلى أحدث الأدوات والتقنيات في هذا المجال، مع ضرورة السعي لإيجاد فرع للمركز في دول مجلس التعاون. وكذلك التعاون مع مبادرات تنظيم الشبكة العنكبوتية ومحاربة الجرائم الإلكترونية كاتفاقية المجلس الأوروبي بشأن الجريمة الإلكترونية وقرارات الأمم المتحدة في منع جرائم الكمبيوتر ومكافحتها، وخطة عمل مؤتمر الدول الصناعية الثمانية (G8) وهي (ألمانيا، إيطالي، روسيا، فرنسا، كندا، المملكة المتحدة، الولايات المتحدة واليابان)، وجهود الاتحاد الدولي للاتصالات بشأن توحيد آليات تطوير تطبيقات تكنولوجيا المعلومات والاتصالات.[1]

ولقد توجت جهود مجلس التعاون لدول الخليج العربية بإنشاء جديد وهو "جهاز الشرطة الخليجية"[2]ومن بين أهداف هذا الجهاز:

---

[1] بحث بعنوان "الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها" من إعداد مركز المعلومات الوطني لوزارة الداخلية السعودية، 2016، ص65-67. منشور بالموقع الرسمي لمجلس التعاون لدول الخليج العربي على الرابط: (متاح بتاريخ 2017/05/4 الساعة 23:15)

https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/ - البحوث الأمنية/الجريمة الالكترونية السعودية.pdf

[2] كان ذلك بمناسبة لقائهم التشاوري الخامس عشر الذي انعقد بدولة الكويت بتاريخ 2014/04/30 حيث قرر وزراء داخلية دول مجلس التعاون إنشاء جهاز الشرطة الخليجية (GCCPOL) ومقره العاصمة الإماراتية أبو ظبي. أنظر (المسيرة والإنجاز، الطبعة العاشرة، 2016) بالمكتبة الرقمية (باب مسيرة مجلس التعاون) للموقع الرسمي لمجلس التعاون لدول الخليج العربي على الرابط: (متاح بتاريخ 2017/05/5 الساعة 09:27):

https://www.gcc-sg.org/ar-sa/CognitiveSources/DigitalLibrary/Lists/DigitalLibrary/مسيرة مجلس التعاون/MASSERA2016_pro.pdf

على مستوى العالم. وتظهر أهمية الإنتربول من خلال ذلك الدعم الذي يقدمه للدول الأعضاء فيما يتعلق بالجريمة الإلكترونية خاصة في مجال التحقيقات.

ويأتي دعمه للتحقيقات في الجريمة الرقمية[1] للبلدان الأعضاء لتنسيق وتيسير التحقيقات في الجرائم السيبرية عبر الوطنية وعملياتها. ويتم توفير الدعم المذكور سواء عن بعد أو بعين المكان. وقد يتضمن الدعم عن بعد تسهيل تبادل المعلومات أو بيانات الاستخبار من خلال تنظيم اجتماعات تجري عن بعد أو تقديم التوجيهات والمشورة فيما يتعلق بأفضل الممارسات في مجال التحقيقات في الجريمة الرقمية.

وتبعا لمتطلبات البلد العضو، قد يسافر الموظفون إلى موقع الحادثة لتوفير الدعم الميداني في تنسيق عمل الخبراء المعنيين. ويمكن أيضا للإدارة الفرعية لدعم التحقيقات في الجريمة الرقمية أن تجتمع مع أجهزة إنفاذ القانون في البلدان الأعضاء، فضلا عن هيئات القطاع الخاص والأوساط الأكاديمية عند الاقتضاء، لتيسير التحقيقات المشتركة.

وتركز الإدارة الفرعية بشكل رئيسي على مكافحة الجريمة السيبرية المتصلة بالبرمجيات الخبيثة والجهات المتطورة التي تسهّل ارتكاب هذه الجريمة، كالشركات المتساهلة في استضافة المواقع الإلكترونية، والشركات المحترفة لتحويل الأموال.

وتقوم الاستراتيجية الشاملة لمكافحة الجريمة السيبرية[2] للإنتربول على خمسة مسارات عمل تهدف كلها إلى مساعدة البلدان الأعضاء على الكشف عن الاعتداءات السيبرية وعن مرتكبيها، ومسارات العمل هذه هي التالية:

1-تقييم التهديدات وتحليلها ورصد اتجاهاتها، بحيث يتم الكشف عن الجرائم السيبرية ومرتكبيها والمجموعات التي تقف وراءها من خلال تقييم التهديدات وتحليلها ورصد اتجاهاتها، والتوصل إلى نتائج مؤكدة في هذا الشأن.

[1] انظر وثيقة بعنوان "دعم التحقيقات في الجريمة الرقمية" من ضمن وثائق الإنتربول منشورة سنة 2017 شهر مارس بالموقع الرسمي للإنتربول https://www.interpol.int .

[2] انظر وثيقة بعنوان "الاستراتيجية الشاملة لمكافحة الجريمة السيبرية " من ضمن وثائق الإنتربول، منشورة سنة 2017 شهر فبراير بالموقع الرسمي للإنتربول https://www.interpol.int

الباب الأول: الجهات المتصلة بالتحقيق الابتدائي في الجريمة الإلكترونية

سعينا من خلال هذا الباب الأول من دراستنا إلى التعرف على تلك الجهات المتصلة بالتحقيق الابتدائي في الجريمة الإلكترونية، فقسمنا هذا الباب إلى فصلين فأفردنا الفصل الأول للحديث عن تلك الجهة المناط بها التحقيق الابتدائي في الجريمة الإلكترونية حيث بادرنا إلى عرض مفهوم التحقيق الابتدائي، ثم حاولنا تحديد الجهة المختصة بالتحقيق الابتدائي في بعض التشريعات الجنائية المقارنة. وبعد ذلك انتقلنا إلى الخوض في مسألة الاختصاص القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية سواء على المستوى الوطني والذي حصرناه في المشرع الجزائري ثم ألقينا نظرة على الاختصاص القضائي بالتحقيق الابتدائي في الجريمة الإلكترونية على المستوى الدولي.

أما الفصل الثاني من هذا الباب فخصصناه لتوضيح صلة الضبطية القضائية بالتحقيق الابتدائي في الجريمة الإلكترونية، كما سعينا إلى تسليط الضوء على دور هذا الجهاز على المستوى الوطني لدى بعض الدول، لننتقل فيما بعد إلى عرض بعض الأمثلة لأجهزة الضبطية القضائية على المستوى الإقليمي وإسهامها في موضوع التحقيق الابتدائي المتعلق بالجريمة الإلكترونية.

وختمنا هذا الباب بإبراز دور الإنتربول باعتباره يمثل الضبطية القضائية المختصة بالتحقيق الابتدائي في الجريمة الإلكترونية على المستوى الدولي.

الباب الثاني:

الجوانب الإجرائية للتحقيق الابتدائي في الجريمة الإلكترونية

الفصل الأول: الصعوبات التي تواجه إجراءات التحقيق الابتدائي في الجريمة الإلكترونية

الفصل الثاني: إجراءات جمع الأدلة في الجريمة الإلكترونية

تمهيد وتقسيم

يهدف التحقيق الابتدائي في الجريمة الإلكترونية إلى وضع اليد على تلك الأدلة التي تفيد في كشف الحقيقة وذلك عبر مجموعة من الإجراءات، غير أن سعي جهات التحقيق نحو كشف الجرائم والوصول إلى الجناة تعترض سبيله العديد من الصعوبات.

أشرنا سابقا بأن إجراءات التحقيق الابتدائي تضم نوعين من الإجراءات، النوع الأول يخص تلك الإجراءات التي تهدف إلى جمع الأدلة وهذا هو النوع الذي نهتم به في بحثنا. في حين أن النوع الثاني من الإجراءات هي تلك التي ترمي إلى تأمين الأدلة من خلال اتخاذ إجراءات احترازية ضد المتهم، وهذا النوع الثاني من الإجراءات لا يدخل ضمن نطاق بحثنا.

وعلى هذا الأساس قسمنا هذا الباب الثاني من الدراسة الحالية إلى فصلين، حيث خصصنا الفصل الأول للخوض في جملة التحديات والصعوبات التي تواجه وتعيق جهود جهات التحقيق، سواء ما ارتبط منها بالعنصر البشري، أو بالدليل الإلكتروني في حد ذاته أو بالإشكالات التي أفرزها بموضوع الخصوصية المعلوماتية وكذلك تلك الصعوبات التي يشهدها التعاون الدولي في مجال التحقيق في الجريمة الإلكترونية.

فيما عرضنا بالفصل الثاني جملة الإجراءات التي تستهدف جمع الأدلة في الجريمة الإلكترونية، والذي من شأنه أن يوصل جهات التحقيق إلى الجناة في عالم الإجرام الإلكتروني. هذه الإجراءات ضمت طائفة من الجوانب الإجرائية تنتمي إلى مجموعة أو فئة الإجراءات التقليدية (الانتقال إلى مسرح الجريمة ومعاينته، التفتيش، الضبط، الخبرة، الشهادة). فيما خصصت المجموعة أو الفئة الثانية لما يسمى أو يوصف بالإجراءات الحديثة المتبعة من طرف جهات التحقيق من أجل استخلاص الدليل في الجريمة الإلكترونية (التسرب، مراقبة الاتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير).

الفصل الأول الصعوبات التي تواجه إجراءات التحقيق الابتدائي في الجريمة الإلكترونية

لطالما واجهت جهات التحقيق صعوبات جمة أثناء سعيها لكشف خيوط الجريمة، سواء تعلقت هذه الصعوبات بشخص الجاني أو المجني عليه أو بالأدلة المرتبطة بالجريمة أو بجهات التحقيق أو لأسباب إجرائية تتعلق بإجراءات وجب التقيد بها خشية خرق ما يسمى بالشرعية الإجرائية التي قد ينجم عنها بطلان الدليل وكذا انتهاك الخصوصية، أو نظرا لقصور هذه الإجراءات وعدم ملائمتها لمواجهة جريمة من الجرائم.

هذه الصعوبات ازدادت بل وتضاعفت في ظل الجريمة الإلكترونية نظرا للميزات التي انفردت بها طبيعة الجريمة الإلكترونية مقارنة بالجريمة التقليدية، فالمجرم الإلكتروني أصبح أكثر فتكا بالضحايا ومقدرة على التخفي، كما أن الدليل الإلكتروني استعصى أكثر فأكثر، ناهيك عن تحدي اكتساب الكفاءة الذي يؤرق جهات التحقيق بغية مجاراة المجرم الإلكتروني، ومتطلبات حماية الخصوصية المعلوماتية وهو الأمر الذي وضع جهات نفاذ القانون بصفة عامة، وجهات التحقيق بصفة خاصة في وضع شديد التعقيد خاصة إذا أخذنا بعين الاعتبار البعد الدولي للجريمة الإلكتروني وهو ما يفرض ضرورة التعاون بين الدول وهي الغاية التي لا يمكن بلوغها وتحقيقها دائما فأضحت بدروها عاملا زاد من الصعوبات التي تواجه جهات التحقيق في الجريمة الإلكترونية.

من خلال ما سبق ذكره، يمكننا إيجاز تلك الصعوبات التي تجابه وتواجه جهات التحقيق في الجريمة الإلكترونية إلى صعوبات مرتبطة بالدليل الإلكتروني وأخرى لها علاقة بالعامل البشري متمثلا في شخص الجاني والمجني عليه والقائم على التحقيق أو جهات التحقيق، كما أن هذه الصعوبات تمتد لتشمل كذلك ما يسمى بالخصوصية المعلوماتية وبقواعد إجرائية ولو أن هذه الأخيرة قد تتداخل بشكل أو بآخر مع جل أو كل هذه الصعوبات التي تحدثنا عنها. يضاف إلى ذلك تلك الصعوبات التي يشهدها مجال التعاون الدولي بخصوص التحقيق في الجرية الإلكترونية.

بروتوكول الإنترنت(IP)[1]. غير أن الواقع أثبت في كثير من الحالات بأن كل هذا غير مجدي دائما، فالهاتف قد يتعرض للسرقة أو الضياع وتنفذ الجريمة من خلاله قبل التبليغ عن ذلك وفي هذه الحالة فإن شخص الجاني ليس هو مالك شريحة الاتصال، كما أن البريد الإلكتروني قد يتم اختراقه أو سرقة كلمة الدخول الخاصة به.

فعنوان (IP) الذي يشير إلى رقم يعين الحاسوب الموصول على الإنترنت إنما يفيد حال التوصل إلى الرقم الذي يحدد هوية الحاسوب الذي استخدم في ارتكاب الجريمة، ولكن في مقابل ذلك فإن هذا الرقم ليس موحد على المستوى العالمي. ففي الولايات المتحدة أو كندا وبعض الدول الأخرى يمكن للشخص فيها اقتناء(IP) خاص به يشير إلى كونه أحد أعضاء الأنترنت ومن ثم يمكن تحديد هذا الشخص من أجل التحقيق معه لاحقا، غير أن مصداقية الهوية عبر الإنترنت (IP)تتقلص في دول أخرى كما هو حال الدول العربية كون كل خط هوية على الإنترنت يصادفه عدد من الهويات. وللتوضيح أكثر فإن المتصل بالإنترنت في الجزائر مثلا يمنح رقما محددا له فور اتصاله بالإنترنت، إلا أنه إذا حدث انقطاع للخدمة ثم عاد الشخص مجددا للاتصال بالأنترنت بعد ذلك، فإن الرقم الذي منح من قبل سوف يتغير ويصبح رقمه السابق لشخص آخر كما أنه قد يكون هو منح أو استفاد من رقم شخص آخر.[2]

كما قد يتم اختراق جهاز الكمبيوتر وارتكاب الجريمة الإلكترونية انطلاقا منه، أي اتخاذه كحصان طروادة أو كجسر من خلال الاستعانة ببرامج خبيثة، فيكون صاحب عنوان (IP) ليس هو مرتكب الجريمة. وكل هذه التعقيدات هي بمثابة صعوبات وعوائق تواجه جهات التحقيق.

[1] عنوان بروتوكول الإنترنت (بالإنجليزية: IP address) هو المعرف الرقمي لأي جهاز (حاسوب، هاتف محمول، آلة طابعة، موجه) مرتبط بشبكة معلوماتية تعمل بحزمة بروتوكولات الإنترنت، سواء أكانت شبكة محلية أو شبكة الشبكات الإنترنت. يقابل عنوان الآي بي مثلا في شبكات الهاتف رقم الهاتف. معلومات أكثر حول هذه التقنية على الرابط (متاح بتاريخ 2018/02/17 الساعة 20:55):
https://ar.wikipedia.org/wiki/عنوان_بروتوكول_الإنترنت

[2] أنظر في هذا المعنى: رشيدة بوكر، المرجع السابق، ص 475-476.

هذا وتجدر الإشارة إلى أن هناك حالات تكون فيها أجهزة تابعة لبعض الدول وراء الجرائم الإلكترونية والتي يتم فيها تحميل المسؤولية للدولة المعنية بدل السعي وراء تحديد الطاقم البشري المشكل لذلك الجهاز، غير أنه وفي الواقع فإن السواد الأعظم من الجرائم الإلكترونية يقترفها أفراد لا يمثلون أية جهة كما هو الحال في الجريمة التقليدية، كما أن العديد من الدول عمدت إلى تجنيد واستخدام أشخاص غير معتمدين بصفة رسمية للقيام لصالحها بمهام تعتبر في حقيقتها جرائم إلكترونية وذلك من أجل تفادي المسؤوليات أو العقوبات المحتملة التي قد يتسبب فيها إلقاء القبض على من تم تجنيدهم، بل قد يلجأ لهذا الأمر بعض الشخصيات المرموقة في المجتمع أو ذات المناصب السياسية أو غيرها من المناصب الحساسة بالمجتمع.

ونذكر كمثال في هذا الصدد قضية التواطؤ المحتمل بين روسيا والرئيس الأميركي دونالد ترامب بخصوص الحملة الانتخابية لهذا الأخير، فبحسب موقع صحيفة "ديلي بيست" الأميركية فإن روجر ستون المستشار السياسي للرئيس الأميركي دونالد ترامب، اعترف بتواصله المباشر عبر تويتر مع القرصان المعروف باسم (Guccifer 2.0)[1] في قضية التواطؤ المحتمل بين روسيا وحملة ترامب الانتخابية. وكان "غوتشيفر2.0" المشهور بلقب "القرصان المنفرد" قد ارتكب خطأ في اتصاله بالإنترنت أدى إلى كشفه وتحديد هويته، وأنه ضابط في إدارة الاستخبارات العسكرية الروسية نسب إليه الفضل في تزويد موقع ويكيليكس برسائل إلكترونية مسروقة من اللجنة الوطنية الديمقراطية. وذكر الموقع أن المحقق الخاص في قضية التدخل الروسي المحتمل في الانتخابات الأميركية روبرت مولر تولى التحقيق في ارتباط (Guccifer 2.0) بروسيا من جهة، وبحملة ترامب من جهة أخرى، مستعينا في ذلك بعملاء من مكتب التحقيقات الاتحادي الأمريكي (أف.بي.آي)[2].

[1] معلومات أكثر حول شخصية هذا القرصان على الرابط (متاح بتاريخ 2018/02/18 الساعة 19:32):
https://en.wikipedia.org/wiki/Guccifer_2.0

[2] ومن شأن الكشف عن هذه المعلومات أن يحمل آثارا جوهرية على التحقيق الجنائي في التواطؤ المحتمل بين الرئيس الأميركي دونالد ترمب وروسيا. يشار إلى أن هذا القرصان أقر بأنه اخترق موقع اللجنة الوطنية الديمقراطية في النصف الثاني من عام 2016، وعرّف نفسه آنذاك بأنه قرصان إنترنت روماني. مقال بعنوان "القرصان المنفرد يسقط أحد رجالات ترمب" منشور بالموقع الإلكتروني للقناة الإخبارية الجزيرة، متوافر بالرابط التالي:

المبحث الثاني: الصعوبات المرتبطة بالدليل الإلكتروني

في ظل تنامي الجريمة الإلكترونية خاصة مع انتشار استعمال الأجهزة الإلكترونية وشبكة الإنترنت، وجدت الجهات المكلفة بالتحقيق في الجريمة الإلكترونية نفسها أمام تحديات جمة، لعل أبرزها البيئة اللامادية والعالم الافتراضي الذي ترتكب داخله الجريمة الإلكترونية.

إن محاربة الجريمة بصفة عامة يقتضي الحصول على الأدلة التي تدين الجناة وتقود جهات التحقيق إلى كشف الحقيقة، ونظرا للطبيعة الخاصة للجريمة الإلكترونية فإنها أفرزت لنا مصطلحا جديدا ألا وهو "الدليل الإلكتروني" والذي يعبر عنه أحيانا باسم الدليل التقني أو الدليل الرقمي، أما في بحثنا هذا فإننا نميل إلى استخدام تسمية الدليل الإلكتروني التي تبناها المشرع الأوروبي في توصيته[1] المتعلقة بمشاكل الإجراءات الجنائية المتصلة بتكنولوجيا المعلومات، وذلك بتاريخ 1995/09/11 تحت رقم (95)13، كما أن تسمية الدليل الإلكتروني تتناسب مع الجريمة الإلكترونية، وسنحاول من خلال هذا المبحث إعطاء تعريف للدليل الإلكتروني و النظر في خصائصه وأنواعه، ثم نلقي نظرة عن تلك الصعوبات المتعلقة به.

المطلب الأول: تعريف الدليل الإلكتروني

المشرع الجزائري لم يعط تعريفا للدليل الإلكتروني، في حين نجد أن نظيره السوري على سبيل المثال قدم تعريفا من خلال المادة 01 من المرسوم التشريعي السوري رقم 12-17 المتعلق بتنظيم التواصل على شبكة الإنترنت والجريمة المعلوماتية[2]، إذ عرف الدليل الإلكتروني بأنه "البيانات الرقمية المخزنة في الأجهزة الحاسوبية أو المنظومات

[1] "IV. La preuve électronique

13. L'intérêt commun de recueillir, de sauvegarder et de présenter des preuves électroniques…"
Recommandation n° R(95)13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information adoptée le 11 septembre 1995. Consultation et téléchargement disponible via le lien (consulté le 28/10/2019):
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804e8ec8

[2] المرجع السابق.

المعلوماتية أو المنقولة بواسطتها، والتي يمكن استخدامها في إثبات أو نفي جريمة معلوماتية ".

أما لدى الفقهاء فلقد تعددت وتنوعت تلك التعريفات التي أعطيت للدليل الإلكتروني، فهناك من يعرفه بأنه " الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية ممكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة وهي مكون رقمي لتقديم معلومات في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات والأشكال والرسوم وذلك من أجل اعتماده أمام أجهزة إنفاذ وتطبيق القانون"[1].

ويعرف الدليل الإلكتروني بأنه " الدليل الذي يجد أساسا له في العالم الافتراضي ويقود إلى الجريمة، فهو ذلك الجزء المؤسس على الاستعانة بتقنية المعالجة الآلية للمعلومات"[2].

كما يعرف الدليل الإلكتروني بأنه "معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتم الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي وملحقاتها وشبكات الاتصال ويمكن استخدامها في أي مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء أو شخص له علاقة بجريمة أو جان أو مجني عليه"[3].

[1] ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، 2006، ص 88.

[2] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، مرجع سابق، ص 969.

[3] محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2014، ص 234.

المطلب الثاني: خصائص الدليل الإلكتروني

من خلال التعريفات السابقة للدليل الإلكتروني، ونظرا لطبيعة البيئة التي يتواجد فيها الدليل الإلكتروني، يبدو جليا أن الدليل الإلكتروني يتميز ويتصف بخصائص نوجزها فيما يلي:

الفرع الأول: الدليل الإلكتروني دليل علمي

يوصف بالدليل العلمي ذلك الدليل المتحصل عليه من الأجهزة والوسائل العلمية التي أقرها العلم الحديث والخبرات الإنسانية المتمثلة في الطب الشرعي وعلم النفس التجريبي، فهو ثمرة توظيف معطيات العلوم الحديثة في مجال الإثبات الجنائي مقربا بين العلم والقانون[1].

وهذه الصفة "علمي" تسري على الدليل الإلكتروني كما تسري على الدليل بمفهومه التقليدي. غير أن الدليل الإلكتروني ينفرد بميزة كونه غير ملموس وغير مادي، بحيث يتكون من بيانات ومعلومات إلكترونية ذات طبيعة غير ملموسة ويتطلب إخراجه في شكل مادي الاستعانة بالوسائل التكنولوجية الحديثة. لذلك فإن ما يطبق على الدليل العلمي يطبق على الدليل الإلكتروني.

فالدليل العلمي يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القانون المقارن مفادها بأن "القانون مسعاه العدالة أما العلم فمسعاه الحقيقة"، وإذا كان الدليل العلمي له منطقه الذي لا يجب أن يخرج عليه، إذ يستبعد تعارضه مع القواعد العلمية السليمة، فإن الدليل التقني له ذات الطبيعة، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه[2].

[1] محمد سعيد عتيق، النظرية العامة للدليل العلمي في الإثبات الجنائي، رسالة دكتوراه غير منشورة، كلية الحقوق، جامعة عين شمس، مصر، 1993، ص 98.

[2] عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، مرجع سابق، ص 977.

الحقيقة، فإن الدليل الإلكتروني يتميز على نظيره في الجريمة التقليدية بكونه قابلا للاسترجاع.

إضافة إلى ذلك، فإن محاولة الجاني التخلص من الدليل الإلكتروني تعد في حد ذاتها دليلا ضده، إذ أن هذا النشاط أو السلوك يتم تسجيله بذاكرة الجهاز المراد التخلص من الدليل بداخله، فيتم استخلاصه لاحقا ويستعمل كدليل إدانة ضده[1].

الفرع الثالث: الدليل الإلكتروني مرتبط بالبيئة التقنية

فالدليل الإلكتروني ينشأ ويبقى داخل البيئة التقنية المتمثلة في الأجهزة الرقمية الإلكترونية وداخل الشبكات، فهو يولد ويعيش بداخلها ولا يمكن رصده أو استنباطه خارج البيئة التقنية.

هذه الخاصية فرضت على جهات التحقيق الجنائي الساعية إلى جمع الأدلة الجنائية اكتساب الخبرات اللازمة من أجل التعامل مع الطبيعة التقنية للدليل الإلكتروني، وهذا أدى بدوره إلى ظهور ما يسمى بالتحقيق الجنائي الرقمي، ولاحقا ظهور تخصص جديد تحت مسمى الطب الشرعي الرقمي.

في الولايات المتحدة الأمريكية قامت الأكاديمية الأمريكية لعلوم الطب الشرعي (American Academy of Forensic Sciences) والمعروفة اختصارا ب(AAFS) بإنشاء قسم جديد خاص بالعلوم الرقمية، فظهر الطب الشرعي الرقمي كتخصص علمي وكمهنة، وفي وقت لاحق أنشأت الولايات المتحدة الأمريكية إلى جانب دول أخرى مجموعات متخصصة للتحقيق في الجرائم ذات الصلة بالحاسوب[2].

---

[1] أنظر في هذا المعنى طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة (28-29 /2009/10م) نظمته أكاديمية الدراسات العليا، طرابلس، ص5.

[2] . يمكن الاطلاع عليه أو تحميله على الرابط (متاح بتاريخ 2018/10/25 على الساعة 19:55):
https://www.aafs.org
أنظر في هذا المعنى كذلك: أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2015، ص 18 و19.

كما دفعت الحاجة إلى تقنيين مختصين في التعامل مع الدليل الإلكتروني بالمشرع في بلجيكا إلى تعديل قانون التحقيق الجنائي وذلك بإدراج المادة 39 مكرر بموجب القانون البلجيكي المتعلق بجرائم بالحاسب الآلي[1] من خلالها سمحت بضبط الأدلة الإلكترونية عن طريق مثلا نسخ المواد المخزنة بنظم المعالجة الآلية للبيانات بهدف عرضها بعد ذلك على الجهات القضائية[2].

الفرع الرابع: الدليل الإلكتروني متطور بطبيعته

وهي خاصية يكتسبها الدليل الإلكتروني من خلال علاقته بالمحيط أو الحاضنة التي يعيش بداخلها ونقصد بها هنا البيئة التقنية. فالتطور التكنولوجي المتسارع والمتواصل يدفع معه البيئة التقنية إلى التطور كذلك، ويحدث تلقائيا بأن يساير الدليل الإلكتروني هذا التطور الحاصل في بيئته.

الفرع الخامس: الدليل الإلكتروني قابل للنسخ

يمكن استخراج نسخ مطابقة للأصل للدليل الإلكتروني، ولها ذات القيمة والحجية الثبوتية، الشيء الذي لا يتوافر في أنواع الأدلة الأخرى (التقليدية) مما يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الضياع أو التلف والتغيير عن طريق عمل استخراج نسخ طبق الأصل من الدليل[3].

---

[1] La loi du 28 novembre 2000 relative à la criminalité informatique, Op.cit.

[2] عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث من ضمن أعمال المؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي بالفترة من 12 إلى 14 = =نوفمبر2007، جامعة نايف العربية للعلوم الأمنية، الرياض، ص 15. أشارت إليه هدى طلب علي، الإثبات الجنائي في جرائم الأنترنت والاختصاص القضائي بها، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة النهرين، العراق، 2012، ص 126. متاحة على الرابط التالي: http://www.law.nahrainuniv.edu.iq/lib_files/ تحت الرمز (2014_11_16_03_17_55) بتاريخ 2019/11/14 الساعة 19:25.

[3] عمر محمد بن يونس، الإثبات الجنائي عبر الإنترنت، المرجع السابق، ص 12.

- الدليل الإلكتروني يسهل التلاعب به عن طريق تدميره أو تعديله مما يؤدي إلى ما يصطلح عليه بتبخر الدليل الإلكتروني. بل وحتى نقله إلى أنظمة معلوماتية بالخارج وذلك نحو بلد معين أو عدة دول، الأمر الذي يصعب أكثر مهام جهات التحقيق التي يستوجب عليها حينئذ انتظار موافقة تلك الدولة أو الدول وما تستهلكه هذه الإجراءات من وقت الذي له أهميته البالغة في الجريمة الإلكترونية.
- الدليل الإلكتروني دليل عصي على جهات التحقيق في كثير من الأحيان بسبب أن الجناة في مجال الإجرام الإلكتروني قد يعمدون إلى تشفير بياناتهم وتسييجها بكلمات مرور سرية، الأمر الذي يعقد أكثر فأكثر من عمل القائمين على التحقيق.

المبحث الثالث: صعوبات متعلقة بالتعاون الدولي

لقد أدى الطابع العالمي للجريمة الإلكترونية إلى اتساع رقعة هذه الجريمة متخطية بذلك الحدود الجغرافية ومستفيدة من البعد العالمي لشبكة الأنترنت. هذا الواقع خلق صعوبات كبيرة ووضع معوقات كثيرة لجهات التحقيق في طريقها لمباشرة إجراءات التحقيق من انتقال لمسرح الجريمة الإلكترونية ومعاينته، وتفتيش الأنظمة المعلوماتية وضبط الأدلة الإلكترونية...، إلى غير ذلك من إجراءات التحقيق الواجب اتباعها من أجل الوصول إلى الجناة. ذلك أن جزء كبير من الجريمة الإلكترونية أو كلها قد ترتكب خارج إقليم الدولة وبالتالي وجدت جهات التحقيق نفسها مقيدة بمدى تجاوب الدول الأخرى معها ومجبرة على ضرورة الانخراط في اتفاقيات دولية أو ما يسمى بالتعاون الدولي في مجال مكافحة الجريمة الإلكترونية، وإن كنا في هذا المقام سنكتفي فقط بما له علاقة بالتحقيق الابتدائي باعتباره يخص نطاق وحدود دراستنا الحالية.

وقبل الخوض في الصعوبات التي تواجه جهات التحقيق والمتعلقة بالتعاون الدولي في مجال الجريمة الإلكترونية، سنسعى لتعريف المقصود بالتعاون الدولي في هذا المجال ثم ننظر في أهمية التعاون الدولي المتعلق بالتحقيق في الجريمة الإلكترونية، لنختم باستعراض صور تلك الصعوبات التي تعرقل التعاون الدولي في هذا الميدان بعد ذلك.

المطلب الأول: تعريف التعاون الدولي في مجال الجريمة الإلكترونية

يصعب وضع تعريف لمصطلح التعاون الدولي نظرا لاتساع مجال هذا التعاون وتعدد تلك الصور التي يمكن أن يتجسد من خلالها هذا التعاون، فالتعاون الدولي عبارة عن ظاهرة متغيرة ومتطورة بشكل مستمر. وتزداد صعوبة تعريف التعاون الدولي إذا ارتبط بالجريمة الإلكترونية كون هذه الأخيرة في حد ذاتها لم تلق إجماعا دوليا حول وضع تعريف جامع ومانع لها تتفق عليه. ولقد أشار بعض الفقهاء إلى فكرة التعاون من خلال تعريف القانون الدولي الجنائي بأنه ذلك الفرع من النظام القانوني الدولي، الذي يمثل إحدى السبل المستخدمة من أجل تحقيق أكبر قدر من التوافق والانسجام بين الدول من أجل منع ومكافحة الجريمة وتوفير الحماية للمصالح العالمية المشتركة التي يعترف بها المجتمع الدولي.[1]

ويعتبر التعاون في مجال التحقيق في الجرائم الإلكترونية إحدى صور التعاون الدولي التي فرضت نفسها نتيجة اتساع رقعة الإجرام الإلكتروني، هذا الأخير الذي استغل شبكة الأنترنت من أجل بسط وتوسيع نطاق جرائمه والتي أضحت تهدد كل الدول دون استثناء، فلا توجد أي دولة في مأمن ومنأى عن هذا الخطر، كما لا يمكن بأي حال من الأحوال لأي دولة في العالم القيام بكافة إجراءات التحقيق في الجرائم الإلكترونية ذات البعد الدولي دونما الحاجة إلى الدول الأخرى والانخراط ضمن الجهود الدولية التي تسعى لتسهيل مهام جهات التحقيق بخصوص الجريمة الإلكترونية.

المطلب الثاني: أهمية التعاون الدولي المتعلق بالتحقيق في الجريمة الإلكترونية

لقد خلقت الجريمة الإلكترونية عدة معوقات إجرائية لجهات التحقيق كانت كفيلة لتبرير وإبراز مدى الأهمية التي تكتسيها ضرورة التعاون الدولي في هذا المجال، فالجريمة الإلكترونية في كثير من الحالات تكون جريمة عابرة للحدود وذات بعد دولي حيث تتوزع عناصر الركن المادي فيها على أكثر من دولة، فيمكن أن يرتكب السلوك الإجرامي في

[1] أنظر في هذا المعنى عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015، ص 15-16.

دولة في حين تتحقق النتيجة في دولة أو عدة دول أخرى، الأمر الذي يجعل من تلك الإجراءات المستندة على مبدأ الإقليمية عاجزة ولا تلبي حاجيات جهات التحقيق.

أمام هذا الوضع تظهر أهمية استحداث آليات جديدة بشأن التعاون الدولي في التحقيق في الجرائم الإلكترونية من الناحية الإجرائية، وذلك لإمكانية تجنب العديد من المشاكل الإجرائية، ومنها تنظيم مسألة الولوج والضبط للنظام المعلوماتي وحجز الأصول غير المادية –الدليل الإلكتروني –والموجودة على إقليم دولة أخرى، والتنسيق بين الدول لعدم رفض أي منهم طلب المساعدة القضائية وخاصة في مرحلة التحقيق الابتدائي بل وسرعة تنفيذ المساعدة وبما يتلاءم مع طبيعة مجتمع المعلومات الذي يتسم بالسرعة[1].

لذلك تبرز أهمية التعاون الدولي في تقديم المساعدة من قبل سلطات البلد الذي انطلقت منه الشرارة الأولى للجريمة (السلوك المادي)، أو من السلطات في البلد أو البلدان التي عبر من خلالها النشاط المجرم وهو في طريقه إلى الهدف، أو حيثما توجد أدلة للجريمة.[2]

[1] جان فرانسوا هنروت، أهمية التعاون الدولي والتجربة البلجيكية في تبادل المعلومات بين عناصر الشرطة والتعاون القضائي، بحث مقدم بالجلسة الرابعة المتعلقة بالإجراءات الوقائية والتعاون الدولي لمحاربة الجرائم المتصلة بالكمبيوتر، برنامج تعزيز حكم القانون في بعض الدول العربية–مشروع تحديث النيابات العامة–ضمن أعمال الندوة الإقليمية حول " الجرائم المتصلة بالكمبيوتر، الدار البيضاء، المملكة المغربية، الفترة ما بين 19 و20 يونيو 2007، ص 97.

Jean-François HENROTTE, L'importance de la collaboration internationale dans l'échange d'informations policières et de coopération judiciaire, in La cybercriminalité, Programme des Nations Unies pour le Développement, Casablanca, Royaume du Maroc, 19-20 juin, 2007, P 97.

أشار إليه محمد كمال شاهين، المرجع السابق، ص 212.

[2] وفي مثال على أهمية التعاون الدولي في مجال مكافحة الجريمة المعلوماتية، قامت المديرية الأمريكية للتفتيش على البريد في عام 1999 بمداهمة مكاتب شركة في ولاية تكساس تدعى (لاندسلايد إنكوربوريتد Landslide Incorporated) حيث تقوم هذه بتشغيل شبكة لتقديم خدمات استضافة مواقع الإنترنت والتحقق من بطاقات الائتمان لعدد كبير من المواقع التي تقدم بشكل رئيسي مواد إباحية. وكان أكثر النشاطات تحقيقا للأرباح من أنشطة هذه الشركة هو المواقع التي تحتوي على صور إباحية يستغل فيها الأطفال. وقد حقق مالكي هذه الشركة أرباح كبيرة من وراء هذا النشاط. وبعد إدانة أصحاب الشركة عام 2001 تم إعطاء نسخة من قاعدة البيانات الخاصة بعملاء الشركة إلى الشرطة البريطانية، وقد ساعدت تلك البيانات على تحديد هوية حوالي 20300 مشتبه به في بريطانيا يعتقد بأنهم قاموا بدفع أموال للدخول على مواقع تقدم صورا إباحية يستغل فيها الأطفال. وقد بدأت الشرطة البريطانية بإجراء تحقيقات موسعة في هذا الموضوع وكان عدد المشتبه بهم ضخما، ولكن تم إعطاء الأولوية إلى المشتبه فيهم الذين يعتقد أنهم يشكلون خطرة على الأطفال، وتم فحص أجهزة الكومبيوتر الخاصة بهم بعد الحصول على أذونات التفتيش لكل واحد

وفي هذا الصدد تناولت المادة 23 من الاتفاقية الأوروبية لبودابست المتعلقة بمواجهة الجريمة الإلكترونية[1] تلك المبادئ العامة ذات الصلة بالتعاون الدولي فدعت الدول الأطراف أن تتعاون فيما بينها على أوسع نطاق ممكن فيما يخص الإجراءات المتعلقة بالتحقيقات أو بالمتابعات التي تتعلق بالجرائم الجنائية ذات الصلة بنظم وبيانات الكومبيوتر، أو من أجل جمع أدلة بشأن جريمة جنائية في شكل إلكتروني.

وجاء التقرير التفسيري لذات الاتفاقية ليحدد المبادئ العامة المتعلقة بالتعاون الدولي التي وردت بالمادة 23 من الاتفاقية والتي لخصها في ثلاثة مبادئ كالآتي:

– التعاون الدولي بين الدول الأطراف على أوسع نطاق ممكن: ويقتضي هذا المبدأ من الأطراف أن تقدم تعاونا واسعا فيما بينها، وأن تقلل إلى أدنى حد من العوائق التي تحول دون التدفق السلس والسريع للمعلومات والأدلة على الصعيد الدولي.

– توسيع النطاق العام للالتزام بالتعاون: إذ ينبغي توسيع نطاق التعاون ليشمل جميع الجرائم ذات الصلة بأنظمة وبيانات الكمبيوتر، فضلا عن جمع الأدلة في شكلها الإلكتروني.

– يجب إنجاز التعاون وفقا لأحكام اتفاقية بودابست وكذلك من خلال تطبيق الاتفاقات الدولية ذات الصلة بالتعاون الدولي في المسائل الجنائية، والترتيبات المتفق عليها على

منهم. ولإثبات الطريقة التي تم بها إدراج أسم= =الشخص في قاعدة البيانات، كان من الضروري مخاطبة الولايات المتحدة الأمريكية وطلب ذلك منها، كما تتطلب الأمر أيضا سفر ضباط بريطانيين لنسخ شبكة أجهزة الكومبيوتر التي استخدمتها شركة (لاندسلايد إنكوربوريتد) لاستعمالها في التحقيقات الجارية في بريطانيا. راسل تاينر – جرائم الإنترنت. التحدي لإنفاذ القانون، برنامج تعزيز حكم القانون في بعض الدول العربية مشروع تحديث النيابات العامة. بحث مقدم بنفس الندوة الإقليمية حول الجرائم المتصلة بالكومبيوتر المشار إليها سابقا، ص 89– 90. أشار إليه محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، المنصورة، 2015، ص 126–127.

[1] Article 23 – Principes généraux relatifs à la coopération internationale
"Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale". Op.Cit.

أساس التشريع الموحد أو المتبادل والقوانين المحلية على حد سواء. وهذا لا يلغي ما ورد في الاتفاقات الدولية المتعلقة بالمساعدة القانونية المتبادلة وتسليم المجرمين.

أما المشرع الجزائري فقد تناول موضوع التعاون الدولي المتعلق الجريمة الإلكترونية بالفصل السادس من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] وذلك من المادة 15 إلى غاية المادة 18، وبشأن التحقيقات في الجريمة الإلكترونية جاء بالفقرة الأولى من المادة 16" في إطار التحريات أو التحقيقات القضائية الجارية لمعاينة الجرائم المشمولة بهذا القانون وكشف مرتكبيها، يمكن السلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في الشكل الإلكتروني ...".

يضاف إلى ذلك، أن التعاون الدولي من شأنه خلق تقارب كبير بين التشريعات الجنائية للدول لاسيما فيما يتعلق بالجوانب الموضوعية وخاصة الإجرائية المتصلة بالتحقيق في الجريمة الإلكترونية، هذا التقارب قد يمهد في المستقبل إلى تبني قانون موحد على المستوى الدولي يضم قواعد إجرائية مشتركة تساهم في تسهيل مهام جهات التحقيق على المستوى الدولي لمواجهة الجريمة الإلكترونية. وإن تحقق ذلك فإنه بالمحصلة سيحول دون اتخاذ المجرم الإلكتروني من شبكة الأنترنت ملاذا يختبئ فيه وينجو بفضله من المتابعة الجزائية، لأنه سيجد نفسه محاطا ومحاصرا بسياج يمنعه من الإفلات من العقاب الأمر الذي يؤدي في نهاية المطاف إلى ردع الإجرام الإلكتروني.[2]

المطلب الثاني: إشكاليات التعاون الدولي بخصوص التحقيق في الجريمة الإلكترونية

رغم الحاجة الملحة لتعاون الدول فيما بينها من أجل مواجهة الجريمة الإلكترونية، وهذا نظرا للطبيعة الخاصة لهذه الجريمة من جهة وكذا اتساع نطاقها نتيجة الاستفادة من شبكة الإنترنت من جهة أخرى، إلا أن هذا التعاون ليس بتلك الفكرة البسيطة التي يمكن

[1] القانون 09-04، المرجع السابق.

[2] أنظر في هذا المعنى كل من عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 17-18. ومحمد كمال شاهين، المرجع السابق، ص 211.

تجسيدها بيسر، وذلك بسبب العديد من المعوقات التي جعلت من موضوع التعاون الدولي في مجال الجريمة الإلكترونية على قدر لا يستهان به من التعقيد.

وهذا ما يدفعنا للحديث عن الإشكاليات التي تواجه التعاون الدولي في مواجهة الجريمة الإلكترونية لاسيما في مجال التحقيق في هذه الجريمة، ولعل أبرزها تلك المتعلقة باختلاف تشريعات الدول وعدم وجود نموذج موحد للنشاط الإجرامي، وكذا تباين النظم القانونية الإجرائية للدول في ظل عدم التنسيق فيما يخص الإجراءات الجنائية، يضاف إلى ذلك مشكل الاختصاص القضائي وتلك المعوقات المتعلقة بالمساعدة القضائية الدولية بما في ذلك التحقيق والإنابة القضائية وتسليم المجرمين. وعليه سوف نحاول من خلال هذا القسم من البحث التطرق لهذه الصعوبات كالآتي:

الفرع الأول: الاختلاف التشريعي بين الدول وعدم وجود نموذج موحد للنشاط الإجرامي

كثيرا ما تتأثر الجهود التشريعية في مختلف الدول بالبيئة السائدة بهذه الدولة أو تلك، ونظرا لاختلاف البيئات وللعناصر المشكلة لها من عادات وتقاليد وكذا الثقافات والديانات وأثر كل ذلك في تباين الدول والشعوب، فإنه كان من الطبيعي أن ينتج على ذلك اختلاف في التشريعات المتعلقة بموضوع الجريمة الإلكترونية. وهذا كله جعلنا نقف أمام عدم وجود اتفاق بين الدول حول صور محددة لتلك الأفعال التي تندرج ضمن الجرائم الإلكترونية، ففي ظل عدم اتفاق الدول على تعريف جامع ومانع للجريمة الإلكترونية وعدم وجود نموذج موحد للنشاط الإجرامي، كل هذا من شأنه عرقلة التعاون الدولي ذلك أن ما تعتبره دولة معينة جريمة قد يكون مباحا في دولة أخرى.

ناهيك عن التعارض الحاصل بين مصالح الدول على الساحة الدولية وهو الأمر الذي يزيد من تعقيد الوضع وساهم في صعوبة إيجاد تفاهم يفضي إلى تعاون دولي جاد بخصوص الجريمة الإلكترونية.

فعندما تتعارض مصالح الدول تلجأ كل دولة إلى تغليب ما تقضيه مصالحها ولو تعارض ذلك مع مصلحة الدولة الأخرى، وتتوقف قدرة الدول على التعاون الدولي في مسائل العدالة الجنائية وتنفيذ القوانين-إلى حد ما-على العلاقات السياسية القائمة بينها، فكلما

كانت العلاقات السياسية سيئة تزايدت احتمالات فشل سبل التعاون الدولي فيما بينها، مما ينعكس أثره على إجراءات وسبل التعاون الدولي.[1]

الفرع الثاني: تباين النظم القانونية الإجرائية للدول وعدم تناسق الإجراءات الجنائية

تتنوع القوانين المتعلقة بالإجراءات الجنائية من دولة لأخرى، وهذا التنوع قد يسفر في كثير من الأحيان عن تباين واختلاف فيما يخص تلك الإجراءات الرامية إلى جمع الأدلة الإلكترونية. فما يمكن اعتباره إجراء مشروعا في دولة ما قد يصنف في دولة أخرى ضمن الإجراءات غير المشروعة والتي يترتب عنها عدم مشروعية الدليل الإلكتروني الذي تم التوصل إليه، وهذا الأمر يعتبر مشكلة تواجه التعاون الدولي في مجال التحقيق الجنائي في الجريمة الإلكترونية، ويتضح ذلك في حال ما إذا امتد إجراء من إجراءات التحقيق المتعلقة بجمع الدليل الإلكتروني خارج نطاق الدولة كأن يتعين مثلا أن يمتد إجراء التفتيش أو الضبط إلى نظام معلوماتي متواجد بدولة أخرى تختلف القواعد الإجرائية الجنائية بها مع الدولة المباشرة للتحقيق.

إن تباين القوانين الإجرائية الجنائية للدول يفضي إلى قيام حالة من عدم التنسيق بين جهات التحقيق، الأمر الذي يعيق الطريق أمامها في سعيها إلى جمع الدليل الإلكتروني، فيستعصي بذلك عليها مواجهة الجريمة الإلكترونية وهو الأمر الذي يشكل في نهاية المطاف صعوبة أمام التعاون الدولي في هذا المجال.

الفرع الثالث: مشكلة الاختصاص القضائي الدولي

تعتبر الجريمة الإلكترونية من بين أكثر الجرائم التي تثير مشكلة تنازع الاختصاص القضائي على المستوى الدولي الأمر الذي يعيق جهات التحقيق بخصوص إجراءاتها المتعلقة بجمع الدليل الإلكتروني. ويقصد بالاختصاص تلك السلطة التي يقررها القانون

[1] أنظر في هذا المعنى هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، الطبعة الأولى، القاهرة، دار النهضة العربية, 2006, ص 536 أشار إليه عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 58.

للقضاء في أن ينظر دعاوى من نوع معين حدده المشرع، والأصل أن ينسب هذا الاختصاص إلى قضاء الحكم، وأن يكون موضوعه تخويله سلطة الفصل في الدعوى.[1]

فعلى المستوى المحلي لا تثير الجريمة الإلكترونية مشاكل كبيرة في تحديد الاختصاص القضائي، فالسلوك الإجرامي إذا كان قد ارتكب فوق إقليم دولة ما وتحققت النتيجة داخل إقليم نفس الدولة وكان كل من الجاني والمجني عليه يحملان جنسية هذه الدولة ويقيمان بها، فحينئذ يتم تحديد الجهة المختصة محليا من خلال المعايير الثلاثة التي سبق وأن تناولناها في الباب الأول من هذه الدراسة ونقصد بها هنا كل من معيار مكان ارتكاب الجريمة ومكان إقامة المتهم وكذا مكان إلقاء القبض على المتهم، وهي المعايير التي يتضمنها مبدأ الإقليمية. لكن إذا تدخل العنصر الأجنبي كأن يكون الجاني أو المجني عليه أو كلاهما يحملان جنسية دولة أو دول أخرى ويتواجد أحدهما أو كلاهما فوق إقليم دولة أجنبية، ففي هذه الحالة ووفقا لمبدأ الشخصية الإيجابية أو مبدأ الشخصية الإيجابية أو كلاهما يمكن لدولة أخرى أو دول أخرى أن تثير اختصاصها قضائيا بالتحقيق في هذه الجريمة الإلكترونية ونكون أمام تنازع للاختصاص القضائي بينها وبين الدولة الأولى تطبيقا لمبدأ الشخصية.

أما إذا كانت الجريمة الإلكترونية فيها مساس بالأمن القومي أو العملة الوطنية أو كل ما له علاقة بما يسمى بالمصالح الأساسية لدولة أو دول أخرى، فهنا يقوم الاختصاص القضائي لهذه الدول كذلك تطبيقا لمبدأ العينية.

إذن فمشكل الاختصاص القضائي بخصوص الجريمة الإلكترونية يبرز على المستوى الدولي نظرا للطبيعة الخاصة للجريمة الإلكترونية، وكذا امتداد شبكة الأنترنت عبر العالم وربطها لمختلف الدول الأمر الذي يجعل نتيجة الأفعال الإجرامية تتحقق فوق إقليم دولة أو أقاليم مجموعة من الدول غير تلك التي انطلق أو ارتكب فوق إقليمها السلوك الإجرامي، كل ذلك يزيد من صعوبة التعاون الدولي ويحول دون قيام جهات التحقيق بمهامها بالسرعة اللازمة التي فرضتها طبيعة الجريمة الإلكترونية والدليل الإلكتروني،

[1] محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، الطبعة الثالثة، 1988، ص 823.

وهذا كله لا يساعد على ردع الإجرام الإلكتروني الذي قد يستغل حالة تنازع الاختصاص القضائي الدولي[1] سواء في صورتها الإيجابية أو خاصة الصورة السلبية من أجل الفرار من المتابعة القضائية.

الفرع الرابع: المعوقات المتعلقة بالمساعدة القضائية الدولية

لا يختلف اثنان حول حقيقة مفادها أن شبكة الأنترنت ساهمت بشكل كبير وغير مسبوق في ربط الدول وكذا الأشخاص ببعضهم البعض وذلك من خلال استفادتهم من سهولة وسرعة نقل البيانات والمعلومات المتعلقة بمختلف مناحي الحياة (الاجتماعية، الاقتصادية، الثقافية، التعليمية، المالية، ...إلخ) فهذه أشياء إيجابية لا يمكن إنكارها. غير أنه وبالمقابل كان للأنترنت جملة من الأثار السلبية كذلك والتي مست مختلف مجالات الحياة، ولعل من أبرزها أنها أصبحت ملاذا للجريمة والمجرمين كما ساهمت في اتساع رقعة الجريمة، فالجريمة الإلكترونية لا تعترف بالحدود بين الدول إذ أن نتائج السلوك الإجرامي قد تتحقق في عدة دول وبمختلف القارات في ظرف زمني وجيز.

لقد أشرنا سابقا إلى أن الجريمة الإلكترونية لا تعترف بالحدود بين الدول، فالفعل الإجرامي قد تنصرف نتائجه وآثاره إلى عدة دول وهو الأمر الذي يضع جهات التحقيق أمام معضلة البحث عن الدليل الإلكتروني خارج حدود الدولة التي تنتمي إليها جهات

[1] وكمثال على ذلك نذكر قضية المبرمج الإنجليزي الذي كان يعمل بأحد البنوك في دولة الكويت، حيث قام بالتلاعب في نظام الحاسب الآلي الخاص بالبنك ليقوم بإجراء خصومات من أرصدة العملاء، ثم يقوم بإيداعها في الحساب الخاص به، وبعد عودة المتهم إلى إنجلترا قام بالكتابة إلى البنك طالبا إياه أن يقوم بتحويل الحساب الخاص به إلى = = عدة حسابات بنكية في إنجلترا، وهو ما قام به البنك بالفعل. قدم المتهم للمحاكمة بتهمة الحصول على أموال الغير بطريق الاحتيال طبقا للقانون الإنجليزي، وحكم عليه بعقوبة السجن، إلا أن المتهم طعن في الحكم استنادا إلى عدم اختصاص القضاء الإنجليزي بالفصل في الجريمة، حيث إن فعلي السحب والإيداع قد تما في دولة الكويت وليس في إنجلترا. رفضت محكمة الاستئناف الطعن المقدم من المتهم، وجاء في حيثيات رفضها أن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل، وما أسفر عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية. أنظر نائلة عادل محمد فريد قورة، المرجع السابق، ص 49 أشار إليها عادل عبد العال إبراهيم خراشي، المرجع السابق، ص 61.

التحقيق هذه. أمام هذا الواقع كان لزاما على الدول التعاون فيما بينها من أجل تمكين جهات التحقيق من مباشرة إجراءاتها وذلك في إطار ما يعرف بالمساعدة القضائية الدولية. غير أن هذا الشكل من أشكال التعاون الدولي لمواجهة الجريمة الإلكترونية تعترض سبيله عدة مشاكل هي بمثابة معوقات تحول دون تجسيده بالكيفية التي تساهم في مجاراة الطبيعة الخاصة للجريمة الإلكترونية والدليل الإلكتروني الذي تسعى جهات التحقيق للوصول إليه.

وتعرف المساعدة القضائية الدولية على أنها " كل إجراء قضائي تقوم به دولة من شأنه تسهيل مهمة المحاكمة في دولة آخري بصدد جريمة من الجرائم"[1]. وبما أن دراستنا هذه تنصب حول التحقيق الجنائي في الجريمة الإلكترونية وبصورة أدق التحقيق الابتدائي، فإننا سنتناول موضوع الصعوبات التي تشهدها المساعدة القضائية الدولية بخصوص الجريمة الإلكترونية في جوانبه المرتبطة بإجراءات التحقيق. وعليه سنتطرق لتلك الصعوبات المتعلقة بالإنابة القضائية وبشكل أقل لتلك المرتبطة بتسليم المجرمين ما دام أنه يتعلق في كثير من الأحيان بالمحاكمة أو توقيع العقاب وليس بموضوع التحقيق.

نظرا لاتساع نطاق الجريمة الإلكترونية لكونها جريمة عابرة للحدود مستفيدة في ذلك من شبكة الأنترنت، فإنه وفي كثير من الأحيان تجد الجهات المكلفة بالتحقيق في الجريمة الإلكترونية نفسها بحاجة إلى مساعدة السلطات القضائية لتلك الدولة أو الدول التي ارتكبت الجريمة فوق إقليمها، سواء كل عناصر الجريمة أو عنصر من عناصرها. وذلك من أجل القيام بإجراء من إجراءات التحقيق وهذا ما يطلق عليه الإنابة القضائية الدولية.

يقصد بالإنابة القضائية الدولية بأنها "طلب من السلطة القضائية المنيبة إلى السلطة القضائية المنابة، باتخاذ إجراء من إجراءات التحقيق يلزم اتخاذه للفصل في القضية المنظورة أمام السلطة المنيبة، وذلك بسبب عائق ما يحول دون اتخاذ هذه الأخيرة لهذا

[1] سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دارسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، 1997، ص 25. أشار إليه كل من محمد كمال شاهين، المرجع السابق، ص 219. وعادل عبد العال إبراهيم خراشي، المرجع السابق، ص 30.

الإجراء"[1]. وبالرغم من أهمية هذا الشكل من أشكال التعاون الدولي إلا أن هناك عراقيل تواجه تحقيقه ولعل أبرزها بطء وتيرة الإجراءات وكذا قيام فكرة السيادة كعائق يحول غالبا دون تنفيذ الإنابة القضائية.

إن تعدد القنوات وكثرة الشكليات التي يفرضها الطريق الدبلوماسي الذي تتم عبره الإنابة القضائية، يساهم في بطء مباشرة إجراءات التحقيق الجنائي في مجال الجريمة الإلكترونية، خاصة وأن هذه الأخيرة تتسم بالسرعة في ارتكابها وطمس أدلتها مما يصعب أكثر فأكثر تقفي آثار مرتكبيها، ذلك أن إجراءات التحقيق الجنائي في هذه الحالة تستوجب كذلك السرعة في اتخاذها كالولوج إلى الأنظمة المعلوماتية واعتراض البيانات وجمعها في الوقت الفعلي لمرورها وكذا التحفظ عليها، الأمر الذي قد لا يتحقق بسبب طول الزمن الذي يستغرقه وصول طلب الإنابة القضائية وكذلك الرد على هذا الطلب.

هذا وتأتي فكرة السيادة كعامل آخر يزيد من صعوبة التعاون الدولي المتصل بالإنابة القضائية الدولية، ذلك أن كل دولة تستأثر بممارسة كل مظاهر السلطة فوق إقليمها وفي كافة الاختصاصات، وبما أن القضاء يعتبر أحد السلطات داخل الدولة كان من البديهي أن تباشر كل دولة إجراءات التحقيق الجنائي الجارية فوق إقليمها عبر أجهزتها باعتبار ذلك مظهر من مظاهر سيادة الدولة. فكل دولة تكون بحاجة للقيام بإجراء من إجراءات التحقيق المرتبط بجريمة ارتكبت انطلاقا من دولة أخرى سوف تصطدم بحاجز فكرة السيادة، وهذا الأمر يعد بمثابة العائق الذي يعرقل عمل جهات التحقيق ويعطل التعاون الدولي في هذا المجال.

أما تسليم المجرمين وإن كان يرتبط بمرحلة المحاكمة أكثر من ارتباطه بمرحلة التحقيق الابتدائي، وذلك كون طلب التسليم إما ينصب على شخص بغرض محاكمته أو بغرض

[1] زياد إبراهيم شيحا، الإنابة القضائية الدولية في المسائل الجنائية ونطاق العلاقات الخاصة الدولية، دار النهضة العربية، القاهرة، مصر، 2015، ص 24. أشار إليه صالح عبد الله محمد راشد الوارد، الإنابة القضائية في قانون الإجراءات الجنائية القطري دراسة تحليليه مقارنة، رسالة ماجستير غير منشورة، كلية الحقوق جامعة قطر، يونيو 2017، ص12.

توقيع العقاب عليه إذا كان قد صدر في حقه حكم، فإنه يشكل كذلك عائقا أمام التعاون الدولي بسبب جملة من الأسباب.

يعد تسليم المجرمين مظهرا من مظاهر التعاون الدولي من أجل مكافحة الجريمة، فعند ارتكاب شخص لجريمة من الجرائم الإلكترونية من خلال وحدة طرفية في دولة أجنبية، وخارج سلطة الدولة المتضررة من فعله لا يجوز إبقاءه دون عقاب، لذلك كان لابد من قيام تعاون دولي لملاحقة المجرمين وتسليمهم لإدانتهم وإنزال العقاب بهم، وهذا التعاون أخذ شكل اتفاقيات بين الدول لتسليم المجرم إلى دولة أجنبية تطلب محاكمته لديها أو تنفيذ عقوبة جزائية بحقه، كي لا يفلت من العقاب، حال كان قانون الدولة المتواجد على أرضها لا يسمح بمحاكمته على فعله الجرمي.[1]

يعرف تسليم المجرمين على أنه "إجراء بمقتضاه تتخلى الدولة عن شخص موجود على إقليمها لسلطات دولة أخرى تطالب بتسليمه إليها لمحاكمته عن جريمة منسوب إليه ارتكابها أو لتنفيذ عقوبة محكوم بها من محاكم الدولة طالبة التسليم"[2] ويعرف بأنه " الإجراء القانوني المؤسس على معاهدة أو معاملة بالمثل أو قانون وطني، حيث تتسلم دولة ما من دولة أخرى شخص متهم أو مرتكب مخالفة جنائية ضد القوانين الخاصة بالدولة الطالبة، أو مخالفة للقانون الجنائي الدولي، حيث يعاقب على ذلك في الدولة الطالبة"[3]. هذا ولقد تناولت اتفاقية بودابست لسنة 2001 والمتعلقة بالجريمة الإلكترونية[4] لتلك المبادئ ذات الصلة بتسليم المجرمين وذلك بالفصل الثاني من الباب الثالث المتعلق بالتعاون الدولي، حيث جاء بالمادة 24 البند 1 الفقرة أ "تطبق هذه المادة على تسليم المجرمين بين الدول الأطراف بالنسبة للجرائم المنصوص عليها في المواد من2 إلى 11

[1] أنظر في هذا المعنى فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010، ص 221.

[2] على صادق أبو هيف، القانون الدولي العام، منشأة المعارف، الإسكندرية، 2015، ص 262.

[3] وهو تعريف تبنته المحكمة العليا الأمريكية، أنظر في هذا الشأن عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، بدون سنة نشر، ص 55. أشار إليه محمد كمال محمود الدسوقي، المرجع السابق، ص 167.

[4] المرجع السابق.

من هذه الاتفاقية، شريطة أن يعاقب على هذه الجرائم بموجب قوانين كلا الطرفين المعنيين، بعقوبة سالبة للحرية لمدة سنة على الأقل أو بعقوبة أشد". كما نصت في البند الرابع من نفس المادة على أنه " في حالة تلقت دولة طرف تخضع تسليم المجرمين لشرط وجود معاهدة ذات الصلة طلباً بالتسليم من طرف دولة طرف أخرى لا تربطها بها معاهدة لتسليم المجرمين، يجوز لتلك الدولة الطرف اعتبار هذه الاتفاقية بمثابة الأساس القانوني لعملية التسليم فيما يتعلق بأي من الجرائم الجنائية المشار إليها في الفقرة 1من هذه المادة".

وبالرغم من أهمية نظام تسليم المجرمين في مكافحة الجريمة الإلكترونية حيث أنه موضوع معاهدات واتفاقيات دولية وحتى العرف الدولي، إلا أن هناك عدة شروطا مقيدة له ولا يتم بموجبها تسليم المجرمين الأمر الذي يجعل كثير من مرتكبي الجرائم الإلكترونية دون عقاب، ومن بين هذه الشروط:

– ازدواجية التجريم في كل من قانون الدولة طالبة التسليم والدولة المطلوب منها التسليم.

– أن تكون الجريمة قد تم ارتكابها فوق إقليم الدولة طالبة التسليم أو ارتكبت بالخارج وكانت قوانينها تعاقب على ذلك.

– عدم جواز تسليم الدولة لمواطنيها في حال تلقت طلبا بذلك.

– عدم جواز تسليم السياسيين كطالبي اللجوء السياسي...إلخ.

كم أنه يفهم من نص المادة 24 من اتفاقية بودابست[1] على حق الدول الأعضاء رفض تسليم المجرمين في حال طلب من إحداها ذلك وهذا من خلال البندين الخامس والسادس من نفس المادة[2].

[1] المرجع السابق.

[2] – البند الخامس من المادة 24 من اتفاقية بودابست " يخضع تسليم المجرمين للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها التسليم أو معاهدات تسليم المجرمين واجبة التطبيق، بما في ذلك الأسباب التي تستند إليها الدولة الطرف المطالبة بالتسليم لرفض التسليم"

كل هذه الشروط وغيرها تقف حجر عثرة في وجه التعاون الدولي بخصوص تسليم المجرمين المتابعين بارتكاب إحدى الجرائم الإلكترونية.

المبحث الرابع: الصعوبات المتعلقة بالخصوصية المعلوماتية

إن سعي الدولة إلى محاربة الجريمة داخل المجتمع بهدف استتباب الأمن وحماية حقوق الأشخاص وصون حرياتهم، يتطلب من الدولة تبني وإعداد قواعد إجرائية تحدد كيفية ملاحقة الجناة، غير أن هذه الإجراءات ليست مطلقة وإنما مقيدة بمبدأ الشرعية بشكل يلزم الدولة العمل على إيجاد توازن بين حق المجتمع في محاسبة الجناة من جهة، ومن جهة أخرى ضمان احترام الحريات والحقوق الشخصية في سعيها لمواجهة الجريمة.

ويعتبر الحق في الحياة الخاصة واحد من أهم الحقوق الشخصية التي يهتم المشرع بصيانتها، بالإضافة إلى الحقوق الثلاثة الأخرى (الحق في الأمن الشخصي والحق في السلامة البدنية والذهنية والحق في حماية حرمة المسكن والحق في حماية حرمة الحياة الخاصة) والتي تشكل مربع الحقوق الأساسية الشخصية، وإن كنا نقر بوجود تباين وعدم اتحاد الرؤى فيما يخص حصر ما يدخل ضمن الحقوق الشخصية الأساسية، إلا أنه وبحسب رأينا فإنها في المجمل تتقاطع مع الحقوق الأربعة السالفة الذكر.

لقد أدى التطور الهائل الذي شهدته البشرية في مجال الاتصالات إلى اتساع تلك المخاطر التي تهدد حرمة الحياة الخاصة لا سيما من خلال الإقبال المتزايد للأشخاص على شبكة الأنترنت واعتمادهم أكثر فأكثر على ما توفره من خدمات في حياتهم اليومية وما يترتب على ذلك من تخزين كم هائل لبياناتهم، وهذا بدوره نتج عنه ما أصبح يسمى بالخصوصية المعلوماتية، هذه الأخيرة أصبحت عرضة لانتهاكات جسيمة، ليس من

ومرد صعوبة إيجاد تعريف متفق عليه للحق في الخصوصية تعود إلى أن مفهوم الحياة الخاصة من المفاهيم النسبية المرنة بمعنى تغير هذا المفهوم وتبدله ما بين المجتمعات التي تتغاير فيما بينها القيم والعادات والتقاليد، وتتبدل المفاهيم الاجتماعية والاقتصادية والسياسية والدينية والثقافية، فضلا عن اختلاف نطاق الخصوصية من فرد لآخر فهناك من يجعل حياته كتابا مفتوحا، وهناك من يجعل حياته سرا غامضا[1]. كل هذا لم يساهم في وضع تعريف موحد للحق في الخصوصية، غير أن هذا الاختلاف لا يمنعنا من التطرق إلى تلك المحاولات الفقهية الكثيرة التي تعرضت لموضوع الحق في الخصوصية.

ينسب إلى القاضي الأمريكي (Thomas Cooley)[2] بأنه أول من أثار موضوع حق الشخص في الوحدة أو في البقاء لوحده أو بمفرده في جملته " the right to be let alone"[3]. وإن كان لم يستخدم مصطلح خصوصية، إلا أن جملته هذه استند عليها غيره فيما بعد للدلالة على الحق في الخصوصية[4]، ونقصد بهما القاضيين (Samuel Warren)[5] و(Louis Brandeis)[6] حينما تناولا في مقال لهما على أن الحق في الخصوصية هو "الحق في أن يترك الشخص وحيدا"[7].

---

[1] أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة 1988.

[2] معلومات أكثر حول هذه الشخصية على الرابط (متاح بتاريخ 2018/03/02 الساعة 21:33):
https://en.wikipedia.org/wiki/Thomas_M._Cooley

[3] Thomas Cooley, A Treatise on the Law of Torts , 2ed Chicago, Callaghan & Co, 1888 p 29. Cité par: David W. Leebron,TheRight to Privacy's Place in the Intellectual History of Tort Law, 41 Case W. Res. L. Rev. 1991, p781.

يمكن الاطلاع أو تحميل النسخة الأصلية للمقال على الرابط (متاح بتاريخ 2018/03/19 على الساعة 06:20):
https://scholarlycommons.law.case.edu/caselrev/vol41/iss3/11/

أنظر كذلك: سليم جلاد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، رسالة ماجستير غير منشورة، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2013، ص 14.

[4] Rigaux François. L'élaboration d'un « Right of Privacy » par la jurisprudence américaine, Revue internationale de droitcomparé. Vol. 32 N°4, Octobre-décembre 1980. p. 710.

يمكن الاطلاع أو تحميل النسخة الأصلية للمقال على الرابط (متاح بتاريخ 2018/03/19 على الساعة 06:20):
https://www.persee.fr/docAsPDF/ridc_0035-3337_1980_num_32_4_3773.pdf

[5] معلومات أكثر حول هذه الشخصية على الرابط (متاح بتاريخ 2018/03/01 الساعة 20:15):
https://en.wikipedia.org/wiki/Samuel_D._Warren

[6] معلومات أكثر حول هذه الشخصية على الرابط (متاح بتاريخ 2018/03/01 الساعة 20:31):
https://en.wikipedia.org/wiki/Louis_Brandeis

[7] "..the right to be let alone.." Samuel D. Warren; Louis D. Brandeis, Harvard " The Right to Privacy ", Law Review, Vol. 4, No. 5. (Dec. 15, 1890), p. 193.

يمكن الاطلاع أو تحميل النسخة الأصلية للمقال على الرابط (متاح بتاريخ 2018/03/22 على الساعة 18:10):

والملاحظ بأن المحاولات الفقهية فشلت في وضع تعريف للحق في الخصوصية كونها لم تقدم لنا معيار واضح يمكن الاستناد عليه، فهي لا تعدو كونها تبريرات لحق الشخص في أن يكون له حيز خاص به.

أمام هذا الوضع حاول بعض الفقهاء مثل الفرنسي Pierre KAYSER جمع العناصر الأساسية والرئيسية التي يتشكل منها الحق في الخصوصية وذلك من خلال التعريفات الفقهية التي تناولت تعريف هذا الحق. بحيث خلص إلى أن الحق في الخصوصية له جانبان هما الغاية من هذا الحق ومضمون هذا الحق، فالغاية تتمثل في ضمان السلام والسكينة لهذا الجانب من حياة الشخص وجعله بمنأى عن التقصي والإفشاء غير المشروعين. أما المضمون يتمثل في الاعتراف لهذا الشخص بحق الاعتراض على التدخل في خصوصياته أو التقصي عنها، وكذلك الاعتراض على وصول معلومات تتعلق بخصوصياته إلى الغير.[1]

أما عن التشريعات المقارنة وإن كانت قد نأت بنفسها عن إعطاء تعريف صريح وواضح للحق في الخصوصية، إلا أنها بالمقابل نصت بقوانينها على حماية هذا الحق. فالمشرع الأمريكي وبموجب المادة (652A)[2] من المدونة الثانية لسنة 1977 المتضمنة تلك الجرائم الماسة بالخصوصية نص على أنه " كل من يعتدي على حق شخص آخر في

---

[1] Pierre KAYSER, Les droits de la personnalité, aspects théoriques et pratiques, Revue trimestrielle de droit civil, 3, 1971, p. 445. Cité par Caroline Vallet LE DÉVOILEMENT DE LA VIE PRIVÉE SUR LES SITES DE RÉSEAUSOCIAL. DES CHANGEMENTS SIGNIFICATIFS, Éditions juridiques associées | Droit et société 2012/1 n° 80 | pages 167.

يمكن الاطلاع أو تحميل النسخة الأصلية للمقال على الرابط (متاح بتاريخ 2018/04/04 على الساعة 19:40):
https://www.cairn.info/revue-droit-et-societe1-2012-1-page-163.htm

أنظر كذلك في هذا المعنى كل من: عفيفي كامل عفيفي، المرجع السابق، ص 266. ومروة زين العابدين سعد صالح، المرجع السابق، ص 40.

[2] 652A. General Principle

(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.

(2) The right of privacy is invaded by:

(a) unreasonable intrusion upon the seclusion of another, as stated in 652B; or

(b) appropriation of the other's name or likeness, as stated in 652C; or

(c) unreasonable publicity given to the other's private life, as stated in 652D; or

(d) publicity that unreasonably places the other in a false light before the public,

See Restatement (Second) of Torts §§ 652A (1997). peut être consulté depuis le lien internet suivant (disponible le 17/09/2019) :http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html

الخصوصية يكون مسؤولا عن الضرر الذي يصيب مصالحه نتيجة لهذا الاعتداء" ويتخذ هذا الاعتداء إحدى الصور التالية:

أ-التدخل في عزلة الغير أو في شؤونه الخاصة.

ب-استخدام اسم الغير أو صفته من أجل تحقيق مصلحة خاصة.

ج-إفشاء أمور متعلقة بالحياة الخاصة للغير.

د-إظهار الغير بمظهر كاذب من خلال نشر أمور تشوه حقيقته في نظر الناس.

المشرع الفرنسي أضفى الحماية الجنائية للحياة الخاصة تحت عنوان (De l'atteinte à la vie privée) أو فيما يتعلق بالاعتداء على الحياة الخاصة، بموجب المواد من 1/226 إلى 4/226 والتي جاء بها القانون رقم 684/92 الصادر بتاريخ 1992/07/22 المعدل لقانون العقوبات[1].

[1] Section 1 De l'atteinte à la vie privée

Art. 226-1. - Est puni d'un an d'emprisonnement et de 300000 F d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui: 1o En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel; 2o En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé. Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé. Art. 226-2. - Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1. Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

Art. 226-3. - Est punie des mêmes peines la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle dont les conditions d'octroi sont fixées par décret en Conseil d'Etat, d'appareils conçus pour réaliser les opérations pouvant constituer l'infraction prévue par le deuxième alinéa de l'article 226-15 ou qui, conçus pour la détection à distance des conversations, permettent de réaliser l'infraction prévue par l'article 226-1 et figurant sur une liste dressée dans des conditions fixées par ce mme décret. Est également puni des mêmes peines le fait de réaliser une publicité en faveur d'un appareil susceptible de permettre la réalisation des infractions prévues par l'article 226-1 et le second alinéa de l'article 226-15 lorsque cette publicité constitue une incitation à commettre cette infraction.

Art. 226-4. - L'introduction ou le maintien dans le domicile d'autrui à l'aide de manoeuvres, menaces, voies de fait ou contrainte, hors les cas où la loi le permet, est puni d'un an d'emprisonnement et de 100000 F d'amende.

La loi N° 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes ,JORF n°169 du 23 juillet 1992.

أما بخصوص المشرع الجزائري فهو بدوره لم يعط تعريفا للحق في الخصوصية، وحرص على إدراج نصوص تصون الحياة الخاصة شأنه في ذلك شأن باقي التشريعات العربية، حيث نصت المادة 47 من الدستور الجزائري[1] بأنه:

" لكل شخص الحق في حماية حياته الخاصة وشرفه.

لكل شخص الحق في سرّية مراسلاته واتصالاته الخاصة في أي شكل كانت.

لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلاّ بأمر معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل انتهاك لهذه الحقوق".

وقبلها الفقرة الأولى من المادة 39 التي جاء بها " تضمن الدولة عدم انتهاك حرمة الإنسان...". كما ورد بالفقرة الأولى من المادة 48 " تضمن الدولة عدم انتهاك حُرمة المسكن...".

كما كفل الحماية الجنائية للمساس بأي شكل بحرمة الحياة الخاصة للأشخاص بموجب المادة 303 مكرر[2] من قانون العقوبات.

وسارت المادة 47 من القانون المدني[1] في هذا الاتجاه إذ نصت بأنه" لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء والتعويض عما يكون قد لحقه من ضرر".

[1] المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020 الصادر بالجريدة الرسمية العدد 82، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020.

[2] المادة 303 مكرر من قانون العقوبات في فقرتها الأولى تنص على يعاقب بالحبس من 6 أشهر إلى 3 سنوات وبغرامة من 50.000 دج إلى 300.000 دج كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأية تقنية كانت وذلك: 1-بإلتقاط أو تسجل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه. 2-بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص بغير إذن صاحبها أو رضاه...". القانون رقم 06-23 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006،المنشور بالجريدة الرسمية رقم 84 الصفحة 23، الصادرة بتاريخ 04 ذو الحجة 1427 الموافق 24 ديسمبر 2006 يعدل ويتمم الأمر رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

"1-لكل إنسان الحق في أن يحترم شرفه وتصان كرامته.

2-لا يجوز أن يتعرض أحد لتدخل اعتباطي أو تعسفي في حياته الخاصة أو في شؤون أسرته أو منزله أو مراسلاته، ولا أن يتعرض لاعتداءات غير مشروعة على شرفه أو سمعته.

3-لكل إنسان الحق في أن يحميه القانون من مثل ذلك التدخل أو تلك الاعتداءات".

كما نصت المادة 8 من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية[1]، وتحت عنوان الحق في احترام الحياة الخاصة والعائلية، على أنه:

"1-لكل شخص الحق في احترام حياته الخاصة والعائلية ومسكنه ومراسلاته.

2-لا يجوز أن تتدخل السلطة العامة في ممارسة هذا الحق إلاّ إذا نص القانون على هذا التدخل، وكان ضروريا، في مجتمع ديمقراطي، لحفظ سلامة الوطن، أو الأمن العام، أو الرخاء الاقتصادي للبلد، أو لحفظ النظام، أو لمنع الجرائم، أو لحماية الصحة أو الأخلاق، أو لحماية حقوق الآخرين وحرياتهم".

بالنسبة للميثاق العربي لحقوق الإنسان[2] وفي نسخته التي اعتمدت ونشرت بموجب قرار مجلس جامعة الدول العربية 5427 المؤرخ في 15 سبتمبر 1997 نص بمادته 17 على أنه " للحياة الخاصة حرمتها، المساس بها جريمة وتشمل هذه الحياة الخاصة خصوصيات الأسرة وحرمة المسكن وسرية المراسلات وغيرها من وسائل الاتصالات الخاصة". غير أنه ما لبث أن تخلى عن هذه المادة وذلك في نسخته التي اعتمدتها القمة العربية السادسة عشرة التي استضافتها تونس بتاريخ 2004/05/23 والذي دخل حيز التنفيذ في 2008/03/15 ووقعت عليه الجزائر، حيث لا أثر لأي محتوى يخص حماية

[1] La Convention de sauvegarde des droits de l'homme et libertés fondamentales, plus connue sous le nom de Convention européenne des droits de l'homme a été ouverte à la signature à Rome le 4 novembre 1950 et est entrée en vigueur le 3 septembre 1953. Disponible pour consultation et téléchargement via le lien (disponible le 24/08/2018 à 21:40): https://www.echr.coe.int/Documents/Convention_FRA.pdf

[2] المصادق عليه بقرار الدورة العادية رقم (121) لمجلس جامعة الدول العربية على المستوى الوزاري رقم 6405 بتاريخ 2004/3/4. يمكن الاطلاع عليه أو تحميله على الرابط (متاح بتاريخ 2018/10/20 على الساعة 07:20):
https://eos.cartercenter.org/uploads/document_file/path/328/ACHR2004_ARA.pdf

الحياة الخاصة باستثناء ما ورد بالفقرة الثامنة من المادة 16 والتي جاء بها " ... وفي جميع الأحوال للمتهم الحق في أن تحترم سلامته الشخصية وحياته الخاصة" ولا نفهم سبب هذا التراجع عن إدراج نص صريح يحمي حرمة الحياة الخاصة للمواطن العربي.

هذا ولقد تناولت الشريعة الإسلامية حق الخصوصية ودعت إلى احترامه من خلال العديد من الآيات القرآنية والأحاديث النبوية الشريفة، حيث يمنع الدخول إلى المنازل دون إذن أصحابها فيقول الله عز وجل " يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّىٰ تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَىٰ أَهْلِهَا ذَٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُونَ(27)فَإِن لَّمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّىٰ يُؤْذَنَ لَكُمْ وَإِن قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَىٰ لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ (28) "[1] وقوله تعالى " يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ"[2] وفيه نهي عن التجسس سترا لعورات الغير. وفي هذا السياق ما جاء عن النبي صلى الله عليه وسلم، فعن سهل بن سعد الساعدي قال " اطلع رجل من جحر في حجر النبي صلى الله عليه وسلم ومع النبي صلى الله علية وسلم مدري يحك به رأسه فقال لو أعلم أنك تنظر لطعنت به في عينك إنما جعل الاستئذان من أجل البصر".[3]

الفرع الثاني: تعريف الحق في الخصوصية المعلوماتية

يعد مصطلح الحق في الخصوصية المعلوماتية من الحقوق الحديثة نسبيا التي ظهرت في عصر المعلوماتية بعدما أصبحت الحاسبات الآلية وشبكة الإنترنت مستودعا للأسرار يخزن عليها الأفراد المعلومات والبيانات الشخصية وغير الشخصية. وينشأ هذا الحق بمجرد أن يحيط الشخص لتلك البيانات أو المعلومات الخاصة به أو التي قام بتجميعها

[1] الآيتين 27 و28 من سورة النور.

[2] الآية 12 من سورة الحجرات.

[3] صحيح البخاري (المؤلف/المشرف: محمد بن إسماعيل البخاري المحقق/المترجم: محب الدين الخطيب، الطبعة الأولى، المكتبة السلفية، القاهرة، 1400هـ، ص 6241.). أنظر الموسوعة الحديثية بالرابط (متاح بتاريخ 2018/10/13 الساعة 17:30): https://www.dorar.net/hadith/sharh/9448

ومعالجة أعداد لا تحصى من البيانات الشخصية، هذه البيانات وإن كان استخدامها قد ساعد في تسهيل و تنظيم حياة الأفراد داخل المجتمعات وفي شتى الميادين (الاقتصادية، الاجتماعية، الصحية، التعليمية،...) إلا أنه وبالمقابل فهذا الأمر يشكل تهديدا على الخصوصية المعلوماتية، إذ عمدت بعض الدول على الاحتفاظ بعدد ضخم من البيانات الشخصية يمكن استخدامها على المستوى الوطني أو الإقليمي أو حتى الدولي.

حيث أنه وفي هذا الشأن يقدر البعض حجم المعلومات الشخصية التي تحتفظ بها الحكومة الأمريكية بثلاثة بليون ملف، كما أن الأنظمة المعلوماتية للمقر العام لحلف شمال الأطلسي المتواجدة ببلجيكا تخزن ملفات تخص كل شخص متواجد فوق الكرة الأرضية أمكنها الوصول إلى بياناته. غير أن البعض يفند ذلك بالقول أن الملفات المخزنة تخص فقط أشخاصا معينين تقوم أجهزة حلف الناتو بمراقبتهم[1].

المطلب الثاني: الاعتداء على الخصوصية المعلوماتية

إن الحديث عن الخصوصية يحمل في طياته حماية تنصرف إلى عدة أشكال مادية ومعنوية ومعلوماتية والتي تشكل صورا للخصوصية، فكان من المنطقي أن يأخذ كذلك الاعتداء على الخصوصية أشكالا وصورا مادية ومعنوية ومعلوماتية. وهذا ما يدفعنا إلى تقسيم هذا المطلب إلى شقين نتناول من خلالهما الحديث عن صور الخصوصية في مقام أول، ثم وفي المقام الثاني نتطرق لصور الاعتداء على الخصوصية مع التركيز فقط على تلك العناصر التي تمت بالصلة لموضوعنا ونقصد بها صور الخصوصية المعلوماتية وصور الاعتداء عليها.

الفرع الأول: صور الخصوصية ومكانة خصوصية المعلومات بينها

للخصوصية بصفة عامة عدة أنواع أو صور أو أشكال، غير أنها تتلاقى وتجتمع تحت غطاء حماية الحق في الخصوصية. فالخصوصية قد تكون مادية تتعلق بكل غرض

[1] أنظر في هذا المعنى عفيفي كامل عفيفي، المرجع السابق، ص 269-270.

مادي يحيطه الشخص بالسرية مانعا الأخرين من الاطلاع عليه، وتشكل الخصوصية الجسدية المثال الأبرز للخصوصية المادية إذ تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم[1] مع العلم بأن هذه الصورة من الخصوصية لا تدخل في نطاق دراستنا، لذلك سوف نكتفي بهذا القدر من الحديث عنها.

كما أن الخصوصية قد تتعلق بمنشآت استراتيجية متصلة بأسرار تكنولوجية أو مرتبطة بالأمن القومي، تعمل الجهات المعنية على حمايتها من كل أشكال الاعتداء ولعل أبرزها التجسس والذي تأثر بالتقنية الحديثة فأصبح تحت مسمى التجسس الإلكتروني، ولاحقا تطورت الأمور وأفرزت لنا مفاهيم جديدة كالجيوش الإلكترونية والحروب الإلكترونية...الخ. ورغم أنه يبدو للوهلة الأولى ارتباط هذا النوع من الخصوصية بموضوعنا إلا أنه في الحقيقة ليس كذلك مادام أننا نسعى في هذا الجزء من البحث إلى إبراز تلك الصورة التي تكون فيها الحياة الخاصة متأثرة بالتقنية أو ما يسمى بالخصوصية المعلوماتية.

نصل الآن إلى الصورة الأهم من بين صور الخصوصية، ومرد الأهمية هنا هو ارتباطها وصلتها بالتحديات التي تواجه جهات التحقيق في الجريمة الإلكترونية في موضوع الخصوصية، ونقصد بها الخصوصية المعلوماتية.

يقصد بالخصوصية المعلوماتية تلك الخصوصية التي تتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة[2]. ولقد ذكرنا آنفا بأن الخصوصية المعلوماتية تضم تلك البيانات الشخصية الخاصة وكذا المراسلات الإلكترونية التي تشمل الرسائل المرسلة أو التي يتم استقبالها إلكترونيا وكذا المحادثات والمكالمات عبر شبكات الاتصال بما فيها الأنترنت.

مع العلم بأن البيانات المتعلقة بحق الخصوصية المعلوماتية قد ترتبط بعدة مجالات مختلفة، تتمثل في الحق في الحياة العاطفية والزوجية والعائلية، والحالة الصحية، والرعاية

[1] أنظر في هذا المعنى كل من: حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبية الحقوقية، بيروت، لبنان، 2014، ص 329. ومروة زين العابدين سعد صالح، المرجع السابق، ص 57.

[2] لمزيد من المعلومات حول ذلك راجع مروة زين العابدين سعد صالح، المرجع السابق، ص 58-59.

والمدمجة بمواقع التواصل الاجتماعي والتي من أشهرها على الإطلاق موقع فيسبوك Facebook.[1]

يمكن تعريف البيانات الشخصية بأنها " أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده (موضوع البيانات) بشكل مباشر أو غير مباشر"[2].

المشرع الجزائري ومن خلال المادة الثالثة بفقرتها الأولى من القانون 18-07 عرف المعطيات ذات الطابع الشخصي بأنها" كل معلومة بغض النظر عن دعامتها متعلقة بشخص معروف أو قابل للتعرف عليه والمشار إليه أدناه " الشخص المعني" بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[3].

قبل عرضنا لصور الاعتداء على البيانات الشخصية بصفة خاصة والخصوصية المعلوماتية لابد لنا من توضيح المراد بحماية هذه البيانات، ويقصد بمفهوم حماية البيانات في المواثيق المتقدمة والقوانين، أن تكون هذه البيانات الشخصية[4]:

1-قد تم الحصول عليها بطريق مشروع وقانوني.

2-تستخدم للغرض الأصلي والمحدد.

3-تتصل بالغرض المقصود من الجمع ولا تتجاوزه، ومحصورة بذلك.

4-صحيحة وتخضع لعمليات التحديث والتصحيح.

---

[1] https://fr.wikipedia.org/wiki/Facebook (consulté le 09/09/2019).

[2] مروة زين العابدين سعد صالح، المرجع السابق، ص 67.

[3] القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 الصادر بالجريدة الرسمية العدد 34 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

[4] أنظر كل من مروة زين العابدين سعد صالح، المرجع السابق، ص 48. وحنان ريحان مبارك المضحكي، المرجع السابق، ص 321.

5-يتوفر حق الوصول إليها.

6-تحفظ في السرية وتحمى سريتها وفق معايير الأمن الملائمة لحماية المعلومات ومظم المعالجة.

7-يتم تدميرها وإتلافها بعد استنفاذ الغرض من جمعها.

إن الشرعية الإجرائية تلزم جهات التحقيق بالتقيد بقواعد معينة لدى سعيها إلى جمع الأدلة المتعلقة بالجريمة الإلكترونية، وهذا من أجل صون وحماية الخصوصية المعلوماتية من أي شكل من أشكال الخروقات والانتهاكات التي قد تتسبب فيها جهات التحقيق في الجريمة الإلكترونية. وهذا الأمر سنتناوله بالتفصيل في دراستنا هذه لدى تطرقنا لإجراءات جمع الدليل الإلكتروني. غير أن هذا لا يمنعنا من تقديم ذلك التصنيف الذي وضعه الأستاذ والفقيه Ulrich Sieber حيث يصنف صور الاعتداء على الخصوصية المعلوماتية كالتالي[1]:

- استعمال بيانات شخصية غير حقيقية.
- جمع أو معالجة بيانات شخصية حقيقية بدون ترخيص.
- إفشاء بيانات بصورة غير قانونية وإساءة استعمالها.
- عدم الالتزام بالقواعد الشكلية الخاصة بتنظيم عميلة جمع ومعالجة ونشر البيانات الشخصية.

ومهما كان فإن تلك القواعد الإجرائية المتعلقة بجمع الدليل الإلكتروني والتي على جهات التحقيق التقيد بها صونا للخصوصية المعلوماتية لا تخرج عن مبادئ أو أطر يمكن إيجازها في (المشروعية، الغائية، التناسبية، تحديد وقت تخزين البيانات الشخصية). فسواء تعلق الأمر بإجراءات التفتيش عن الأدلة الإلكترونية وحجزها أو بإجراءات التسرب ومراقبة الاتصالات الإلكترونية و حفظ تلك المعطيات المتعلقة بحركة السير، فجميعها

[1] Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME Study) (Jan. 1, 1998), p 64-67. Disponible pour consultation et téléchargement via le lien (disponible le 29/08/2020 à 07:20): https://www.law.tuwien.ac.at/sieber.pdf

العملية والقانونية التي أثيرت بشأنها، وكيف كانت ردة فعل التشريعات المقارنة حيال كل ذلك.

هذه الإجراءات التقليدية تتمثل في الانتقال إلى مسرح الجريمة ومعاينته، التفتيش، الضبط، الخبرة والشهادة.

المطلب الأول: الانتقال والمعاينة لمسرح الجريمة الإلكترونية

بعد اقتراف الجريمة، فغالبا ما يخلف الجاني ورائه آثارا تكون بمثابة الدليل الذي تستعين به جهات التحقيق للوصول إلى شخص الجاني. هذه الآثار وإن كانت ذات طبيعة مادية في الجرائم التقليدية إلا أنها وفي الجريمة الإلكترونية تكتسي طبيعة خاصة.

حتى تتمكن جهات التحقيق من الاستفادة من الآثار التي تركها الجاني بمسرح الجريمة عليها التنقل بسرعة من أجل معاينة كل ما له علاقة بالجريمة، فالمعاينة إجراء هام يدعم كثيرا سلطات التحقيق في سعيها لكشف الحقيقة.

الفرع الأول: تعريف المعاينة

يقصد بالمعاينة الرؤية بالعين لمكان أو لشخص أو لشيء لإثبات حالته وضبط كل ما يلزم لكشف الحقيقة، وهي إجراء يتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها[1].

والمعاينة هي إجراء من إجراءات التحقيق نص عليها المشرع الجزائري في المادة 79 من قانون الإجراءات الجزائية[2] بقوله " يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها، ويخطر بذلك وكيل الجمهورية الذي له

[1] محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة للنشر، الإسكندرية، 2005، ص 233.

[2] الأمر رقم 66-155، المرجع السابق.

الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات".

ويقصد بالمعاينة في الجريمة الإلكترونية معاينة الآثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت وتشمل الرسائل المرسلة منه أو التي يستقبلها وكافة الاتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية[1]. ويرى البعض أن أهمية المعاينة تتضاءل في الجريمة المعلوماتية وذلك لندرة تخلف آثار مادية عند ارتكاب الجريمة المعلوماتية، كما أن طول الفترة بين وقوع الجريمة أو ارتكابها وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب العبث أو المحو أو التلف لتلك الآثار[2].

الفرع الأول: الانتقال لمعاينة مسرح الجريمة

مسرح الجريمة بمفهومه التقليدي يقصد به تلك الرقعة الجغرافية أو الحيز المكاني الذي ارتكبت بداخله الجريمة، إذن فهو في هذه الحالة يأخذ مفهوم مادي، فالانتقال هنا لا يطرح أي إشكال.

في حين أن مسرح الجريمة الإلكترونية هو عبارة عن بيئة غير مادية، فهي مجرد بيانات رقمية تمتد إلى مكونات الحاسب الآلي وشبكات الإنترنت. وهنا يطرح إشكال بشأن الانتقال إلى الجريمة الإلكترونية، فجهات التحقيق هنا تجد نفسها أمام مسرحين للجريمة وليس واحدا فحسب.

فالمسرح الأول للجريمة هو المكان الذي توجد به المكونات المادية للحاسب الآلي وكل تلك الأجهزة المعلوماتية والعتاد المتصل بالتقنية الحديثة، والتي استعان بها المجرم في تنفيذ جريمته. أما المسرح الثاني فهو البيئة الإلكترونية والعالم الافتراضي الذي ارتكبت داخله الجريمة.

[1] خالد ممدوح، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009.

[2] هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط ،1994، ص 59.

فالانتقال هنا يتم من خلال الاتصال بجهاز الحاسوب ومكوناته أو الاتصال بشبكة الإنترنت وذلك من طرف خبراء ومختصين تحت إشراف سلطات التحقيق، كما قد يتم ذلك انطلاقا من مقر مزودي خدمة الإنترنت.

وتواجه المعاينة هنا مشكلة أخرى تتمثل في امتداد النطاق المكاني الذي تمت فيه الجريمة الإلكترونية، فقد يستعمل الجاني أو الجناة عدة حواسيب أو شبكات لاقتراف الجريمة، هذه الحواسيب والشبكات قد تتواجد بمكان واحد، كما قد تتواجد بأماكن متفرقة، وفي صورة أخرى أكثر تعقيدا قد يتواجد بعضها أو كلها خارج إقليم الدولة أو يتوزع على عدة دول. فالنطاق المكاني لمسرح الجريمة قد يشمل عدة دول، وكل منها ينعقد لها الاختصاص بالتحقيق والمعاينة.

الفرع الثالث: أهمية المعاينة في الجريمة الإلكترونية

المعاينة ليست إجراء تلقائي في مباشرتها بل إجراء هادف، غايته الكشف عن العناصر المادية التي تتعلق بالجريمة وتفيد في التحقيق الجاري بشأنها، فإذا انعدم ذلك الهدف كما هو الحال في جريمة التزوير المعنوية وجريمة السب التي تقع بالقول في غير علانية وغيرهما، لم يكن ثمة مجال أو مقتضى لإجرائها[1].

وبالنظر للطبيعة الخاصة للجريمة الإلكترونية التي قلما أو نادرا ما تخلف آثارا مادية خلفها تقود إلى الجاني، فإن أهمية المعاينة في الجرائم الإلكترونية تبدو ضئيلة.

زيادة على ذلك، فإن تردد العديد من الأشخاص على مسرح الجريمة في الفترة الممتدة ما بين وقت اقتراف الجريمة ووقت العلم بارتكابها قد يؤدي إلى زوال آثار الدليل. هذا دون نسيان إمكانية عبث الجاني نفسه بالدليل بعد ارتكابه للجريمة.

الفرع الرابع: إجراءات المعاينة لمسرح الجريمة الإلكترونية

إذ يمكن اتباع الإجراءات التالية عند معاينة مسرح الجريمة الإلكترونية[2]:

[1] هشام محمد فريد رستم، المرجع نفسه، ص 57.

[2] لمزيد من الإجراءات راجع نبيلة هبة هروال، المرجع السابق، ص 219 و220.

1-إبعاد الأشخاص الغير مرخص لهم من التواجد بمسرح الجريمة، ومن المساس بأي من الأجهزة الإلكترونية.

2-التريث في نقل أية مادة معلوماتية إلى حين التأكد من عدم وجود أي عامل قد يؤدي إلى إتلافها (كالمجالات المغناطيسية مثلا).

3-القيام بتصوير شاشة الحاسوب.

إلى غير ذلك من الإجراءات التي يجب أن يشرف عليها خبراء في مجال الأدلة الإلكترونية.

المطلب الثاني: التفتيش عن الدليل في الجريمة الإلكترونية

يعد التفتيش من أهم إجراءات التحقيق الابتدائي، إذ يهدف إلى ضبط الأدلة المادية للجريمة والتي تفيد في الكشف عن الحقيقة.

إن التفتيش بمفهومه التقليدي ينصب على الأشخاص والمساكن وهذا في حد ذاته كان موضوع جدل يرتبط بحق الأفراد في صون حياتهم الشخصية وأسرارهم من الانتهاك، غير أن الجدل احتدم أكثر بخصوص التفتيش الذي يقع على النظم المعلوماتية في الجريمة الإلكترونية مادام أن الأمر هنا يتعلق بعالم افتراضي وغير مادي. فبالإضافة لموضوع الخصوصية المعلوماتية للأفراد المتعلقة بمراسلاتهم وملفاتهم المخزنة بالنظم المعلوماتية، طفت إلى السطح تساؤلات حول مدى اعتبار الولوج إلى النظام المعلوماتي نوعا من التفتيش، ومدى خضوع البيئة المعلوماتية للقواعد التقليدية في التفتيش، وماهي الشروط الواجب مراعاتها.

الفرع الأول: ماهية التفتيش المتعلق بالجريمة الإلكترونية

من أجل بيان معنى التفتيش المتعلق بالنظام المعلوماتي في الجريمة الإلكترونية، يقتضي منا هذا الأمر التطرق لتعريف التفتيش أولا ثم النظر في مدى اعتبار الولوج للنظم المعلوماتية نوعا من التفتيش.

أولا: تعريف التفتيش بصفة عامة

لغة، فإن التفتيش عن الشيء هو البحث عن مظان وجوده، أما اصطلاحا فالتفتيش هو البحث عن الشيء في مستودع السر[1].

المشرع الجزائري وعلى غرار نظرائه في غالبية الدول، لم يعط تعريفا للتفتيش مفضلا ترك أمر وضع تعريف له من طرف الفقهاء. غير أنه تطرق للتفتيش كإجراء من إجراءات التحقيق الابتدائي بموجب المواد من 81 إلى 83 من قانون الإجراءات الجزائية[2]، و خصه كذلك بنص المادة 48 من الدستور الجزائري[3]التي نصت على أنه " تضمن الدولة عدم انتهاك حرمة المسكن. فلا تفتيش إلا بمقتضى القانون، وفي إطار احترامه. ولا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

ويتضح لنا بأن المشرع الجزائري لم يورد تعريفا خاصا ودقيقا للتفتيش بقدر ما أعتبره إجراء من إجراءات التحقيق وإحاطته بضوابط صارمة نظرا لأهميته في كشف الأدلة وخطورته فيما قد يترتب عنه من مساس بحرية الأشخاص وبكرامتهم[4].

في حين عرف المشرع المصري تفتيش المنازل بموجب المادة 91 من قانون الإجراءات الجنائية[5] على أنه "....عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناءً على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة".

[1] طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، 2015، ص 352.

[2] الأمر رقم 66-155، المرجع السابق.

[3] المرسوم الرئاسي رقم 20-442 المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020، المرجع السابق.

[4] زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011، ص 130.

[5] القانون رقم 150 لسنة 1950، المرجع السابق.

أما من جانب الفقه، فلقد تعددت وتنوعت التعريفات التي اقترحها الفقهاء والتي تناولت موضوع التفتيش، ونذكر من بينها:

يعرف التفتيش على أنه "إجراء من إجراءات التحقيق يهدف إلى التوصل إلى أدلة جريمة ارتكبت فعلا، وذلك بالبحث عن الأدلة في مستودع السر، سواء أجري على شخص المتهم أو في منزله دون توقف على إرادته"[1]. ويلاحظ بأن هذا التعريف لم يشر إلى الجهة القائمة بالتفتيش فاكتفى بالقول إنه إجراء من إجراءات التحقيق.

وهناك من عرفه على أنه "إجراء تقوم به السلطة القضائية للاطلاع على محل يتمتع بحرمة خاصة للبحث عن الأدلة اللازمة للتحقيق الجنائي"[2]. أما هذا التعريف ورغم إشارته إلى الجهة المباشرة للتفتيش كونها جهة قضائية إلا أنه خص به المحل دون الشخص، كما لم يشر إلى إرادة الشخص المراد تفتيش محله، هل يعتد برضاه أم لا.

كما يعرف التفتيش بأنه "إجراء من إجراءات التحقيق يباشر من مختص عند وقوع جناية أو جنحة للبحث عن أدلة الجريمة متى استلزمت ضرورة التحقيق ذلك، ويباشر في محل له حرمة سواء رضي به من يباشر حياله أو لم يرض"[3]. نجد هذا التعريف الأخير أكثر إلماما بتعريف التفتيش مقارنة بالتعريفات السابقة، ولو أنه هو الآخر تناول تفتيش المحل دون الشخص.

والملاحظ بأن التعريفات الفقهية رغم تعددها إلا أنها تكاد تتفق أو بالأحرى أنها لا تخرج عن كون التفتيش هو من إجراءات التحقيق تباشره جهة قضائية مختصة بهدف الوصول إلى أدلة تخص جريمة وقعت، ويجري التفتيش بمكان يتمتع بالخصوصية رغم إرادة صاحب المكان الخاضع للتفتيش.

[1] مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، 2004، ص 530.

[2] توفيق محمد الشاوي، حرمة الحياة الخاصة ونظرية التفتيش، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006، ص 27.

[3] عبد الإله النوايسة، ضمانات المتهم أثناء التحقيق الابتدائي (دراسة مقارنة بين التشريعين الأردني والمصري)، أطروحة دكتوراه غير منشورة، جامعة عين شمس، مصر، 2000، ص 301.

وكما يتضح، فإن التفتيش ليس غاية في حد ذاته، وإنما هو وسيلة لغاية تتمثل فيما يمكن الوصول من خلاله إلى أدلة مادية تسهم في بيان وظهور الحقيقة[1].

ثانيا: تفتيش نظم المعلوماتية

بتطبيق مفهوم التفتيش كما سبق بيانه على الولوج داخل النظام المعلوماتي، يمكن القول أن هذا الولوج يعد تفتيشا ما دام أنه بحث في مستودع سر الأشخاص والاطلاع على خصوصية أضفى عليها القانون حماية. غير أن اعتبار الولوج إلى النظام المعلوماتي تفتيشا لا يعني انطباق المفهوم التقليدي للتفتيش عليه، ولكن يتعين استحداث قواعد خاصة تتماشى مع الطبيعة الخاصة لهذا الإجراء المستمد من طبيعة الجريمة الإلكترونية في حد ذاتها[2].

يعرف جانب من الفقه الولوج داخل النظام المعلوماتي بأنه " الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون هذا المحل جهاز الحاسوب أو نظمه أو الإنترنت"[3].

وفيما يلي سنتطرق إلى التفتيش المنصب على كل من المكونات المادية والمعنوية للحاسب الآلي وكذا شبكات الأنترنت.

أ-تفتيش المكونات المادية للحاسب الآلي

يتفق الفقهاء على أن التفتيش في مجال الجريمة الإلكترونية إذا كان ينصب على المكونات المادية للأجهزة المعلوماتية للحاسب الآلي ومختلف ملحقاته وأوعيته، أو أية

[1] حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف، الإسكندرية 1982، ص 385. أشار إليه: أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، 2015، ص 140.

[2] محمد كمال شاهين، المرجع السابق، ص 275.

[3] علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الثانية، منشورات جامعة العلوم التطبيقية، مملكة البحرين 2010، ص 20.

وسيلة من وسائل التقنية الحديثة المستعملة في مجال الجريمة الإلكترونية، فهذا التفتيش إذا كان بمناسبة جريمة إلكترونية حدثت فإنه يتم وفق القواعد العامة للتفتيش والمطبقة على الجريمة التقليدية، ولا إشكال يطرح هنا ما دام التفتيش سيرد على المكونات المادية كما أشرنا.

وتجدر الإشارة هنا أن قواعد التفتيش في هذه الحالة تراعي طبيعة المكان الموجودة فيه هذه المكونات المادية المراد تفتيشها، هل الأمر يتعلق بأماكن عامة أو أماكن خاصة أو أماكن عامة بالتخصيص. فإذا كانت موجودة بمسكن المتهم أو ملحقاته وجب مراعاة الحالات التي أجاز فيها القانون تفتيش المسكن وكذا الضمانات التي يقررها المشرع في هذه الحالة.

المشرع الجزائري تناول موضوع التفتيش المتعلق بالجرائم الإلكترونية والتي عبر عنها بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بالفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية[1] والتي جاءت كاستثناء لإجراء التفتيش الذي نص عليه في المادة 64 من نفس القانون[2].

[1] القانون 06-22، المرجع السابق. "...وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص. عندما يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك. كما يمكنه اتخاذ التدابير الأخرى المنصوص عليها في التشريع المعمول به، وأن يأمر بأية تدابير تحفيظية، إما تلقائيا أو بناء على تسخير من النيابة العامة أو بناء على طلب من ضابط الشرطة القضائية. لا تمس هذه الأحكام بالحفاظ على السر المهني المنصوص عليه في الفقرة الثالثة من المادة 45 من قانون الإجراءات الجزائية."

[2] المادة 64 لا يجوز تفتيش المساكن ومعاينتها وضبط للأشياء المثبتة للتهمة إلا بإذن مكتوب من وكيل الجمهورية المختص ورضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات ، ويكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن فإن لم يعرف الكتابة فيمكنه الاستعانة بشخص يختاره بنفسه ويذكر ذلك في المحضر مع الإشارة لرضاه.

وتطبق فضلاً عن ذلك أحكام المواد من 44 إلى 47 من هذا القانون.

أما إذا كانت هذه المكونات المادية بحوزة شخص متواجد بأماكن عامة بطبيعتها كالشوارع والساحات العامة مثلا، أو الأماكن العامة بالتخصيص كالمحلات والمقاهي والمطاعم...الخ، فإن تفتيشها يخضع لتلك الأحكام والقواعد المقررة لتفتيش الأشخاص مع ما تحمله من ضمانات وما يرد عليها من قيود[1].

ونجد في التشريعات المقارنة أن هناك بعض القوانين في مجال الإجراءات الجنائية تناولت موضوع تفتيش المكونات المادية للحاسب الآلي كقانون الإجراءات الجنائية اليوناني مثلا، فلقد منحت المادة 251 من قانون الإجراءات الجنائية اليوناني سلطات التحقيق صلاحية القيام ب" أي شيء يكون ضروريا لجمع وحماية الدليل"[2] وهذا ما استند عليه الفقه في اليونان[3]، إذ فسر عبارة "...أي شيء..." بأنها تشمل البيانات المخزنة أو المعالجة إلكترونيا, وبالتالي فإن ضبط المعطيات الإلكترونية بمختلف صورها المخزنة في الذاكرة الداخلية للحاسوب لا تثير أي خلاف في اليونان[4]. وكذلك بالقانون الجنائي الكندي[5] وكذا قانون إساءة استعمال الحاسب الآلي البريطاني[6].

غير أنه عندما يتعلق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 47 (الفقرة 3) من هذا القانون, تطبق الأحكام الواردة في تلك المادة وكذا أحكام المادة 47 مكرر" المرجع نفسه.

[1] أنظر في هذا المعنى كل من: محمد كمال شاهين، المرجع السابق، ص 278 وما بعدها. طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 364 وما بعدها. أشرف عبد القادر قنديل، المرجع السابق، ص 140 و ما بعدها. بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011، ، ص 68 و ما بعدها.

[2] عمار عباس الحسيني، التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات الجنائي، المركز العربي للدراسات والبحوث العلمية، 2017، ص 63.

[3] Irini VASSILAKI, Computer crime and other crimes against information technology, RIDP (Revue Internationale de droit pénal), 1993, p. 371.

[4] حابس يوسف زيدات، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية، مجلة مركز حكم القانون ومكافحة الفساد، العدد 2، 2019، ص 10. يمكن الاطلاع على هذا المقال أو تحميله على الرابط (متاح بتاريخ 2020/04/14 على الساعة 19:20):

https://www.qscience.com/content/journals/10.5339/rolacc.2019.9?crawler=true

[5] Donald K. PIRAGOFF, Computer crimes and other crimes against information technology in Canada, RIDP (Revue Internationale de droit pénal), 1993, p 241.

[6] David FERBRACHE, Pathology of Computer Viruses, Springer-Verlag, London Ltd, 1992, p 233.

أشار إليهم كل من: محمد كمال شاهين، المرجع السابق، ص 280. طارق إبراهيم الدسوقي عطية، المرجع السابق، ص 365-366.

أمر قضائي لتفتيش وضبط أي شيء تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأن جريمة قد وقعت أو يشتبه في وقوعها. أو أن هناك نية لاستخدامه في ارتكاب جريمة، أو أنه سيتيح دليلا على وقوع الجريمة[1].

المشرع الفرنسي حسم الأمر من خلال تعديله لقانون الإجراءات الجزائية سنة 2004 وذلك بإدراجه عبارة "أو معطيات معلوماتية ou des données informatiques " للمادة 94[2] من قانون الإجراءات الجزائية وذلك بموجب المادة 42 من القانون رقم 575-2004 المتعلق بالثقة في الاقتصاد الرقمي.

فجاءت المادة 94 من قانون الإجراءات الجزائية الفرنسي في صيغتها المعدلة كالتالي " يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء أو معطيات معلوماتية والتي يكون الكشف عنها مفيدا لإظهار الحقيقة "

المشرع الجزائري بدوره تدارك موضوع تفتيش المكونات المعنوية وذلك من خلال المادة الخامسة من القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات

---

peut à tout moment décerner un mandat autorisant un agent de la paix ou, dans le cas d'un fonctionnaire public nommé ou désigné pour l'application ou l'exécution d'une loi fédérale ou provinciale et chargé notamment de faire observer la présente loi ou toute autre loi fédérale, celui qui y est nommé :

- d) d'une part, à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir;

e) d'autre part, sous réserve de toute autre loi fédérale, dans les plus brefs délais possible, à transporter la chose devant le juge de paix ou un autre juge de paix de la même circonscription territoriale ou en faire rapport, en conformité avec l'article 489.1".

Article 487 du Code criminel de Canada (L.R.C. (1985), ch. C-46)."… à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir…" Disponible sur le lien (consulté le 22/26/2020): https://laws-lois.justice.gc.ca/fra/lois/C-46/page-109.html#docCont

[1] عبد اللاه أحمد هلالي، المرجع السابق، ص 201.

[2] Article 94 du CPP "Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver des objets ou des données informatiques dont la découverte serait utile à la manifestation de la vérité…". la loi n° 57-1426 instituant un code de procédure pénale, Op.cit. Modifié et complété.

Article 42 **(**LOI n° 2004-575 du 21 juin 2004, JORF n°0143 du 22 juin 2004- pour la confiance dans l'économie numérique**):** A l'article 94 du code de procédure pénale, après les mots: « des objets », sont insérés les mots: « ou des données informatiques ».

1-تفتيش حاسوب المتهم عند اتصاله بحاسوب آخر موجود بمكان آخر داخل الدولة

عالجت العديد من التشريعات المقارنة وكذا الفقه المقارن هذه الحالة، كما تناولت هذه المسألة الاتفاقية الأوربية[1] لبودابست 2001 والمتعلقة بالجرائم الإلكترونية.

ففي ألمانيا تحظر المادة 103 من قانون الإجراءات الجنائية[2] الألماني تفتيش منزل أو محلات شخص لا يشتبه في ارتكابه لجريمة، إلا إذا كان الغرض من هذا التفتيش القبض على متهم، أو طلب معلومات بخصوص جريمة أو ضبط أشياء محددة. ولا يجوز التفتيش إلا إذا توافرت أدلة تفيد بأن هذا التفتيش سوف يؤدي إلى الكشف عن شخص أو قرائن أو أشياء.

ولقد استند الفقه الألماني على نص هذه المادة من أجل دعم موقفه القائل بجواز امتداد التفتيش إلى سجلات البيانات المخزنة بموقع أو مكان آخر خارج الموقع أو المكان الذي يتم فيه التفتيش[3].

في بلجيكا وقبل صدور القانون المتعلق بالجريمة الإلكترونية بتاريخ 2000/11/28 والذي بدأ سريانه بتاريخ 2001/02/13 لم يكن هناك أي تشريع يختص بالجريمة الإلكترونية والمعاقبة عليها، وبعد صدور هذا القانون وبموجب المادة الثامنة منه أدخل تعديلا على قانون التحقيق الجنائي من أجل تكييف نصوصه مع طبيعة الجريمة الإلكترونية، فأضاف له المادة 88 مكرر1 (88ter)[4] والتي تناولت موضوع تفتيش

---

[1] Convention sur la cybercriminalité Budapest.Op.Cit.

[2] قانون الإجراءات الجنائية الألماني الصادر في 7 أبريل 1987 المعدل بالمادة 3 من قانون 23 أبريل 2014

THE GERMAN CODE OF CRIMINAL PROCEDURE "Code of Criminal Procedure as published on 7 April 1987 (Federal Law Gazette I, p. 1074, 1319), as last amended by Article 3 of the Act of 11 July 2019 (Federal Law Gazette I, p. 1066)."

Section 103 [Searches in Respect of Other Persons] "Searches in respect of other persons shall be admissible only for the purpose of apprehending the accused or to follow up the traces of a criminal offence or to seize certain objects, and only if certain facts support the conclusion that the person, trace, or object sought is located on the premises to be searched…". A consulter via le lien:
https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html (disponible le 19/09/2018 à 22:35)

[3] أنظر في هذا المعنى:

Henrik W.K. Kaspersen, Computer crime and other crimes against information technology, AIDP (International review of penal law), 1993, p 479.

[4] Art. 88ter. " Le juge d'instruction peut étendre la recherche dans un système informatique ou une partie de celui-ci, entamée sur la base de l'article 39bis, vers un système informatique ou une partie de celui-ci qui se

في هولندا وبتاريخ 21 سبتمبر2018[1] تم نشر القانون المتعلق بالجريمة الإلكترونية بالجريدة الرسمية والذي دخل حيز التنفيذ وبدأ سريانه بتاريخ 01 مارس 2019، وجاء هذا القانون من أجل إضفاء فعالية أكثر في مواجهة الجريمة الإلكترونية لا سيما في الشق الإجرائي منه، إذ أدخل تعديلات على قانون الإجراءات الجزائية يسمح بموجبها لجهات التحقيق من الولوج إلى الأنظمة المعلوماتية للمشتبه بهم تشمل كل تلك الأجهزة التي بها نظام معالجة آلية للبيانات (كجهاز الكمبيوتر أو الهواتف الذكية والخوادم). وقيد ذلك بشروط صارمة تلزم الجهات المباشر للتفتيش بتحديد الهدف من التحقيق، كما أن التحقيق في هذه الحالة لابد أن يقتصر فقط على الجرائم الخطيرة. وبما أن الاطلاع على البيانات المخزنة بالأنظمة المعلوماتية فيه انتهاك جسيم للحياة الخاصة للشخص المستهدف فإن المشرع قيد اللجوء إلى هذا الإجراء بشرط وجود حالة استعجال قصوى تطلبها التحقيق، وأن يصدر الأمر من قاض التحقيق، وأن تكون الأفعال ضمن الجرائم الخطيرة (نشر أو حيازة مواد إباحية للأطفال، المشاركة في منظمة إجرامية، تجنيد إرهابيين، تزور الوثائق وغسيل الأموال).

وبما أن هولندا بلد طرف في اتفاقية بودابست، فالاتفاقية تنص كذلك على إمكانية أن يمتد التفتيش إلى مواقع داخل الشبكة إذا تبين أثناء التفتيش أن هناك بيانات مفيدة وذات صلة بموضوع التفتيش مخزنة بنظام معلوماتي آخر. وهذه النقطة كانت هولندا قد نصت عليها في قانون جرائم الحاسوب لسنة 1993. وبحسب المادة 125ذ/1 (125j/1)[2] من قانون الإجراءات الجزائية الهولندي فإنها تسمح للجهة المباشرة للتفتيش بأن يمتد تفتيشها

[1] لمزيد من المعلومات بالرابط: (متاح بتاريخ 2019/04/09 الساعة 17:20)

http://www.elexica.com/en/legal-topics/crime-fraud-and-investigations/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force

[2] Section 125j

1. In the case of a search, a computerised device or system located elsewhere may be searched for data stored in that device or system that is reasonably required in order to reveal the truth from the place where the search takes place. If such data is found, then it may be recorded.=

= نشير هنا إلى أنه ينتظر تعديل قانون الإجراءات الجزائية الهولندي لسنة 1993 بعد الاقتراحات المقدمة بتاريخ 2015/09/30، متوفر بالرابط:

https://www.government.nl/topics/modernisation-code-of-criminalprocedure/contents-new-code-of-criminal-procedure

ليشمل أنظمة معلوماتية أخرى انطلاقا من النظام المعلوماتي المتواجد بالمكان الذي تجري فيه عملية التفتيش[1].

المشرع الجزائري بدوره تناول هذه المسألة وذلك بموجب المادة 05 الفقرة 02 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]. إذ نصت المادة صراحة على جواز تمديد التفتيش بقولها "... في الحالة المنصوص عليها في الفقرة (أ) من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد 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 مسبقة بذلك...".

الاتفاقية الأوربية لسنة 2001 ببودابست والمتعلقة بالجرائم الإلكترونية وبنص المادة 19 الفقرة الثانية من القسم الرابع منها[3] أجازت لكل دولة طرف في الاتفاقية سن ما يلزمها من التدابير التشريعية، بحيث تتيح للسلطات القائمة بتفتيش نظام معلوماتي معين (أو جزء منه) و المتواجد فوق أراضيها، وفي حالة ما إذا كانت هناك أسباب تجعل هذه السلطات تعتقد بأن البيانات المطلوبة هي مخزنة بنظام معلوماتي آخر، يمكن إذن لهذه السلطات أن توسع نطاق التفتيش بحيث يمتد إلى أي النظام معلوماتي الآخر متى أتيح لها الوصول لهذه البيانات المخزنة انطلاقا من النظام المعلوماتي الأصلي محل التفتيش.

---

[1] أنظر في هذا المعنى:

Bert-Jaap Koops, Cybercrime Legislation in the Netherlands, Electronic Journal of Comparative Law, vol. 14.3, (December 2010), p 18.

لمزيد من المعلومات بالرابط: (متاح بتاريخ 2019/04/09 الساعة 20:45) https://www.ejcl.org/143/art143-10

[2] القانون09-04، المرجع السابق.

[3] Article 19 (Convention sur la cybercriminalité Budapest.Op.Cit)

"……..……..

2. Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système……..

(Convention sur la cybercriminalité Budapest.Op.Cit)

المعلوماتي الأولي، هي مخزنة بنظام معلوماتي آخر متواجد خارج الإقليم الوطني، يتم جمعها من طرف ضابط الشرطة القضائية مع ضرورة مراعاة الالتزامات الدولية السارية في هذا الشأن".

في هولندا فإن المادة 125ذ/2 (125j/2)[1] من قانون الإجراءات الجزائية الهولندي تبدو مبهمة كونها تتحدث عن أن كون التفتيش داخل الشبكة يقتصر فقط على القدر التي تكون فيه الشبكة متاحة بشكل قانوني وبموافقة الشخص المخول استخدام الجهاز أو النظام المعلوماتي. وفقا للتفسير الحالي، لا يمكن للبحث في الشبكة أن يتجاوز الحدود الهولندية. إلى غاية الآن لا توجد معلومات متاحة حول كيفية تفسير هولندا للاستثناء الذي جاءت به اتفاقية بودابست المتعلقة بالجرائم الإلكترونية فيما يتعلق بالتفتيش المنصب على الشبكات الواقعة خارج الحدود الإقليمية بموافقة السلطات القانونية المخولة[2]، ونقصد به هنا ما جاء بمحتوى المادتين[3] 31 و32 من الاتفاقية.

وعلى ذكر اتفاقية بودابست المتعلقة بالجرائم الإلكترونية[4]، فإن هذه الأخيرة قد تناولت في فصلها الثاني المساعدة المتبادلة ذات الصلة بسلطات التحقيقات، حيث نصت المادة 31

[1] Section 125j "……..**2.** The search shall be limited to the extent that the persons, who normally work or reside at the place where the search is being conducted, have access thereto from that place with the consent of the person entitled to use the computerised device or system"

[2] أنظر في هذا المعنى:

Bert-Jaap Koops, Op.Cit, p 18.

[3] **Article 31** – Entraide concernant l'accès aux données stockées

1-Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2-La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3-La demande doit être satisfaite aussi rapidement que possible dans les cas suivants:

a- il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification; ou

b- les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public Une Partie peut, sans l'autorisation d'une autre Partie :

a- accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données; ou

b- baccéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

[4] Convention sur la cybercriminalité Budapest.Op.Cit

على المساعدة المتبادلة ذات الصلة بالنفاذ إلى بيانات الكومبيوتر المخزنة في حين جاء بمحتوى المادة 32 موضوع النفاذ العابر للحدود إلى بيانات الكومبيوتر المخزنة عبر الموافقة أو عندما تكون متاحة للجمهور أي عامة الناس.

فالمادة 31 من الاتفاقية في فقرتها الأولى أجازت لأي دولة طرف الولوج إلى بيانات مخزنة في نظام معلوماتي متواجد بإقليم دولة أخرى وذلك بعد تقديمها لطلب بهذا الموضوع لتلك الدولة الأخرى. وبالمقابل على الدولة الأخرى الاستجابة لهذا الطلب بل وبشكل مستعجل إذا كان هناك اعتقاد أن البيانات المتصلة بموضوع التفتيش معرضة للضياع أو للتعديل، وهذا ما جاء بالفقرة الثالثة لنفس المادة.

كما أجازت اتفاقية بودابست[1] لأي دولة طرف الولوج إلى نظام معلوماتي متواجد بإقليم دولة أخرى دون تقديم طلب أو الحاجة إلى موافقة الدولة الأخرى، ويكون ذلك في حالتين أشارت إليهما المادة 32، الأولى إذا تعلق الأمر ببيانات متاحة للجمهور أي بإمكان أي شخص من عامة الناس المستخدمين للشبكة الولوج إليها. في حين أتاحت الحالة الثانية للدولة المباشرة للتفتيش الولوج إلى البيانات المخزنة بنظام معلوماتي متواجد بإقليم دولة أخرى طرف بالاتفاقية، وذلك في حال حصولها على الموافقة القانونية والطوعية للجهة التي تملك السلطة القانونية للكشف عن البيانات المتواجدة بالنظام المعلوماتي المذكور.

وفي اعتقادنا، فإن هذه الحالة الثانية ورغم أنها تجد مبررا في ضرورة سرعة التحرك مجاراة لطبيعة الجريمة الإلكترونية ودونما انتظار خشية ضياع البيانات التي قد تشكل دليل مهما، إلا أنها في الواقع تعد خرقا لسيادة الدولة الأخرى وهذا الأمر يستوجب وضع آليات مناسبة تراعي في نفس الوقت سيادة الدول ومتطلبات جهات التحقيق معا، ولا يتسنى ذلك إلا من خلال التعاون الدولي الذي لا مناص منه.

المبدأ المطبق أو المعمول به في هولندا هو"computer-based jurisdiction" أو "الاختصاص القضائي المستند إلى الكمبيوتر" أي الآخذ بالموقع الجغرافي للخادم أو "لجهاز الكمبيوتر أو النظام المعلوماتي" والذي يحدد الاختصاص القضائي بالتفتيش. هذا

[1] Ibid.

يعني أن جهات نفاذ القانون لا يمكنها أن تفعل أي شيء إذا كان الخادم خارج هولندا. وبتطبيق هذا المبدأ فإن عمليات التفتيش خارج الحدود الإقليمية لهولندا غير مسموح بها[1].

وأيد هذا الاتجاه القضاء الألماني الذي أبدى تحفظه بشأن هذه المسألة ويعتبر بأن امتداد التفتيش إلى أنظمة معلوماتية في الخارج وما يتبعه من الحصول على البيانات المخزنة هو بمثابة خرق لسيادة الدول في ظل عدم وجود اتفاقية ثنائية أو دولية تجيز ذلك. وهذا الطرح أيده كذلك القضاء بألمانيا في قضية الحصول على بيانات تواجدت بنظام معلوماتي بالخارج وتحديد بدولة سويسرا[2].

في الجزائر فإن المشرع الجزائري وبموجب المادة 05 الفقرة 03 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3] أجاز تمديد التفتيش إلى المنظومة المعلوماتية الواقعة خارج الإقليم الوطني وذلك من خلال مساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

وكما أشرنا إلى ذلك سابقا، فإنه وبحسب رأينا فإننا نعتقد بأن تمديد سلطات التحقيق لإجراءات التفتيش إلى المنظومة المعلوماتية خارج إقليم الدولة هو أمر لا مناص منه بغية وضع اليد على كافة الأدلة الإلكترونية التي من شأنها إظهار الحقيقة، غير أن ذلك يجب أن يتم وفق أطر قانونية تكفل صيانة واحترام سيادة الدول، وهذا يحتم على الدول ضرورة التعاون في مجال التحقيق في الجريمة الإلكترونية.

[1] Frederik Paul Emile WIEMANS, Onderzoek van gegevens in geautomatiseerde werken, Nijmegen, Wolf Legal Publishers, 2004, p. 152-162. Cité par:
Odinot, Geralda & Verhoeven, Maite & Pool, Ronald & De Poot, Christianne, Organised Cybercrime in the Netherlands. Empirical findings and implications for law enforcement, Den Haag: WODC, Ministry of Security and Justice, February 2017, p 24. À consulter via le lien:
https://www.wodc.nl/binaries/Cahier%202017-1_Full%20text_tcm28-244615.pdf
disponible le 14/12/2018 à 20h10.

[2] Manfred Möhrenschlager, Computer crime and other crimes against information technology in Germany, R.I.D.P, Vol. 64, 1-2, 1993, p 351.
أشار إليه كل من: بكري يوسف بكري، المرجع السابق، ص 83. وطارق إبراهيم الدسوقي عطية، المرجع السابق، ص 372. ومحمد كمال شاهين، المرجع السابق، ص 288.

[3] القانون 09-04، المرجع السابق.

الفرع الثاني: شروط تفتيش النظم المعلوماتية

يعتبر التفتيش من الإجراءات التي تمس بالحرية الشخصية للأفراد وكذا بحرمة حياتهم الخاصة، لدى عمدت معظم التشريعات على تقييده وإحاطته بشروط تحافظ على التوازن بين حق المجتمع في ردع الجناة من جهة، وبالمقابل صيانة الحريات الفردية من جهة أخرى.

تنقسم شروط التفتيش إلى قسمين، شروط موضوعية وأخرى شكلية.

أولا: الشروط الموضوعية للتفتيش

يقصد بالشروط الموضوعية تلك الضوابط التي لابد من توافرها حتى نكون أمام تفتيش صحيح. هذه الشروط تتلخص في السبب، المحل والسلطة المختصة بالتفتيش.

أ-سبب التفتيش في النظام المعلوماتي

بصفة عامة فإن السبب والمبرر للتفتيش هو السعي من أجل الحصول على دليل مادي يفيد جهات التحقيق في الوصول إلى الحقيقة. ويقوم هذا السبب في حالة وقوع جريمة توصف بجناية أو جنحة، واتهام شخص أو عدة أشخاص بارتكابها، وقيام قرائن قوية بوجود أشياء قد تفيد في الوصول إلى الحقيقة وذلك إما لدى المتهم أو بمسكنه أو لدى شخص آخر أو في مسكنه.

وفي حال تطبيق ما سبق على الجريمة الإلكترونية، فإن سبب تفتيش النظام المعلوماتي يتحقق كالآتي:

وقوع جريمة إلكترونية، اتهام شخص أو عدة أشخاص بارتكاب جريمة من الجرائم الإلكترونية أو المشاركة فيها، توافر قرائن قوية على وجود بيانات أو أجهزة أو معدات معلوماتية لدى المتهم بالجريمة الإلكترونية أو غيره.

1-وقوع جريمة إلكترونية

إن كلمة أو لفظ "وقوع" يفيد هنا بأن الجريمة تكون قد حدثت بالفعل، فلا يكفي احتمال حدوثها في المستقبل للقيام بإجراءات التفتيش.

غير أنه وبحسب رأينا، نجد بأن المشرع الجزائري قد أورد استثناء على ذلك بموجب المادة 04 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها [1]. حيث أن المادة 05 من نفس القانون أجازت تفتيش المنظومات المعلوماتية في الحالات المنصوص عليها في المادة 04 من نفس القانون، وعند تفحص محتوى المادة 04 نجد بأن المشرع نص في الفقرة (ب) من هذه المادة على أنه "في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني".

إذن يفهم من محتوى المادة بأن مباشرة إجراءات التفتيش في الجريمة الإلكترونية جائزة حتى إذا كانت الجريمة لم تقع بعد، وهذا الاستثناء يسري فقط على ما جاءت به الفقرة (ب) من المادة 04 أعلاه.

وحتى يصدر إذن بالتفتيش للمنظومة المعلوماتية يجب أن يكون الفعل مجرما أولا، وذلك احتراما لمبدأ الشرعية، إذ لا جريمة ولا عقوبة إلا بنص من القانون. أضف إلى ذلك أن يوصف الفعل المجرم بكونه جناية أو جنحة، فلا تفتيش إذا تعلق الأمر بمخالفة نظرا لقلة خطورتها.

وهذا هو النهج الذي سارت عليه التشريعات المقارنة وسار عليه أيضا المشرع الجزائري حيث أدرج في الفصل السابع من القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004[2] جرائم الاعتداء على نظم المعالجة الآلية للمعطيات وكذا القانون رقم 09-04 القانون

[1] القانون 09-04، المرجع السابق.

[2] القانون رقم 04-15 المؤرخ في 17 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، الصادر بالجريدة الرسمية العدد 71. المعدل والمتمم لقانون العقوبات.

المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها [1].

2-اتهام شخص أو عدة أشخاص معينين بارتكاب جريمة إلكترونية:

إن مجرد وقوع جريمة إلكترونية لا يكفي لقيام سبب لتفتيش شخص ما أو تفتيش مسكنه، بل يجب أن يوجه إليه الاتهام بصفته فاعلا أصليا أو شريكا ساهم في ارتكاب واقتراف تلك الجريمة التي وقعت، ويجب أن تكون هناك دلائل قوية على ذلك.

ويقصد بالدلائل الكافية في الجريمة الإلكترونية مجموعة من المظاهر المعينة التي تنهض على السياق العقلي والمنطقي لملابسات الواقعة وكذلك خبرة وحرفية القائم بالتفتيش والتي تؤيد نسبة جريمة الإنترنت إلى شخص معين سواء بصفته فاعلا أو شريكا [2].

3-توافر قرائن قوية على وجود بيانات أو معدات معلوماتية لدى المتهم بالجريمة الإلكترونية أو غيره:

من المستقر عليه في التشريعات المقارنة أن الإذن بالتفتيش يلزم أن يصدر بناء على تحريات جدية، فلا يكفي لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش مجرد وقوع جريمة من الجرائم الإلكترونية، واتهام شخص معين بارتكابها، بل يجب أن تتوافر لدى المحقق أسباب كافية أنه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة الإلكترونية، أو أشياء متحصلة منها، أو أي أدلة إلكترونية يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتهم أو غيره [3].

[1] القانون 09-04، المرجع السابق.

[2] عبد اللاه أحمد هلالي، المرجع السابق، ص 120.

[3] أشرف عبد القادر قنديل، المرجع السابق، ص 149.

التشريعات المشرقية كلبنان ومصر) صلاحية مباشرة التفتيش والذي يعد أصلا من اختصاص جهة التحقيق.

يثار تساؤل بخصوص التلبس في مجال الجريمة الإلكترونية، فهل يتصور إمكانية ضبط المجرم الإلكتروني متلبسا؟ إن الإجابة بالإيجاب تعتبر في غاية الصعوبة ذلك أن الجريمة الإلكترونية يتم اكتشافها عادة بعد انتهاء المجرم الإلكتروني من سلوكه الإجرامي. بيد أنه يمكن تصور حالة التلبس فقط في حالة تواجد ضابط الشرطة القضائية والمجرم الإلكتروني في نفس الوقت في إحدى فضاءات الإنترنت فيتم ضبط الجاني وهو بصدد نشر صور ومحتويات جنسية للأطفال مثلا، أو قام بتحميلها وتعبئتها داخل مفتاح الذاكرة أو نقلها إلى حاسوبه المحمول ...الخ. ففي هذه الحالة يمكن تصور مباشرة ضابط الشرطة القضائية بتفتيش المتهم.

2-تفتيش النظم المعلوماتية بناء على صدور الإذن أو الإنابة:

الأصل هو أن تباشر جهات التحقيق الابتدائي جميع إجراءات التحقيق بنفسها، غير أنه ونظرا لانشغالها بأعمال أخرى فيجوز لها أن تكلف غيرها للقيام بإجراء أو أكثر من إجراءات التحقيق.

لقد أجازت المادة 68 (الفقرة 06) من قانون الإجراءات الجزائية الجزائري[1] لقاض التحقيق أن يندب ضباط الشرطة القضائية للقيام بتنفيذ جميع أعمال التحقيق اللازمة وذلك ضمن الشروط المنصوص عليها في المواد من 138 إلى 142 من قانون الإجراءات الجزائية[2].

[1] القانون رقم 01-08 المؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001 الصادر بالجريدة الرسمية العدد 34 المؤرخة في 5 ربيع الثاني 1422 الموافق 27 يونيو سنة 2001 يعدل ويتمم الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية.

[2] المواد (138-141) بموجب الأمر66-155، المرجع السابق، وكذلك القانون رقم 82-03 المؤرخ في 19 ربيع الثاني عام 1402 الموافق 13 فبراير 1982، الصادر بالجريدة الرسمية العدد 7 الصادرة بتاريخ 22 ربيع الثاني عام 1402 الموافق 16 فبراير سنة 1982.المعدل والمتمم للأمر رقم 66-155 والمتضمن قانون الإجراءات الجزائية. وكذلك القانون رقم 01-08، المرجع السابق.

ويقصد بالندب تكليف مأمور الضبط القضائي من قبل السلطة المختصة بالتحقيق بعمل محدد أو أكثر من أعمال التحقيق، ويترتب عليه اعتبار العمل من حيث قيمته القانونية كما لو كان صادرة عن سلطة التحقيق المختصة[1]. وتسري أحكام الندب على الإذن بالتفتيش والذي يقصد به "ذلك التفويض الموجه من سلطة التفتيش المختصة إلى أحد مأموري الضبط القضائي متضمنا تخويله إياه إجراء التفتيش الذي تختص به تلك السلطة"[2].

بالنسبة للندب أو الإذن القضائي المتعلق بتفتيش المنظومات المعلوماتية فإن المشرع الجزائري يحيلنا إلى القواعد الإجرائية المنصوص عليها في قانون الإجراءات الجزائية، وهذا ما نصت عليه الفقرة الأولى من المادة 05 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3] بقولها "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 4 من نفس القانون "الدخول بغرض التفتيش...".

هناك إشكال يثار بشأن مجال الإذن بالتفتيش المتعلق بالنظم المعلوماتية، فهل يمتد هذا الإذن إلى شخص المتهم ومسكنه وكل المعدات المعلوماتية والبيانات وكل الملفات التي يحتوي عليها الحاسب بما فيها تلك الملفات المتعلقة بالخصوصية المعلوماتية للأشخاص، أم يجب تحديد هذا الإذن بالتفتيش بحيث يجب أن يكون لكل محل بالتفتيش إذن مستقل به، كإذن لتفتيش ما يحوزه المتهم، وإذن مستقل يخص تفتيش كل ملف منفرد عن بقية الملفات، بمعنى تقييد ضباط الشرطة القضائية فلا تطلق أيديهم لتفتيش كل ما يصادفونه فقط لكونهم حصلوا على إذن وحيد بالتفتيش من السلطة المكلفة بالتحقيق.

[1] محمد عبد القادر العبودي، ندب مأموري الضبط القضائي لأعمال التحقيق، الطبعة الثانية، دار النهضة العربية، القاهرة، 2011، ص 11.

[2] قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005، ص 55.

[3] القانون 09-04، المرجع السابق.

أجاب المشرع الفيدرالي الأمريكي على ذلك عنما نص على ضرورة معاملة الحاسوب كحاوية مغلقة مثل حقيبة اليد أو خزانة الملفات[1]. ومعنى ذلك أنه بمجرد الولوج إلى الأنظمة المعلوماتية تفقد الخصوصية، فبمجرد الولوج مثلا إلى جهاز الكمبيوتر فإن البيانات ومختلف أشكال الملفات التي يحتوي عليها تفقد خصوصيتها، وفي الحقيقة يمثل ذلك صورة من أخطر صور انتهاك حرمة الحياة الخاصة أو الخصوصية المعلوماتية للأشخاص والتي بسببها لطالما انتقدت وتنتقد دائما جهات التحقيق.

وفي تقديرنا يجب أن يكون الإذن بالتفتيش محددا بدقة وإلا سيكون في ذلك مساسا بالخصوصية المعلوماتية للأشخاص وانتهاكا لحرمتهم وحرمة مساكنهم.

ويشترط لصحة هذا الإجراء عدة شروط ومنها أن يكون الإذن بالتفتيش محددا وواصفا بشكل خاص ودقيق الأشياء المراد البحث عنها، كأن يتضمن الإذن بالتفتيش تحديد القطع الصلبة المكون منها الحاسوب. ولا يبدو ذلك بالأمر السهل إذ أن الإذن بالتفتيش الصادر بخصوص الجريمة الإلكترونية لابد أن يصدر وينفذ من طرف جهة لها دراية فنية بالأجهزة الإلكترونية والأنظمة المعلوماتية[2].

وفي هذا المقام نرى أنه من الضروري أن يتدخل المشرع سواء في التشريعات المقارنة أو المشرع الجزائري، لحسم هذا الأمر بنصوص قانونية واضحة تصون حرمة الأفراد وخصوصيتهم من جهة، وتحدد أطر واضحة لسلطات التحقيق والضبطية القضائية، وذلك من أجل تمكينهم من مباشرة إجراءاتهم في إطار شرعي وسلس يسمح لهم بمجاراة سرعة المجرم الإلكتروني دون استباحة لحرمة الأشخاص.

3-تفتيش النظام المعلوماتي بناء على رضا وموافقة المتهم:

المشرع الجزائري لم يقدم لنا نص يتناول فيه تفتيش النظام المعلوماتي بناء على موافقة المتهم، ولو أنه عندما يتعلق الأمر بالقواعد العامة للجريمة في صورتها التقليدية (بعيدا

[1] علي حسن محمد الطوالبة، المرجع السابق، ص 122.

[2] أنظر في هذا المعنى: نبيلة هبة هروال، المرجع السابق، ص 243.

عن الجريمة الإلكترونية) فإننا نجد بنص المادة 47 من قانون الإجراءات الجزائية[1] عبارة " ... إلا إذا طلب صاحب المنزل ذلك..." وإن كانت هذه العبارة توحي أو يفهم منها موافقة الشخص ورضاه بالتفتيش، غير أنه لا يمكن تطبيقها إذا تعلق الأمر بالجريمة الإلكترونية. فما الذي يدفع شخصا أن يطلب أو أن يقدم طواعية دليلا قد يدينه.

وعلى أي حال، فحتى في التشريعات المقارنة لم نتوصل إلى نص قانوني يتناول تفتيش النظم المعلوماتية بناء على طلب المتهم.

4-تفتيش النظم المعلوماتية بناء على القبض على الأشخاص:

هنا نقول ما قد قيل عن الحالة السابقة (تفتيش النظام المعلوماتي بناء على رضا المتهم) وذلك أمام غياب نصوص قانونية صريحة تتناول تفتيش النظم المعلوماتية بناء على القبض على الأشخاص.

ثانيا: الشروط الشكلية للتفتيش

بالإضافة للشروط الموضوعية التي سبق ذكرها، فإنه يشترط لصحة إجراءات تفتيش النظم المعلوماتية شروط شكلية يجب احترامها كونها تمثل ضمانات تحمي الحريات الفردية وتصونها من التعسف الذي قد يصدر عن الجهات القائمة بالتفتيش.

ويمكن حصر هذه الشروط الشكلية في ثلاثة شروط تتمثل في ضرورة حضور بعض الأشخاص كشرط أول، ووقت إجراء التفتيش كشرط ثان وأخيرا تحرير محضر التفتيش.

أ-ضرورة حضور أشخاص معينين أثناء تفتيش النظام المعلوماتي:

يعد حضور شخص المتهم أو من ينوب عنه أو من هم في مقام الشهود من الشروط الضرورية والهامة التي يفرضها القانون، وذلك لضمان صحة التفتيش وما يتبعه من ضبط للأدلة.

تميز التشريعات المقارنة هنا بين تفتيش الأشخاص وتفتيش المساكن. فأما بخصوص تفتيش الأشخاص، فمن البديهي أن الشخص الذي يشترط القانون حضوره هو المتهم،

[1] القانون 06-22، المرجع السابق.

وهنا لم تشترط التشريعات حضور الشهود عندما يتعلق الأمر بتفتيش شخص المتهم. غير أن الوضع يتغير فيما يخص تفتيش المساكن وذلك تماشيا مع صفة الشخص القائم بالتفتيش.

فالمشرع المصري مثلا يميز في تفتيش المساكن بين حالتين، حالة تتولى فيها سلطة التحقيق التفتيش وحالة أخرى يتم التفتيش فيها عن طريق مأمور الضبط القضائي.

وتبعا لذلك فالمشرع المصري وبموجب المادة 51 من قانون الإجراءات الجنائية[1] يشترط حضور شاهدين في حالة ما إذا كان التفتيش يباشر بواسطة أحد مأموري الضبط القضائي. في حين أنه لم يشترط حضور شهود عندما يتم التفتيش بواسطة قاض التحقيق وذلك بموجب المواد 91 و92 من نفس القانون.

المشرع الأردني وبنص المادة 83 من قانون أصول المحاكمات الجزائية الأردني[2] لم يفرق بين ذلك التفتيش الذي يتم بواسطة السلطة المختصة بالتفتيش أو بواسطة موظفي الضابطة العدلية بناء على إذن بالتفتيش، فنص على حضور شاهدين في كلا الحالتين[3].

[1] القانون رقم 150 لسنة 1950، المرجع السابق "يحصل التفتيش بحضور المتهم أو من ينيبه عنه كلما أمكن ذلك، وإلا فيجب أن يكون بحضور شاهدين، ويكون هذان الشاهدان بقدر الإمكان من أقاربه البالغين أو من القاطنين معه بالمنزل أو من الجيران، ويثبت ذلك في المحضر".

المادة 91 "تفتيش المنازل عمل من أعمال التحقيق ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضي التحقيق بناء على اتهام موجه إلى شخص يقيم في المنزل المراد تفتيشه بارتكاب جناية أو جنحة أو باشتراكه في ارتكابها أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة.

ولقاضي التحقيق أن يفتش أي مكان ويضبط فيه الأوراق والأسلحة وكل ما يحتمل أنه استعمل في ارتكاب الجريمة أو نتج عنها أو وقعت عليه وكل ما يفيد في كشف الحقيقة.

وفى جميع الأحوال يجب أن يكون أمر التفتيش مسببا.

المادة 92 "يحصل التفتيش بحضور المتهم أو من ينيبه عنه إن أمكن ذلك.

وإذا حصل التفتيش في منزل غير المتهم يدعى صاحبه للحضور بنفسه أو بواسطة من ينيبه عنه إن أمكن ذلك"

[2] القانون رقم 1961/09، المرجع السابق.

[3] المادة 83 من قانون أصول المحاكمات الجزائية الأردني (القانون رقم 1961/09، المرجع السابق)

1-يجري التفتيش بحضور المشتكى عليه إذا كان موقوفا.

المشرع السوداني اشترط كذلك حضور شاهدين بنص المادة 95 الفقرة (أ) من قانون الإجراءات الجنائية[1].

في حين أن المشرع الجزائري عندما اشترط وجود شاهدين أثناء تفتيش المساكن لم يعر اهتمام للجهة القائمة على التفتيش، فيستوي أن يكون قاض التحقيق أو ضابط الشرطة القضائية.

وفي حالة تعذر حضور المتهم أو امتناعه عن تعيين من يمثله أو كان هاربا، فحضور الشاهدين ضروري وذلك بغض النظر عمن أجرى التفتيش طبقا لنص المادة 45 من قانون الإجراءات الجزائية[2].

هذا فيما يخص التفتيش في الجريمة التقليدية، غير أنه عندما يتعلق الأمر بالجريمة الإلكترونية، نجد أن المشرع الجزائري وبموجب الفقرة الأخيرة من المادة 45 من قانون الإجراءات الجزائية قد أسقط الشرط المتعلق بحضور الأشخاص أثناء التفتيش عندما يتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، والعلة في ذلك بحسب تقديرينا هو أن الجريمة الإلكترونية جريمة تتطلب السرعة في إجراء التفتيش في حين أن اشتراط حضور الأشخاص يستهلك الكثير من الوقت، وبالتالي سيعطل سلطات التحقيق عن الوصول إلى الدليل في الجريمة الإلكترونية.

2-فإذا لم يكن موقوفا وأبى الحضور أو تعذر عليه ذلك أو كان موقوفً خارج المنطقة التي يجب أن يحصل التفتيش فيها أو كان غائبا يجري التفتيش بحضور مختار محلته أو من يقوم مقامه أو بحضور اثنين من أقاربه أو شاهدين يستدعيهما المدعي العام.

[1] المادة 95 الفقرة (أ) من قانون 1991، المرجع السابق.

"يجرى في حضور شاهدين يكلفان بالحضور من جانب الشخص المنفذ لأمر التفتيش، ويكونان بقدر الإمكان من أقارب المتهم أو المقيمين معه بالمنزل أو الجيران، ويثبت الإجراء في المحضر، ما لم يأمر وكيل النيابة أو القاضي، بحسب الحال، بخلاف ذلك، نظراً للطبيعة المستعجلة للتفتيش...."

[2] القانون 06-22، المرجع السابق.

ب-وقت إجراء التفتيش في الجرائم الإلكترونية:

يقصد بشرط الوقت تحديد الميقات الزمني أو الفترة الزمنية التي يتم فيها التفتيش، وذلك صونا لحريات الأفراد ولحرمة مساكنهم والحيلولة دون انتهاكها والتعدي عليها.

لقد اختلفت التشريعات المقارنة حول تحديد وقت معين لإجراء التفتيش، فهناك تشريعات لم تتبن نصوص قانونية تحدد فيها وقت إجراء التفتيش، فيما أخرى قيدت إجراء التفتيش بحيز وحدود زمنية بموجب نصوص قانونية.

فالمشرع العراقي وكذا نظيره المصري لم يحددا وقتا لإجراء التفتيش وبالتالي يمكن إجرائه في أي وقت ليلا أو نهارا، في حين أن المشرع القطري أجاز التفتيش في النهار فقط وأجازه استثناء خارج أوقات النهار، أي ليلا إذا تعلق الأمر بحالة الاستعجال ويقصد بها الجريمة المتلبس بها وذلك بموجب المادة 53 من قانون الإجراءات الجنائية القطري[1] التي نصت على أنه " لا يجوز أن يجرى تفتيش المساكن إلا نهاراً، ويجوز التفتيش ليلاً إذا كانت الجريمة متلبساً بها، أو إذا اقتضت مصلحة التحقيق ذلك، ويثبت ذلك في محضر التحقيق"

المشرع الفرنسي وبموجب المادة 59 من قانون الإجراءات الجزائية الفرنسي[2] حدد وقت التفتيش ما بين السادسة صباحا والتاسعة ليلا. أما المشرع الجزائري وبموجب المادة 47 من قانون الإجراءات الجزائية الجزائري[3] حدد وقت إجراء التفتيش ما بين الخامسة صباحا والثامنة ليلا، حيث جاء بنص المادة "لا يجوز البدء في تفتيش المساكن ومعاينتها قبل الساعة الخامسة (5) صباحاً, ولا بعد الساعة الثامنة (8) مساء..." غير أن هناك حالات استثنائية يمكن من خلالها إجراء التفتيش في أي وقت سواء بالليل أو بالنهار، هذه

[1] القانون رقم 23 الصادر بتاريخ 2004/06/30 الموافق 1425/05/12 هجري بالجريدة الرسمية العدد 12 المنشورة بتاريخ 2004/08/29 الموافق 1425/07/14 هجري المتضمن قانون الإجراءات الجنائية القطري.

[2] La loi n° 93-1013 du 24 août 1993 modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme de la procédure pénale (rectificatif, JORF n°0171 du 26 juillet 1994.

[3] القانون 06-22، المرجع السابق.

الحالات وردت بنص المادة 47 أعلاه، حيث جاء بالفقرة الأولى "..إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا...".

أما الاستثناء الثاني جاء بالفقرة الثانية التي نصت على أنه "غير أنه يجوز إجراء التفتيش والمعاينة والحجز في كل ساعة من ساعات النهار أو الليل قصد التحقيق في جميع الجرائم المعاقب عليها في المواد 342 إلى 348 من قانون العقوبات[1] وذلك في داخل كل فندق أو منزل مفروش أو فندق عائلي أو محل لبيع المشروبات أو ناد أو منتدى أو مرقص أو أماكن المشاهدة العامة وملحقاتها، وفي أي مكان مفتوح للعموم أو يرتاده الجمهور، إذا تحقق أن أشخاصاً يستقبلون فيه عادة لممارسة الدعارة".

وجاءت الفقرة الثالثة باستثناء ثالث فنصت على أنه " وعندما يتعلق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وجرائم تبييض الأموال والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنه يجوز إجراء التفتيش والمعاينة والحجز في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص".

والملاحظ بأن هذه الفقرة الثالثة تضمنت جرائم لها صلة بموضوع دراستنا ويتعلق الأمر بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات والتي تدخل ضمن الجرائم الإلكترونية. ولقد خصها المشرع بتلك الأحكام الواردة في الفقرة الرابعة من المادة 47 بقوله "عندما

[1] الأمر 66-156، المرجع السابق. وكذلك:

- الأمر رقم 75-47 المؤرخ في 7 جمادى الثانية عام 1395 الموافق 17 يونيو سنة 1975 الصادر بالجريدة الرسمية العدد 53 بتاريخ الجمعة 24 جمادى الثانية عام 1395 هـ الموافق 4 يوليو 1975 م. المعدل والمتمم للأمر رقم 66-156 المؤرخ المتضمن قانون العقوبات.
- القانون رقم 82-04 المؤرخ في 19 ربيع الثاني عام 1402 الموافق 13 فبراير 1982، الصادر بالجريدة الرسمية العدد 7 الصادرة بتاريخ 22 ربيع الثاني عام 1402 الموافق 16 فبراير سنة 1982. المعدل والمتمم للأمر رقم 66-156 المؤرخ المتضمن قانون العقوبات.
- القانون رقم 14-01 المؤرخ في 4 ربيع الثاني 1435 الموافق 4 فبراير 2014، الصادر بالجريدة الرسمية العدد 07 الصادرة بتاريخ 16 ربيع الثاني عام 1435 الموافق 16 فبراير سنة 2014. المعدل و المتمم للأمر رقم 66-156 المؤرخ المتضمن قانون العقوبات.

يتعلق الأمر بالجرائم المذكورة في الفقرة الثالثة أعلاه، يمكن قاضي التحقيق أن يقوم بأية عملية تفتيش أو حجز ليلا أو نهارا وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية المختصين للقيام بذلك".

بخصوص الميقات الزمني المتعلق بالجريمة الإلكترونية محل دراستنا، نجد أنها وردت ضمن المادة 47 من قانون الإجراءات الجزائية الجزائري[1] الفقرة الثالثة أعلاه، فالمشرع الجزائري وحينما يتعلق الأمر بتفتيش النظم المعلوماتية لم يحدد حيز زمني للسلطة القائمة بالتفتيش، وذلك مرتبط بطبيعة الجريمة الإلكترونية والتي يمكن ارتكابها في أي وقت ليلا أو نهارا من جهة، ومن جهة أخرى بقدرة المجرم الإلكتروني على إخفاء ومحو وتدمير وبسرعة فائقة تلك الآثار الإلكترونية التي تدل عليه وتدينه.

إن عدم تقييد سلطة التفتيش بحدود زمنية لمباشرة التفتيش في الجريمة الإلكترونية هو تصرف صائب من طرف المشرع يساهم في دعم النواحي الإجرائية في التصدي للجريمة الإلكترونية.

المشرع الجزائري لم يتوقف عند هذا الحد، بل واصل مساعيه من أجل إضفاء السرعة والمرونة الإجرائية لمجابهة الجريمة الإلكترونية، ولعل أكثر ما يدل على ذلك العبارة التي وردت بنص المادة 05 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] المشار إليه سابقا، حيث جاء فيها " يجوز للسلطات..... ولو عن بعد" فعبارة "عن بعد" تفيد بإمكانية الولوج إلى المنظومة المعلوماتية وتفتيشها في أي وقت دون الحاجة إلى الانتقال للمكان الذي تتواجد به الأوعية المادية التي تتضمن هذه الكيانات والبيانات المنطقية المراد تفتيشها، وهذا ما يعبر عنه في فرنسا بالتفتيش على المباشر (perquisition en ligne)[3].

[1] القانون 06-22، المرجع السابق.

[2] القانون 09-04، المرجع السابق.

[3] أنظر في هذا المعنى:

Yann PADOVA, Un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénal comparé ,n°4, octobre-décembre, Dalloz ,2002, p.770.

ج-تحرير محضر بالتفتيش في الجرائم الإلكترونية:

باعتبار التفتيش عملا من أعمال التحقيق، وجب تحرير محضر يثبت كل تلك الإجراءات التي اتخذت بشأن التفتيش وما أسفر عنه من أدلة. هذا ولم يتطلب المشرع شكلا خاصا في محضر التفتيش، ومن ثم فإنه لا يشترط لصحته سوى ما نصت عليه القواعد العامة بخصوص المحاضر بصفة عامة كأن يتم تحريره باللغة الرسمية للدولة وأن يحمل التاريخ الذي تم تحريره فيه وبالطبع توقيع الشخص الذي قام بتحريره وكل الإجراءات التي اتخذت بشأن الوقائع التي يثبتها[1].

وفيما يتعلق بالمحاضر التي يتم تحريرها بمناسبة تفتيش النظم المعلوماتية في الجريمة الإلكترونية يسري عليها ما جاء في الفقرة أعلاه، غير أنه وما دام الأمر يتعلق بأمور فنية فإنه يتوجب على السلطة الملزمة بتحرير محضر التفتيش الإلمام بتقنية المعلومات وإلا فعليها الاستعانة بمن لهم دراية بتقنيات الحاسب الآلي والإنترنت من أجل المساعدة في الصياغة السليمة لمسودة محضر التفتيش.

المطلب الثالث: ضبط الدليل الإلكتروني

إن الهدف من التفتيش هو الوصول إلى الأدلة وضبطها، لذلك يعتبر الضبط بمثابة النتيجة المنطقية التي ينتهي إليها التفتيش. نتناول من خلال هذا المطلب تعريف الضبط في الجريمة الإلكترونية، وكذا محله والإشكالات المثارة حوله.

الفرع الأول: تعريف الضبط

إن الهدف الذي تسعى إليه جهات التحقيق من وراء التفتيش، هو ضبط الأدلة التي قد يستعان بها في الوصول إلى الجاني وإظهار الحقيقة.

[1] قدري عبد الفتاح الشهاوي، المرجع السابق، ص 160. أشارت إليه نبيلة هبة هروال، المرجع السابق، ص 263.

ويعرف الضبط بأنه وضع اليد على شيء يتصل بجريمة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبها[1]. أما الضبط في الجريمة الإلكترونية فيمكن تعريفه بأنه إجراء يتم بموجبه وضع اليد على المكونات المادية والمعنوية للأجهزة الإلكترونية والشبكات وسائر الأنظمة المعلوماتية التي تخزن فيها تلك البيانات الإلكترونية التي تتصل بجريمة إلكترونية وقعت وتفيد لاحقا في الكشف عن الحقيقة والوصول إلى الجناة.

الفرع الثاني: محل الضبط

معلوم أن الضبط لا يرد إلا على الأشياء المادية كمحل للضبط، غير أن الأدلة المتحصل عليها جراء تفتيش النظم المعلوماتية لا تتمثل فقط في المكونات المادية، وإنما تشمل أيضا البيانات والمراسلات والاتصالات الإلكترونية، وهي مكونات ذات طبيعة معنوية.

فإذا كان ضبط المكونات المادية لا يثير إشكالا، فبالمقابل فإن ضبط المكونات ذات الطبيعة المعنوية عرف اختلافا فقهي وتشريعي حول مدى قابلية هذه البيانات اللامادية للضبط دونما الحاجة إلى وسيط أو دعامة مادية تضفي عليها صفة الكيان المادي.

هناك من يرى بأنه لا يجوز ضبط تلك المكونات ذات الطبيعة المعنوية أو المنطقية والمتمثلة في البيانات الإلكترونية ما دام أن الصفة المادية تنتفي فيها. إلا إذا تم لاحقا إفراغها في كيان مادي.

ومن ضمن التشريعات المقارنة التي دعمت هذا الطرح قانون الإجراءات الجنائية الألماني، فالمشرع الألماني وبموجب المادة 94 من هذا القانون[2] حصر الضبط كإجراء

[1] أنظر كل من: توفيق محمد الشاوي، فقه الإجراءات الجنائية، الجزء الثاني، دار الكتاب العربي، القاهرة، الطبعة الثانية، 1954، ص 323. وهشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 93.

[2] **Section 94**
Securing and seizure of objects for evidentiary purposes
(1) Objects which may be of importance, as evidence, for the investigation shall be taken into custody or otherwise secured.
(2) Such objects shall be seized if they are in the custody of a person and are not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driving licences which are to be confiscated.
(4) The surrender of movable property shall be governed by sections 111n and 111o.
German Code of Criminal Procedure, Op.Cit.

في الأشياء ذات الكيان المادي الملموس وبالتالي أخرج كل ما هو غير مادي من دائرة الأشياء القابلة للضبط. ولقد وجد الفقه الألماني سنده في مضمون هذه المادة لإعطاء تفسير لسبب عدم قابلية البيانات الإلكترونية للضبط. ويواصل الفقه الألماني شرح موقفه بتقديم اقتراح من أجل جعل البيانات الإلكترونية تقبل الضبط فيجد بأن إفراغ هذه البيانات في دعامة مادية أو نقلها وتحويلها إلى طبيعة مادية يجعلها قابلة للضبط لاحقا لأنها تكون حينئذ قد تخلصت من طبيعتها اللامادية واكتسبت كيان مادي[1].

ونرى بأنه يمكن إدراج موقف المشرع الفرنسي ضمن هذا السياق وذلك بموجب المادة57-1 الفقرة الثالثة من قانون الإجراءات الجزائية الفرنسي[2]، إذ نصت على أن " البيانات التي جاز الولوج إليها وفق الشروط المنصوص عليها في بالمادة الحالية، يتعين نسخها على دعامات. ودعامات التخزين المعلوماتية هذه يتعين وضعها في أحراز مختومة وفق الشروط المنصوص عليها في هذا القانون ".

ويرى آخرون بأن البيانات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، تقبل التسجيل والحفظ والتخزين على وسائط مادية، وبالإمكان نقلها وبثها واستقبالها وإعادة إنتاجها. فالوجود المادي لا يمكن إنكاره[3]. ويدعم هذا الرأي المشرع الكندي بنص المادة 487-1-d من قانون الإجراءات الجنائية الكندي[4] التي جاء بمضمونها "... من أجل البحث في هذا المبنى أو الحاوية أو المكان، للبحث عن هذا الشيء وحجزه". ما جعل الفقه في كندا يرى بأن هذه المادة أعطت لجهات التحقيق صلاحية ضبط "أي شيء" طالما أن هناك جريمة قد ارتكبت وأن ضبط هذا "الشيء"

---

[1] أنظر في هذا المعنى كل من: هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 93 و: عبد اللاه أحمد هلالي، المرجع السابق، ص 85.

[2] Article 57-1 Alinéa 3(Créé par la loi 2003-239, Op.cit)

« Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code. »

[3] سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، 2008، ص 322.

[4] Article 487 (1)-d, du Code criminel de Canada, Op.cit. "… à faire une perquisition dans ce bâtiment, contenant ou lieu, pour rechercher cette chose et la saisir…"

سلطاتها المختصة من ضبط أو الحصول بطريقة مماثلة على البيانات المعلوماتية التي تم الولوج إليها عملاً بالفقرتين 1 أو 2. وتشمل هذه التدابير الصلاحيات التالية:

أ-الضبط أو الحصول بطريقة مماثلة على نظام معلوماتي أو جزء منه أو على المعلومات المخزنة بدعائم أو وسائط التخزين للمعلومات.

ب-أخذ نسخة من البيانات المعلوماتية، والحفاظ على هذه البيانات المعلوماتية.

ج-الحفاظ على سلامة البيانات المعلوماتية المخزنة ذات الصلة.

د-جعل البيانات المعلوماتية غير قابلة للنفاذ إليها والحيلولة دون الوصول إليها، أو إزالتها من النظام المعلوماتي الذي تم الولوج إليه".

وكما يبدو من خلال نص المادة فإنها استخدمت عبارة "الحصول بطريقة مماثلة " وأضافتها للمصطلح السائد وهو "الضبط".

وأخيرا يتم تحريز ما تم ضبطه من أدلة بوضعها في أحراز مختومة، مع مراعاة الطبيعة الخاصة للأدلة الإلكترونية، حيث أنه وإلى جانب تطبيق ما جاء بالمادة 84 من قانون الإجراءات الجزائية[1]، خاصة ما تعلق منها بالسرية، فالمشرع الجزائري وبخصوص تلك المعطيات التي استحال حجزها، فإنه نص على إجراء آخر بموجب المادة 07 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] والمتمثل في المنع من الوصول إلى هذه المعطيات وإلى نسخها، عن طريق استخدام التقنيات التي تحقق ذلك، وهذا بهدف المحافظة عليها بقولها" إذا استحال إجراء الحجز وفقا لما هو منصوص...(يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول الى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها).. ".

[1] الأمر رقم 66-155، المرجع السابق.

[2] القانون 09-04، المرجع السابق.

كما أنه وفي نفس السياق، يمنع الاطلاع على تلك المعطيات التي يشكل محتواها جريمة، لذلك وجب استعمال الوسائل التقنية المتاحة لتحقق هذا المنع كما جاء بنص المادة 08 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] " يمكن السلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك".

نستنتج في نهاية هذا المطلب بأن ضبط الأدلة ذات الطبيعة المعنوية والكيان اللامادي في الجريمة الإلكترونية، ليس بالأمر البسيط بل يتطلب وسائل تقنية فرضتها طبيعته التقنية المميزة له، لذلك فالمواجهة الدائرة بين سلطات التحقيق في الجريمة الإلكترونية من جهة، والمجرم الإلكتروني من جهة أخرى هي مواجهة تكنولوجية وليست معركة قضائية فقط.

المطلب الرابع: الخبرة في مجال الجريمة الإلكترونية

قد يحدث أن تجد سلطات التحقيق نفسها أمام جرائم تلفها مشاكل فنية، الأمر الذي يجعل من الاستعانة بأهل الخبرة ضرورة ملحة حتى تتمكن سلطات التحقيق من مواصلة طريقها في جمع الأدلة من أجل كشف الحقيقة.

وتتنوع مجالات الخبرة بتنوع الجرائم، فنجد مثلا الخبرة الطبية، الخبرة العقلية والنفسية، خبرة متعلقة بالأسلحة والمواد الكيماوية...الخ.

إن الجريمة الإلكترونية وبالنظر لطبيعتها الخاصة جعلت أمر الاستعانة بالخبراء أمر لا مناص منه، وذلك نظرا للتعقيدات التي صاحبت التقنيات الحديثة في مجال المعلوماتية.

سنحاول التطرق للخبرة المتعلقة بالجريمة الإلكترونية وذلك من خلال تعريف معنى الخبرة أولا ثم النظر إلى أهميتها في مجال الجريمة الإلكترونية ودور الخبير فيها.

[1] القانون 09-04، المرجع السابق.

الفرع الأول: تعريف الخبرة

لغة، يقصد بالخبرة (بكسر الخاء) العلم بالشيء ومعرفته على حقيقته[1]. أما اصطلاحا يقصد بها البعض البصيرة والمعرفة.

والخبرة القضائية هي إجراء يستهدف الاستعانة بالقدرات الفنية أو العلمية لشخص الخبير، والتي لا تتوافر لدى رجل القضاء أو المحقق، من أجل الكشف عن دليل يفيد في معرفة الحقيقة بشأن جريمة وقعت، أو نسبتها إلى المتهم أو تحديد ملامح شخصيته الإجرامية[2]. أو هي الاستشارة الفنية التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته في المسائل التي يحتاج تقديرها إلى معرفة أو دراية علمية خاصة لا تتوافر لدى المحقق[3].

مما تقدم يمكن القول إن الخبير هو ذلك الشخص الذي له دراية ومعرفة في علم من العلوم تؤهله لإبداء رأيه في مجال معين من مجالات العلوم. وعليه فإن الخبير في مجال الجريمة الإلكترونية يقصد به ذلك الشخص الذي تلقى تكوينا أكسبه كفاءة تؤهله لإبداء رأيه في مجال المعلوماتية وما يرتبط بها من أجهزة إلكترونية وشبكات الإنترنت.

وقد تناول المشرع الجزائري مسألة الخبرة في القسم التاسع من قانون الإجراءات الجزائية[4]، وذلك ابتداء من المادة 143 إلى غاية المادة 156، وأجاز لجهات التحقيق ندب خبير أو خبراء وذلك بمقتضى المادتين 143 و147 من ذات القانون.

[1] ابن منظور، لسان العرب، الطبعة الثالثة، الجزء الرابع، دار إحياء التراث العربي، بيروت، لبنان، 1999، ص 12.

[2] أحمد شوقي شلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 259.

[3] عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2015، ص 184.

[4] الأمر رقم 66-155، المرجع السابق. وكذلك:

- القانون 06-22، المرجع السابق.
- الأمر رقم 69-73 مؤرخ في 5 رجب عام 1389 الموافق 16 سبتمبر 1969 الصادر بالجريدة الرسمية العدد 80 بتاريخ 8 رجب عام 1389 هـ الموافق 19 سبتمبر 1969.

الفرع الثاني: أهمية الخبرة المتعلقة بالجريمة الإلكترونية

أثبت الواقع مدى أهمية الخبرة في المجال القضائي ومدى حاجة سلطات التحقيق للخبراء في شتى التخصصات وذلك مسعى جهات التحقيق لفك خيوط الجرائم والكشف عن مرتكبيها.

وإذا كان هذا هو حال الجريمة في مفهومها التقليدي، فإن حاجة سلطات التحقيق للخبرة في مجال الجريمة الإلكترونية تبدو أكثر إلحاحا ذلك أن الجرائم الإلكترونية ذات طبيعة غير مادية، كما أن اقترافها يتم داخل عالم افتراضي يفرض على القائم بالتحقيق الاستعانة بالخبراء في مجال المعلوماتية والتقنيات الحديثة.

إن الاعتماد على الخبير للوصول إلى الدليل الإلكتروني أضحى أمر إجباري وليس اختياري، فالسلطات ستقف عاجزة دون حضور الخبراء، فيستحيل من دونهم المضي في التحقيق وهذا يعكس مدى أهمية الخبرة المتعلقة بالجريمة الإلكترونية.

الفرع الثالث: إجراءات الخبرة في مجال الجريمة الإلكترونية

الخبرة تتضمن عدة إجراءات يقوم بها الخبير، ونظرا لكثرة هذه الإجراءات وتنوعها فلا يمكننا حصرها، غير أننا نقدم أبرز الخطوات والمراحل التي تمر بها إجراءات الخبرة وهي كالآتي:

أولا: مرحلة ما قبل التشغيل والفحص، ويتم من خلالها عادة إحصاء وجرد المكونات التي تم ضبطها.

ثانيا: مرحلة التشغيل والفحص، ومن خلالها يتم نسخ البيانات الموجودة، وإظهار تلك التي تم إخفاءها واسترجاع ما تم محوه.

ثالثا: مرحلة تحديد الارتباط بين الدليل المادي والدليل الإلكتروني.

رابعا: مرحلة تدوين النتائج التي توصل إليها الخبير وذلك من أجل إعداد تقرير الخبرة بخصوص المهام التي أسندت إليه لدى تكليفه بالمهمة.

هذا وتجدر الإشارة إلى أن الخبير المعلوماتي وهو بصدد إجراء الخبرة التي أسندت إليه بخصوص الجريمة الإلكترونية، فإنه يستعين بعدة برمجيات كتلك التي تسمح له بنسخ البيانات الموجودة بالحاسب الآلي للمتهم الإلكتروني أو الشبكة المعلوماتية.

لذلك توجد عدة أدوات تساهم في عمل الخبير، ونذكر منها على سبيل المثال برنامج معالجة الملفات مثل X tree Pro Gold وبرنامج LapLink للنسخ وبرامج اتصالات مثل LANtastic.[1]

المطلب الخامس: الشهادة في الجريمة الإلكترونية

تعد الشهادة من بين الإجراءات الهامة في إقامة الدليل، فهي بمثابة السند للجهات القضائية حيث أنها تساهم في كشف الحقيقة.

وسنحاول من خلال هذا المطلب إعطاء تعريف للشهادة في الجريمة بمفهومها التقليدي، وكذا في الجريمة الإلكترونية، والتعرف على الشاهد والتزاماته أمام جهات التحقيق.

الفرع الأول: تعريف الشهادة

سنحاول إعطاء تعريف للشهادة بصفة عامة، ثم نتطرق لتعريف الشاهد في الجريمة الإلكترونية.

أولا: الشهادة بصفة عامة

لغة، يقال: شَهِدَ يَشْهَدُ شَهَادَةً. كما يقال: شَهِدَ فلان عند القاضي، أي بيَّن وأعلَمَ لمَنْ الحق وعلى من هو[2]. هذا وقد وردت في القرآن الكريم مفردات مشتقة من كلمة الشهادة

[1] – برنامج معالجة الملفات X tree Pro Gold: وهو برنامج يمكن من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب.

– برنامج LapLink للنسخ وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي parallel port أو على التوالي serial port وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

–برنامج الاتصالات LANtastic: برنامج يعمل على ربط جهاز حاسب الخبير بجهاز حاسب المتهم لنقل ما به من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

أنظر: ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، المرجع السابق، ص 92.

[2] أبو الحسين أحمد بن فارس، معجم مقاييس اللغة، الطبعة الأولى، دار الفكر، بيروت، 1994، ص539.

في عدة مواضع كقوله تعالى في سورة النور " وَلْيَشْهَدْ عَذَابَهُمَا طَائِفَةٌ مِّنَ الْمُؤْمِنِينَ"[1] وقوله تعالى في سورة المزمل" إِنَّا أَرْسَلْنَا إِلَيْكُمْ رَسُولا شَاهِدًا عَلَيْكُمْ كَمَا أَرْسَلْنَا إِلَى فِرْعَوْنَ رَسُولا"[2] وقوله تعالى في سورة الأحقاف " وَشَهِدَ شَاهِدٌ مِّن بَنِي إِسْرَائِيلَ"[3].

وتعرف الشهادة بأنها تلك الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها[4].

والشاهد بصفة عامة، هو ذلك الشخص الذي يدلي أمام جهات التحقيق بما سمعه أو رآه بخصوص جريمة ما، سواء بنفيها أو بإثباتها، ويكون ذلك شفاهة. وقد تكون الشهاد تلقائية فيبادر الشاهد إلى تقديم شهادته دون إلزامه بذلك من طرف السلطات القضائية، أو تكون إلزامية وذلك من خلال استدعاء الشاهد للإدلاء بشهادته أمام الجهات القضائية.

لقد نص المشرع الجزائري على سماع الشهود وذلك في القسم الرابع من الفصل السادس للكتاب الأول من قانون الإجراءات الجزائية[5] بموجب المواد من (88 إلى 99).

ثانيا: الشاهد في الجريمة المعلوماتية

إن الشهادة في الجريمة الإلكترونية لا تختلف من حيث أهميتها عن الشهادة في الجريمة بمفهومها التقليدي، ما دامت تساهم في جمع الأدلة المتعلقة بالجريمة. غير أن الاختلاف يمكن أن يكمن في محل الشهادة في الجريمة الإلكترونية نظرا لميزتها وطبيعتها الخاصة، كما يمتد هذا الاختلاف إلى صفة الشاهد في الجريمة الإلكترونية والذي يصطلح عليه تسمية الشاهد المعلوماتي تمييزا له عن الشاهد التقليدي.

[1] سورة النور، الآية 2.

[2] سورة المزمل، الآية 15.

[3] سورة الأحقاف، الآية 10.

[4] إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 1980، ص 30.

[5] الأمر رقم 66–155، المرجع السابق.

ويعرف الشاهد المعلوماتي الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب والذي تكون لديه معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله[1].

فهو بذلك يقدم لجهات التحقيق ما يملكه من معلومات مرتبطة بالنظم المعلوماتية التي هي محل تحقيق.

قد يحدث وأن تتداخل صفة الشاهد مع صفة الخبير في مجال النظم المعلوماتية، ويمكن أن نتصور قيام ذلك في تلك الحالة التي يكون فيها شخص الشاهد يملك أيضا – وبحكم وظيفته في ميدان من ميادين المعالجة الآلية للبيانات–معرفة وقدرات تؤهله للتحكم في النظم المعلوماتية. في هذه الحالة سوف لن يكتف بما رآه أو سمعه، بل إن شهادته ستتضمن تصريحات يظهر من خلالها معرفته بالنظم المعلوماتية.

إذن، ومن أجل إبراز استقلال صفة الخبير عن الشاهد، نذكر في هذا السياق بأن الخبير يتم اختياره من ضمن قائمة الخبراء المتواجدة لدى الجهات القضائية، ويتم تكليفه بإعداد خبرة تحدد من خلالها المهام المناطة به، ثم بعد ذلك يلتزم بتحرير تقرير يقدمه إلى جهات التحقيق.

ثالثا: الفئات التي تأخذ حكم الشاهد المعلوماتي

إن صفات التخصص والتحكم في النظم المعلوماتية وامتلاك المعرفة في مجال تقنيات الحاسب الآلي وشبكات الإنترنت، أضفت على فئات عديدة صفة الشاهد المعلوماتي، والذين قد تستدعيهم سلطات التحقيق لإبداء ما يعرفونه بخصوص الجرائم الإلكترونية.

هذه الفئات قد تتمثل في:

- المبرمجون.
- المحللون.

[1] عبد اللاه أحمد هلالي، التزام الشاهد بالإعلام في الجريمة المعلوماتية، الطبعة الثانية، دار النهضة العربية،2009.

- مشغلي الحاسب الآلي.
- مديرو النظم.
- مهندسو الصيانة والاتصالات.
- مزودو خدمات الإنترنت.

الفرع الثاني: التزامات الشاهد في الجريمة الإلكترونية

لم يخصص المشرع الجزائري نصوصا قانونية تنظم الشهادة في الجريمة الإلكترونية، الأمر الذي يدعونا إلى التطرق لالتزامات الشاهد وفقا للقواعد العامة المنصوص عليها بمقتضى المواد من 88 إلى 99 من قانون الإجراءات الجزائية[1].

لقد حملت لنا المادة 97 من قانون الإجراءات الجزائية[2] الجزائري تلك الالتزامات الملقاة على عاتق الشاهد، فكل شخص استدعي لسماع شهادته ملزم بما يلي:

–الحضور.

–حلف اليمين.

–الإدلاء بشهادته.

ويتم ذلك مع مراعاة الأحكام المتعلقة بسر المهنة.

وفي حالة امتناع الشاهد عن الحضور، أو حضر لكنه امتنع عن حلف اليمين والإدلاء بشهادته، فإنه يكون عرضة للغرامة والمقدرة ما بين 200 و2000 دينار جزائري.

إن أهم التزام للشاهد هو أداء الشهادة، والسؤال يطرح هنا حول التزامات الشاهد المعلوماتي وما مدى إلزامه بالإدلاء بكل ما يملكه من معلومات. هذا ما سنسعى لشرحه من خلال ما سيأتي.

[1] الأمر رقم 66–155، المرجع السابق.

[2] المرجع نفسه.

أولا: التزامات الشاهد المعلوماتي

لقد ذكرنا سابقا أن الشاهد المعلوماتي شخص يمتلك كفاءات في موضوع النظم المعلوماتية بما فيها الحاسب الآلي وشبكات الإنترنت، كما يملك معلومات تخص الولوج لنظم المعالجة الآلية للبيانات.

إذن في حالة وقوع جريمة إلكترونية وتم استدعاء الشاهد المعلوماتي من أجل الاستفادة من شهادته فعليه الاستجابة، لكن يكون ذلك في ظل أحكام النصوص العامة التي أشرنا إليها سابقا وهي المواد من 88 إلى 99 من قانون الإجراءات الجزائية[1]، وهذا أمام انعدام نصوص تشريعية تنظم الشهادة في الجريمة الإلكترونية.

لذلك وجب على المشرع التدخل من أجل مواكبة التحديات التي فرضتها الطبيعة الخاصة للجريمة الإلكترونية على القواعد الإجرائية، وهذا من أجل تسهيل عمل سلطات التحقيق من جهة، ومن جهة أخرى من أجل المحافظة على الشرعية الإجرائية وذلك من خلال تفادي التوسع في النصوص التقليدية القائمة ومحاولة تطويعها وتطبيقها على المستجدات التي جاءت بها الجريمة الإلكترونية.

ثانيا: مدى إلزام الشاهد المعلوماتي بالإدلاء بكل ما يملكه من معلومات

بالرجوع إلى القواعد العامة السالفة الذكر، نجد أن الشاهد ملزم بالأدلاء بما سمعه أو شاهده، غير أن الطبيعة الخاصة للجريمة الإلكترونية كونها تتخذ من النظم المعلوماتية محلا لها، تضع الشاهد المعلوماتي أمام التزامات غير منصوص عليها في القواعد العامة.

إن النظم المعلوماتية تتضمن كم هائل من البيانات ومنها ما هو محمي بكلمات مرور أو برامج يلزم لتشغيلها مفاتيح الشفرات...الخ. فالشاهد المعلوماتي قد يجد نفسه مدعوا لتقديم كم هائل من المعلومات يتعلق بنظم المعالجة الآلية للمعطيات. وهنا يطرح سؤال حول مدى إمكانية إلزام الشاهد المعلوماتي بالإدلاء بهذه المعلومات ضمن شهادته.

[1] الأمر رقم 66-155، المرجع السابق.

انقسم الفقه المقارن والتشريعات المقارنة بخصوص هذه المسألة، ويمكن حصر هذه الانقسامات في اتجاهين، أحدهما يرى بأن الشاهد المعلوماتي ملزم بالإفصاح عن كل المعلومات التي يتطلبها التحقيق، في حين يرى أصحاب الاتجاه الآخر بأن الشاهد المعلوماتي غير ملزم بذلك، وسنتناول التفصيل في هذين الاتجاهين كالآتي:

أ-الاتجاه الأول:

يرى أنصار هذا الاتجاه بأن الشاهد المعلوماتي ملزم بتقديم كل البيانات والمعلومات التي يمكن أن تستفيد منها جهات التحقيق في الوصول إلى الحقيقة. ويدعم هذا الرأي مشروع قانون الحاسب الآلي الهولندي الذي يجيز في مادته 125 لسلطات التحري والتحقيق أمر القائم بتشغيل النظام بالإفصاح عن تلك المعلومات اللازمة من أجل اختراق النظام والولوج إليه بما في ذلك كلمات المرور السرية ومفاتيح الشفرات.[1]

أما المشرع اليوناني ومن خلال المادة 223 من قانون الإجراءات الجنائية اليوناني، يرى إمكانية الحصول من القائم بتشغيل نظام الحاسب على كلمات المرور السرية للولوج إلى نظام المعلومات، غير أنه غير ملزم بطباعة ملفات البيانات المخزنة في ذاكرة الحاسب.[2]

في فرنسا يذهب جانب من الفقه إلى أن القواعد العامة الخاصة بالشهادة أمام جهات التحقيق تسري كذلك في مجال الإجراءات المعلوماتية، وبالتالي يرون بالتزام الشاهد بتقديم كلمات المرور السرية ومفاتيح الشفرات التي تسمح بتشغيل البرامج.[3]

ويبدو بأن الدول الأطراف بالاتفاقية الأوربية المتعلقة بالجرائم الإلكترونية (بودابست 2001) بإمكانها تجاوز الفراغ التشريعي في هذا الموضوع وذلك من خلال الاستفادة من مضمون المادة 18 من الاتفاقية[4] والتي خولت لكل دولة من الدول الأطراف اتخاذ ما يلزم

[1] Henrik W.K. Kaspersen, Op.Cit, p 496.

[2] أنظر في هذا المعنى: هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، المرجع السابق، ص 85.

[3] عبد اللاه أحمد هلالي، التزام الشاهد بالإعلام في الجريمة المعلوماتية، الرجع السابق، ص 23.

[4] Article 18: (Convention sur la cybercriminalité Budapest, Op.Cit)
"1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner: =

من تدابير تشريعية وتدابير أخرى تمنحها صلاحية توجيه الأمر لأي مقدم خدمة من أجل تقديم المعلومات التي بحوزته. حيث نصت على أنه: تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة إصدار أمر إلى:

أ .أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزة ذلك الشخص أو تحت سيطرته، ومخزنة على نظام الكومبيوتر أو على أي دعامة أخرى لتخزين بيانات الكمبيوتر.

ب .أي مزود خدمة يعرض خدماته داخل أراضي الدولة الطرف بتقديم معلومات عن المشترك ذات الصلة بتلك الخدمات الموجودة بحوزته أو تحت سيطرته.

إن عبارة"...تدابير أخرى" التي جاءت بها نص المادة 18 من الاتفاقية الأوربية المتعلقة بجرائم الإنترنت أتاحت للدول الأطراف تجاوز العائق المتمثل في الفراغ التشريعي.

ب-الاتجاه الثاني:

على نقيض الاتجاه الأول، يرى أصحاب هذا الاتجاه بأن الشاهد المعلوماتي غير ملزم بتقديم البيانات المخزنة أو طباعتها أو نسخها، كما أنه غير ملزم بالإفصاح عن كلمات المرور السرية ومفاتيح الشفرات التي تتيح تشغيل البرامج وهذا هو حال الفقه في تركيا، كما أن نظيره في ألمانيا يعتبر بأن الشاهد المعلوماتي غير ملزم بطباعة البيانات المخزنة بالحاسب.

أما عن رأينا الخاص وموقفنا من الاتجاهين السابقين، فإننا وإن كنا ندرك خطورة الجريمة الإلكترونية وما تشكله من تهديدات وأضرار على الأفراد والمؤسسات والدول، وما يجب أن يقابل ذلك من تسهيل لمهام جهات التحقيق ومساعدتها ومساندتها في سعيها لجمع الأدلة

= a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

من أجل كشف الحقيقة والوصول إلى الجناة، غير أننا وبالمقابل فإننا نتمسك بالشرعية الإجرائية وما تكفله من حماية وصيانة لحريات الأفراد وحياتهم الخاصة.

فالإشكال المطروح بخصوص إلزام الشاهد المعلوماتي بالإفصاح عن المعلومات، يجب معالجته من خلال سن نصوص قانونية تسد الفراغ التشريعي في موضوع الشهادة والشاهد المعلوماتي. وإلى حين التوصل إلى ذلك، يبقى الشاهد المعلوماتي ملزم فقط بما جاءت به القواعد العامة فقط لأن كل محاولة للتوسع في إلزامه بتقديم معلومات أخرى غير ما رآه أو سمعه سيكون غير قانوني، أو سيغير من المركز القانوني للشاهد بحيث سيأخذ حينئذ صفة الخبير وليس الشاهد. هذا دون أن ننسى إعفاءه من الإدلاء بتلك المعلومات التي هي من ضمن أسرار المهنة.

المبحث الثاني: الإجراءات الحديثة المتعلقة بجمع الدليل الإلكتروني

بعض عرضنا للطرق التقليدية المتعلقة بجمع الأدلة، اتضح لنا مدى الصعوبات التي واجهت جهات التحقيق، ومرد ذلك الطبيعة الخاصة للدليل الإلكتروني الذي يتواجد في بيئة جديدة تختلف عن البيئة المادية للجريمة التقليدية، لذلك كان لابد من أن تتوجه اهتمامات وجهود الدول نحو إيجاد أساليب وطرق أخرى بإمكانها دعم جهات التحقيق في سعيها للحصول على الدليل في الجريمة الإلكترونية، وقد كللت هذه الجهود باستحداث إجراءات جديدة تساير التطور التكنولوجي في مجال الاتصالات وتراعي طبيعة الدليل الإلكتروني المراد استخلاصه.

سنتناول في هذا الجزء من البحث كل من الإجراءات التالية: التسرب، مراقبة الاتصالات الإلكترونية، وحفظ المعطيات المتعلقة بحركة السير.

المطلب الأول: التسرب

إن سعي جهات التحقيق إلى جمع كل الأدلة التي من شأنها أن توصلها إلى كشف الحقيقة، أدى إلى تنوع وتعدد أساليب وإجراءات الحصول على الدليل.

يعد التسرب أحد أهم هذه الإجراءات، وسنتعرف على هذا الإجراء في هذا المطلب من خلال التعريف به ثم التطرق إلى شروطه، وكيف تتم الاستعانة به في مجال الجريمة الإلكترونية.

الفرع الأول: تعريف التسرب

تناول المشرع الجزائري موضوع التسرب من خلال التعديل الذي أدخله على قانون الإجراءات الجزائية[1] وذلك بإضافته للفصل الخامس الذي شمل المواد من المادة 65 مكرر 11 إلى المادة 65 مكرر 18. فنصت المادة 65 مكرر 12 من قانون الإجراءات الجزائية[2] على أنه " 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 أنه فاعل معهم أو شريك أو خاف".

وفي السياق المتصل بالجريمة الإلكترونية، أكد المشرع الجزائري من خلال المادة 65 مكرر 11 من قانون الإجراءات الجزائية[3] على شرعية اللجوء إلى التسرب كإجراء إذا دعت مقتضيات التحري أو التحقيق إلى ضرورة مباشرة التسرب في الجرائم المنصوص عليها في المادة 65 مكرر5 التي أوردت الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من بين تلك الجرائم المعنية بالتسرب.

بخصوص اللجوء إلى التسرب كإجراء من إجراءات جمع الأدلة المتعلقة بالجريمة الإلكترونية يمكننا تصور حصوله في صورتين:

أولا-الصورة الأولى: صورة مادية تتمثل في مزاملة ومخالطة القائم بالتسرب لأولئك الأشخاص المشتبه بهم أو المتهمين بارتكاب جرائم إلكترونية أو يخططون لها وذلك من خلال الالتقاء الفعلي والحقيقي بهم.

[1] القانون 06-22، المرجع السابق.

[2] المرجع نفسه.

[3] المرجع نفسه.

ثانيا-الصورة الثانية: كما يمكن تصور التسرب في صورة ثانية تكون داخل العالم الافتراضي كأن يدخل القائم بالتسرب إلى غرفة من غرف الدردشة المنتشرة عبر شبكة الإنترنت أو إلى موقع من مواقع التواصل الاجتماعي أو موقع آخر معروف بتداول ملفات ذات طابع إباحي كصور للأطفال أو موقع يعرض للبيع أسلحة أو فيروسات مدمرة للأنظمة والبيانات، أو مواقع يبث من خلالها أشخاص محتويات تخص الحياة الخاصة للأفراد بغرض ابتزازهم أو التشهير بهم، إلى غير ذلك من الجرائم التي تتخذ من العالم الافتراضي مسرحا لها. فيقوم العون المتسرب بإيهامهم بكونه شخص مهتم بشراء ما يعرضونه أو أن يغريهم بأن يعرض عليهم مثلا محتويات أفضل من تلك التي يملكونها وبسعر أفضل من شأنه أن يحقق لهم أرباحا أعلى في ظرف وجيز، إلى غير ذلك من الأساليب التي يكون الهدف منها ربط الاتصال بالجناة والالتقاء بهم في الواقع بعيدا عن العالم الافتراضي وذلك من أجل الإيقاع بهم.

الفرع الثاني: شروط مباشرة التسرب

لما كان التسرب من الإجراءات التي قد تمس بالحريات الخاصة للأفراد وخصوصيتهم، فإن المشرع قيده بشروط يجب أن تتوافر فيه. هذه الشروط تتمثل في:

أولا: الحصول على إذن قضائي مكتوب يتضمن الجريمة موضوع التسرب وهوية المسؤول عن عملية التسرب.

إذ نصت المادة 65 مكرر 11 من قانون الإجراءات الجزائية[1] على أنه "... يجوز لوكيل الجمهورية أو القاضي التحقيق، بعد إخطار وكيل الجمهورية، أن يأذن تحت رقابته ...".

يتضح من نص المادة أعلاه وجوب صدور إذن إما من وكيل الجمهورية، أو من قاض التحقيق بعد إخطاره لوكيل الجمهورية من أجل مباشرة عملية التسرب. فلا يمكن لضباط الشرطة القضائية المبادرة من دون حصولهم على إذن من وكيل الجمهورية أو قاض التحقيق.

[1] المرجع نفسه.

كما يشترط أن يكون هذا الإذن مكتوبا وذلك بحسب المادة 65 مكرر 15 من قانون الإجراءات الجزائية[1] التي جاء بها " يجب أن يكون الإذن المسلم طبقا للمادة (65مكرر 11) أعلاه مكتوبا...وذلك تحت طائلة البطلان".

فلا يجوز أن يصدر الأمر شفاهة وإلا كان الإجراء باطلا.

يجب أن يتضمن الإذن القضائي المكتوب تلك الجريمة موضوع التسرب وكذا هوية ضابط الشرطة القضائية الذي يشرف على عملية التسرب وذلك طبقا للمادة 65 مكرر 15 الفقرة الثانية من قانون الإجراءات الجزائية[2] التي جاء بها " ...تذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته...".

هذا ونشير إلى أن الوثيقة المتضمنة لإذن التسرب تبقى خارج ملف الإجراءات إلى غاية انتهاء عملية التسرب وذلك حفاظا على السرية.

ثانيا: الشخص القائم بالتسرب

تناط عملية التسرب إما لضباط الشرطة القضائية أو أعوان الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المشرف على عملية التسرب، وذلك طبقا للفقرة الأولى من نص المادة 65 مكرر 12 من من قانون الإجراءات الجزائية[3]"... يقصد بالتسرب قيام ضابط أو عون الشرطة القضائية، تحت مسؤولية ضابط الشرطة القضائية...".

كما يفهم من نص المادة 65 مكرر 14 الفقرة الأولى من قانون الإجراءات الجزائية[4] التي نصت "... يمكن ضباط وأعوان الشرطة القضائية المرخص لهم بإجراء عمليات التسرب والأشخاص الذين يسخرونهم لهذا الغرض..." بأنه يمكن تسخير أشخاص آخرين للقيام بالتسرب.

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] المرجع نفسه.

[4] المرجع نفسه.

ثالثا: مدة عملية التسرب

من خلال نص المادتين (المادة 65 مكرر15 بالفقرات الثالثة والرابعة وكذا الخامسة والمادة 65 مكرر 17)[1] من قانون الإجراءات الجزائية[2] نستنتج بأنه تحدد مدة التسرب بمدة لا تتجاوز 4 أشهر يتم تجديدها بحسب مقتضيات التحري أو التحقيق وضمن نفس الشروط الشكلية والزمنية، كما يجوز الأمر بوقف عملية التسرب وذلك في أي وقت قبل أن ينقضي أجلها.

إذا تقرر وقف عملية التسرب أو انقضى أجلها أو تقرر عدم تمديدها، فإنه يمكن للقائم بالتسرب مواصلة القيام بالنشاطات المذكورة بنص المادة 65 مكرر 14 من قانون الإجراءات الجزائية[3] لمدة لا تتجاوز الأربعة أشهر إلى غاية توقيف عمليات المراقبة في ظروف تضمن أمنه وهذا دون أن يكون مسؤولا جزائيا.

أما إذا انقضت مهلة الأربعة أشهر ولم يتمكن القائم بالتسرب أيضا من توقيف نشاطه في ظروف تضمن أمنه، أمكن للقاضي الذي أصدر الإذن بالتسرب أن يرخص بتمديد المهلة لمدة لا تتجاوز أربعة أشهر.

[1] المادة 65 مكرر15 من قانون الإجراءات الجزائية بالفقرات الثالثة والرابعة وكذا الخامسة بأنه "... ويحدد هذا الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة أشهر.

ويمكن أن تجدد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية.

ويجوز للقاضي الذي رخص بإجرائها أن يأمر، في أي وقت، بوقفها قبل انقضاء المدة المحددة".

المادة 65 مكرر 17 من قانون الإجراءات الجزائية على أنه "إذا تقرر وقف العملية أو عند انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها، يمكن العون المتسرب مواصلة النشاطات المذكورة في المادة 65 مكرر 14 أعلاه للوقت الضروري الكافي لتوقيف عمليات المراقبة في ظروف تضمن أمنه دون أن يكون مسؤولا جزائيا، على ألا يتجاوز ذلك مدة أربعة أشهر.

يخبر القاضي الذي أصدر الرخصة المنصوص عليها في المادة 65 مكرر 11 أعلاه، في أقرب الآجال، وإذا انقضت مهلة الأربعة (4) أشهر دون أن يتمكن العون المتسرب من توقيف نشاطه في ظروف تضمن أمنه، يمكن هذا القاضي أن يرخص بتمديدها لمدة أربعة (4) أشهر على الأكثر".

[2] المرجع نفسه.

[3] المرجع نفسه.

هذا، ونشير في الأخير إلى أن القانون يجيز للقائم بالتسرب طبقا لنص المادة 65 مكرر 14 من قانون الإجراءات الجزائية[1] القيام بما يأتي:

- 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 تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

وهذا مع إعفائه من المتابعة الجزائية التي قد تنجم عن الأفعال المشار إليها في المادة 65 مكرر 14 أعلاه.

كما أنه وطبقا للمادة[2] 65 مكرر16 من قانون الإجراءات الجزائية[3] فإن القائم بالتسرب يستفيد هو وأفراد عائلته من عدم كشف هوياتهم، على أن يكون محل متابعة كل من يتسبب في إظهار الهوية الحقيقية للقائم بالتسرب لأن ذلك يشكل جنحة.

[1] المرجع نفسه.

[2] المادة 65 مكرر 16 "لا يجوز إظهار الهوية الحقيقية لضابط أو أعوان الشرطة القضائية الذين باشروا عملية التسرب تحت هوية مستعارة في أي مرحلة من مراحل الإجراءات.

يعاقب كل من يكتشف هوية ضباط أو أعوان الشرطة القضائية بالحبس من سنتين إلى خمس سنوات وبغرامة من 50000دج إلى 200000 دج. وإذا تسبب الكشف عن الهوية في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس إلى عشر سنوات والغرامة من 2000000دج إلى 500000دج.

وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر سنوات إلى عشرين سنة والغرامة 500000 دج إلى 100000 دج من دون الإخلال، عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات"

[3] المرجع نفسه.

وإذا أدى إظهار وكشف الهوية الحقيقية للقائم بالتسرب إلى أعمال عنف ضده أو ضد زوجه أو أبناءه أو أصوله المباشرين، فإن ذلك يشكل جناية يعاقب عليها من 05 إلى 10 سنوات. وإذا أدى الأمر إلى وفاة أحد هؤلاء تكون العقوبة من 10 إلى 20 سنة.

المطلب الثاني: مراقبة الاتصالات الإلكترونية

حرصا منه على مواكبة التشريعات المقارنة فيما يتعلق بالإجراءات الجنائية في مجال المعلوماتية، ودعما منه لجهات التحقيق في مواجهة الجريمة الإلكترونية، عمد المشرع الجزائري إلى مواصلة سن تلك النصوص القانونية التي تسهل إلى حد ما على تقفي أثر المجرم الإلكتروني وجمع أكبر قدر من الأدلة التي تفضي إلى كشف الحقيقة.

وفي هذا السياق أقر إجراء حديث لجمع الدليل الإلكتروني ألا وهو مراقبة الاتصالات الإلكترونية.

سنسعى من خلال هذا المطلب إلى التعرف على مفهوم هذا الإجراء وكذا الشروط المتعلقة به.

الفرع الأول: مفهوم مراقبة الاتصالات الإلكترونية

من أجل محاولة فهم المقصود بمراقبة الاتصالات الإلكترونية، سنقدم تعريفا للاتصالات الإلكترونية ثم نتطرق لصور الاتصالات الإلكترونية محل المراقبة، وبعد ذلك ننظر في معنى مراقبة الاتصالات الإلكترونية كإجراء من إجراءات جمع الأدلة الإلكترونية.

أولا: تعريف الاتصالات الإلكترونية

عرف المشرع الجزائري مصطلح الاتصالات الإلكترونية بموجب المادة 02 الفقرة (و) من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]على أنها " أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".

[1] القانون 09-04، المرجع السابق.

غير أن المشرع الجزائري عاد لإعطاء تعريف آخر معدل مقارنة بالتعريف السابق، وذلك بموجب المادة الخامسة من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1]، حيث عرف الاتصالات الإلكترونية على أنها " كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات أيا كانت طبيعتها عن طريق أي وسيلة إلكترونية، بما في ذلك وسائل الهاتف الثابت والنقال".

يلاحظ بأن المشرع استبدل كلمة "مختلفة" الواردة في التعريف السابق بعبارة "أيا كانت طبيعتها" كما حذف كلمة "بواسطة" واستعمل بدلها عبارة "عن طريق"، كما أضاف في نهاية المادة عبارة "بما في ذلك وسائل الهاتف الثابت والنقال" التي لم تكن موجودة في المادة السابقة. ويبدو جليا أن الأمر يتعلق باستدراك لثغرة يعتقد المشرع أن المادة السابقة تضمنتها.

نشير إلى أن الهيئة التي أنشأت سنة 2015 بموجب المرسوم الرئاسي[2] كان المشرع قد أشار إليها سنة 2009 بموجب القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].

ويعرفها المشرع الأمريكي بموجب قانون المراقبة السلكية على أنها " أي تحويل لمؤشرات أو إشارات أو كتابة أو صور أو أصوات أو بيانات أو أي معلومات من أية نوع يتم بثها جزئيا أو كليا بواسطة نظام سلكي أو لاسلكي أو كهرومغناطيسي أو كهروضوئي أو ضوئي".

ثانيا: صور الاتصالات الإلكترونية

من خلال ما جاء في محتوى المادة 05 المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[4] والتي

[1] المرسوم الرئاسي رقم 15-261، المرجع السابق.

[2] المرجع نفسه.

[3] القانون 09-04، المرجع السابق.

[4] المرسوم الرئاسي رقم 15-261، المرجع السابق.

تناولت تعريف المقصود بالاتصالات الإلكترونية، نستنتج بأنه قد يدخل في مفهوم الاتصالات الإلكترونية المراسلات السلكية واللاسلكية وكذا البريد الإلكتروني.

1 – المراسلات السلكية واللاسلكية:

يقصد بالمراسلات كافة الرسائل المكتوبة أيا كانت الطريقة التي ترسل بها سواء كانت داخل مظروف مغلق أو مفتوح أو كانت عبارة عن بطاقة مكشوفة طالما أن مرسلها أراد عدم اطلاع غير المرسلة إليه عليها.[1]

أما المراسلات السلكية واللاسلكية، فقد عرفها المشرع الجزائري بموجب المادة الثامنة الفقرة 21 من القانون الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية[2] على أنها " كل تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى كهربائية مغناطيسية"

إذن من خلال ما سبق يتضح بأن المراسلات التي قصدها المشرع الجزائري عند تعريفه للاتصالات الإلكترونية هي تلك المراسلات التي تتم عن طريق الاتصال السلكي واللاسلكي وبالتالي فلقد استبعد ضمنيا المراسلات التقليدية كالرسائل والبطاقات الورقية المرسلة عن طريق البريد العادي.

[1] أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 1993م ص578.

[2] القانون رقم 2000-03 المؤرخ في 5 جمادى الأول عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية العدد 48 الصادرة في 6 جمادى الأول عام 1421 الموافق 6 غشت سنة 2000.

أما المشرع الأمريكي وبموجب القانون المتعلق بخصوصية الاتصالات الإلكترونية لسنة 1986 فقد عرف البريد الإلكتروني على أنه "وسيلة اتصال يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تليفونية عامة أو خاصة وفي الشكل الغالب تتم كتابة الرسالة على جهاز الحاسب ويتم إرسالها إلكترونيا إلى حاسب مورد الخدمة الذي يتولى تخزينها لديه حتى يأتي المرسل إليه ليستعيدها"[1].

ولدى الفقه من يرى بأن البريد الإلكتروني يمكن تعريفه بأنه "نظام للتراسل باستخدام شبكات الحاسب يستخدم كمستودع لحفظ المستندات والأوراق والمراسلات التي تتم معالجتها رقميا في صندوق خاص وشخصي للمستخدم ولا يمكن الدخول إليه إلا عن طريق كلمة المرور".[2]

كما عرفه الفقه بأنه "طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات".[3]

ثالثا: المقصود بمراقبة الاتصالات الإلكترونية

المشرع الجزائري لم يقدم تعريفا لمراقبة الاتصالات الإلكترونية، فاكتفى إذن بتعريف الاتصالات الإلكترونية وتناول مراقبة الاتصالات الإلكترونية كإجراء بنص المادة الثالثة القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[4] التي نصت على أنه "مع مراعاة الأحكام القانونية التي تضمن

[1] " Electronic mail is a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common from, messages are typed in to a computer terminal, and then transmitted over telephone lines to a recipient computer operated by an electronic mail company, If The intended addressee subscribes to the service, the message is stored… such as systems operated by private companies for internal correspondence".
Calendar No. 1064. C O P . 2 RESS. REPORT. SENATE. 99-541. ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986. OCTOBER 17 (legislative day, OCTOBER 10), 1986, p 08.
The link below allows you to download the file from the Internet (Available 09/07/2018):
https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf
أنظر كذلك عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة، 2005، ص 14.

[2] مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى، عين مليلة، 2008، ص 59.

[3] عبد الهادي فوزي العوضي، المرجع السابق، ص12.

[4] القانون 09-04، المرجع السابق.

ويعرف الفقه المراقبة الإلكترونية على أنها " العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع بيانات أو معلومات عن المشتبه فيه سواء أكان شخصا أو مكانا أو شيئا حسب طبيعته لتحقيق غرض أمني أو لأي غرض آخر"[1].

ويقترح الدكتور سامي جلال فقي حسين تعريفا للمراقبة الإلكترونية فيرى بأنها "اعتراض الاتصالات الإلكترونية أيا كان نوعها بموجب إذن قضائي من قبل الخبير المعلوماتي المخول قانونا وباستخدام التقنيات اللازمة لهذه العملية""[2].

رابعا: أشكال مراقبة الاتصالات الإلكترونية

من بين صور مراقبة الاتصالات الإلكترونية نجد اعتراض المراسلات السلكية واللاسلكية وكذا اعتراض البريد الإلكتروني.

1 – اعتراض المراسلات السلكية واللاسلكية:

خول المشرع الجزائري للجهات القضائية الاستعانة بإجراء حديث يساعدها في سعيها من أجل جمع الأدلة، وذلك لمجابهة الجرائم الإلكترونية. هذا الإجراء يتمثل في اعتراض المراسلات السلكية واللاسلكية والذي ورد ذكره بنص المادة 65 مكرر 05 من قانون الإجراءات الجزائية[3].

المشرع الجزائري لم يقدم تعريفا لعملية اعتراض المراسلات السلكية واللاسلكية أو كما يسميها البعض بالتنصت.

بالرجوع إلى الفقه يمكن تعريف اعتراض المراسلات بأنه" إجراء تحقيقي يباشر خلسة وينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع

---

https://uscode.house.gov/view.xhtml?req=(title:18%20section:2510%20edition:prelim)#2510_1

[1] مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، الطبعة الأولى، مطابع الشرطة، القاهرة، 2003، ص 192.

[2] أنظر: سامي جلال فقي حسين، المرجع السابق، ص 284.

[3] القانون 06-22، المرجع السابق.

إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية لمواجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية"[1].

2 – اعتراض البريد الإلكتروني:

بالإضافة إلى اعتراض المراسلات السلكية واللاسلكية، فإن اعتراض البريد الإلكتروني يعتبر صورة من صور مراقبة الاتصالات الإلكترونية، ونظرا لكون البريد الإلكتروني يعتمد على شبكة الأنترنت كوسيلة للتواصل فإن الطرق التقليدية لا تصلح لمراقبة البريد الإلكتروني، ولهذا ظهرت إلى الوجود أساليب متطورة قادرة على مراقبة البريد الإلكتروني نذكر من بينها نظام كارنيفور CARNIVOR[2] والذي تستخدمه وكالة المباحث الفيديرالية الأمريكية للتجسس.

---

[1] ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009، ص 150.

[2] وتعني تسمية كارنيفور "آكل اللحوم" في إشارة إلى كون هذا البرنامج يقوم بالتهام كافة البيانات المتدفقة عبر الشبكة. أنظر في هذا المعنى فهد عبد الله العبيد العازمي، المرجع السابق، ص 76.

وكارنيفور CARNIVORE هو برنامج تم تطويره من طرف مكتب التحقيقات الفيديرالي (FBI) وهو مصمم ليسمح بجمع معلومات محددة حول رسائل البريد الإلكتروني أو أية اتصالات إلكترونية أخرى. وتجدر الإشارة إلى أنه وبعد أحداث 2001/09/11 تم تغيير تسمية البرنامج من كارنيفور إلى دي سي آس 1000 (DCS1000). وإذا كان كارنيفور هو البرنامج الأشهر إلا أن هناك برامج أخرى منافسة له ففي بريطانيا أصدر مجلس العموم قانونا يحمل اسم (RIP) وبموجبه يفرض على كافة الشركات المزودة لخدمات إنترنت أن تقوم بالتعاون مع السلطات في التحقيقات الأمنية بتثبيت جهاز (صندوق أسود) مشابه لكارنيفور بجانب أجهزتها المزودة. وكذلك الوضع في روسيا، حيث هناك صدر قانون يحمل اسم (SORM) ويفرض على الشركات المزودة لخدمات الإنترنت إلزامية تحويل كافة البيانات المتداولة إلى جهاز وكالة الاستخبارات الروسية (FSB) للاطلاع عليها واستخدامها دون أمر من المحكمة. لمزيد من المعلومات على الرابطين التاليين: (متاحين بتاريخ 2018/10/10):

https://www.epic.org/privacy/carnivore/default.html
https://ar.wikipedia.org/wiki/كارنيفور

لحياتهم الخاصة.[1] لذلك كان من الضروري وعلى قدر بالغ من الأهمية وضع ضمانات تحفظ وتصون حرمة الحياة الخاصة للأفراد لدى استغلالهم لوسائل الاتصالات الإلكترونية.

هذه الضمانات عبارة عن مجموعة من الشروط والضوابط وجب التقيد بها عند لجوء جهات التحقيق لمراقبة الاتصالات الإلكترونية كإجراء يتيح لها جمع الأدلة التي قد تساعدها على الوصول إلى الجاني وتساهم بالتالي في كشف الحقيقة.

قبل الخوض في عرض تلك الشروط التي تنظم عملية تنفيذ مراقبة الاتصالات الإلكترونية، لابد لنا من التوقف عند نقطة نراها مهمة، وبالتالي يتعين علينا إيفائها قدر من التوضيح. فلدى اطلاعنا على المواد التي جاء بها القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2] وكذلك تلك المواد التي تضمنها المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3]، خلصنا إلى نتيجة مفادها بأن المشرع الجزائري تناول عملية مراقبة الاتصالات الإلكترونية في حالتين مختلفتين. الحالة الأولى هي تلك التي ترد فيها مراقبة الاتصالات الإلكترونية كإجراء وقائي من أفعال معينة أو في حالة احتمال حدوث اعتداء لم يقع بعد، ففي هذه الحالة الجريمة لم تقع بعد والاعتداء لم يحدث، فنحن هنا أمام المراقبة الوقائية للاتصالات الإلكترونية، هذا من جهة.

من جهة أخرى، ففي الحالة الثانية تكون الجريمة قد وقعت وبدأت التحريات والتحقيقات بشأنها، وهذه الحالة هي التي تهمنا في موضوع مراقبة الاتصالات الإلكترونية باعتبارها إجراء من إجراءات التحقيق الابتدائي يهدف إلى جمع الأدلة من أجل الكشف عن الحقيقة.

[1] محمد كمال شاهين، المرجع السابق، ص 325.

[2] القانون 09-04، المرجع السابق.

[3] المرسوم الرئاسي رقم 15-261، المرجع السابق.

إذن كان لابد من الإشارة لهذا الأمر وذلك من أجل رفع اللبس وتجنب الخلط بين الإجرائين لأن النصوص القانونية الواردة في القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] والمرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2] لا تبدو واضحة من أول وهلة.

بعد أن أصبح الفرق واضحا بين الحالتين، نمر الآن إلى عرض تلك الضوابط التي يجب احترامها والتقيد بها عند مراقبة الاتصالات الإلكترونية وهذا مراعاة للشرعية الإجرائية. هذه الضوابط هي:

أولا: وجود سبب ضروري يبرر اللجوء لمراقبة الاتصالات الإلكترونية

يمكن لمستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية، وهذا ما تضمنته المادة 65 مكرر5 من قانون الإجراءات الجزائية[3] فيجوز اللجوء إلى اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية وذلك إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات. وفي السياق ذاته، جاءت كذلك المادة 03 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة

[1] القانون 09-04، المرجع السابق.

[2] المرسوم الرئاسي رقم 15-261، المرجع السابق.

[3] المادة 65 مكرر 5 "إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهورية المختص أن يأذن بما يأتي- :اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية - .وضع الترتيبات التقنية, دون موافقة المعنيين, من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية أو التقاط صور لشخص أو عدة أشخاص يتواجدون في مكان خاص . يسمح الإذن المسلم بغرض وضع الترتيبات التقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم أو رضا الأشخاص الذين لهم حق على تلك الأماكن .تنفذ العمليات المأذون بها على هذا الأساس تحت المراقبة المباشرة لوكيل الجمهورية المختص .في حالة فتح تحقيق قضائي، تتم العمليات المذكورة بناء على إذن من قاضي التحقيق وتحت مراقبته المباشرة"، القانون 06-22، المرجع السابق.

بتكنولوجيات الإعلام والاتصال ومكافحتها[1] والتي نصت على أنه ""مع مراعاة الأحكام القانونية التي تخص سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية".

غير أن هذا الأمر لا يمكن أخذه على إطلاقه، فاللجوء إلى مراقبة الاتصالات الإلكترونية ليس إجراء آلي نستعين به كلما كنا أمام تحقيقات قضائية وإنما هو مقيد بأسباب، والسبب الذي يهمنا نصت عليه المادة الرابعة من نفس القانون بالفقرة (ج) حيث اشترطت أن تواجه التحقيقات القضائية الجارية صعوبة للوصول إلى نتيجة، بمعنى أن يكون أمر اللجوء إلى مراقبة الاتصالات الإلكترونية ضروريا.

لكن كيف يمكننا التأكد من أن جهات التحقيق في حاجة ماسة فعلا إلى مراقبة الاتصالات الإلكترونية؟ بحسب المادة الثامنة بفقرتها الثانية من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2] فإن اللجنة المديرة، والتي تعتبر جهاز من ضمن الأجهزة التي تتشكل منها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، هي من تتولى النظر في حقيقة ومدى توافر وقيام شروط اللجوء للمراقبة الوقائية الاتصالات الإلكترونية. لكن هنا الأمر يتعلق بالمراقبة "الوقائية"، إذن بحسب رأينا فإن تقدير مدى الحاجة إلى اللجوء لمراقبة الاتصالات الإلكترونية لا يخرج عن جهتين، إما يخضع لتقدير قاض التحقيق المختص مادام أنه هو من يمنح الإذن بمباشرة المراقبة في حالة فتح تحقيق قضائي، كما أنه يشرف مباشرة ويراقب تنفيذ العمليات المأذون بها، وذلك طبقا للمادة 65 مكرر5 من قانون الإجراءات الجزائية[3] في فقرتها الأخيرة. أو أن

[1] القانون 09-04، المرجع السابق.

[2] المرسوم الرئاسي رقم 15-261، المرجع السابق.

[3] القانون 06-22، المرجع السابق.

يخضع هذا التقدير لوكيل الجمهورية في حالة التلبس ما دام أنه هو من يأذن بعملية المراقبة، وهذا ما يمكن استنتاجه من نفس المادة في فقرتها الأولى.

ثانيا: صدور إذن مكتوب من السلطة القضائية المختصة

حيث اشترطت المادة الرابعة من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] في فقرتها الأخيرة وجوب صدور رخصة عن الجهة القضائية المختصة، هذه الجهة حددتها المادة 65 مكرر5 من قانون الإجراءات الجزائية[2] ففي حالة التلبس يصدر الإذن عن وكيل الجمهورية، أما في حالة فتح تحقيق قضائي فإن الإذن يصدر عن قاض التحقيق. يرد هذا الإذن في شكل مكتوب، وطبقا لنص المادة 65 مكرر 7 يجب أن يتضمن الإذن العناصر التالية[3]:

– الاتصالات المراد التقاطها.

– الأماكن المقصودة لهذا الغرض، سواء تعلق الأمر بالمساكن أو غيرها.

– ذكر الجريمة التي تبرر اللجوء إلى هذه التدابير.

ثالثا: الجهة المناط بها تنفيذ مراقبة الاتصالات الإلكترونية

بما أن عملية المراقبة الإلكترونية هي عمل تقني، فقد أجاز المشرع الجزائري لوكيل الجمهورية أو لضابط الشرطة القضائية الذي أذن له، ولقاض التحقيق أو ضابط الشرطة القضائية الذي ينيبه، تسخير جهات مختصة وذلك من أجل التكفل بالجوانب التقنية وهذا ما نصت عليه المادة 65 مكرر8 من قانون الإجراءات الجزائية[4] التي نصت على أنه "

[1] القانون 09-04، المرجع السابق.

[2] القانون 06-22، المرجع السابق.

[3] المادة 65 مكرر 7 " يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه، كل العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها .يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية"، المرجع نفسه.

[4] المرجع نفسه.

يجوز لوكيل الجمهورية أو ضابط الشرطة القضائية الذي أذن له, ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينيبه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة في المادة 65 مكرر 5 أعلاه."

والجهة المختصة يقصد بها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وهذا ما جاء بالمادة الرابعة في فقرتها الرابعة من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1] والتي بدورها تحيلنا إلى المادة 14 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[2]، غير أن هاتين المادتين لم تحددا بشكل دقيق تلك الوحدة وأولئك الأشخاص داخل الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال والمناط بهم التكفل التقني بمراقبة الاتصالات الإلكترونية.

لكن هذا لا يعني بأن المشرع قد أغفل ذلك، بل نجده أسند مهمة تنفيذ عملية مراقبة الاتصالات الإلكترونية لجهة حصرية وحدد أشخاصا معينين للقيام والإشراف على هذه العملية وذلك بموجب المادة 22 من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3] والتي نصت على أنه:

" يمكن الهيئة لتنفيذ عملية لمراقبة الاتصالات الإلكترونية، أن تضع وحدة مراقبة واحدة أو أكثر، تزود بالوسائل والتجهيزات التقنية الضرورية.

تتكون الوحدة من مستخدمين تقنيين يعملون تحت إدارة ومراقبة قاض يساعده ضابط واحد من الشرطة القضائية أو أكثر ينتمي للهيئة.

[1] المرسوم الرئاسي رقم 15-261، المرجع السابق.

[2] القانون 09-04، المرجع السابق.

[3] المرسوم الرئاسي رقم 15-261، المرجع السابق.

تمتثل الوحدة في عملها إلى أحكام التشريع الساري المفعول وشروط الرخصة المسلمة من الشرطة القضائية.

وتحرر أشغالها في محضر يعد طبقا لأحكام قانون الإجراءات الجزائية".

سوف نتطرق لهذه الجهة وهؤلاء الأشخاص كالآتي:

أ – الجهة: بحيث يتم إنشاء وحدة تسمى "وحدة مراقبة" وذلك من طرف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، يتم تزويد هذه الوحدة بالوسائل والتجهيزات التقنية الضرورية.

ب – الأشخاص: حددت الفقرة الثانية من المادة 22 من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[1] أولئك الأشخاص الذين تتشكل منهم وحدة المراقبة، وهؤلاء الأشخاص هم:

1 – المستخدمون التقنيون: وهم أولئك المستخدمين الذين يتم جلبهم من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني من أجل الدعم التقني. وهذا ما جاء في المادة 18 الفقرة الأخيرة من المرسوم الرئاسي 15-261[2] "...وتزود أيضا بمستخدمي الدعم التقني والإداري، ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني".

2 – قاض: ويتولى هذا القاضي مهمة إدارة وحدة المراقبة، وكذا مراقبة عمل المستخدمين التقنيين. ويتم جلب هذا القاضي من بين أولئك القضاة المنتمين للهيئة

[1] المرجع نفسه.

[2] المادة 18 من المرسوم الرئاسي 15-261 "تزود الهيئة بقضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول.

كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية.

وتزود أيضا بمستخدمي الدعم التقني والإداري، ويجلب هؤلاء المستخدمون من ضمن مستخدمي المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني"، المرجع نفسه.

الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، حيث يتم تزويد الهيئة بقضاة وذلك طبقا لنص المادة 18 الفقرة الأولى من المرسوم الرئاسي 15-261[1] التي جاء بها " تزود الهيئة بقضاة وفقا للشروط والكيفيات المنصوص عليها بموجب التشريع الساري المفعول".

3 – ضابط أو أكثر من ضباط الشرطة القضائية: وتتمثل مهمتهم في مساعدة القاضي الذي يتولى إدارة ومراقبة عمل وحدة المراقبة. ويتم اختيار هذا الضابط أو هؤلاء الضباط من بين أولئك الضباط الذين تم تزويد الهيئة (الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال) بهم، والذين تم جلبهم من بين ضباط المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، ويتم تحديد عددهم بموجب قرارات مشتركة ما بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية. وهذا ما نصت عليه الفقرة الثانية للمادة 18 من المرسوم الرئاسي 15-261[2] "... كما تزود بضباط وأعوان للشرطة القضائية من المصالح العسكرية للاستعلام والأمن والدرك الوطني والأمن الوطني، يحدد عددهم بموجب قرارات مشتركة بين الوزراء المكلفين بالعدل، والدفاع الوطني، والداخلية...".

رابعا: إحاطة العملية بالسرية

بحيث يجب ضمان سرية إجراء مراقبة الاتصالات الإلكترونية ووجوب حماية تلك المعلومات التي يتم الحصول عليها نتيجة عملية المراقبة طبقا للفقرة الثانية للمادة 23 من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3] والتي نصت على " يتخذ مسؤول الوحدة أثناء سير العملية كل التدابير اللازمة، بالاتصال مع المسؤولين المعنيين في الهيئة، من أجل ضمان سرية العملية وحماية المعلومات المستقاة من المراقبة".

[1] المرجع نفسه.

[2] المرجع نفسه.

[3] المرجع نفسه.

وإذا كان المستهدف من عملية مراقبة الاتصالات الإلكترونية هم أشخاصا ملزمون قانونا بكتمان السر المهني وجب اتخاذ تلك الإجراءات التي تضمن عدم المساس بهذا السر، وذلك طبقا للمادة 65 مكرر 6 من قانون الإجراءات الجزائية[1]، والتي جاء بها " تتم العمليات المحددة في المادة 65 مكرر 5 أعلاه، دون المساس بالسر المهني المنصوص عليه في المادة 45 من هذا القانون...". وكما يلاحظ فإن ذات المادة تحيلنا إلى المادة 45 من قانون الإجراءات الجزائية[2] التي نصت بفقرتها الرابعة على أنه "...غير أنه يجب عند تفتيش أماكن يشغلها شخص ملزم قانوناً بكتمان السر المهني أن تتخذ مقدماً جميع التدابير اللازمة لضمان احترام ذلك السر...".

خامسا: تحرير محضر

طبقا للمادة 22 الفقرة الأخيرة من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3] تقوم وحدة المراقبة بإعداد محضر يتضمن تلك الإجراءات التي قامت بها هذه الوحدة، فجاء بمضمون الفقرة " ...وتحرر أشغالها في محضر يعد طبقا لأحكام قانون الإجراءات الجزائية". ويتم تحرير هذا المحضر وفقا لأحكام قانون الإجراءات الجزائية لا سيما المادة 65 مكرر 9 من قانون الإجراءات الجزائية[4] التي نصت بأنه "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 وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري. يذكر بالمحضر تاريخ وساعة بداية هذه العمليات والانتهاء منها".

[1] القانون 06-22، المرجع السابق.

[2] المرجع نفسه.

[3] المرسوم الرئاسي رقم 15-261، المرجع السابق.

[4] القانون 06-22، المرجع السابق.

المطلب الثالث: حفظ المعطيات المتعلقة بحركة السير

يعتبر حفظ المعطيات المتعلقة بحركة السير إجراء من بين تلك الإجراءات الحديثة التي أقرها المشرع بخصوص جمع الدليل الإلكتروني، فما المقصود بهذا الإجراء؟ وماهي تلك الضوابط التي أحاطها المشرع بحفظ المعطيات؟ ومن هي الجهة المخولة بحفظ هذه المعطيات؟ هذه التساؤلات سوف نحاول الإجابة عنها وذلك من خلال هذا المطلب الذي يتناول آخر إجراء من إجراءات جمع الدليل الإلكتروني والتي تضمنها بحثنا.

الفرع الأول: مفهوم حفظ المعطيات المتعلقة بحركة السير

سنسعى أولا إلى التعرف على المراد بالمعطيات المتعلقة بحركة السير، ثم نتطرق إلى الإجراء المتعلق بحفظها.

أولا: المعطيات المتعلقة بحركة السير

عرف المشرع الجزائري المعطيات المتعلقة بحركة السير بموجب المادة الثانية الفقرة (ه) من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] على أنها " أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة".

ونجد بأن هذا التعريف الذي أخذ به المشرع الجزائري للمعطيات المتعلقة بحركة السير هو تقريبا نفس التعريف الذي سبقته إليه الاتفاقية الأوربية المتعلقة بالجرائم الإلكترونية[2] في قسمها الأول بالمادة الأولى الفقرة الرابعة.

[1] القانون 09-04، المرجع السابق.

[2] Chapitre I – Terminologie, Article 1 – Définitions Aux fins de la présente Convention,

.....

d- «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent". (Convention sur la cybercriminalité Budapest.Op.

ثانيا: المقصود بحفظ المعطيات المتعلقة بحركة السير

المشرع الجزائري استعمل كلمة "حفظ" التي وردت بالمادة 11 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]، كما وردت بالفقرة 05 من المادة الرابعة من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[2] في الصيغة التالية "...وحفظ المعطيات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية". علما بأن هذه الفقرة وردت ضمن المادة 04 من المرسوم الرئاسي المشار إليه أعلاه وهي المادة نفسها التي تضمنت المهام التي تمارسها الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وذلك تحت رقابة السلطة القضائية ووفقا لقانون الإجراءات الجزائية وكذا القانون رقم 09-04 المتضمن للقواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها. غير أن المشرع الجزائري لم يعرف لنا ما المقصود بحفظ المعطيات.

الاتفاقية الأوربية لبودابست والمتعلقة بالجريمة الإلكترونية[3] نصت في مادتها 16 الفقرة الأولى على أنه " تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها من التدابير لتمكين سلطاتها المختصة من أن تأمر أو تفرض بطريقة أخرى الحصول على الحفظ المعجل لبيانات إلكترونية محددة، بما في ذلك المعطيات المتعلقة بحركة السير المخزنة عن طريق نظام معلوماتي، خاصة في حال وجود أسباب للاعتقاد أن تلك البيانات معرضة بشكل خاص للضياع أو التعديل". فنجد بأنها تطرقت لحفظ المعطيات المتعلقة بحركة السير كإجراء يتم اللجوء إليه للحيلولة دون ضياع أو تعديل تلك البيانات التي تهم التحقيق لاحقا.

[1] القانون 09-04، المرجع السابق.

[2] المرسوم الرئاسي رقم 15-261، المرجع السابق.

[3] Convention sur la cybercriminalité Budapest.Op.Cit.

المشرع الفرنسي وبموجب المادة L32 في بندها 15 من قانون البريد والاتصالات الإلكترونية[1]اعتبر أن مزود الخدمات هو "كل شخص طبيعي أو معنوي يستغل شبكة الاتصالات عن بعد، والمفتوحة للجمهور، أو يورد لهم خدمة الاتصالات عن بعد".

ثم ما لبث أن وسع من تعريفه لمزودي الخدمات بموجب المادة 68 من القانون 2016-1321 الذي جاء من أجل جمهورية رقمية[2]، إذ عدل المادة L32 من قانون البريد والاتصالات الإلكترونية بحيث أضاف البند رقم 23 والذي بموجبه أدخل فئات تحت مفهوم مزودي الخدمات أو مزودي خدمات الاتصالات عن بعد، بحيث شملت الفئات المذكور بالمادة الأولى البند الرابع من القانون 2004-575 المتعلق بالثقة في الاقتصاد الرقمي[3] وهم:

- أولئك الذين يتيحون للجمهور أو فئات منه التواصل الإلكتروني، من خلال عملية اتصال إلكتروني أو علامات أو إشارات أو كتابات أو صور أو أصوات أو رسائل من أي نوع التي ليس لها طابع المراسلات الخاصة.

---

[1] Article L32-15° du Code des postes et des communications électroniques
"Opérateur.
On entend par opérateur toute personne physique ou morale exploitant un réseau de communications électroniques ouvert au public ou fournissant au public un service de communications électroniques". Loi n° 52-223 du 27 février 1952 relative à la procédure de codification des textes législatifs concernant le service des postes, télégraphes et téléphones JORF nº 56 du 4 mars 1952. Modifié par l'ordonnance n° 2021-650 du 26 mai 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation des pouvoirs de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. JORF n°0121 du 27 mai 2021.

[2] Article L32-23° (Code des postes et des communications électroniques, la loi n° 52-223, Op.Cit. Modifié par La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, parue au JO n° 235 du 8 octobre 2016**):**
Fournisseur de services de communication au public en ligne.
"On entend par fournisseur de services de communication au public en ligne toute personne assurant la mise à disposition de contenus, services ou applications relevant de la communication au public en ligne, au sens du IV de l'article 1er de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. Sont notamment considérées comme des fournisseurs de services de communication au public en ligne les personnes qui éditent un service de communication au public en ligne, mentionnées au deuxième alinéa du II de l'article 6 de la même loi, ou celles qui assurent le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature mentionnées au 2 du I du même article 6".

[3] La loi n° 2004-575, Op.Cit

– أولئك الذين يتيحون للجمهور التواصل عبر الإنترنت من خلال نقل للبيانات الرقمية، بناء على طلب فردي، لا يكون له طابع مراسلات خاص، عن طريق وسيلة اتصال إلكترونية تسمح بتبادل المعلومات بين المرسل والمستقبل.

– أولئك الذين يتيحون التواصل من خلال البريد الإلكتروني ويقصد به إرسال أي رسالة، في شكل نص أو صوت أو صوت أو صورة، يتم إرسالها بواسطة شبكة اتصال عامة، يتم تخزينها على خادم شبكة أو في الجهاز الطرفي للمستلم، حتى يقوم هذا الأخير باسترجاعها.

إلى جانب أولئك الذين نصت عليهم المادة (6-I/2) وهم " كل شخص طبيعي أو معنوي يضع ولو من دون مقابل تحت تصرف الجمهور عبر الإنترنت تخزين النصوص والصور والصوت والرسائل أياً كان طبيعتها التي تزود بواسطة المستفيد من هذه الخدمات".[1]

وفئة أخرى جاءت بها المادة 6 البند الثاني الفقرة الثانية[2]من نفس القانون ويقصد بهم أولئك الذين يوفرون الوسائل التقنية للأشخاص الذين ينشرون خدمة اتصال عبر الإنترنت للجمهور، لتمكينهم من تلبية متطلبات تحديد الهوية.

أما المشرع الكويتي فقدم لنا مزودي خدمة الإنترنت على أنهم "مزودي خدمة الأنترنت تشمل شركات الأنترنت الرئيسية والفرعية المرخصة من قبل وزارة المواصلات لتقديم خدمات الأنترنت بما في ذلك المشتركين من مقدمي خدمة الأنترنت".[3]

---

[1] Article 6-1/2: **(**Ibid)
" Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ...".

[2] Article 6-2 alinéa 2, **(**Ibid)
"…Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification…"

[3] المادة 01 الفقرة الثانية من القرار الوزاري الكويتي رقم 70 الصادر بتاريخ 2002/05/22 المتعلق بأسس وضوابط الترخيص لمقدمي الإنترنت البوابة القانونية على الرابط (متاح بتاريخ 2019/12/21):
http://www.law.gov.kw/MainTabsPage.aspx?val=AL1
أنظر في هذا الموضوع كذلك: زينة حازم خلف الجبوري، القانون الواجب التطبيق على مسؤولية مزودي خدمة الأنترنت، مجلة جامعة تكريت للحقوق، المجلد 1، العدد 4، الجزء الثاني، حزيران 2017، ص 387–388.

إلكتروني بغية استقبال وإرسال الرسائل، فتتيح له بذلك هذه الخدمة الوصول إلى المواقع الإلكترونية التي يرغب في الاطلاع على مضمونها.[1]

إذن يمكن القول بأن طبيعة النشاط الرئيسي لعمل متعهدي الوصول هو عمل فني بحت، فعملهم يقتصر فقط على خدمة وصول وليس خدمة معلومات فهو بمثابة ناقل، كما في حالة نقل البريد الإلكتروني، أو يقوم بدور المرحل أو بالحفظ المؤقت للصفحات التي يطلبها المستخدمون بصفة دائمة ويقصد من هذا الحفظ تأدية الخدمة على وجه السرعة ودون الاطلاع على المحتوى[2].

إذن وبناءً على ما تقدم، يتضح بأن هذا الصنف من مزودي الخدمات لا يمس بخصوصية الاتصالات الإلكترونية.

ب – الصنف الثاني: مزودو خدمة معالجة المعلومات عن بعد

(متعهدي الإيواء/fournisseur d'hébergement):

المشرع الفرنسي ومن خلال المادة (6-I/2) من القانون رقم 2004-575 المتعلق الثقة في الاقتصاد الرقمي عرف متعهد الإيواء بأنه" كل شخص طبيعي أو معنوي يضع ولو من دون مقابل تحت تصرف الجمهور عبر الإنترنت تخزين النصوص والصور والصوت والرسائل أياً كان طبيعتها التي تزود بواسطة المستفيد من هذه الخدمات"[3].

أما الفقه في فرنسا فقد عرف متعهد الإيواء بأنه " شخص طبيعي أو معنوي يتولى تخزين التطبيقات والسجلات المعلوماتية لعملائه ويمدهم بالوسائل التقنية والمعلوماتية لعملائه، ويمدهم بالوسائل التقنية والمعلوماتية التي تمكنهم من الوصول إلى ذلك المخزون عبر

[1] المرجع نفسه، ص 394.

[2] جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي "الأحكام الموضوعية المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، 2001، ص 129.

[3] Article 6-I.2 "Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services", La loi n° 2004-575, Op.Cit, modifié par la loi loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, JORF n°0156 du 25 juin 2020.

الأنترنت خلال الأربع والعشرون ساعة يوميا"[1]، في حين أننا لم نجد في التشريع الجزائري نصا صريحا يتضمن تعريفا مباشرا لمتعهد الإيواء رغم أهميته.

فالشخص المسؤول عن الإيواء، يقوم بخدمة تخزين المعلومة وإدارة محتواها بشكل يسمح لمورد المعلومة بعرضها على الجمهور، بمعنى أن هذا الشخص يجعل المعلومات التي يزوده بها المنتج أو المورد في متناول الجمهور من خلال إعداد مكان للجمهور يمكنه من الاتصال بشبكة الإنترنت والاطلاع على المواقع المتاحة، والحصول على المعلومات المطروحة.[2]

وعلى النقيض من الصنف الأول من مزودي الخدمات (متعهدي الوصول ـ fournisseur d'accès)، فإن الخدمات التي يقدمها متعهدي الإيواء (fournisseur d'hébergement) فيها مساس بالخصوصية المعلوماتية للأشخاص حيث أن إمكانية التخزين الإلكتروني المتاحة لهم تسمح بوصولهم إلى محتوى البيانات. ويقصد بالتخزين الإلكتروني بأنه أي تخزين للاتصال بواسطة أي خدمة اتصالات إلكترونية بغرض حماية هذا الاتصال وإمكانية استرداده.[3]

ج – الصنف الثالث: موردو المعلومات (fournisseurs de contenu)

مورد المعلومات (fournisseur du contenu) هو" شخص طبيعي أو معنوي بقوم ببث المعلومات والرسائل المتعلقة بموضوع معين على الإنترنت، بحيث يتمكن مستخدم هذه الشبكة من الحصول عليها مجانا أو بمقابل مادي. ويعتبر بمثابة القلب النابض لبث الحياة فى هذه الشبكة وتدفق المعلومات إليها، ويعد هو المسؤول الأول عن هذه

[1] محمد حسين منصور، المسؤولية الإلكترونية، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، 2003، ص 170.

[2] حسين محمد عبد الظاهر، المسؤولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، القاهرة، 2002، ص28-35.

[3] عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية)، دار النهضة العربية للطبع والنشر والتوزيع، 2004، ص 282.

المعلومات، وبالتالي فإن له دورا رئيسا في إطار المسئولية عنها، لأنه هو الذي يملك سلطة رقابة مشروعية هذه المعلومات، والتحكم في بثها عبر الإنترنت.[1] فخدمة التوريد هي خدمة نشر، والمورد هو الناشر، أما خدمة الإيواء فهي خدمة تأجير أو إعارة مكان على الشبكة، ومتعهد الإيواء هو المؤجر للمكان أو المعير له. وبالرغم من هذا الاختلاف، إلا أنهما يلتقيان في المساهمة بتقديم الخدمة المعلوماتية عبر الإنترنت. لأن البيانات والمعلومات لا يمكن أن تبث عبر الشبكة دون تدخلهما، ولا يمكن، في نفس الوقت، أن تصل للجمهور دون وجود الوسائل الفنية اللازمة للربط المادي بين شبكات الاتصال عن بعد والحاسبات الآلية للمستخدمين.[2]

ثانيا: التزامات مزودي الخدمات عبر الأنترنت

تعد خصوصية الاتصالات الإلكترونية من صميم حرمة الحياة الخاصة للأفراد، لذلك سعت مختلف التشريعات إلى إحاطتها بسياج من الضمانات.

إن سعي جهات التحقيق إلى الحصول على أدلة تمكنها من الوصول إلى الحقيقة لا ينبغي أن يسمح بانتهاك خصوصية الأفراد، بل لابد من إحداث توازن تكفل بموجبه حماية حريات الأفراد وخصوصيتهم، وبالمقابل العمل على تسهيل مهام جهات التحقيق من خلال إقرار قواعد إجرائية في هذا الشأن.

وبما أننا بصدد الحديث عن الحفظ لمعطيات تتضمن معلومات وبيانات متصلة بالخصوصية المعلوماتية للأفراد، نجد بأن المشرع الجزائري وتحت الفصل الرابع من

---

[1] Christiane FERAL-SCHUHL, Cyberdroit. Le droit à l'épreuve de l'Internet, 3e édition, Dalloz Dunod 2002, p 129.

أشار إليه: عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمة الإنترنت، مجلة الفكر القانوني والاقتصادي، كلية الحقوق، جامعة بنها، مصر، 2011، ص 487. مقال منشور بالموقع الإلكتروني للكلية على الرابط (متاح بتاريخ 2018/04/09):

http://www.flaw.bu.edu.eg/flaw/images/part2.pdf

[2] أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الأنترنت، جامعة آل البيت، مجلة المنارة، المجلد 13، العدد 9، الأردن، 2008. متوفر على موقع المجلة: www.lawjo.net/vb/showthread.php?10514

(متاح بتاريخ 2018/04/09)بصيغة وورد (Word) بالرابط التالي:

https://web2.aabu.edu.jo/nara/manar/suportFile/13910.doc

له المادة[1] (L. 32-3-1). كما أن المشرع الفرنسي حدد كذلك تلك المعطيات المعنية بمدة الحفظ لمدة سنة من تاريخ التسجيل، هذه المعطيات هي تلك المتعلقة بتحديد وتعريف الأشخاص الذين يستغلون الخدمات المقدمة من طرف مزود الأنترنت وكذلك تلك المعطيات المتعلقة بالخصائص التقنية للاتصالات التي يقدمها هذا الأخير.

غير أن هذا الوضع لم يدم طويلا، إذ عاد المشرع الفرنسي في سنة 2003 وضم محتوى المراسلات إلى تلك المعطيات المعنية بمدة الحفظ المحددة بسنة واحدة، فقام بتعديل المادة 29 المذكورة أعلاه وذلك بموجب المادة 20 من القانون 2003-239 المؤرخ في 18 مارس 2003 والمتعلق بالأمن الداخلي[2]. هذا التدخل من طرف المشرع الفرنسي جاء في نظرنا احتراما للحق في خصوصية الاتصالات الإلكترونية.

ثالثا: تصنيف المعلومات المعنية بالحفظ لدى مقدمي الخدمات

جاء بنص المادة 24 من المرسوم الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها[3] "تحفظ المعلومات المستسقاة أثناء عملية المراقبة خلال حيازتها من الهيئة وفقا للقواعد المطبقة على حماية المعلومات المصنفة" من خلال هذه المادة يتضح بأن المعلومات المعنية بالحفظ موزعة إلى عدة أصناف أو درجات، غير أن المشرع الجزائري لم يقدم لنا هذا التصنيف الذي تخضع له المعلومات المعنية بالحفظ.

المشرع الأمريكي ووفقا لقانون خصوصية الاتصالات الإلكترونية، فإنه يصنف المعلومات التي تكون بحوزة مزودي الخدمات إلى ثلاث مجموعات أو أصناف وهذا كالآتي:

---

[1] Article L32-3-1 (crée par l'article 29 de la loi n°2001-1062 du 15 novembre 2001 - art. 29 JORF 16 novembre 2001, modifié par la loi 2003-239 Op.cit): "... II. - Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire d'informations, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le IV, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs".

[2] La loi n° 2003-239, Op.cit.

[3] المرسوم الرئاسي رقم 15-261، المرجع السابق.

الفئة الأولى: تضم المعلومات الشخصية المتعلقة بالمشترك (كالاسم والعنوان ورقم الهاتف وعنوان برتوكول الأنترنت).

الفئة الثانية: تضم معلومات تخص المتعاملين مع المشترك كعناوين البريد الإلكتروني لأولئك الذين يتواصل معهم المشترك.

الفئة الثالثة: هذه الفئة تضم المعلومات الأكثر خطورة ومساسا بالخصوصية الإلكترونية لكونها تتعلق بمضمون ومحتوى الملفات.

رابعا: مدى إلزام مقدمي الخدمات بتقديم المعلومات التي بحوزتهم:

لقد ألزمت المادة 10 من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1] مقدمي الخدمات بضرورة تقديم المساعدة للسلطات المكلفة بالتحريات القضائية وذلك من خلال وضع المعطيات التي يتعين حفظها طبقا للمادة 11 من نفس القانون[2] تحت تصرف السلطات المكلفة بالتحريات القضائية. غير أن المادتين أعلاه لم توضحا ما إذا كان هذا الالتزام تلقائيا أم بناء على طلب السلطات المكلفة بالتحريات القضائية، كما أن مضمون المادتين لم يحدد فئة أو صنف المعلومات التي يتعين على مزودي الخدمات تقديمها للسلطات المكلفة بالتحريات القضائية من بين الفئات الثلاث اللاتي أشرنا إليها سابقا عند حديثنا عن تصنيف المعلومات المعنية بالحفظ لدى مقدمي الخدمات.

[1] المادة 10 "في إطار تطبيق أحكام هذا القانون. يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها و بوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكور... "، القانون 09-04، المرجع السابق.

[2] المادة 11 "مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدمو الخدمات بحفظ:

أ-المعطيات التي تسمح بالتعرف على مستعملي الخدمة.

ب-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

ج-الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.

د-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

هـ-المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في الفقرة "أ" من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه..."، المرجع نفسه.

الأصل أن يلتزم مقدمو الخدمات بالسر المهني فيحظر عليهم الإفصاح أو الإفشاء بما يملكونه من معلومات. غير أن هذا الحظر لا يمكنه الاستمرار أمام استثناءات تدفع مزودو الخدمات إلى تقديم ما يملكونه من معلومات.

بالرجوع إلى التشريعات المقارنة نجد أن مزودي الخدمات قد يبادرون أحيانا، وبصفة تلقائية بالإفصاح عن صنف من المعلومات ويتعلق الأمر بذلك الصنف الذي يضم البيانات الأساسية المتعلقة بالمشترك، والتي تكون بحوزة مقدمي الخدمات كاسم المشترك وعنوانه ورقم هاتفه. غير أنه وعندما يتعلق الأمر بصنف المعلومات التي لها علاقة بمضمون ومحتوى الملفات، فإن مزودي الخدمات لا يمكنهم الإفصاح عنها تلقائيا بل يجب على السلطات القضائية تقديم طلب بذلك، وهذا نظرا لارتباط محتوى المعلومات بالخصوصية المعلوماتية للأشخاص.

وكاستثناء عن القاعدة القائلة بعدم جواز إفصاح مقدمي الخدمات عما لديهم من معلومات، فإن المشرع الأمريكي ومن خلال قانون الاتصالات الإلكترونية أجاز لمقدمي الخدمات الإفصاح طواعية عن تلك المعلومات التي تكون بحوزتهم نتيجة عملهم كمتعهد للوصول أو متعهد إيواء، حيث أنهم وبمناسبة عملهم اليومي قد يكتشفون جريمة من الجرائم الإلكترونية فيبادرون تلقائيا إلى الإفصاح عنها.[1]

وعلى أي حال، فإن التعاون بين مقدمي الخدمات والسلطات القضائية المناط بها التحقيق في الجرائم الإلكترونية هو أمر بالغ الأهمية أكدته وحثت عليه مختلف التشريعات المقارنة والاتفاقيات الدولية لعل أبرزها الاتفاقية الأوربية بودابست[2] التي حضت الدول الأطراف على تبني تشريعات تلزم مقدمي الخدمات بالتعاون مع السلطات القضائية لاسيما تلك القائمة بالتحقيق، وذلك من خلال التزام مقدمي الخدمات بمساعدة السلطات القضائية وتمكينها من تلك البيانات المتعلقة بالمشترك سواء كان ذلك بصورة اختيارية أو بناء على إذن من السلطات القضائية عندما يتعلق الأمر بتلك البيانات التي تمس بالخصوصية المعلوماتية.

[1] أنظر في هذا المعنى: محمد كمال شاهين، مرجع سابق، ص 130-131.

[2] Convention sur la cybercriminalité Budapest.Op.Cit.

خامسا: مسؤولية مزودي الخدمات

لقد ألزم المشرع الجزائري مقدمي الخدمات بمساعدة السلطات القضائية في إطار التحريات والتحقيق الجنائي، كما ألزمهم بكتمان سرية العمليات المتعلقة بالتحقيق وإلا كانوا عرضة للمتابعة الجزائية ولتلك العقوبات المقررة لإفشاء أسرار التحري والتحقيق وذلك طبقا للمادة العاشرة من القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[1]. وعند إخلالهم بالالتزامات المنصوص عليها في المادة 11 من نفس القانون فإنهم يصبحون محل عقوبات إدارية سواء كانوا أشخاصا طبيعيين أو معنويين، هذا بالإضافة للعقوبات المترتبة على المسؤولية الجزائية في حالة ما إذا أدى الإخلال بالتزاماتهم إلى عرقلة حسن سير التحقيقات القضائية.

لقد أقر المشرع الجزائري بموجب المادة 11 المشار إليها أعلاه عقوبات على الأشخاص الطبيعيين وذلك بالحبس لمدة تتراوح ما بين 6 أشهر إلى 5 سنوات وكذا غرامة مالية من خمسون ألف دينار إلى خمسمائة ألف دينار. أما إذا تعلق الأمر بشخص معنوي فإن العقوبة تكون بتلك الغرامة المقررة في قانون العقوبات.[2]

[1] القانون 09-04، المرجع السابق.

[2] المادة 11 الفقرة الأخيرة تنص على أنه "... دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين والمعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية، ويعاقب الشخص الطبيعي بالحبس من 6 أشهر إلى 5 سنوات وبغرامة من 50000دج إلى 500000دج. يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات"، القانون رقم 09-04، المرجع نفسه.

خصصنا هذا الباب الثاني والأخير لدراستنا لشرح الجوانب الإجرائية المرتبطة بالتحقيق الابتدائي في الجريمة الإلكترونية. لذلك نعتبر بأن هذا الجزء يعد العصب الأساسي لهذا البحث ويشكل جوهر ولب هذه الدراسة كونه يتناول موضوع جمع الأدلة في الجريمة الإلكترونية وما يواجهه من تحديات وصعوبات، سواء تلك المتعلقة بالعنصر البشري في صورة المجرم الإلكتروني والضحية وكذا الجهات المباشرة للتحقيق في الجريمة الإلكترونية، أو الصعوبات المرتبطة بالدليل الإلكتروني، أو تلك الصعوبات المطروحة بخصوص مسألة التعاون الدولي بالتحقيق في الجريمة الإلكترونية.

يضاف إلى ما سبق موضوع الخصوصية المعلوماتية وما يشكله من صعوبات لجهات التحقيق الابتدائي في الجريمة الإلكترونية، حيث تقف هذه النقطة حجر عثرة أمام سعي جهات التحقيق للحصول على الأدلة الإلكترونية.

وانتقلنا في الفصل الثاني من هذا الباب لعرض جملة الإجراءات المنصبة على جمع الدليل الإلكتروني في الجريمة الإلكترونية، فبدئنا بعرض لجملة الإجراءات التقليدية المتعلقة بجمع الأدلة في الجريمة الإلكترونية من انتقال إلى مسرح الجريمة الإلكترونية ومعاينته، فالتفتيش عن الدليل الإلكتروني ثم ضبطه، وصولا إلى مسألة الخبرة في مجال الجريمة الإلكترونية ثم الشاهد في الجريمة الإلكترونية.

ولدى حديثنا عن الإجراءات الحديثة لجمع الدليل الإلكتروني، تناولنا كل من إجراءات التسرب ومراقبة الاتصالات الإلكترونية وحفظ المعطيات المتعلقة بحركة السير. وختمنا بذلك الباب الثاني من هذه الدراسة.

الخاتمة:

بعد أن أنهينا بفضل الله وعونه عرض هذه الدراسة، نشير في مستهل هذه الخاتمة إلى أن موضوع التحقيق الجنائي في الجريمة الإلكترونية هو موضوع عميق ومتشعب ومترامي الأطراف إذ أنه يحتوي على جوانب تقنية وفنية تتسع وتصلح لوحدها بأن تشكل مواضيع لدراسات وبحوث، ناهيك عن الجانب القانوني الذي يبقى ميدانا خصبا لدراسة الجريمة الإلكترونية في جوانبها الموضوعية والإجرائية. هذا ولقد حاولنا وحرصنا على محاصرة موضوع "التحقيق الجنائي في الجرائم الإلكترونية" في مجال ونطاق أدق، حتى نتمكن من القدرة على التحكم فيه أكثر كموضوع للدراسة والبحث. لذلك ركزنا جهودنا على الجوانب الإجرائية المتعلقة بجمع الأدلة في الجريمة الإلكترونية من طرف تلك الجهة أو الجهات التي أُسندت لها مهمة التحقيق الابتدائي، وبطبيعة الحال كان منطقيا ووجيها أن تشمل دراستنا عرضا لهذه الجهات المتصلة بالتحقيق الابتدائي في الجريمة الإلكترونية سواء على المستوى الوطني أو المستوى الدولي.

هذا، ولقد أفردنا فصلا تمهيديا في بداية هذه الدراسة لعرض مفهوم الجريمة الإلكترونية وهي خطوة كان لابد منها نظرا لأهميتها في التعريف بعدة جزئيات لها ارتباط بباقي محاور الرسالة لعل أبرزها هو شرح لتلك الخصائص التي تميز الجريمة الإلكترونية والتي بسببها تعقدت مهمة جهات التحقيق الابتدائي في الجريمة الإلكترونية، وبسببها أيضا وجدت التشريعات الجنائية نفسها –لاسيما الإجرائية منها– أمام ضرورة سن تشريعات جديدة كون النصوص القائمة أصبحت غير ملائمة للمساهمة في التحقيق في الجرائم الإلكترونية لأنها صيغت ووُضعت لمواجهة الجرائم التقليدية المادية، كما أنها وُجدت قبل ظهور الأنترنت وانتشار وسائل الاتصال الحديثة.

كما أن التطرق في بداية الدراسة لخصائص الجريمة الإلكترونية يمنح فكرة مسبقة عن صعوبة بلوغ الدليل الذي تسعى خلفه جهات التحقيق داخل بيئة إلكترونية لا مادية. يضاف إلى ذلك أن التعريف بالمعلومات باعتبارها هدفا للمجرم الإلكتروني كان تمهيدا لمصطلح تم تداوله كثيرا في عدة مواضع بهذه الدراسة وذلك لعلاقته وصلته الوطيدة

بجوانب الدراسة وبموضوع حساس ألا وهو الخصوصية المعلوماتية. وبعد الفصل التمهيدي قسمنا دراستنا هذه إلى بابين، تناولنا بالباب الأول عرضا لتلك الجهات المتصلة بالتحقيق الابتدائي في الجريمة الإلكترونية، في حين خصصنا الباب الثاني للجوانب الإجرائية للتحقيق الابتدائي في الجريمة الإلكترونية.

وبما أن السؤال الرئيسي لإشكالية هذه الدراسة كان يتمحور حول مدى كفاية ومقدرة أجهزة التحقيق الابتدائي في الجرائم التقليدية المادية ـ بما تملكه من صلاحيات وإجراءات ـ على التحقيق الابتدائي في الجرائم الإلكترونية، فإن هذه الدراسة أثبتت من جهة مدى عجز تلك الجهات المكلفة بالتحقيق الابتدائي والتي أنشأت في ظل قوانين كانت سابقة لظهور الجريمة الإلكترونية، وكذا مدى قصور الإجراءات المتعلقة بجمع الأدلة في الوصول إلى الدليل الإلكتروني. ومن جهة أخرى اتضحت لنا مدى أهمية وضرورة تعديل تلك النصوص القانونية واستحداث تشريعات جديدة تركز أكثر على الجوانب الإجرائية لتلائم طبيعة الجريمة الإلكترونية والدليل الإلكتروني، وكذا الحاجة الماسة إلى إنشاء هيئات جديدة مدعمة بأجهزة وتقنيات حديثة وبعنصر بشري كفء من أجل دعم جهات التحقيق الابتدائي في الجريمة الإلكترونية.

من خلال هذه الدراسة، وبحسب رأينا المتواضع يمكننا الخروج بالنتائج التالية:

1–تأثر الجهات المناط بها التحقيق الابتدائي في الجريمة الإلكترونية وما تحمله هذه الأخيرة من خصائص، ذلك أن المشرع الجنائي في مختلف الدول وقف على حقيقة مفادها أن الاكتفاء بتعديل التشريعات الجنائية في شقها الموضوعي والإجرائي لا يمكنه تقديم الدعم الكافي لجهات التحقيق التي وجدت نفسها عاجزة أمام الجريمة الإلكترونية. لذلك فلقد فرضت الجريمة الإلكترونية على مختلف الدول ضرورة استحداث هيئات جديدة مختصة بالتحقيق في الجرائم الإلكترونية تكون مدعمة بأحدث التكنولوجيا والوسائل التقنية المتطورة في مجال الاتصالات يتم تسييرها من طرف عناصر بشرية على قدر عال من التكوين والكفاءة والاطلاع الدقيق بعالم الجريمة الإلكترونية والقدرة على التحكم في التقنيات الحديثة وفي شبكات الإنترنت حتى يتسنى لها نقل معركتها داخل العالم الافتراضي الذي

يتخذ منه المجرم الإلكتروني مسرحا لجرائمه. ففي الولايات المتحدة الأمريكية تم إنشاء "قسم جرائم الحاسوب" كهيئة مستحدثة تختص بالتحقيق وتابعة لجهاز الشرطة، أما عن الوضع في الجزائر فقد أنشأت " الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها" بموجب المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم وكيفية سير هذه الهيئة، وذلك من أجل تقديم الدعم للجهة الأصيلة بالتحقيق الابتدائي. كما تم في الأردن إنشاء قسم خاص بجرائم الحاسوب والإنترنت. وهذه الصور سقناها وذكرناها على سبيل المثال لا الحصر وهي تؤكد حقيقة تأثر الجهات المناط بها التحقيق الابتدائي بالجريمة الإلكترونية.

2-إن تأثير الجريمة الإلكترونية لم يطل فقط الجهات الأصيلة بالتحقيق الابتدائي بل امتد كذلك إلى جهاز الضبطية القضائية ذات الصلة بالتحقيق الابتدائي في الجريمة الإلكترونية، وهذا التأثير تجلى في مستويات ثلاث، على الصعيد الوطني والإقليمي والدولي.

فالضبطية القضائية لها صلة بإجراءات جمع الأدلة وبالتحقيق الابتدائي من خلال مثلا الندب القضائي أو الإنابة القضائية. ففي إطار الجريمة الإلكترونية بادرت العديد من الدول إلى تطوير أجهزة الضبط القضائي بما يتلاءم مع طبيعة الجريمة الإلكترونية والدليل الإلكتروني وكذا العالم الافتراضي الذي ينشط فيه المجرم الإلكتروني. حيث تم إنشاء وحدات مختصة في هذا الشأن مكونة من عناصر بشرية تم إعدادها من خلال التكوين والتدريب على التعامل مع وسائل وتقنيات الاتصال الحديثة، فكانت نتيجة ذلك بأن ظهرت لاحقا ما تعرف بشرطة الإنترنت (Cyber police) وكذلك درك الإنترنت (Cyber gendarme) فأصبح للضبطية القضائية وجود بالعالم الافتراضي.

3- التعقيدات التي أفرزتها الجريمة الإلكترونية ألقت بظلالها كذلك على موضوع الاختصاص القضائي والذي من خلاله يتم تحديد تلك الجهة القضائية التي تؤول إليها صلاحيات مباشرة التحقيق الابتدائي في الجريمة الإلكترونية. فتنازع الاختصاص القضائي على المستوى الدولي يفرض نفسه كأحد أهم صور تلك

الصعوبات التي تواجه التعاون الدولي في مجال التحقيق الجنائي في الجريمة الإلكترونية، فالسلوك الإجرامي في الجريمة الإلكترونية قد يقع ويُرتكب بدولة معينة لكن تحدث آثاره وتتحقق نتيجته في دولة أخرى. فالتحقيق في هذه الحالة يتطلب ما يسمى بامتداد الاختصاص القضائي إلى الخارج، ذلك أن جمع الأدلة الإلكترونية يستوجب الولوج إلى أنظمة معلوماتية متواجدة بخارج إقليم الدولة المعنية. وهذا بدوره يطرح فكرة السيادة حتى وإن كان الولوج في هذه الحالة يتم بصورة غير مادية (من خلال شبكة الإنترنت). باعتبار الجريمة الإلكترونية جريمة عابرة للقارات فقد ساهم ذلك في إثارة مشكل تنازع الاختصاص القضائي، حتى وإن بدا بأن اللجوء لمبدأ العالمية في هذه المسألة مجديا مقارنة بالمبادئ الأخرى المعالجة لمسألة الاختصاص القضائي ونقصد بها (مبدأ الإقليمية، مبدأ الشخصية، مبدأ العينية) غير أن مبدأ العالمية بدوره يصطدم بتعقيدات ناجمة عن تطبيق وإعمال المبادئ الثلاثة السابقة الذكر، وهذا ما يدعو إلى تعاون دولي حقيقي وجاد وصادق بين الدول. فالاتفاقيات الدولية وعلى رأسها اتفاقية بودابست وإن كانت قد تصدت إلى حد ما لهذه المسألة وخاضت فيها (خاصة من خلال المادتين 31 و32 من الاتفاقية) إلا أن ذلك يبقى غير كاف بسبب عدم انخراط كل الدول بهذه الاتفاقية من جهة، ومن جهة أخرى بسبب ما قد قيل آنفا بخصوص مسألة السيادة وكذا تنازع الاختصاص القضائي.

4-يواجه التحقيق الجنائي في الجريمة الإلكترونية صعوبات جمة منها ما هو متعلق بالعنصر البشري، ومنها ما هو مرتبط بالدليل الإلكتروني، كما أن هناك صعوبات متعلقة بمسألة التعاون الدولي، دون إغفال تلك الصعوبات المتصلة بالخصوصية المعلوماتية. ومن خلال خوضنا في جملة هذه الصعوبات توصلنا إلى:

أ- أن الصعوبات المتعلقة بالعنصر البشري قد تتصل بشخص المجرم الإلكتروني، كما أنها قد ترتبط بالضحية في الجريمة الإلكترونية، وقد تكون بسبب ذلك العنصر البشري المكلف بمهام التحقيق وجمع الأدلة.

- التعرف على مقترف الجريمة الإلكترونية وتحديد هويته الحقيقية أمر معقد، خاصة إذا كان شخصا محترفا يجيد التخفي، ذلك أن التعرف على العنوان

(IP) للجهة التي ارتكبت الجريمة لا يوصل جهات التحقيق بالضرورة إلى الجاني الحقيقي، فعنوان (IP) يمكن التلاعب به وإخفاءه بل وحتى لو تم التعرف على جهاز الكمبيوتر أو الهاتف الذكي الذي استعمل في ارتكاب الجريمة قد لا يقود ذلك جهات التحقيق إلى الجاني، فمجرم الإنترنت قد يعمد أحيانا إلى اختراق أجهزة أشخاص أخرين عن بعد ثم ينفذ جرائمه انطلاقا من تلك الأجهزة المخترقة مستخدما بالتالي عنوان (IP) الخاص بها وذلك دون أن يتفطن صاحب الجهاز المخترق للأمر، وهذا يساهم في تضليل جهات التحقيق كما قد يتسبب في توريط أشخاص أبرياء لا ذنب لهم سوى أن عنوان (IP) الخاص بهم تمت الاستعانة به في الجريمة نتيجة تعرضهم للاختراق.

- الضحية في الجريمة الإلكترونية قد يكون شخصا طبيعيا أو شخصا معنويا، وفي كثير من الأحيان لا يبادر الضحايا إلى التبليغ عن الجرائم الإلكترونية لسبب أو لآخر، فقد لا يكتشفون أصلا بأنهم كانوا ضحية لجريمة الإلكترونية أو يكتشفون ذلك في وقت متأخر، وأحيانا قد يمتنعون عن التبليغ خوفا من الفضيحة خصوصا عندما يتعلق الأمر بأمور ذات طابع أخلاقي. كما أن الضحية إذا كان شخصا معنويا كالمصارف والشركات التجارية والمالية قد تعزف عن التبليغ خشية الإضرار بسمعتها وما قد يترتب عن ذلك من فقدانها لثقة زبائنها والمتعاملين معها، وكل هذا يزيد من صعوبة جهات التحقيق في تصديها ومحاربتها للجريمة الإلكترونية.
- قد لا يتمتع فريق التحقيق بالخبرة الكافية في مجال التحقيق في الجريمة الإلكترونية أو يفتقد لمهارة التعامل مع الوسائل التقنية الحديثة، إما بسبب عدم تلقيه واستفادته من تكوين ذو مستوى وجودة عالية، وإما لأن الطرف الآخر (المجرم الإلكتروني) شخص محترف ويملك قدرات عالية وبالتالي تصعب مجاراته. يضاف إلى ذلك أن العنصر البشري المشكل لفريق التحقيق قد يفتقد التكوين القانوني المطلوب وهو ما قد ينجر عنه خرق

لقواعد ولإجراءات التعامل مع الدليل الإلكتروني أثناء التفتيش أو الضبط وبالتالي المساس بالشرعية الإجرائية، وهو ما يؤثر لاحقا على مصداقية الدليل الإلكتروني المستخلص. فهذه كلها صعوبات تزيد من تعقيد مهمة التحقيق في الجرائم الإلكترونية.

ب- إن الخصائص والميزات التي يتميز بها الدليل الإلكتروني في حد ذاته تشكل صعوبات لجهات التحقيق لكونه دليل غير مادي وغير مرئي ويتواجد داخل كم هائل من البيانات قد يتطلب الوصول إليه المساس ببيانات أخرى محاطة بالخصوصية. كما أن الدليل الإلكتروني يسهل التلاعب به وتعديله وتدميره ونقله إلى أنظمة معلوماتية أخرى قد تكون خارج الدولة التي صدر السلوك الإجرامي أو تحققت النتيجة بداخلها. كما أن البيانات التي يمكن أن تصلح كدليل قد تكون مشفرة من خلال الاعتماد على برامج معقدة وكلمات سرية ورموز تحول دون وصول جهات التحقيق إلى الدليل الإلكتروني.

ت- بالرغم من أن الجريمة الإلكترونية أضحت تشكل تهديدا مشتركا للمجتمع الدولي وهو ما يعد سببا كافيا لتحفيز الدول من أجل تعزيز سبل التعاون فيما بينها لمواجهة هذا التهديد المشترك، إلا أن الواقع أثبت لنا بأن التعاون الدولي ليس بذاك القدر من البساطة التي تسمح بتجسيده دائما على أرض الواقع دونما أن يثير ذلك إشكاليات. وفي الحقيقة فإن التعاون الدولي تكتنفه الكثير من التعقيدات والتي شكلت في مناسبات عديدة صعوبات في وجه كل تلك الجهود الرامية لتحقيقه كخطوة أساسية لابد منها لكي تتمكن جهات التحقيق في الجرائم الإلكترونية بلوغ مسعاها في الحصول على الأدلة المرتبطة بالجريمة الإلكترونية والتي تفيد في الوصول إلى الجناة، ومن جملة تلك الصعوبات نذكر:

- اختلاف تشريعات الدول وعدم وجود تعريف موحد، جامع ومانع للجريمة الإلكترونية وهو الأمر الذي نتج عنه تباين وعدم وجود نموذج موحد للنشاط الإجرامي، فالسلوك الذي قد تعتبره دولة ما سلوكا مباحا وغير مجرم قد يشكل جريمة في دولة أخرى. يضاف إلى ذلك تعارض

المصالح بين الدول ففي نهاية المطاف فإن الدول تراعي مصالحها حتى لو كانت تلك المصالح تقف حجر عثرة أمام التعاون في مجال التحقيق في الجرائم الإلكترونية. كما أن توافق سياسات الدول أو تعارضها مع بعضها البعض من شأنه كذلك أن يقوض جهود جهات التحقيق.

- يدخل ضمن صعوبات التعاون الدولي اختلاف النظم القانونية الإجرائية مما يؤثر بصورة مباشرة على إجراءات جمع الدليل الإلكتروني، فالإجراء الذي يعتبر مشروعا في نظر دولة ما قد تعتبره دولة أخرى خارج إطار الشرعية الإجرائية وهذا ما يترتب عنه لاحقا عدم مشروعية الدليل الإلكتروني، وهذا كله يفضي إلى عدم التفاهم وعدم التنسيق ويساهم في تقويض جهود التعاون بين سلطات التحقيق في الجرائم الإلكترونية.
- تعتبر المساعدة القضائية الدولية شكل من أشكال التعاون الدولي في مجال التحقيق الجنائي في الجرائم الإلكترونية، ومن صورها الإنابة القضائية أو الندب القضائي على المستوى الدولي بحيث تتعاون جهات التحقيق في كل دولة مع نظيراتها في باقي الدول الأخرى من خلال تبادل المساعدات مع بعضها البعض بخصوص إجراء من إجراءات التحقيق المتعلق بجريمة من الجرائم الإلكترونية. غير أن بطء الإجراءات بسبب الطرق الدبلوماسية الطويلة التي يتوجب على الدولة طالبة الإنابة القضائية أن تسلكها بعد تقديمها الطلب إلى البلد الآخر وانتظار الرد على طلبها تشكل معوقات لجهات التحقيق في الجريمة الإلكترونية، كما أنها تصب في مصلحة المجرم الإلكتروني والذي يستفيد أصلا من عامل السرعة الذي تمتاز به عملية تنفيذ الجريمة الإلكترونية. ناهيك عن فكرة السيادة والتي هي الأخرى تعيق بدورها إجراءات الإنابة القضائية الدولية، فكل دولة تتمسك بحقها في ممارسة إجراءات التحقيق فوق إقليمها ومن خلال أجهزتها القضائية وهذا الأمر

يفوت على الدولة صاحبة طلب الإنابة القضائية الكثير من الوقت في طريق بحثها عن الأدلة الإلكترونية.

- كما أن تسليم المجرمين والذي يعد هو الآخر من صور المساعدة القضائية ليس بالأمر السلس، فهو بدوره مقيد بشروط تساهم هي الأخرى في عرقلة جهود ومساعي جهات التحقيق رغم أن اتفاقية بودابست تناولت هذا الموضوع بالمادة 24 في بندها الأول والرابع من الاتفاقية، إلا أنها ربطت موضوع تسليم المجرمين بشروط مع إقرار حق رفض التسليم لكل دولة تلقت طلبا بهذا الخصوص وذلك بالبندين الخامس والسادس من نفس المادة أي المادة 24 من الاتفاقية، وهذا كله يندرج ضمن جملة الصعوبات التي تواجه جهات التحقيق ذات الصلة بالجريمة الإلكترونية.

ث- أصبحت أجهزة الاتصالات الحديثة (أجهزة الكمبيوتر، الهواتف الذكية، الألواح الذكية ...الخ) وكذا وسائط التخزين بما فيها تلك المتوفرة على شبكة الإنترنت تشكل مستودعا لبيانات الأشخاص والذين من حقهم المحافظة على سريتها، وهذا ما يمكن تسميته بالحق في الخصوصية المعلوماتية.

غير أن سعي جهات التحقيق للوصول إلى الأدلة من خلال ما تعتمده من إجراءات قد يفضي إلى انتهاك الخصوصية المعلوماتية للأشخاص، فالتفتيش مثلا داخل أنظمة البيانات المعالجة آليا ومراقبة الاتصالات الإلكترونية بما فيها تلك التي تتم بواسطة شبكة الإنترنت، إلى غير ذلك من إجراءات جمع الأدلة، كلها قد تؤدي إلى المساس بحق محمي قانونا ألا وهو الحق في الخصوصية فتقع بذلك في المحظور والذي يشكل غالبا انتهاكا للشرعية الإجرائية وما قد ينتج عنها من ضياع لمصداقية الدليل الإلكتروني. كل هذا إنما يشكل في الواقع صعوبات وعوائق تقيد جهات التحقيق في الجريمة الإلكترونية.

5- من أجل الكشف عن الحقيقة والوصول إلى الجناة، تحتاج جهات التحقيق في الجريمة الإلكترونية إلى الحصول على الأدلة وهذا بدوره يتطلب لجوء جهات التحقيق إلى عدة إجراءات تتعلق بجمع الدليل الإلكتروني.

لقد تأثرت إجراءات جمع الأدلة في الجريمة الإلكترونية بالطبيعة الخاصة لهذه الجريمة وكذلك بتلك الخصائص التي يتميز بها الدليل الإلكتروني، وهذا التأثر لم يقتصر على ما يعرف بالإجراءات التقليدية لجمع الأدلة بل امتد كذلك لتلك الطائفة من الإجراءات التي يصطلح عليها بالطرق الحديثة لجمع الأدلة.

أ- من أهم مظاهر تأثير الجريمة الإلكترونية على الإجراءات التقليدية لجمع الأدلة:

- الهدف من الانتقال إلى مسرح الجريمة ومعاينته هو الاستفادة من تلك الآثار التي قد يتركها الجاني خلفه بعد اقتراف الجريمة، غير أن الطابع الخاص للجريمة الإلكترونية وطبيعة الدليل الإلكتروني فيها ساهم في تغيير مفهوم الانتقال والمعاينة، وحتى مسرح الجريمة لم يعد بتلك الصورة المألوفة التي ترسخت في أذهان الناس عامة وجهات التحقيق بصفة خاصة، وهي الصورة الموروثة منذ العصر الذي سادت فيه فقط الجريمة بطابعها المادي التقليدي قبل أن تقتحم الجريمة الإلكترونية عالم الإجرام.
- أفرزت لنا الجريمة الإلكترونية مسرحين للجريمة وليس مسرحا واحدا فقط، فبالإضافة للمسرح المادي والذي قد تتواجد به المكونات المادية للحاسب الآلي أو غيرها من المعدات الحديثة والأجهزة المعلوماتية التي قد يستعين بها المجرم في تنفيذ جرائمه، أوجدت الجريمة الإلكترونية مسرحا آخر يتمثل في بيئة رقمية غير مادية تمتد إلى مكونات الأجهزة الإلكترونية وشبكات الإنترنت، وهذه البيئة المعقدة والطابع الافتراضي الذي يتميز به مسرح الجريمة الجديد الذي فرضته الجريمة الإلكترونية كان له أثر مباشر على عملية الانتقال إلى مسرح الجريمة ومعاينته.

- بخلاف ما هو عليه الوضع في الجريمة التقليدية أين يمكن لقاض التحقيق الانتقال شخصيا إلى مسرح الجريمة ومعاينته، فإنه وحينما يتعلق الأمر بالبيئة الإلكترونية لمسرح الجريمة الإلكترونية فإن الانتقال يباشره خبراء ومختصين في تقنيات الاتصال الحديثة وذلك من خلال الاتصال بجهاز الحاسوب وبشبكة الإنترنت وتكتفي جهات التحقيق بالإشراف على عملية الانتقال (من خلال منح الإذن بذلك على سبيل المثال) ولا يختلف الوضع كثيرا حينما يتعلق الوضع بالمعاينة كذلك.
- المعاينة في الجريمة الإلكترونية تهدف إلى تتبع تلك الآثار الإلكترونية التي قد يخلفها المجرم الإلكتروني خلفه، وتتجسد صعوبة المعاينة هنا في امتداد واتساع مسرح الجريمة في حد ذاته والذي قد يتوزع على عدة حواسيب وشبكات قد تمتد إلى خارج إقليم الدولة، كما أن تردد الكثير من الأشخاص (خاصة داخل شبكة الإنترنت) على مسرح الجريمة قد يساهم في تبخر الدليل خاصة أن اكتشاف الجريمة والعلم بها وعملية الانتقال من أجل معاينة مسرح الجريمة قد تأخذ الكثير من الوقت بعد ارتكاب الجريمة.
- إذا انصب التفتيش على المكونات المادية (الكمبيوتر، الهاتف الذكي، مفاتيح الذاكرة، وسائط وأوعية التخزين المادية...) في حد ذاتها والتي تكون قد استخدمت في الجريمة الإلكترونية، فهنا لا إشكال يطرح كونها تخضع لقواعد التفتيش التقليدية فهي تلائمها مادام أنها حافظت على طابعا المادي.

غير أن التفتيش الذي يكون موضوعه المكونات المعنوية وكذا شبكات الإنترنت يطرح إشكالات عديدة، بداية بالولوج إلى هذه المكونات المعنوية والذي لم يلق ـ ونقصد هنا الولوج ـ إجماعا على اعتباره نوعا من التفتيش. وحتى مع التسليم بذلك والأخذ به امتد الجدل إلى مدى ملائمة خضوع البيئة المعلوماتية لقواعد التفتيش التقليدية، بل أن الجدل استمر حتى بعد استحداث قوانين جديدة تنظم إجراء التفتيش في

الجريمة الإلكترونية وتراعي الطبيعة الخاصة للأنظمة المعلوماتية، بحيث لم يكن ذلك كافيا لإنهاء الجدل المتعلق بالتفتيش المتعلق بالجريمة الإلكترونية حيث برزت تعقيدات أخرى منها ما هو مرتبط بمشكلة الخصوصية مادام أن التفتيش سيمس حتما بيانات محاطة بالخصوصية، ومنها ما هو متصل بموضوع التعاون الدولي كون الأنظمة المعلوماتية المراد تفتيشها قد تتواجد بدولة أخرى أي خارج إقليم الدولة التي تباشر فيه جهات التحقيق إجراءات التفتيش.

- يعتبر الضبط أحد إجراءات جمع الأدلة التي تعتمد عليها جهات التحقيق، فهو بمثابة النتيجة المنطقية التي تؤول إليها عملية التفتيش في حال تُوجت هذه الأخيرة بالوصول إلى أدلة.

إذا كان ضبط المكونات المادية التي استعملت في الجريمة الإلكترونية لا يطرح إشكالا، إلا أن الأدلة ذات الطبيعة المعنوية كانت محل جدل فقهي، ولقد خلصنا إلى أن هذه المكونات المعنوية يمكن ضبطها إذا تم إفراغها في وسط مادي كالدعامة المادية أو تحويلها إلى طبيعة مادية كتصوير هذه البيانات فوتوغرافيا أو طباعتها على الورق حتى يصبح لها وجود مادي، وبالتالي فما كان على المشرع إلا سن قوانين تجيز ذلك وتحدد إجراءات القيام به من أجل تفادي إثارة موضوع الشرعية الإجرائية وما يترتب عنها من مساس بمصداقية الأدلة التي يتم ضبطها.

- لقد فرضت الخبرة نفسها كإجراء لا يمكن تجاوزه أو الاستغناء عنه في مجال التحقيق في الجريمة الإلكترونية، فبدونها سوف تقف جهات التحقيق عاجزة وهذا يبرز مدى أهمية اللجوء إلى الخبراء في مجال المعلوماتية حينما يتعلق الأمر بجريمة من الجرائم الإلكترونية، بل حتى أن الهيئات التي تم استحداثها لمساعدة جهات التحقيق في الجريمة الإلكترونية على غرار "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها" في الجزائر، نصت على

الاستعانة بالخبراء وذلك بنص المادة 19 من المرسوم الرئاسي رقم 15-261 الذي يحدد تشكيلة وتنظيم وكيفية سير هذه الهيئة، فالطبيعة الخاصة للجريمة الإلكترونية تفرض الاستعانة بالخبراء لاسيما في مجال القرصنة والفيروسات والتعامل مع التكنولوجيا الحديثة المرتبطة بالمعلوماتية وشبكة الإنترنت.

- جمع الأدلة في الجريمة الإلكترونية قادنا إلى التعرف على صنف جديد من الشهود وهو "الشاهد المعلوماتي" وسمي كذلك تمييزا له عن الشاهد في الجرائم التقليدية. غير أن الشاهد المعلوماتي في موضوع الجريمة الإلكترونية هو شخص يملك مؤهلات وقدرات في مجال الاتصالات والأنظمة المعلوماتية وهي مواصفات قد تجعله يتداخل مع شخص "الخبير".

إن إلزام الشاهد المعلوماتي بالإدلاء وتقديم كل ما من شأنه مساعدة جهات التحقيق، قد يصطدم بموانع قانونية تجبر هذا الشاهد على رفض تقديم شيفرات أو كلمات سرية أو نسخ بيانات كونها تدخل في إطار ما يسمى بالسر المهني أو الخصوصية المعلوماتية، لذلك وجب تدخل تشريعي في هذا الإطار من أجل تبني نصوص تنظم بوضوح التزامات الشاهد المعلوماتي، ذلك أن القواعد العامة في هذا الموضوع تجاوزها الزمن فلم تعد مجدية نظرا للطبيعة الخاصة للشاهد المعلوماتي وكذلك طبيعة المعلومات التي يدلي بها كونها ترتبط ببيانات داخل أنظمة معلوماتية. يضاف إلى كل ذلك وجوب التقيد بالشرعية الإجرائية.

ب- من مظاهر تأثير الجريمة الإلكترونية على إجراءات جمع الأدلة مساهمتها في استحداث إجراءات جديدة تساير الطبيعة الخاصة للبيئة التي ترتكب فيها الجريمة الإلكترونية، ومن بين هذه الإجراءات (التسرب، مراقبة الاتصالات الإلكترونية، حفظ المعطيات المتعلقة بحركة السير).

- تستعين جهات التحقيق في مختلف الدول بالتسرب كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية من خلال مخالطة المجرمين داخل العالم الافتراضي (غرف الدردشة، مواقع التواصل الاجتماعي، المواقع التي تشهد عرض أو تداول أو بيع بيانات أو برامج أو ملفات أو سلع معاقب عليها قانونا ...إلخ) وهذا ما يمكن التعبير عنه بالتسرب الإلكتروني تمييزا له عن التسرب الذي يتم اللجوء إليه في الجرائم التقليدية. وبحسب رأينا فإن هذا التسرب يعد إجراءً فعالا كونه يقتحم عالم الإجرام الإلكتروني وهو ما يمكن اعتباره أسلوبا ناجعا نظرا للطبيعة الخاصة للجريمة الإلكترونية والتي جعلتها تستعصي على جهات التحقيق في حال اقتصرت فقط على الطرق التقليدية التي ذكرناها آنفا.

ولقد أحسن المشرع الجزائري بحذوه حذو التشريعات المقارنة من خلال اعتماده على التسرب كإجراء من إجراءات جمع الأدلة في الجريمة الإلكترونية وذلك بنص المادتين 65 مكرر11 و65 مكرر 5 من قانون الإجراءات الجزائية.

- يعتمد المجرمون في التواصل فيما بينهم على وسائل الاتصالات الإلكترونية كإجراء المحادثات وإرسال الرسائل النصية عبر الهاتف النقال. وبما أن شبكة الإنترنت أعطت للجريمة الإلكترونية بعدا آخر، فلقد أصبح البريد الإلكتروني أو برامج التواصل التي يتم تحميلها وتثبيتها على الهواتف الذكية وأجهزة الكمبيوتر والألواح الذكية ...إلخ وسائل لتواصل المجرمين فيما بينهم، لذلك كان لابد من الاعتماد على "مراقبة الاتصالات الإلكترونية" من أجل اعتراض كل أشكال المراسلات التي تتم عبر وسائل الاتصال السلكية واللاسلكية وكذلك عبر البريد الإلكتروني والتي قد يشكل محتواها دليلا في إثبات جريمة من الجرائم الإلكترونية.

غير أنه وفي المقابل، وبالرغم من الدعم الذي يمنحه إجراء "مراقبة الاتصالات الإلكترونية" لجهات التحقيق في الجريمة الإلكترونية إلا أنه يشكل تهديدا ومساسا خطيرا بالخصوصية، وهو الأمر الذي يستدعي تقييد اللجوء إلى هذا الإجراء بشروط صارمة تصون وتحفظ حرمة الحياة الخاصة للأشخاص.

- لقد ساعد التطور التكنولوجي على زيادة سرعة تدفق الإنترنت بشكل مذهل وهو الأمر الذي ساهم في زيادة حجم البيانات المتداولة عبر شبكتها. وبما أن الجريمة الإلكترونية قد لا تكتشف أحيانا إلا بعد مرور مدة زمنية من ارتكابها لجأت التشريعات المقارنة إلى إلزام مزودي الخدمات عبر الإنترنت بحفظ تلك المعطيات المتعلقة بحركة سير البيانات التي تتم من خلال المنظومات المعلوماتية المتصلة ببعضها البعض.

هذا الإجراء ونقصد به "حفظ المعطيات المتعلقة بحركة السير" يكفل لجهات التحقيق إمكانية الرجوع إلى بيانات تم تداولها قبل اكتشاف الجريمة الإلكترونية، والبحث داخل هذه البيانات على ما من شأنه أن يشكل دليلا. وبما أن المعطيات التي تشملها عملية الحفظ تنصب على معلومات تتصل بالخصوصية المعلوماتية للأفراد وجب تقييدها بشروط من ضمنها الالتزام بتمديد مدة الاحتفاظ بهذه المعطيات، ولقد حددها المشرع الجزائري بمدة سنة واحدة وهو ما يفهم منه أنه وبعد مرور هذه المدة يمكن لمقدمي الخدمة غبر الإنترنت التخلص من هذه المعطيات، وكنتيجة لذلك يمكننا القول بأن الاستفادة من هذا الإجراء "حفظ المعطيات المتعلقة بحركة السير" مرتبط بمدة الاحتفاظ بهذه المعطيات، فيصبح إذن هذا الإجراء غير مجدي بمجرد التخلص من تلك المعطيات التي تم حفظها وهذا في حالة ما إذا احتاجت إليها جهات التحقيق بعدما يتم التخلص منها.

وفي الأخير نشير إلى أن التطور المستمر واللامحدود للجريمة الإلكترونية يجعلنا نعتقد جازمين بأن باب البحث في موضوع التحقيق الجنائي في الجريمة الإلكترونية يبقى مفتوحا وخصبا ومجديا طالما أن جهات التحقيق محكوم هي الأخرى عليها بمجاراة التطور الحاصل في مجال الإجرام الإلكتروني، وذلك سعيا لاكتساب وسائل وتبني إجراءات تمكنها من وضع يدها على الأدلة التي من شأنها الوصول إلى الجناة وكشف الحقيقة.

ـ تم بحمد الله وعونه ـــ

قائمة لأهم الاختصارات

أولا: باللغة العربية

ص: صفحة

ط: الطبعة

ثانيا: باللغة الأجنبية

ADSL : Asymmetric Digital Subscriber Line

AAFS: American Academy of Forensic Sciences.

Afripol: Mécanisme de l'Union africaine pour la Coopération Policière

AIDP : International review of penal law

Aim-council: Arab Interior Ministers Council

Art : Article

ASEANAPOL: Association of Southeast Asian Nations Police

BCRCI: Brigade centrale de répression de la criminalité informatique

CA: Cour d'appel

CH: chambre

Chron : Chronique

C3N: le centre d'action contre les criminalités numériques

EC3: European Cyber Crime Centre

ECPA: Electronic Communications Privacy Act

Eurojust: European Union Agency for Criminal Justice Cooperation

Europol: European Police Office

FBI: Federal Bureau of Investigation

G8: Groupe des huit

GCCPOL: Gulf Cooperation Council Police

Http: Hypertext Transfer Protocol

IC3: Internet Crime Complaint Center

ICPO-INTERPOL: The International Criminal Police Organization

IFCC: Internet Fraud Complaint Center

IP : Internet Protocol

JCP : Juris-Classeur périodique

JOCE : Journal officiel des Communautés européennes

JORF: Journal officiel de la République française

JOUE : Le Journal officiel de l'Union européenne

D: document (une extension de nom de fichier, traditionnellement utilisée pour la documentation en format texte).

N: Numéro

NW3C: National White Collar Crime Center

OCLCTIC: l'Office central contre la criminalité liée aux technologies de l'information et de la communication

Op. Cit: ouvrage précité

P: Page

RIDP: Revue Internationale de droit pénal

STAD: Système de traitement automatisé de données

TCP/IP: Transmission Control Protocol/Internet Protocol

Wi-Fi: Wireless Fidelity

WWW: world wide web

Vol: Volume

قائمة المراجع

أولا: المراجع باللغة العربية

أ- المصادر

❖ القرآن الكريم

❖ الأحاديث النبوية الشريفة (منقولة عن صحيح البخاري).

❖ متون الحديث:

- صحيح البخاري (المؤلف/المشرف: محمد بن إسماعيل البخاري المحقق/المترجم: محب الدين الخطيب، الطبعة الأولى، المكتبة السلفية، القاهرة، 1400هـ، ص 6241.).

ب- المعاجم

1-ابن منظور، لسان العرب، الطبعة الأولى، الجزء الثامن، دار الأميرية،1883.

2-ابن منظور، لسان العرب، الطبعة الثالثة، الجزء الرابع، دار إحياء التراث العربي، بيروت، لبنان، 1999.

3-أبو الحسين أحمد بن فارس، معجم مقاييس اللغة، الطبعة الأولى، دار الفكر، بيروت، 1994.

4-عمر أحمد مختار، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، 2008.

ج-الكتب:

❖ **المؤلفات العامة:**

1-أحمد شوقي شلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر، 1999.

2-أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة السابعة، 1993.

3-أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة 1988.

4-أشرف توفيق شمس الدين، شرح قانون الإجراءات الجنائية، الجزء الأول، دار النهضة العربية، الطبعة الأولى، 2009.

5-توفيق محمد الشاوي، حرمة الحياة الخاصة ونظرية التفتيش، الطبعة الأولى، منشأة المعارف، الإسكندرية، 2006.

6-توفيق محمد الشاوي، فقه الإجراءات الجنائية، الجزء الثاني، دار الكتاب العربي، القاهرة، الطبعة الثانية، 1954.

7-جلال ثروت، نظم القسم العام في قانون العقوبات، دار الهدى للمطبوعات، الإسكندرية، 1999.

8-حسن الجوخدار، التحقيق الابتدائي في قانون أصول المحاكمات الجزائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، 2008.

9-حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف، الإسكندرية 1982.

10- رمزي رياض عوض، الإجراءات الجنائية في القانون الأنجلو أمريكي، دار النهضة العربية، القاهرة، 2009.

11- زياد إبراهيم شيحا، الإنابة القضائية الدولية في المسائل الجنائية ونطاق العلاقات الخاصة الدولية، دار النهضة العربية، القاهرة، مصر، 2015.

12- سليمان عبد المنعم، أصول الإجراءات الجزائية في التشريع والقضاء والفقه، الطبعة الثانية، المؤسسة الجامعية للدراسات والنشر والتوزيع، بيروت، 1999.

13- سليمان محمد الطماوي، الوجيز في القانون الإداري، دار الفكر العربي، 1997.

14- شريف سيد كامل، الجريمة المنظمة في القانون المقارن، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001.

15- طارق سرور، الاختصاص الجنائي العالمي، الطبعة الأولى، دار النهضة العربية، القاهرة، 2006.

16- طعيمة الجرف، القانون الإداري والمبادئ العامة في تنظيم نشاط السلطات الإدارية، دار النهضة العربية، القاهرة، 1978.

17- قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005.

18- عباس توفيق البستاني تافطة، مبدأ الاختصاص العالمي في القانون العقابي، الطبعة الأولى، مطبعة آراس، أربيل، 2009.

19- عبد الفتاح محمد سراج، النظرية العامة لتسليم المجرمين، دار النهضة العربية، القاهرة، بدون سنة نشر.

20- على صادق أبو هيف، القانون الدولي العام، منشأة المعارف، الإسكندرية، 2015.

21- عمار عباس الحسيني، التحقيق الجنائي والوسائل الحديثة في كشف الجريمة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2015.

22- عمار عباس الحسيني، التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات الجنائي، المركز العربي للدراسات والبحوث العلمية، 2017.

23- ماجد راغب الحلو، القانون الإداري، دار المطبوعات الجامعية، الإسكندرية، 1994.

24- مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، دار النهضة العربية، القاهرة، 2004.

25- محمد عبد القادر العبودي، ندب مأموري الضبط القضائي لأعمال التحقيق، الطبعة الثانية، دار النهضة العربية، القاهرة، 2011.

26- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، الطبعة الثالثة، 1988.

27- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثالثة، 1995.

28- محمود نجيب حسني، شرح قانون الإجراءات الجنائية وفقا لأحدث التعديلات التشريعية تنقيح فوزية عبد الستار، دار النهضة العربية، الجزء الأول، الطبعة الرابعة، 2011.

29- ممدوح إبراهيم السبكي، حدود سلطات مأمور الضبط القضائي في التحقيق، دار النهضة العربية، القاهرة، 1998.

30- هشام عبد العزيز مبارك، تسليم المجرمين بين الواقع والقانون، الطبعة الأولى، القاهرة، دار النهضة العربية, 2006.

31- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، الطبعة الأولى، دار المطبوعات الجامعية، الإسكندرية، 2009.

❖ **المؤلفات الخاصة:**

1-أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006.

2-أحمد محمد عبد الباقي، التحقيق الجنائي الرقمي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2015.

3-أحمد محمود مصطفى، جرائم الحاسبات الآلية في التشريع المصري، الطبعة الأولى، دار النهضة العربية، 2010.

4-أسامة أحمد المناعسة، جرائم الحاسب الآلي والأنترنت، الطبعة الأولى، دار وائل للطباعة والنشر، عمان، الأردن، 2001.

5-أسامة أحمد بدر، الوسائط المتعددة بين الواقع والقانون، دار النهضة العربية، 2002.

6-أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دار الجامعة الجديدة، 2015.

7-أيمن عبد الله فكري، الجرائم المعلوماتية "دراسة مقارنة في التشريعات العربية والأجنبية" الطبعة الأولى، مكتبة القانون والاقتصاد، الرياض، 2014.

8-أيمن عبد الله فكري، جرائم نظم المعلومات، دار الجامعة الجديدة، الإسكندرية. 2007.

9-بكري يوسف بكري، التفتيش عن المعلومات في وسائل التقنية الحديثة، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2011.

10- ثائر موسى يونس، شبكات الحاسب، دار الراتب الجامعية، بيروت، لبنان، 1994.

11- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي "الأحكام الموضوعية المتعلقة بالإنترنت"، دار النهضة العربية، القاهرة، 2001.

12- جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالإنترنت، دار النهضة العربية، القاهرة، 2002.

13- حسين محمد عبد الظاهر، المسؤولية القانونية في مجال شبكات الإنترنت، دار النهضة العربية، القاهرة، 2002.
14- حنان ريحان مبارك المضحكي، الجرائم المعلوماتية، الطبعة الأولى، منشورات الحلبية الحقوقية، بيروت، لبنان، 2014.
15- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والأنترنت، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.
16- خالد ممدوح إبراهيم، حجية البريد الإلكتروني في الإثبات الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2008.
17- خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الإلكترونية، دار الفكر الجامعي، 2009.
18- رشا مصطفى أبو الغيط، تطور الحماية القانونية للكيانات المنطقية، دار الفكر الجامعي، الإسكندرية، 2006.
19- رشاد خالد عمر، المشاكل القانونية والفنية للتحقيق في الجرائم المعلوماتية، المكتب الجامعي الحديث، الإسكندرية،2013.
20- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2012.
21- زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، عين مليلة، الجزائر، 2011.
22- سامي جلال فقي حسين، التفتيش في الجرائم المعلوماتية، دار الكتب القانونية، 2011.
23- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الأنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
24- سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الإنترنت، الطبعة الأولى، دار النهضة العربية، 1999.

25- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الإنترنت)، دار النهضة العربية، القاهرة، 2008.
26- سهيل محمد العزام، الوجيز في جرائم الإنترنت، الطبعة الأولى، دائرة المكتبة الوطنية، عمان، 2009.
27- صبري حمد خاطر، مدى تطويع القواعد القانونية التقليدية في مواجهة المعلومات، دار الكتب القانونية، 2014.
28- طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي (النظام القانوني لحماية المعلوماتية)، دار الجامعة الجديدة، الإسكندرية، 2015.
29- عادل عبد العال إبراهيم خراشي، إشكاليات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، دار الجامعة الجديدة، الإسكندرية، 2015.
30- عبد الفتاح مراد، شرح جرائم الكمبيوتر والأنترنت، دار البهاء للنشر الإلكتروني، الإسكندرية، 2009.
31- عبد اللاه أحمد هلالي، التزام الشاهد بالإعلام في الجريمة المعلوماتية، الطبعة الثانية، دار النهضة العربية،2009.
32- عبد اللاه أحمد هلالي، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2008.
33- عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الإلكتروني، دار النهضة العربية، القاهرة،2005.
34- عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون (تقديم فتوح الشاذلي) دراسة مقارنة، الطبعة الثانية، منشورات الحلبي الحقوقية، 2007.
35- علي بن عبد الله العسيري، الآثار الأمنية لاستخدام الشباب للإنترنت، الطبعة الأولى، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2004.

36- علي حسن محمد الطوالبة، التفتيش الجنائي على نظم الحاسوب والإنترنت، الطبعة الثانية، منشورات جامعة العلوم التطبيقية، مملكة البحرين 2010.
37- علي كحلون، المسؤولية المعلوماتية، مركز النشر الجامعي، 2005.
38- عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المسجلة إلكترونيا، دار النهضة العربية، 2010.
39- عمر الفاروق الحسيني، المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، الطبعة الثانية، بدون ناشر، 1990.
40- عمر محمد أبو بكر بن يونس، الإجراءات الجنائية عبر الأنترنت في القانون الأمريكي (المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الإلكتروني في التحقيقات الجنائية)، دار النهضة العربية للطبع والنشر والتوزيع، 2004.
41- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الإنترنت (الأحكام الموضوعية والجوانب الإجرائية)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2004.
42- فتحي محمد أنور عزت، الأدلة الإلكترونية في المسائل الجنائية والمعاملات المدنية والتجارية، الطبعة الأولى، دار الفكر والقانون، مصر، 2010.
43- فريد منعم جبور، حماية المستهلك عبر الإنترنت ومكافحة الجرائم الإلكترونية، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2010.
44- فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2016.
45- محمد الأمين البشرى، التحقيق في الجرائم المستحدثة، الطبعة الأولى، دار الحامد للنشر والتوزيع، عمان، الأردن، 2014.
46- محمد أمين الرومي، المستند الإلكتروني، الطبعة الأولى، دار الفكر الجامعي، 2007.
47- محمد حسين منصور، المسؤولية الإلكترونية، الطبعة الأولى، دار الجامعة الجديدة للنشر، الإسكندرية، 2003.

48- محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة، عمان، 2004.
49- محمد زكي أبو عامر، الإجراءات الجنائية، الطبعة السابعة، دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
50- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، 1994.
51- محمد عبد الرحمن عنانزة، القصد الجرمي في الجرائم الإلكترونية، الطبعة الأولى، دار الأيام، عمان، الأردن، 2017.
52- محمد عبد الله أبوبكر، موسوعة جرائم المعلوماتية، المكتب العربي الحديث، الإسكندرية، 2007.
53- محمد كمال شاهين، الجوانب الإجرائية للجريمة الإلكترونية في مرحلة التحقيق الابتدائي، دار الجامعة الجديدة، الإسكندرية، 2018.
54- محمد كمال محمود الدسوقي، الحماية الجنائية لسرية المعلومات الإلكترونية، دار الفكر والقانون، المنصورة، 2015.
55- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2009.
56- مروة زين العابدين سعد صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت بين القانون الدولي الاتفاقي والقانون الوطني، مركز الدراسات العربية للنشر والتوزيع، 2016.
57- مصطفى محمد موسى، المراقبة الإلكترونية عبر شبكة الإنترنت، الطبعة الأولى، مطابع الشرطة، القاهرة، 2003.
58- ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والأنترنت، دار الكتب القانونية، 2006.
59- مناني فراح، أدلة الإثبات الحديثة في القانون، دار الهدى، عين مليلة، 2008.

60- منير محمد الجنبيهي، جرائم الإنترنت والحاسب الآلي ووسائل مكافحتها، دار الفكر الجامعي، الإسكندرية، 2006، ص34.
61- نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة الأولى، منشورات الحلبي الحقوقية، 2005.
62- ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، الطبعة الأولى، مركز الإمارات للدراسات والبحوث الاستراتيجية، أبو ظبي، 2008.
63- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2007.
64- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط ،1994.
65- وضاح محمود الحمود ونشأت مفضي المجالي، جرائم الإنترنت، دار المنار للنشر والتوزيع، عمان، 2005.

الرسائل العلمية

1-إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة، 1980.
2-سالم محمد سليمان الأوجلي، أحكام المسئولية الجنائية عن الجرائم الدولية في التشريعات الوطنية، دارسة مقارنة، رسالة دكتوراه، كلية الحقوق جامعة عين شمس، 1997.
3-سليم جلاد، الحق في الخصوصية بين الضمانات والضوابط في التشريع الجزائري والفقه الإسلامي، رسالة ماجستير غير منشورة، كلية العلوم الإنسانية والحضارة الإسلامية، جامعة وهران، 2013.
4-صالح عبد الله محمد راشد الوارد، الإنابة القضائية في قانون الإجراءات الجنائية القطري دراسة تحليليه مقارنة، رسالة ماجستير غير منشورة، كلية الحقوق جامعة قطر، يونيو 2017.

5-عبد الإله النوايسة، ضمانات المتهم أثناء التحقيق الابتدائي (دراسة مقارنة بين التشريعين الأردني والمصري)، أطروحة دكتوراه غير منشورة، جامعة عين شمس، مصر، 2000.

6-محمد سعيد عتيق، النظرية العامة للدليل العلمي في الإثبات الجنائي، رسالة دكتوراه غير منشورة، كلية الحقوق، جامعة عين شمس، مصر، 1993.
7-هدى طلب علي، الإثبات الجنائي في جرائم الأنترنت والاختصاص القضائي بها، رسالة ماجستير غير منشورة، كلية الحقوق، جامعة النهرين، العراق، 2012.

المقالات والبحوث والمؤتمرات وأوراق العمل:

1-أحمد قاسم فرح، النظام القانوني لمقدمي خدمات الإنترنت، مجلة المنارة، المجلد 13، العدد 9، جامعة آل البيت، الأردن، 2008.
2-خديجة خالدي، "آلية الاتحاد الإفريقي للتعاون الشرطي (أفريبول)"، مجلة العلوم الاجتماعية والإنسانية المجلد 11, العدد 1, جامعة العربي التبسي، تبسة، الجزائر.
3-حابس يوسف زيدات، مدى استيعاب النصوص التقليدية للسرقة الإلكترونية، مجلة مركز حكم القانون ومكافحة الفساد، العدد 2، 2019.
4-زينة حازم خلف الجبوري، القانون الواجب التطبيق على مسؤولية مزودي خدمة الأنترنت، مجلة جامعة تكريت للحقوق، المجلد 1، العدد 4، الجزء الثاني، حزيران 2017.
5-طارق محمد الجملي، الدليل الرقمي في مجال الإثبات الجنائي، ورقة عمل مقدمة للمؤتمر المغاربي الأول حول المعلوماتية والقانون المنعقد في الفترة (28- 29 /2009/10م) تنظمه أكاديمية الدراسات العليا، طرابلس.
6-عبد الفتاح محمود كيلاني، مدى المسؤولية القانونية لمقدمي خدمة الإنترنت، مجلة الفكر القانوني والاقتصادي، كلية الحقوق، جامعة بنها، مصر.
7- عبد الناصر محمد محمود فرغلي ومحمد عبيد سيف المسماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية، بحث من ضمن أعمال المؤتمر

العربي الأول لعلوم الأدلة الجنائية والطب الشرعي بالفترة من 12 إلى 14 نوفمبر2007، جامعة نايف العربية للعلوم الأمنية، الرياض.

8-غايب محروس نصار، الجريمة المعلوماتية، مجلة كلية التراث الجامعية، العدد السابع عشر المجلد 24 الإصدار التاسع، 2011.

9-عمر محمد أبو بكر بن يونس، الإثبات الجنائي عبر الإنترنت، ندوة الدليل الرقمي، مقر جامعة الدول العربية، مصر، من 5 إلى 8 مارس 2006.

10- مشتاق طالب وهيب، مفهوم الجريمة المعلوماتية ودور الحاسوب بارتكابها، مجلة العلوم القانونية والسياسية، جامعة ديالي، العراق، المجلد 3، العدد 1، 20014.

11- ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP/IP) في بحث وتحقيق الجرائم على الكمبيوتر، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، نظمته أكاديمية شرطة دبي / مركز البحوث والدراسات، العدد 4 المحور الأمني والإداري، الفترة ما بين 26 و28 أبريل 2003، دبي، الإمارات العربية المتحدة.

12- موسى مسعود ارحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، بحث مقدم إلى المؤتمر المغاربي الأول حول المعلوماتية والقانون، المنعقد بالفترة 28 -10/29/ 2009، أكاديمية الدراسات العليا – طرابلس.

13- هشام محمد فريد رستم، الجرائم المعلوماتية، بحث مقدم لمؤتمر القانون والكمبيوتر والأنترنت المنظم بكلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، 1-3 ماي 2000.

14- بيان الأمانة العامة لمجلس وزراء الداخلية العرب بمناسبة اختتام أعمال المؤتمر العربي السادس عشر لرؤساء أجهزة المباحث والأدلة الجنائية المنعقد بتونس بتاريخ 2017/05/18.

15- "الجريمة الإلكترونية في المجتمع الخليجي وكيفية مواجهتها" بحث من إعداد مركز المعلومات الوطني لوزارة الداخلية السعودية، 2016، ص65- 67. منشور بالموقع الرسمي لمجلس التعاون لدول الخليج العربي.

النصوص القانونية*:

❖ **النصوص القانونية الخاصة بالجزائر:**

1-دستور الجمهورية الجزائرية الديمقراطية الشعبية:

- المرسوم الرئاسي رقم 20-442 المؤرخ في 15 جمادى الأولى عام 1442 الموافق 30 ديسمبر سنة 2020 الصادر بالجريدة الرسمية العدد 82، المتعلق بإصدار التعديل الدستوري المصادق عليه في استفتاء أول نوفمبر سنة 2020.

2-قانون الإجراءات الجزائية:

- الأمر رقم 66-155 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو 1966 الوارد بالجريدة الرسمية رقم 48 بتاريخ 20 صفر عام 1386 الموافق 10 يونيو 1966.
- الأمر رقم 69-73 مؤرخ في 5 رجب عام 1389 الموافق 16 سبتمبر 1969 الصادر بالجريدة الرسمية العدد 80 بتاريخ 8 رجب عام 1389 هـ الموافق 19 سبتمبر 1969. المعدل والمتمم للأمر رقم 66-155 والمتضمن قانون الإجراءات الجزائية.

* النصوص القانونية المذكورة بالقائمة –بما فيها التعديلات– محصورة فقط على تلك المواد القانونية التي لها صلة بموضوع الرسالة الحالية.

- القانون رقم 82-03 المؤرخ في 19 ربيع الثاني عام 1402 الموافق 13 فبراير 1982، الصادر بالجريدة الرسمية العدد 7 الصادرة بتاريخ 22 ربيع الثاني عام 1402 الموافق 16 فبراير سنة 1982.المعدل والمتمم للأمر رقم 66-155 والمتضمن قانون الإجراءات الجزائية.

- القانون 90-24 المؤرخ في 27 محرم عام 1411 الموافق 18 غشت 1990 الصادر بالجريدة الرسمية رقم 36 بتاريخ أول صفر عام 1411 الموافق 22 غشت سنة 1990 المعدل والمتمم لقانون الإجراءات الجزائية.

- الأمر رقم 95-10 مؤرخ في 25 رمضان عام 1415 الموافق 25 فبراير سنة 1995 الصادر بالجريدة الرسمية رقم 11 بتاريخ 29 رمضان 1415 الموافق 01 مارس سنة 1995 المعدل والمتمم لقانون الإجراءات الجزائية.

- القانون رقم 01-08 المؤرخ في 4 ربيع الثاني عام 1422 الموافق 26 يونيو سنة 2001 الصادر بالجريدة الرسمية العدد 34 المؤرخة في 5 ربيع الثاني 1422 الموافق 27 يونيو سنة 2001 المعدل المتمم لقانون الإجراءات الجزائية.

- القانون 04-14 المؤرخ في 27 رمضان 1425 الموافق 10 نوفمبر 2004 الصادر بالجريدة الرسمية رقم 71 المعدل والمتمم لقانون الإجراءات الجزائية.

- القانون رقم 06-22 المؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر لسنة 2006 والصادر بالجريدة الرسمية العدد 84 المؤرخة في 24 ديسمبر 2006 المعدل المتمم لقانون الإجراءات الجزائية.

- المرسوم التنفيذي رقم 06-348 المؤرخ في 12 رمضان 1427 الموافق 05 أكتوبر سنة 2006 الصادر بالجريدة الرسمية رقم 63 بتاريخ 15 رمضان عام 1427 الموافق 08 أكتوبر سنة 2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

رقم 66-156 المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966 والمتضمن قانون العقوبات.

- القانون رقم 14-01 المؤرخ في 4 ربيع الثاني 1435 الموافق 4 فبراير 2014، الصادر بالجريدة الرسمية العدد 07 الصادرة بتاريخ 16 ربيع الثاني عام 1435 الموافق 16 فبراير سنة 2014. المعدل و المتمم للأمر رقم 66-156 المؤرخ المتضمن قانون العقوبات.
- القانون رقم 04-15 المؤرخ في 17 رمضان عام 1425 الموافق 10 نوفمبر سنة 2004، الصادر بالجريدة الرسمية العدد 71. المعدل والمتمم لقانون العقوبات.

4- القانون المدني الجزائري:

- القانون المدني الجزائري الأمر رقم 75-58 المؤرخ في 20 رمضان عام 1395 الموافق 26 سبتمبر سنة 1975، المتضمن القانون المدني، المعدل والمتمم.

5- قانون البريد وبالمواصلات السلكية واللاسلكية:

- القانون رقم 2000-03 المؤرخ في 5 جمادى الأول عام 1421 الموافق 5 غشت سنة 2000 الذي يحدد القواعد العامة المتعلقة بالبريد وبالمواصلات السلكية واللاسلكية، الجريدة الرسمية للجمهورية الجزائرية العدد 48 الصادرة في 6 جمادى الأول عام 1421 الموافق 6 غشت سنة 2000.

6- قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي:

- القانون رقم 18-07 المؤرخ في 25 رمضان عام 1439 الموافق 10 يونيو سنة 2018 الصادر بالجريدة الرسمية العدد 34 يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

7-قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها:

- القانون رقم 09-04 المؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية للجمهورية الجزائرية العدد 47 الصادرة في 25 شعبان 1430 الموافق 16 غشت 2009.
- المرسوم الرئاسي رقم 15-261 المؤرخ في 24 ذي الحجة عام 1436 الموافق 8 أكتوبر 2015 الذي يحدد تشكيلة وتنظيم وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية العدد 53 الصادرة في ذي الحجة عام 1436 الموافق 8 أكتوبر 2015.

❖ **النصوص القانونية الخاصة ببعض الدول العربية:**

1. **المملكة الأردنية الهاشمية:**

❖ القانون رقم 1961/09 الصادر بتاريخ 1961/01/01 والمنشور بالصفحة 311 للجريدة الرسمية العدد 1539 والمتضمن قانون أصول المحاكمات الجزائية.

❖ القانون رقم 2015/27 الصادر بتاريخ 2015/01/06 والمنشور بالصفحة 631 للجريدة الرسمية العدد 5343 والمتضمن قانون الجرائم الإلكترونية.

2. **دولة الكويت:**

❖ القرار الوزاري الكويتي رقم 70 الصادر بتاريخ 2002/05/22 المتعلق بأسس وضوابط الترخيص لمقدمي الإنترنت.

3. **جمهورية السودان:**

❖ قانون الإجراءات الجنائية الجزائية السوداني لسنة 1991.

7. **الجمهورية العربية السورية:**

❖ المرسوم التشريعي رقم 12-17 الصادر بتاريخ 2012/02/08 المتعلق بتنظيم التواصل على شبكة الإنترنت والجريمة المعلوماتية.

8. **مملكة البحرين:**

❖ القانون رقم 28 الصادر بتاريخ 08/18/ 2002 والمتعلق بالمعاملات الإلكترونية المنشور بالجريدة الرسمية لمملكة البحرين تحت رقم 2548.

- **المواثيق والعهود الدولية**:

- الإعلان العالمي لحقوق الإنسان المعتمد من طرف الجمعية العامة بتاريخ 10 ديسمبر 1948 بموجب القرار 217(أ).
- العهد الدولي الخاص بالحقوق المدنية والسياسية اعتمد وعرض للتوقيع والتصديق والانضمام بموجب قرار الجمعية العامة للأمم المتحدة 2200 ألف (د-21) المؤرخ في 16 ديسمبر 1966 تاريخ بدء النفاذ في 23 مارس 1976.
- الميثاق العربي لحقوق الإنسان المصادق عليه بقرار الدورة العادية رقم (121) لمجلس جامعة الدول العربية على المستوى الوزاري رقم 6405 بتاريخ 2004/3/4.

مواقع الأنترنت:

❖ موقع أرضية المجلات العلمية الجزائرية:

https://www.asjp.cerist.dz/

❖ موقع المجلات الأكاديمية العلمية العراقية

https://www.iasj.net/iasj

❖ صفحة جريدة الوقائع العراقية (الجريدة الرسمية لجمهورية العراق)
https://www.moj.gov.iq/iraqmag

❖ موقع هيئة التشريع والرأي القانوني لمملكة البحرين:
https://www.legalaffairs.gov.bh

❖ الموقع الإلكتروني للقناة الإخبارية الجزيرة:

- توملينسون.. مخترع البريد الإلكتروني يترجل:

https://www.aljazeera.net/encyclopedia/icons/2016/3/7-توملينسون-مخترع-البريد-الإلكتروني-يترجل/

- "القرصان المنفرد" يسقط أحد رجالات ترمب:

https://www.aljazeera.net/news/international/2018/3/23-القرصان-المنفرد-يسقط-أحد-رجالات-ترمب/

❖ موقع Academia: https://www.academia.edu

❖ موقع ويكيبيديا: https://en.wikipedia.org/wiki/Main_Page

ثانيا: المراجع باللغة الأجنبية

- **Ouvrages** :

❖ Ouvrages généraux :

1- Alain Madec; Pierre Leclercq, Les flux transfrontières de données : vers une économie internationale de l'information, La Documentation française, Paris 1982.

2- Étienne MONTERO, La responsabilité civile du fait des bases de données (Travaux de la Faculté de droit de Namur,21), Presses universitaires de Namur, 1998.

3- M. PLANIOL, G. RIPERT, Traité pratique de droit civil français, t. III, Paris, LGDJ, 2e éd., 1952.

❖ Ouvrages spéciaux :

1- Christiane FERAL-SCHUHL, Cyberdroit. Le droit à l'épreuve de l'Internet, 3e édition, Dalloz Dunod 2002.

2- David FERBRACHE, Pathology of Computer Viruses, Springer-Verlag, London Ltd, 1992.

3- Martin Wasik, "Crime and the computer", Oxford University press, USA, 1991.

4- Michael D. Rostoker, Robert H. Rines, Computer jurisprudence: legal responses to the information revolution, New York, N.Y. : Oceana Publications, 1986.

5- M. Vivant, A propos des " biens informationnels", JCP 1984, I, n° 3132.

6- Parker Donn, Fighting computer crime - A new framework for protecting information-, John Wiley and Sons Inc., New York, 1998.

7- Pierre CATALA, Ébauche d'une théorie juridique de l'information, Dalloz, n° 5, 1984.

8- Pierre CATALA, «La «propriété» de l'information», Mél. Raynaud, Paris, Dalloz-Sirey, 1985.

9- Richard Totty and Anthony Hardcastle, Computer –Related crime, in "information Technology & the law",Chris Edwards and Nigel savage, Macmillan Publishers U.K., 1986.

10- Ulrich Sieber, "The international Handbook on Computer Crime "Computer related Economic crime and infringements of privacy", John Wiley & Sons, 1986.

- **Articles et chroniques** :

1- Donald K. PIRAGOFF, Computer crimes and other crimes against information technology in canada, RIDP (Revue Internationale de droit pénal), 1993.

2- Henrik W.K. Kaspersen, Computer crime and other crimes against information technology, AIDP (International review of penal law), 1993.

3- Irini VASSILAKI, Computer crime and other crimes against information technology,RIDP (Revue Internationale de droit pénal), 1993.

4- Manfred Möhrenschlager, Computer crime and other crimes against information technology in Germany, R.I.D.P, Vol. 64, 1-2 ,1993.

5- Mohamed KAHLOULA, le délit d'accès ou de maintien frauduleux dans un système de traitement automatise de données (S.T.A.D), Revue des Sciences Juridiques, Administratives et Politiques, N° 12, la faculté de Droit et des sciences politiques, université Abou- Bekr Belkaid, Tlemcen, 2011.

6- Hervé CROZE, L'apport du droit pénal à la théorie générale de l'informatique, JCP, 1988.

7- Yann PADOVA, Un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénal comparé, n°4, octobre-décembre, Dalloz ,2002.

- **Conférences** :

6- Leïla Marchand, "La cybercriminalité coûte 600 milliards de dollars par an" https://www.lesechos.fr/2018/02/la-cybercriminalite-coute-600-milliards-de-dollars-par-an-984995.

7- Louis Nizer, The Right of Privacy, A Half Century's Developments, 39 MICH. L. REV. 1941.

8- Lucien Martin, Le secret de la vie privée, Revue trim. de droit civil, 1959.

9- Marc Lomazzi, " Cybercriminalité: les entreprises françaises de plus en plus attaquées"

https://www.leparisien.fr/economie/cybercriminalite-les-entreprises-francaises-de-plus-en-plus-attaquees-18-04-2019-8055717.php

10- Mohamed Chawki, "Essai sur la notion de cybercriminalité, juillet 2006". https://www.ie-ei.eu/IE-EI/Ressources/file/biblio/cybercrime.pdf

11- Nerson Roger. La protection de la vie privée en droit positif français, Revue internationale de droit compare, Vol. 23 N°4,Octobre-décembre 1971.

12- Odinot, Geralda & Verhoeven, Maite & Pool, Ronald & De Poot, Christianne, Organised Cybercrime in the Netherlands. Empirical findings and implications for law enforcement, Den Haag: WODC, Ministry of Security and Justice, February 2017.
https://www.wodc.nl/binaries/Cahier%202017-1_Full%20text_tcm28-244615.pdf

13- Pierre KAYSER, Les droits de la personnalité, aspects théoriques et pratiques, Revue trimestrielle de droit civil, 3, 1971.

14- Rigaux François. L'élaboration d'un « Right of Privacy » par la jurisprudence américaine. In: Revue internationale de droitcomparé. Vol. 32 N°4, Octobre-décembre 1980.

15- Samuel D. Warren; Louis D. Brandeis, Harvard " The Right to Privacy ", Law Review, Vol. 4, No. 5. (Dec. 15, 1890).
https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

16- Thomas Cooley, A Treatise on the Law of Torts , 2ed Chicago, Callaghan & Co, 1888.

17- Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society (COMCRIME Study) (Jan. 1, 1998).

- **Canada** :

Code criminel de Canada (L.R.C. (1985), ch. C-46
https://laws-lois.justice.gc.ca/fra/lois/C-46/page-107.html#docCont

- **France** :

- La loi n° 52-223 du 27 février 1952 relative à la procédure de codification des textes législatifs concernant le service des postes, télégraphes et téléphones JORF nº 56 du 4 mars 1952.
- La loi n° 57-1426 du 31 décembre 1957 instituant un code de procédure pénale JORF du 8 janvier 1958.
- L'Ordonnance n° 58-1296 du 23 décembre 1958 modifiant et complétant le code de procédure pénale JORF n°0300 du 24 décembre 1958.
- La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés JORF du 7 janvier 1978.
- La loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle JORF du 30 juillet 1982.
- La loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique. JORF du 6 janvier 1988.
- La loi n°92-683 du 22 juillet 1992 portant réforme des dispositions générales du code pénal . JORF n°169 du 23 juillet 1992.
- La loi no 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes ,JORF n°169 du 23 juillet 1992.
- La loi n° 93-1013 du 24 août 1993 modifiant la loi n° 93-2 du 4 janvier 1993 portant réforme de la procédure pénale (rectificatif), JORF n°0171 du 26 juillet 1994.

- La loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet, JORF n°0156 du 25 juin 2020.
- La loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales JORF n°0187 du 31 juillet 2020.
- La loi n° 2020-1672 du 24 décembre 2020 relative au Parquet européen, à la justice environnementale et à la justice pénale spécialisée. JORF n°0312 du 26 décembre 2020.
- L'ordonnance n° 2021-650 du 26 mai 2021 portant transposition de la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen et relative aux mesures d'adaptation des pouvoirs de l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse. JORF n°0121 du 27 mai 2021.

- **The United States of America**:

  - CRIMES AND CRIMINAL PROCEDURE 18 USC 2510: https://uscode.house.gov/view.xhtml?req=(title:18%20section:2510%20edition:prelim)#2510_1

  - CRIMES AND CRIMINAL PROCEDURE PART II-CRIMINAL PROCEDURE CHAPTER 211-JURISDICTION AND VENUE (June 25, 1948, ch. 645, 62 Stat. 826). https://uscode.house.gov/download/releasepoints/us/pl/116/344/pdf_usc18@116-344.zip
  - ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986. OCTOBER 17 (legislative day, OCTOBER 10), 1986. https://www.justice.gov/sites/default/files/jmd/legacy/2014/08/10/senaterept-99-541-1986.pdf
  - Restatement (Second) of Torts §§ 652A (1997). http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html

- **Le Conseil de l'Union européenne:**

- Convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un office européen de police (convention Europol) Journal officiel n° C 316 du 27/11/1995.

- Décision du Conseil de l'Union européenne du 6 avril 2009 portant création de l'Office européen de police (Europol) JO L 121 du 15.5.2009.
- Décision du Conseil 2002/187/JAI du 28 février 2002 instituant Eurojust afin de renforcer la lutte contre les formes graves de criminalité, JOCE N° L 63/1, 06/03/2002.
- Le règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil.
- Recommandation n° R(95)13 du Comité des Ministres aux Etats membres relative aux problèmes de procédure pénale liés à la technologie de l'information adoptée le 11 septembre 1995.

- **Décisions des juridictions judiciaires:**
  - Décisions des juges du fond:
- CA Paris 12ème ch, section A Arrêt du 30 octobre 2002. Kitetoa / Sté Tati.

- **Sites internet** :

- Le site officiel du Parlement européen: www.europarl.europa.eu
- le journal officiel de l'union européenne https://eur-lex.europa.eu
- Obama White House Archives: https://obamawhitehouse.archives.gov
- Législation belge: http://www.ejustice.just.fgov.be
- Moteur de recherche des thèses de doctorat françaises, le site: www.theses.fr
- le service public de la diffusion du droit par l'Internet via le site: https://www.legifrance.gouv.fr
- l'actualité du droit des nouvelles technologies: https://www.legalis.net
- Electronic Privacy Information Center: https://www.epic.org/

قائمة المحتويات

قائمة المحتويات

الملخص:

أجبرت الجريمة الإلكترونية التشريعات الوطنية والدولية على ضرورة تطوير تلك الأجهزة القضائية المكلفة بالتحقيق الابتدائي في الجريمة الإلكترونية وكذا استحداث هيئات أخرى لمساعدتها، لذلك كان من البديهي أن يمتد تأثير الجريمة الإلكترونية إلى جهاز الضبطية القضائية لما له من صلة بجهات القضاء المختصة بالتحقيق الابتدائي في الجريمة الإلكترونية، بحيث شهد جهاز الضبطية القضائية بدوره تطورات عديدة سواء على المستوى الوطني والإقليمي والدولي وذلك استجابة للتحولات التي فرضتها طبيعة الجريمة الإلكترونية.

اصطدمت جهود جهات التحقيق الرامية إلى جمع تلك الأدلة المرتبطة بالجريمة الإلكترونية بجملة من الصعوبات منها ما هو مرتبط بالعامل البشري ومنها ما هو مرتبط بالدليل الإلكتروني في حد ذاته، كما تبرز الخصوصية المعلوماتية كموضوع حساس زاد من صعوبات جهات التحقيق.

وبما أن إجراءات جمع الدليل الإلكتروني تعتمد في كثير من الأحيان على تعاون الدول فيما بينها، شهد موضوع التعاون الدولي في مجال التحقيق الجنائي في الجريمة الإلكترونية إشكاليات عديدة ثبطت من عزيمة جهات التحقيق.

بدورها عرفت عملية جمع الدليل الإلكتروني تعقيدات كبيرة بداية من الانتقال إلى مسرح الجريمة الإلكترونية ومعاينته وصولا إلى موضوع الشاهد المعلوماتي، وذلك بعد المرور بإجراءات التفتيش والضبط والخبرة المتعلقة بالدليل الإلكتروني. كما أن هناك إجراءات أخرى تستهدف الوصول إلى الدليل الإلكتروني ونقصد بها التسرب ومراقبة الاتصالات الإلكترونية وحفظ المعلومات، أبانت كلها عن جملة من الإشكالات تقف كشاهد على مدى تأثر التحقيق الجنائي (الابتدائي) بالجريمة الإلكترونية.

الكلمات المفتاحية:

التحقيق الجنائي، التحقيق الابتدائي، الجريمة الإلكترونية، الدليل الإلكتروني، مراقبة، اعتراض، الاتصالات الإلكترونية، المعلومات، الخصوصية المعلوماتية، الضبط القضائي، الإنترنت. التعاون الدولي.

Abstract :

Cybercrime has made it necessary for national and international legislative bodies to develop judicial authorities who are responsible for the preparatory investigation in cybercrime matters, as well as the creation of other entities to assist them. Therefore, it has become evident that the impact of cybercrime must be extended to the judicial police because of its link to the competent judicial authorities in the preparatory investigation of cybercrimes.

Consequently, the judicial police agency has experienced many developments at the national, regional and international levels in response to the changes brought on by the very nature of cybercrime.

In their efforts to collect evidence related to cybercrime, the investigating authorities encountered a series of difficulties, some of which were related to a human factor and others related to the electronic evidence itself.

Additionally, privacy and information confidentiality were sensitive subjects that have increased the difficulties for the investigating authorities.

Since the procedures for collecting electronic evidence often depend on the cooperation among states themselves, the issue of international cooperation in the field of preparatory criminal investigation in cybercrime has encountered many problems which have discouraged the authorities who are responsible for the investigation.

Furthermore, the process of collecting electronic evidence presents its own challenges, starting with access to the location of the commission of the offense (virtual digital space) and its inspection. The process ends with testimony on the matter of cybercrime after having followed the inspection, seizure and expert procedures related to electronic evidence.

In addition, there are other measures aimed at attaining electronic evidence--namely, infiltration, surveillance of electronic communications, and the preservation of information. All of these revealed a number of issues that testify to the extent to which criminal (preparatory) investigations are affected by electronic crimes.

Keywords:

Cybercrime, judicial police, internet, Informations**,** Information privacy**,** Juridic legal protection, Criminal investigation, Preparatory investigation, Electronic surveillance, Intercept, Monitoring, Digital evidence, Internet, Judicial authorities, International cooperation.

Résumé :
La cybercriminalité a imposé aux législations nationales et internationales la nécessité de développer les organes et les autorités judiciaires chargées de l'instruction préparatoire en matière de cybercriminalité ainsi que la création d'autres organes pour les assister. Il était donc évident que l'impact de la cybercriminalité s'étendait à la police judiciaire en raison de son lien avec les autorités judiciaires compétentes dans l'instruction préparatoire sur la cybercriminalité. De sorte que l'organisme de la police judiciaire a connu de nombreux développements, tant au niveau national, régional qu'international, en réponse aux changements imposés par la nature de la cybercriminalité.

Les efforts des autorités chargées de l'instruction pour collecter ces preuves liées à la cybercriminalité se sont heurtés à un ensemble de difficultés, dont certaines étaient liées au facteur humain, et d'autres liées aux preuves électroniques en elles-mêmes, ainsi qu'à la vie privée et confidentialité de l'information en tant que sujet sensible qui a accru les difficultés des autorités d'instruction.

Étant donné que les procédures de collecte de preuves électroniques dépendent souvent de la coopération des États entre eux, la question de la coopération internationale dans le domaine de l'instruction pénale préparatoire en matière de cybercriminalité a été témoin de nombreux problèmes qui ont découragé les autorités chargées de l'enquête.

À son tour, le processus de collecte des preuves électroniques a connu de grandes complications, commençant par le transport sur le lieu de la commission de l'infraction (espace numérique virtuel) et son inspection, et se terminant par le sujet du témoignage en matière de cybercriminalité, après avoir suivi les procédures d'inspection, de saisie et d'expertise liées aux preuves électroniques.

En outre, il existe d'autres mesures visant à atteindre les preuves électroniques et nous parlons de l'infiltration, de la surveillance des communications électroniques et de la préservation des informations. Toutes ont révélé un certain nombre de problèmes qui témoignent de la mesure dans laquelle l'instruction pénale (préparatoire) est affectée par la criminalité électronique.
Mots clés :
Cybercriminalité, L'instruction préparatoire, L'instruction pénale, Police judiciaire, Crime, Preuve numérique, Preuve électronique, Internet, confidentialité de l'information, La vie privée, Coopération internationale.