جامعة محمد بوضياف – المسيلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث

تخصص: القانون الجنائي

بعنوان:

التحقيق الجنائي في الجريمة الإلكترونية

إعداد الطالب:

بوقرة جمال الدين

إشراف الأستاذ الدكتور:

عنان جمال الدين

لجنة المناقشة:

الأستاذ	الجامعة	الصفة
أ د: العيساوي حسين	المسيلة	رئيسا
أ د: عنان جمال الدين	المسيلة	مشرفا ومقررا
د: عبدلي حمزة	المسيلة	مناقشا
د: شردود الطيب	المسيلة	مناقشا
أ د: خلفي عبد الرحمان	بجاية	مناقشا
أ د: روابح فريد	سطيف	مناقشا

السنة الجامعية: 2025/2024

جامعة محمد بوضياف – المسيلة

كلية الحقوق والعلوم السياسية

قسم الحقوق

أطروحة مقدمة لنيل شهادة الدكتوراه الطور الثالث

تخصص: القانون الجنائي

بعنوان:

التحقيق الجنائي في الجريمة الإلكترونية

إعداد الطالب:

بوقرة جمال الدين

إشراف الأستاذ الدكتور:

عنان جمال الدين

السنة الجامعية: 2025/2024

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

الإهداء

إلى الوالدين الكريمين أطال الله في عمرهما

وأمدهما بموفور الصحة والعافية

إلى زوجتي و أولادي

إلى إخوتي وأخواتي

إلى كل من ساعدني من قريب أو بعيد

أهدي ثمرة جهدي.

بوقرة جمال الدين

شكر وعرفان

اللهم لك الحمد كله، ولك الملك كله

بيدك الخير كله، وإليك يرجع الأمر كله

والصلاة والسلام على سيدنا مُحَمَّد

وعلى آله وصحبه أجمعين، وبعد:

أتوجه بجزيل الشكر للأستاذ الفاضل: أ.د عنان جمال الدين

على كل الدعم والمساندة والتوجيه الذي قدمه لي طيلة مسار هذا البحث.

كما أتقدم بالشكر الخاص لأعضاء اللجنة الموقرة على قبول مناقشة هذا العمل وتصويبه.

قائمة المختصرات باللغة العربية:

- ا أ م ج إ: الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية.

- ا ع م ج ت م: الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

- الهيئة: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

- ج: الجزء.

- ط: طبعة.

- ص: صفحة.

- ق إ ج: قانون الإجراءات الجزائية.

- ق ع: قانون العقوبات.

قائمة المختصرات باللغة الأجنبية:

- AFRIPOL: Agence Africaine de Police Criminelle.

- Ed: édition

- EUROPOL: Agence Européenne de Police Criminelle.

- EUROJUST: L'Unité de Coopération Judiciaire de l'Union Européenne.

- E.MAIL: Electronic Mail

- FTP: File Transfer Protocol

- Internet: International Network

- INTERPOL : Organisation Internationale de Police Criminelle.

- IP : Internet Protocol

- ITU :International Telecommunication Union

- LAN: Local Area Network

- P: page

-WAN : Wide Area Network

- WWW : The World Wide Web:

مقدمـــــة

مقدمة:

الجريمة ظاهرة اجتماعية تتأثر طبيعتها وحجمها بتحولات المجتمع، لكن بسرعة قد تتجاوز حركته أحيانا، فمع بروز شبكة الإنترنت في نهاية القرن الماضي عرف العالم تقدما رهيبا، أسهم في التعجيل بالتقدم الاقتصادي والاجتماعي والسياسي على حد سواء، كما اختزل المسافات بين الدول، وألزمها على فتح حدودها، فتمت مشاركة الأفكار بين البشرية رغم تنوع ثقافاتها، وأضحى العالم قرية صغيرة تتقاسم الأفكار والأحداث.

وبقدر ما ساهم التطور المستمر لتكنولوجيات الإعلام والاتصال واندماجهما من زيادة في حجم التواصل بين الأشخاص، وإحداث قفزة نوعية في حياة الأفراد والدول، إلا أن هذا الجانب الإيجابي لم ينف الانعكاسات السلبية التي أفرزتها إساءة استخدام هذا التطور، مما أدى إلى ظهور جرائم تعتمد بدورها على التقنية المعلوماتية، سميت بجرائم الحاسوب أو الجرائم الإلكترونية.

وقد شكلت هذه الجرائم تحديا حقيقيا للسياسات الجنائية للدول، ومختلف أجهزتها التشريعية التنفيذية، الأمنية والقضائية، إذ وجدت نفسها أمام نمط جديد من الإجرام لم تألف التعامل معه بالنظر إلى صعوبة اكتشافه وإثباته، نتيجة وقوعه وسط فضاء افتراضي غير ملموس، يختلف عن الواقع المادي، ممَا جعلها تقف عاجزة عن مواجهته في ظل نقص القوانين، وتأخرها عن مواكبة التطورات التكنولوجية.

ولم يتوقف نطاق هذه الجرائم عند حدود الدولة، بل تجاوزه إلى أماكن موزعة عبر قارات مختلفة، متأثرا بالطبيعة العالمية لشبكة الإنترنت، التي فتحت أبوابا مغلقة، ووسعت حدودا أصبحت بلا حراسة، لتتوزع بذلك عناصر الجريمة على أكثر من رقعة، وتجد الدول نفسها مرة أخرى مترددة في تتبع أثر الجريمة حين تصطدم بسيادة غيرها، بما عجّل بدق ناقوس الخطر من المجتمع الدولي، والدعوة إلى تكاتف الجهود لمواجهة هذه الظاهرة التي لا تستثني أحدا.

كما دفعت خصوصيات هذه الجريمة وما خلَفته من صعوبات الدول إلى مراجعة قوانينها الداخلية، وسنَ نصوص قادرة على مسايرة هذا النمط المستحدث والحد من خطورته، سواء

النصوص الموضوعية المجرمة لهذه الأفعال، أو الإجرائية باستحداث أساليب تعتمد بدورها على نفس التقنية الرقمية المستعملة في ارتكاب الجريمة.

ويأتي التحقيق الابتدائي كمرحلة متقدمة في مواجهة الجريمة الإلكترونية، يتم خلالها جمع الأدلة من أجل توضيح معالم الجريمة وكشف ملابساتها، وهو ما يتطلب تحقيق نوع من التوازن بين مقتضيات السرعة لكشف الحقيقة، وما يتخلل هذه المرحلة من إجراءات تمتد أحيانا لتطال حرمة الحياة الخاصة للأفراد، التي تحفظها مختلف المواثيق الدولية والدساتير.

والجزائر كغيرها من الدول، لم تدّخر جهدا في سبيل مكافحة هذه الجريمة، من خلال مواكبتها للتطور التكنولوجي في شتى القطاعات، والعمل على تكوين فرق بحث وتحري خاصة بمكافحتها، واستحداث جهات قضائية متخصصة بمتابعتها، فضلا عن مراجعة مختلف القوانين المتعلقة بها، سواء بتعديل قانوني العقوبات والإجراءات الجزائية، أو بسن نصوص قانونية خاصة أهمها القانون رقم 09-04، الذي عزز آليات التحقيق التقليدية بآليات جديدة، بحثا عن النجاعة اللازمة لمواجهة هذه الجرائم.

أهمية الدراسة:

تتجلى أهمية دراسة موضوع "**التحقيق الجنائي في الجريمة الإلكترونية**" في حداثته؛ إذ أنه أحد إفرازات تكنولوجيات الإعلام والاتصال التي تشهد تطورا مستمرا ومتزايدا، كشف قصور أساليب التحقيق التقليدية عن مواجهة هذه الظاهرة الإجرامية، بشكل فرض الحاجة إلى إعادة النظر في السياسة التشريعية الجنائية، خاصة جانبها الإجرائي، نتيجة ما عرفه جهاز التحقيق من صعوبات خلال تحرّيه عن هذه الجرائم التقنية، بما استدعي البحث عن أساليب أكثر فعالية.

وتزداد أهميته بالنظر إلى الطابع الدولي لهذه الجريمة، نتيجة استغلالها للتطور الرهيب لوسائل الاتصال الحديثة، فلم تعد متمركزة في دولة معينة، ولا موجهة لمجتمع بعينه، بل أصبحت تهديدا للبشرية جمعاء، بما جعل الحاجة ماسة إلى تكاتف الجهود لإيجاد أساليب قادرة على مواجهتها دوليا، واتخاذ تدابير فعالة للتقليل من حدَتها، وما يقتضيه كل ذلك من اتفاقيات ثنائية إقليمية ودولية.

فضلا عمَا يثيره هذا الموضوع من ضرورة وضع ضوابط قانونية كفيلة بحماية حقوق الأفراد وحرمة حياتهم الخاصة، التي تكفلها مختلف المواثيق الدولية والدساتير، بالنظر إلى ما قد يتخلل مرحلة التحقيق من إجراءات تصل إلى حد انتهاكها.

الهدف من الدراسة:

نهدف من خلال هذه الدراسة إلى الإلمام بالجوانب الإجرائية الخاصة بمكافحة الجريمة الإلكترونية، من خلال التعرف على الجهاز المكلف بالتحقيق فيها على المستويين الوطني والدولي، وإبراز خصوصية الأساليب التي يعتمد عليها خلال تحرَيه عن هذه الجريمة وسط بيئة افتراضية، فضلا عن الإحاطة بأهم العقبات التي تعترضه، وذلك لمعرفة قدرته على مسايرة التطورات التكنولوجية من جهة، والوقوف على مدى كفاية النصوص القانونية التي تنظم إجراءاته من جهة أخرى.

أسباب اختيار الموضوع:

ما دفعني أساسا لتناول هذا الموضوع بالدراسة هو التحدي الذي فرضته الجرائم الإلكترونية في مواجهة النصوص التشريعية القائمة، نتيجة عدم مسايرة الأخيرة للتطور النوعي لهذه الجرائم وما يترتب عنه من تزايد مخاطرها على الفرد والمجتمع، فضلا عن دوافع أخرى يمكن اختزالها فيما يلي:

01- أسباب ذاتية:

أ- الرغبة الشخصية في دراسة هذا الموضوع، خصوصا أنه حديث مرتبط بتكنولوجيات الإعلام والاتصال التي لا تزال في حالة تطور مستمر، والفضول إلى معرفة خصائص الجريمة الإلكترونية، وكيفية الوصول إلى أدلتها الرقمية وسط بيئة افتراضية.

ب- اهتماماتي العملية في تناول هذا الموضوع نظرا لكثرة تداوله على مستوى الجهات القضائية.

02- أسباب موضوعية:

الانتشار الواسع للجرائم الإلكترونية في المجتمع، وتزايدها بشكل لافت، وما يشكله من خطر حقيقي على الأمم والشعوب، يستدعي معرفة الدور الذي يلعبه جهاز التحقيق في التصدي لهذه الجرائم، وتشخيص مختلف العقبات التي تعتريه، حتى يمكن الوصول إلى حلول كفيلة بعلاجها.

الدراسات السابقة:

توجد بعض الدراسات السابقة التي تطرقت لهذا الموضوع، لكنها تعتبر قليلة إذا ما قورنت بغيرها، ويرجع ذلك أساسا إلى كونه يعالج قضية معاصرة، مرتبطة ارتباطا وثيقا بتطور تكنولوجيات الإعلام والاتصال، التي لا يزال أفقها غير محدد.

ولعلَ أبرز الدراسات التي تناولت هذا الموضوع، كتاب الجرائم الإلكترونية والوقاية منها في القانون الجزائري، لمؤلفه يزيد بوحليط، طبعة 2019، الذي اهتم بتوضيح الجوانب الموضوعية والإجرائية للوقاية من الجريمة الإلكترونية ومكافحتها على ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات وقانوني العقوبات والإجراءات الجزائية، بما يجعله مختلفا عن موضوع الدراسة الذي ينصب على الجوانب الإجرائية للجريمة الإلكترونية دون الجوانب الموضوعية.

إضافة إلى أطروحة دكتواره للباحثة بوحزمة نصيرة، تمت مناقشتها بجامعة سيدي بلعباس سنة 2022، والموسومة بـ: التحقيق الجنائي في الجريمة الإلكترونية (دراسة مقارنة)، وقد تناولت مختلف الجوانب الإجرائية والموضوعية للتحقيق الجنائي في الجريمة الإلكترونية، مع دراسة بعض التشريعات المقارنة، الأمر الذي يجعلها كذلك مختلفة عن دراستنا، بالنظر إلى تركيزها على الجوانب الإجرائية للتحقيق الجنائي في هذه الجريمة على ضوء التشريع الجزائري، مع التعريج على مواقف بعض التشريعات الدولية للاستفادة من تجاربها، ودون الخوض في الجوانب الموضوعية التي تتطلب بحثا مستقلا بذاته.

وكذلك أطروحة دكتوراه للباحث براهيمي جمال، تمت مناقشتها بجامعة تيزي وزو سنة 2018، والمعنونة بـ: "التحقيق الجنائي في الجرائم الإلكترونية"، والتي تطرق من خلالها صاحبها

إلى مختلف آليات التحقيق في الجريمة الإلكترونية، مع شيء من التفصيل في الدليل الإلكتروني وحجيته أمام القضاء، وهي موضع الاختلاف بيننا، بحيث استغنينا عن هذا الجانب، الذي يتطلب بحثا مستقلا بذاته.

عموما، يمكن القول أن هذه الدراسات وعلى أهميتها فهي موسَعة، تختلف عن دراستنا التي اهتمت بالجوانب الإجرائية لمكافحة الجريمة الإلكترونية، وتحديدا خلال مرحلة التحقيق.

إشكالية الدراسة:

نتيجة ظهور جرائم مستحدثة في ظل التطور التكنولوجي، واعتماد مرتكبيها على تقنيات معلوماتية تجاوزت الحدود المكانية والقيود الزمنية، ركنت الدول إلى تحيين منظومتها القانونية موضوعيا وإجرائيا لمواكبة هذا التطور النوعي، بما في ذلك المشرع الجزائري الذي بادر إلى استحداث آليات تحقيق جديدة تضاف للآليات التقليدية، سعيا منه للحد من خطورة هذه الجرائم الأمر الذي يجعل إشكالية هذه الدراسة تتمحور حول:

– ما مدى فعالية أساليب التحقيق التقليدية في مكافحة الجريمة الإلكترونية؟

صعوبات الدراسة:

لم يكن من السهل وضع خطة متوازنة ودراسة شاملة ودقيقة، بالنظر إلى طبيعة البحث التي تمزج بين الجانبين القانوني والتقني، والتي شكلت تحديا صعبا، خصوصا عند التعامل مع الجانب التقني، وما يميزه من صبغة علمية ومصطلحات دقيقة، تحتاج إلى شخص متخصَص في مجال المعلوماتية لفهمها، فكان من الصعب البحث في الجوانب القانونية دون الإلمام الكافي بالجوانب الفنية للموضوع، إضافة إلى صعوبات أخرى، أهمها:

– نقص الدراسات الميدانية والإحصائيات المحيَنة المتعلقة بالجريمة الإلكترونية، وهو ما جعلنا نسعى جاهدين للحصول عليها.

– قلة الاجتهادات القضائية الوطنية المتعلقة بالموضوع، وما يعتريه من إشكالات، وذلك راجع لحداثته، مما جعلنا في رحلة بحث عن بعض الآراء الفقهية والاجتهادات القضائية المقارنة.

مناهج البحث:

سعيا للإجابة عن الإشكالية التي تناولتها الدراسة وفق طريقة علمية ومنهجية سليمة تمت الاستعانة بمناهج البحث العلمي الآتية:

1- المنهج الوصفي التحليلي: إذ يشكل المنهج الأساسي لأغلب مواطن الدراسة، فقد تم اعتماده قصد الإلمام بالموضوع وتأصيل عناصره، من خلال وصف المفاهيم العامة المتعلقة بإجراءات التحقيق المتبعة لاستخلاص الدليل الرقمي، وتأصيل الإشكالات الإجرائية التي تثيرها أساليب التحقيق في الجريمة الإلكترونية، إضافة إلى تحليل النصوص القانونية التي تحكمها.

2- المنهج المقارن: والذي تمت الاستعانة به لضرورة التعرف على موقف المشرع الجزائري في بعض المسائل المهمة مقارنة بالتشريعات الأخرى، بغية الاطلاع على ما وصل إليه الفكر القانوني المقارن، والاستفادة من تجارب الدول التي سبقتنا في هذا المجال، دون أن يرقى ذلك إلى مرتبة الدراسة المقارنة.

03-المنهج التاريخي: والذي استدعت بعض المواضع ضرورة الأخذ به، لاسيما حين تتبع التطور الزمني لجهاز الكمبيوتر، وتكنولوجيات الإعلام والاتصال، لما لهما من أثر مباشر على تطور الجريمة الإلكترونية من جهة، وآليات مكافحتها من جهة أخرى.

تقسيم الخطة:

للإجابة على الإشكالية المطروحة وما تثيره من تساؤلات فرعية على ضوء ما هو مستجد في النصوص القانونية الوطنية وبعض الاتفاقيات الدولية ذات الصلة، ارتأينا تقسيم موضوع دراستنا إلى بابين:

الباب الأول، تم تخصيصه للجانب المفاهيمي للموضوع، من خلال التطرق إلى الأحكام العامة للتحقيق الجنائي في الجريمة الإلكترونية.

أما **الباب الثاني،** فقد خُصَ بمعرفة أساليب التحقيق الجنائي في الجريمة الإلكترونية.

كما تم تقسيم كل منهما إلى فصلين، إذ يحتوى الباب الأول على:

الفصل الأول: بعنوان "الإطار المفاهيمي للجريمة الإلكترونية"، وضمّ بدوره مبحثين، الأول تطرق للجانب التقني للجريمة الإلكترونية، وتطرق الثاني إلى مفهومها.

الفصل الثاني: بعنوان "جهاز التحقيق الجنائي في الجريمة الإلكترونية"، وتناول المبحث الأول منه "السلطة المختصة بالتحقيق في الجريمة الإلكترونية"، فيما تناول الثاني "الأجهزة المساعدة على التحقيق في الجريمة الإلكترونية".

وكذلك احتوى **الباب الثاني** على فصلين:

الفصل الأول: عنوانه "الأساليب التقليدية للتحقيق في الجريمة الإلكترونية"، وتم تقسيمه إلى مبحثين، تناول أولهما المعاينة والخبرة في الجريمة الإلكترونية، وتناول الثاني التفتيش والحجز في الجريمة الإلكترونية.

الفصل الثاني: بعنوان "الأساليب الحديثة للتحقيق في الجريمة الإلكترونية"، خصص مبحثه الأول لدراسة أساليب التحري الخاصة، وخصص الثاني لدراسة المساعدة القضائية.

الباب الأول

الأحكام العامة للتحقيق الجنائي في الجريمة الإلكترونية

الباب الأول

الأحكام العامة للتحقيق الجنائي في الجريمة الإلكترونية

غزت المعلوماتية في السنوات الأخيرة مختلف جوانب الحياة حتى سمي هذا العصر باسمها، ورغم إيجابياتها العديدة إلّا أنها لم تخل من السلبيات، إذ استغل المجرمون تطور تكنولوجيات الإعلام والاتصال في جانبه السلبي، بما أدى إلى بروز جرائم لم تكن معروفة من قبل، تعدى نطاق تأثيرها من المساس بحياة الأفراد وممتلكاتهم إلى المساس بأمن المجتمعات واستقرارها، بشكل دفع المجتمع الدولي إلى دق ناقوس الخطر داعيًا إلى تضافر الجهود لمواجهتها نظريًا وعمليًا.

ورغم عدم اختصاص رجال القانون في الجوانب التقنيّة للجرائم الإلكترونية بحكم تكوينهم العلمي، إلا أن ضرورة التعامل معها لمعرفة ما يلزمهم لتحديد طبيعتها وطريقة ارتكابها، يفرض عليهم الإطلاع على عالم التكنولوجيا، حتى يتسنى لهم اتباع سُبل التحقيق المجدية لاكتشافها وضبط أدلتها، تماشيًا والحاجة الماسّة إلى مواجهة هذا الإجرام تشريعيًا وفنيا.

لكن وقبل التعرف على أساليب التحقيق الجنائي في الجريمة الإلكترونيّة، وجب علينا أن نُعَرِّج على الجانب التقني لهذه الجرائم، وأن نتعرف على جهاز التحقيق الجنائي المكلف بالتحري عنها، وهو ما سنتناوله من خلال الفصلين الآتيين:

الفصل الأول: الإطار المفاهيمي للجريمة الإلكترونية.

الفصل الثاني: جهاز التحقيق الجنائي في الجريمة الإلكترونية.

الفصل الأول

الإطـــــار المفاهيمي

للجريمة الإلكترونية

الفصل الأول

الإطار المفاهيمي للجريمة الإلكترونية

تعد الجرائم الإلكترونية من الجرائم المستحدثة جراء الاستخدام السلبي لتكنولوجيات الإعلام والاتصال، بما جعلها تشكّل تحديا جديدا أمام رجال القانون للإحاطة بمختلف جوانبها، إذ أن الجانب الفني للتكنولوجيات الحديثة وإن كان يبدو بعيدا عن لغة القانون، إلا أن تحقيق إدراك عميق لهذه الجرائم يستلزم إدراك أبعادها التقنية.

والجزائر كغيرها من الدول، تبذل جهودا معتبرة لمكافحة هذه الجرائم من خلال مواكبة التطور التكنولوجي في شتّى القطاعات، وتعزيز المنظومة التشريعية بالقوانين والأنظمة المتعلقة بمكافحتها، إضافة إلى استحداث آليات جديدة قادرة على التصدي لها، بالموازاة مع الآليات التقليدية التي لم تعد قادرة على مواكبة هذا التطور.

فالتحقيق في الجريمة الالكترونية يقتضي التعرف على معناها ودراسة جوانبها التقنية، لما يوفره ذلك من مساعدة للمحقق على إدراك أركان الجريمة كما حددها القانون، ومعرفة الأساليب التي يستعملها مجرمو المعلوماتية للوصول إلى ضحاياهم وتحقيق غاياتهم الإجرامية، مما يسهل تتبعهم وضبط الأدلّة الإلكترونية في إطارها الشرعي.

وتبيانا للنقاط سالفة الذكر، قمنا بدراستها وفق المبحثين الآتيين:

المبحث الأول: الجانب التقني للجريمة الإلكترونية.

المبحث الثاني: مفهوم الجريمة الإلكترونية.

المبحث الأول

الجانب التقني للجريمة الإلكترونية

لا شك في أن للحاسوب دورا بارزا في مجال ارتكاب الجريمة الإلكترونية، فقد يكون هدفا لها كما في حالة الدخول غير المصرح به لمنظومة معالجة آلية، أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وقد يكون أداة لارتكابها كما في حالة استغلاله لاختلاس أموال الغير بإجراء تحويلات غير مشروعة، أو استخدام تكنولوجيا الإعلام والاتصال في عمليات النصب والتزوير وغيرها من الجرائم.

ومن أجل الوصول إلى فهم دقيق لهذه الجرائم المستحدثة ومعرفة طرق ارتكابها، وجب علينا التعرف على الحاسوب، بالنظر إلى دوره البارز الذي جعل منه عنصرا مفترضا في هذه الجرائم، وذلك من خلال معرفة مكوناته، وطريقة عمله، وشبكات اتصاله، خصوصا وأن مصطلحاته العلمية ستصاحبنا طيلة هذه الدراسة، وهو ما سنتناوله من خلال:

المطلب الأول: جهاز الحاسوب.

المطلب الثاني: تكنولوجيات الإعلام والاتصال.

المطلب الأول

جهاز الحاسوب

أحدثت الثورة التكنولوجية قفزة هائلة في مجال صناعة تكنولوجيات الإعلام والاتصال، تمثلت أساسا في انتشار استعمال الحاسوب على كافة الأصعدة، خاصة مع وجود شبكة الإنترنت التي جعلت من العالم قرية صغيرة، وأتاحت فرصا جديدة للاطلاع على المعلومات وتبادلها بين ملايين البشر بضغطة زر واحدة.

ولاعتماد مجرمي المعلوماتية في ارتكاب جرائمهم اعتمادا كليا على جهاز الحاسوب، وجب علينا التعرف على هذا الجهاز لفهم طبيعة عمله، وهو ما سنتناوله في هذا المطلب.

الفرع الأول: مفهوم الحاسوب

لعب الحاسوب الآلي دورا مميزا في التطور والتقدم العلمي، حيث أضحى وسيلة لا يمكن الاستغناء عنها في أغلب مجالات الحياة العلمية والإدارية والاقتصادية وغيرها.

أولا: تعريف الحاسوب وتطوره التاريخي

01- تعريف الحاسوب: لغويا، تستخدم كلمة الحاسوب كمقابل لكلمة (COMPUTER)، وهي تسمية إنجليزية الأصل، مشتقة من (COMPUTER-COMPUTE) بمعنى (يحسب- الحساب) ويقابلها في اللغة الفرنسية (ORDINATEUR) وتعني المنظم.[1]

وللحاسوب تسميات متعددة في الفقه، إذ يسميه البعض بالكمبيوتر وهي أبرز تسمياته، ويسميه آخرون بالحاسب الالكتروني، وغيرهم بالحاسوب، إضافة إلى تسمية الحاسب الآلي، وهي التسمية العربية الأكثر شيوعا.[2]

[1]- علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية والأدبية، لبنان، 2013، ص: 35.

[2]- محمد حماد مرهج الهيتي، جرائم الحاسوب، ط1، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006، ص: 19.

أما فقها، فقد عرَفه البعض بأنه: "جهاز الكتروني يتكون من مجموعة من الأجهزة أو الوحدات التي تعمل بصورة متكاملة مع بعضها بهدف تشغيل البيانات الداخلة طبقا لبرنامج محدد تم وضعه مسبقا للحصول على نتائج معينة"،[1] وعرفه البعض الآخر بأنه: "جهاز مكون من مجموعة من القطع والأجزاء الإلكترونية، وهو ما يسمى بالجزء المادي (HARD WARE)، إضافة إلى الجزء المعنوي أو المنطقي (SOFT WARE)، وبتكامل هذه الأجزاء يقوم جهاز الحاسوب باستقبال البيانات ومعالجتها من خلال مجموعة عمليات حسابية بسرعة عالية وتسلسل منطقي، لتظهر بعدها النتائج المطلوبة، ويمكن تخزين هذه النتائج والاستفادة منها عدة مرات".[2]

ورغم أهمية الحاسب الآلي واستعمالاته المتعددة، إلا أنه يبقى مجرد جهازٍ متلقٍ للأوامر لا يمكنه أن يعمل لوحده، بل من خلال مجموعة من الأوامر يزوده بها الإنسان.[3]

02- **التطور التاريخي لجهاز الحاسوب:** شهدت الحواسيب منذ منتصف القرن العشرين إلى وقتنا الحالي سلسلة من التطورات في أجزائها المادية والبرمجية، تحولت معها من نظام يعُج بالشرائح والتوصيلات والدارات المتكاملة، إلى مجرد رقاقة هي في حد ذاتها حاسبا.[4]

ففي القرن التاسع عشر ابتكر العالم بلير باسكال "BLAIR PASCAL" أول آلة حساب رقمية بسيطة، ثم تبعه العالم ليبنتيز "LIBNTIZ" الذي صنع آلة مشابهة لها، إلا أن عدم دقتهما حال دون الاعتماد عليهما كثيرا، ليقوم العالم بابيج "BABBAGE" سنة 1822 بتصميم نموذج آلة أسماها (المحرك التفاضلي) تستطيع التعامل مع أعداد مؤلفة من ستة أرقام، كما صمّم آلة أخرى أكثر تطورا سنة 1834 أسماها (المحرك التحليلي)، واستخدم البطاقات المثقبة للتحكم بسير العمليات، باعتبارها وسيلة لإدخال الأرقام.[5]

---

[1]- هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992، ص: 06.

[2]- علي حسن الطوالبة، الجرائم الإلكترونية، ط1، مؤسسة فخراوي للدراسات والنشر، البحرين، 2008، ص: 16.

[3]- المرجع نفسه، ص: 16.

[4]- يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، درا الجامعة الجديدة، الإسكندرية، 2019، ص: 16.

[5]- فادي حجار، بنية الحاسب، ط 1، دار شعاع للنشر والعلوم، حلب، سوريا، 1999، ص: 09.

بينما تمت صناعة أول جهاز كمبيوتر ببعض الأجزاء الإلكترونية سنة 1937 بجامعة هارفارد، وتم تطويره سنة 1946 بتمويل من وزارة الدفاع الأمريكية التي احتفظت بهذا الاختراع سرًا، وقد كانت كامل أجزائه إلكترونية، يستطيع القيام بـ: 500 عملية جمع و30 عملية ضرب في الثانية الواحدة، غير أنه كان يزن ما يقارب 30 طنا، ويشغل مساحة كبيرة.[1]

وتواصلت عمليات تطوير جهاز الحاسب الآلي إلى أن أصبح متاحا تجاريا ابتداء من سنة 1950 من طرف شركة (IBM) الرائدة في مجال مبيعات الحواسيب،[2] ولا تزال عمليات تطويره مستمرة إلى غاية يومنا، مرورا عبر عدة أجيال:

* **الجيل الأول (1951-1959):** شهدت هذه الفترة تطوير أول جهاز حاسوب لأغراض تجارية وتميزت حواسيب هذا الجيل بحجمها الكبير، واستخدام الصمامات المفرغة التي تتميز بغلاء الثمن والبطء، إضافة إلى صعوبة عملية البرمجة،[3] وكذا ارتفاع تكاليف إنجازه وصيانته.

* **الجيل الثاني (1959-1964):** تفاديا لبعض نقائص حواسيب الجيل الأول، تم خلال هذه المرحلة استبدال الصمامات الالكترونية للحاسوب بالترانزيستور،[4] مما أدى إلى زيادة سرعة تنفيذ العمليات الحسابية، فضلا عن انخفاض نسبي في حجم وتكلفة الحاسوب.

* **الجيل الثالث (1964-1970):** استمرارا لعملية تطوير أجهزة الحاسوب، استحدثت تقنية الدوائر المتكاملة التي كان لها أثر كبير في تصغير حجم الحاسوب وزيادة سرعة عملياته، فضلا

[1]- لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر، 2018، ص: 17.

[2]- العياشي زرزار، كريمة غياد، استخدامات تكنولوجيا المعلومات والاتصال في المؤسسة الاقتصادية ودورها في دعم الميزة التنافسية، دار صفاء للنشر والتوزيع، عمان، الأردن، 2015، ص: 37.

[3]- نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2010، ص: 31.

[4]- الترانزيستور: "عبارة عن قطعة معدنية صغيرة جدا على شكل حلقة ممغنطة تستعمل لتخزين المعلومات"، علي عبود جعفر، المرجع السابق، ص: 49.

عن انخفاض تكاليفه، كما تم تحسين أجهزة الإدخال والإخراج بعد إدخال تعديلات على الأقراص المغناطيسية والشاشات.[1]

* **الجيل الرابع (1970-1981):** ظهرت خلاله الشرائح الالكترونية (Chipsets)، التي أدت إلى تطور مذهل في الحاسوب سعة، سرعة، حجما وتكاليفا، وساعدت على اختراع أجهزة الكمبيوتر المحمولة لاحقا،[2]ومن بينها: (الكاميرات الذكية، أجهزة الراديو، الألعاب الإلكترونية، الأجهزة الإلكترونية القابلة للارتداء مثل النظارات، الأساور الرقمية، السماعات الملحقة بالهواتف السلكية أو اللاسلكية وغيرها من الأجهزة).[3]

* **الجيل الخامس (1981-1991):** أعلن اليابانيون سنة 1981 عن مشروع الجيل الخامس للحاسبات الإلكترونية، التي تمتاز بالتطور الفائق للذكاء الاصطناعي، والقدرة على الاستنتاج بصورة سريعة، بحيث وصلت سرعتها إلى (1000) مليون عملية في الثانية.[4]

* **الجيل السادس (1992 إلى يومنا هذا):** أطلق مشروع حواسيب الجيل السادس سنة 1992، ومن خصائصه تقليد الدماغ البشري والتشبه به (الذكاء الاصطناعي)، ومحاولة تقريب الأسلوب المتبع في معالجة المعلومات مع الأسلوب البشري.[5]

ثانيا: خصائص الحاسوب: للحاسوب عدة خصائص جعلت منه جوهر التكنولوجيا الحديثة ومادة رئيسية في حياة الفرد، يمكن إيجازها فيما يلي:

01- السرعة: يقصد بها الزمن الذي يستغرقه الحاسب الآلي لإجراء أي عملية، سواء أكانت حسابية أم منطقية، أو نقل للبيانات أو التعليمات بين أجزائه المختلفة.[6]

---

[1]- زياد القاضي، أساسيات علم الحاسوب، ط1، دار صفاء للنشر والتوزيع، عمان، الأردن، 1997، ص: 13.

[2]- لحسن ناني، المرجع السابق، ص: 17.

[3]- بهاء المرّي، جرائم المحمول ووسائل التواصل الاجتماعي وحجية الدليل الإلكتروني في الإثبات، ط1، دار الأهرام للنشر والتوزيع والإصدارات القانونية، مصر، 2022، ص: 36.

[4]- انتصار نوري الغريب، أمن الكمبيوتر والقانون، ط1، دار الراتب الجامعية، بيروت، 1994، ص: 13.

[5]- نهلا عبد القادر المومني، المرجع السابق، ص: 33.

[6]- طارق الشدي، آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، 1999، ص: 4.

فالحاسوب يمتاز بسرعة فائقة تُمكنه من إنجاز عدد كبير من العمليات الحسابية تصل إلى مليون عملية أو أكثر في الثانية الواحدة، الأمر الذي ساعد على استخدامه في مختلف مجالات الحياة، وصار الإنسان يعتمد عليه اعتمادا كبيرا في أعماله اليومية،[1] بشكل وفّر عليه الكثير من الوقت الذي كان سيمضيه في إجراء العمليات الحسابية والمنطقية.

02- قوة الذاكرة: يملك الحاسوب ذاكرة قوية يستطيع من خلالها تخزين أكبر عدد من المعطيات والمعلومات في الذاكرة الرئيسية، أو الذاكرة المساعدة أو الثانوية كالأقراص والأشرطة المغناطيسية، كما يستطيع استرجاع تلك المعلومات في أي وقت، وعرضها بسرعة فائقة.[2]

03- الدقّة: يتميز جهاز الحاسوب بدقة لا متناهية في التعاطي مع المعلومات والمعطيات، تجعله قادرا على تنفيذ عدة مهام في ثوان معدودة وبدقة متناسقة تكاد تكون معدومة الأخطاء، وهذا ما لا يستطيع أن ينفذه عشرات الأشخاص في أسابيع،[3] وكلما كانت المعلومات والبيانات المقدمة للتنفيذ صحيحة فليس هناك من سبب لقيام الحاسوب بإعطاء نتائج خاطئة.[4]

04- القابلية للبرمجة: يمكن تصميم الحاسوب الآلي وتأهيله لتأدية وظائف معينة، وذلك عن طريق البرمجيات التي يمكن تطويرها وتطويعها لتؤدي وظائف لا حدود لها.[5]

05- سعة مجال استخدامه: نظرا لدقة الحواسيب وقدرتها الفائقة في التعامل مع المعطيات فإن مجالات استخدامها واسعة جدا، فهي تستخدم في مختلف التطبيقات العلمية، كالبحوث الطبية والفضائية والكيميائية، والتطبيقات الهندسية، إضافة إلى استخدامها في المجال الجنائي.[6]

---

[1]- أحمد كيلان عبد الله، الجرائم الناشئة عن إساءة استخدام الحاسوب، رسالة ماجستير، جامعة بغداد، 2002، ص: 20.

[2]- سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2011 ص: 47.

[3]- فاروق الحفناوي، موسوعة قانون الكمبيوتر ونظم المعلومات، ط1، دار الكتاب الحديثة، القاهرة، 2001، ص: 30.

[4]- نهلا عبد القادر المومني، المرجع السابق، ص: 24.

[5]- المرجع نفسه، ص: 24

[6]- أحمد كيلان عبد الله، المرجع نفسه، ص: 18.

كانت هذه بعض أهم مزايا جهاز الحاسوب التي بقدر مساهمتها الكبيرة في فتح آفاق واسعة أمام البشرية للابتكار والاختراع، فتحت في الوقت ذاته بابا واسعا أمام الأشخاص ذوي المصالح الضيقة وأصحاب الغايات غير المشروعة لتوظيفها في ارتكاب جرائمهم.

الفرع الثاني: مكونات الحاسوب

يتكون الحاسوب من مكونات مادية (Computer Hardware) تتمثل في مجموع الأجهزة المكونة له، وأخرى منطقية (Computer Software) تتمثل في مجموع البرمجيات، غير أن هذه المكونات لا قيمة لها دون وجود المستخدمين، وهم الأشخاص الذين يتعاملون معها لأهداف خاصة بهم تختلف من مستخدم لآخر.

أولا: المكونات المادية (Computer Hardware): يتكون الحاسوب من مجموعة وحدات لكل منها وظيفة محددة، وتتصل مع بعضها البعض بشكل يجعلها تعمل كنظام متكامل من أجل تأدية ثلاث عمليات رئيسية (الإدخال، المعالجة والتخزين، الإخراج)، وهي العمليات التي سنتعرف عليها تباعا عل النحو الآتي:

01- وحدات الإدخال (Input Unit): تعمل هذه الوحدات على إدخال المعطيات المراد معالجتها من الوسط الموجودة فيه إلى ذاكرة الحاسوب،[1] وتتيح للمستخدم التفاعل مع الجهاز والتعامل معه بحكم دورها الوظيفي المتمثل في استقبال البيانات وتمريرها إلى داخل الحاسوب، تتكون هذه الوحدات من عدة أجهزة أهمها: لوحة المفاتيح (Key Board)، الفأرة (Mousse)، مشغل الأقراص (Disk Drive)، الماسح الضوئي (Scanner)، إضافة إلى الأقراص المرنة والممغنطة والدسكات.[2]

تستخدم حاليا وحدات إدخال عالية الجودة والسرعة، مثل الفأرة، وشاشات الكمبيوتر التي تعمل باللمس (Touche screen)، وتقوم بقراءة الوثائق المكتوبة والخرائط المرسومة، والصور التي تحولها إلى إشارات ترسلها إلى أجهزة الكمبيوتر لقراءتها، كما توجد وحدات للتعرف على الحروف

[1]- انتصار نوري الغريب، المرجع السابق، ص: 16.

[2]- علي عبود جعفر، المرجع السابق، ص: 40.

والعلامات ضوئيا، تستخدم بكثرة في شركات الطيران والمؤسسات التجارية، من أجل وضع الأسعار وبيانات التخزين على السلع.[1]

02- وحدة المعالجة المركزية (Central Processing Unit): يشار لها اختصارا بـ (CPU)، وتعتبر بمثابة العقل المسيطر على عمل باقي الوحدات المكونة لجهاز الحاسوب، إذ تتم فيها جميع العمليات الحسابية أو المنطقية،[2] وتتكون هذه الوحدة من وحدتين رئيسيتين هما:

أ- وحدة التحكم والسيطرة (Control Unit): وهي عبارة عن دوائر إلكترونية تتحكم في عمليات تنفيذ التعليمات، وعمليات الإدخال والإخراج والتخزين والمعالجة داخل الحاسوب،[3] فهي تعمل مثل نظام الأعصاب المركزي لباقي وحدات الحاسوب في حالة التشغيل.[4]

ب- وحدة الحاسب والمنطق (Arithmetic and Logic Unit): تقوم بتنفيذ العمليات الحسابية (الطرح، الضرب، القسمة والجمع) والمنطقية (المقارنة بين قيمتين) على البيانات الواردة إليها.[5]

ج- وحدة الذاكرة (Memory Unit): وهي الوحدة التي تتم فيها عمليات تخزين المعلومات الواردة للجهاز، بحيث توجد بالحاسبات الشخصية عدة أنواع لهذه الوحدة هي:

*** الذاكرة المؤقتة (Random Access Memory):** وتسمى بذاكرة القراءة والكتابة، يرمز لها اختصارا بـ (RAM)، تستخدم لتخزين البرامج والبيانات التي تقع تحت المعالجة، أي أن محتويات هذه الذاكرة قابلة للتعديل (حذف، إضافة، تغيير)، غير أنها تفقدها بمجرد انقطاع التيار الكهربائي عنها.[6]

*** ذاكرة القراءة فقط (Read only Memory)**: تعرف اختصارا بـ (ROM)، وتعني أن الحاسب يستطيع قراءة البيانات المخزنة به، غير أنه لا يمكنه الكتابة عليها، عكس الذاكرة العشوائية، وتتم

---

[1]- محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007، ص 19.

[2]- محمد الدريني، مقدمة في أساسيات الحاسب، ط1، معهد الإدارة العامة، المملكة العربية السعودية، 1991، ص: 10.

[3]- المرجع نفسه، ص: 12.

[4]- يحيى مصطفى حلمي، الحاسبات الإلكترونية، مكتبة عين شمس، القاهرة، 1996، ص: 70.

[5]- مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009، ص: 33.

[6]- علي حسن الطوالبة، المرجع السابق، ص: 19.

برمجة هذه الذاكرة (تخزينها بالبيانات المطلوبة) أثناء مرحلة التصنيع، ولا يمكن تخزين أي معلومات جديدة أثناء استخدامها، لذلك تمتاز هذه الذاكرة بعدم محو بياناتها المخزنة عند فصل التيار الكهربائي عن الحاسب.[1]

* **الذاكرة المساعدة (Auxiliary Memory Unit):** وتسمى أيضا بالذاكرة الخارجية، وهي عبارة عن وحدة ثانوية لتخزين المعلومات والبرامج، تتمثل في مختلف وسائط التخزين التي يتعامل معها المستخدم بشكل مباشر مثل: القرص الصلب، القرص المرن، القرص المضغوط، وتعد من أكثر الوسائل التي تساهم في نشر الفيروسات بين المستخدمين عند استعمالها في تبادل المعطيات المصابة بالفيروس، فتنقل العدوى للجهاز المتصل به.[2]

03- وحدات الإخراج (Output Unit): عكس وحدات الإدخال التي تشكل واسطة اتصال بين الوسط الخارجي والحاسب، فإن وحدات الإخراج تعمل على إيصال الحاسب بالوسط الخارجي فتنقل النتائج المستخرجة حلولا كانت أم معالجات من وحدة المعالجة المركزية إلى الخارج،[3] مثل الشاشة، الطابعة ومشغلات الأقراص.

ثانيا: مكونات منطقية (Computer Software): إلى جانب المكونات المادية للحاسب الآلي هناك مكونات معنوية، تكتسي أهمية بالغة، كونها تمثل الروح بالنسبة للحاسب الآلي، ويطلق عليها تسمية (Software)، التي يُترجمها البعض بالبرمجيّات، والبعض الآخر بالمكونات غير المادية، وغيرهم بالكيان المنطقي، وهناك من يطلق عليها تسمية المكونات المعنوية.

ويعرف الكيان المنطقي بأنه: "مجموعة البرامج والأساليب والقواعد، وعند الاقتضاء الوثائق المتعلقة بتشغيل وحدة معالجة البيانات"،[4] وتشمل هذه المكونات إضافة إلى برمجيات الحاسوب المعلومات والمعطيات.

---

[1]- مصطفى محمد موسى، المرجع السابق، ص: 43.

[2]- محمد خليفة، المرجع السابق، ص: 23.

[3]- علي عبود جعفر، المرجع السابق، ص: 43.

[4]- رشا مصطفى أبو الغيط، الحماية القانونية للكيانات المنطقية، ملتقى الفكر، الإسكندرية، 2000، ص: 05.

01- برمجيات الحاسوب: يشير مصطلح البرمجيات إلى مجموعة البرامج أو التعليمات المرشدة لمكونات الحاسب المادية للقيام بعملها، والاستجابة لأوامر المستخدمين، وكيفية معالجتها للبيانات، فالحاسب بدون برمجيات مجرد كتلة من السيليكون والبلاستيك والمعدن، لذلك تعتبر أجهزة الحاسب بمثابة السلعة، بينما تشكل البرمجيات محور الإثارة والمال، ومعدل تطورها يحدد بشكل كبير آفاق تطور ثورة التقنية الحديثة.[1]

ورغم الخلط بين مصطلحي البرمجيات (Software) والبرنامج (Program)، إلا أن الأولى أعم وأشمل من الثانية، إذ يدخل في مفهوم برمجيات الحاسوب أمورا أخرى غير البرنامج، كالوثائق والمستندات والمواد المساعدة، وهي مواد مكتوبة في صورة كتيبات أو منشورات، مهمتها شرح البرنامج وتيسير فهمه ومساعدة مستعمليه على كيفية تشغيله، كما يندرج ضمن مفهوم البرمجيات كل الوثائق والمستندات التي تنتج في مرحلة تصميم البرنامج وتطويره،[2] وتنقسم برمجيات الحاسوب إلى قسمين:

أ- برمجيات النظم أو التشغيل (Système Software): وهي مجموعة القواعد أو التعليمات التي تمثل النظام التشغيلي للحاسوب، وتسيطر على العمليات الأساسية للأداء الآلي داخله، وتساعد أجزائَه على العمل سويا،[3] إذ تتحكم في جميع عمليات الحاسوب، بدءا باستقبال البيانات من وحدات الإدخال، إلى التحكم في المعلومات المُرسَلة إلى وحدات الإخراج، كما تُتابع استخدام الذاكرة وتخزين البيانات على الأقراص الثابتة، وتُعَد إصدارات ميكروسوفت المعروفة بالنوافذ (Windows) أكثر أنظمة التشغيل المستخدمة لأجهزة الحاسوب[4] إضافة إلى بعض البرامج الأخرى مثل برامج ترجمة اللغات.

ب- البرمجيات التطبيقية (Applications Software): وهي برامج تُبيّن للحاسوب كيفية القيام بأعمال محددّة لفائدة المستخدم، فهي مُصَممة لأداء وظائف معينة استجابة لمتطلبات العملاء،

[1]- علي جعفر عبود، المرجع السابق، ص: 44.

[2]- فاروق الحفناوي، المرجع السابق، ص 79.

[3]- انتصار نوري الغريب، المرجع السابق، ص: 35.

[4]- مصطفى محمد موسى، المرجع السابق، ص: 50.

مثل: البرامج المستخدمة في البنوك لمسك حسابات العملاء، أو الربط بين فروع البنك،[1] وكل برنامج منها يقوم بمهام محددة، مثل برمجيات تحرير النصوص ومعالجة الكلمات (Word) أو برمجيات الجداول والمحاسبة (Excel)، أو برنامج تحرير الصور وتصميم الرسوم، وغيرها.

02- المعلومات: المعلومة اسم مشتق من المصدر"علم"، وهو نقيض الجهل، وتعني: "المعرفة والتعليم والإدراك واليقين والإرشاد والوعي"، يقابلها في اللغة الفرنسية "Information"، وأصلها الكلمة اللاتينية "Informatio"، وتدل على عملية الإبلاغ أو النقل أو التوصيل،[2] وقد عرَفها معجم لاروس (Dictionnaire Larousse) بأنها: "الأخبار والتحقيقات وكل ما يؤدي إلى كشف الحقائق وإيضاح الأمور".[3]

أما اصطلاحا فتعرف بأنها: "ترجمة للبيانات ومعالجتها، وهي قابلة للتخزين والاسترجاع والتشكيل"،[4] أو هي: "تعبير يستهدف جعل رسالة قابلة للتوصيل إلى الغير عن طريق علامة أو إشارة من شأنها أن توصل المعلومة لهذا الغير".[5]

03- المعطيات: وتعني البيانات، وتدل على شيء مُعْطى مُسْبقا أو مُسَلم به أو معروف، يقابلها في اللغة اللاتينية DATUM، وجمعها DATA، وهو المصطلح المستعمل في اللغة الإنجليزية، أما في اللغة الفرنسية فتقابلها كلمة "Données"، وهو المصطلح الذي استعمله المشرع الجزائري للدلالة على البيانات.[6]

هكذا يظهر الفرق واضحا بين المعلومات والمعطيات، فالمعطيات عبارة عن أرقام وكلمات ورموز وحقائق وإحصائيات خام، لا علاقة لها ببعضها البعض، ولم تخضع بعد لعملية التفسير أو

---

[1]- فاروق الحفناوي، المرجع السابق، ص: 79.

[2]- غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016، ص: 59.

[3]- يحيى عطوة الزنط، الممارسات العملية لأمن نظم المعلومات الحكومية ومنهجية مكافحة الجرائم السيبرانية، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2022، ص: 30.

[4]- العياشي زرزار، كريمة غياد، المرجع السابق، ص: 20.

[5]- حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد 1، 1990، ص: 4.

[6]- غنية باطلي، المرجع نفسه، ص: 70.

التجهيز للاستخدام، وقد سُميت بالمعطيات لأنها تُعطى للحاسب الآلي لمعالجتها وتقديمها لمتلقيها كمعلومة مُخَزّنة،[1] أما المعلومات فهي المعنى الذي يُستخلص من المعطيات عن طريق العُرف أو الاتفاق أو الخبرة أو المعرفة، وبعبارة أخرى فإن المعطيات هي معلومات في حالة سكون، وأن المعلومات معطيات في حالة معالجة، وهو ما جعل الكثير من الباحثين يطلق مصطلح المعلومات على الاثنين معا.

وعلى غير العادة، عمد المشرع الجزائري إلى وضع تعريف للمعطيات ضمن المادة الثانية الفقرة ج من القانون 09-04،[2] بالقول أنها: "كل عملية عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها".

ونظرا لعلاقة الكيانات المنطقية بحياة الأشخاص ونشاط المؤسسات، وما يتطلبه ذلك من حفاظ على سرية المعلومات المتداولة لإبعادها عن القرصنة، فهي تحتاج إلى الحماية القانونية، ومن هنا ظهرت الحاجة إلى تشريعات خاصة لحماية برامج ونظم الحاسوب وشبكة الإنترنت.

المطلب الثاني

تكنولوجيات الإعلام والاتصال

أضحت الحواسيب ضرورة حتمية في مجالات حياة الإنسان المعاصرة من اقتصاد، خدمات واتصالات، وأصبحت تكنولوجيات الإعلام والاتصال أداة هامة في تحديد القرارات السليمة.

وبظهور الأجهزة والوسائط الناتجة عن اندماج تكنولوجيا المعلومات مع تكنولوجيا الاتصال وصولا إلى الاعتماد على الذكاء الاصطناعي برز مصطلح تقنية المعلومات الحديثة أو تكنولوجيات الإعلام والاتصال، وهو ما سنحاول توضيحه.

---

[1]- محمد خليفة، المرجع السابق، ص: 88.

[2]- القانون 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية لسنة 2009، العدد 47.

الفرع الأول: مفهوم تكنولوجيات الإعلام والاتصال

عرفت تكنولوجيات الإعلام والاتصال عديد التسميات منذ أول ظهور لها، إذ بعد أن وُصِفت في بداياتها بالتكنولوجيا الحديثة للمعلومات والاتصال (NTIC)، تم حذف منها مصطلح الحداثة لتصبح تكنولوجيا المعلومات والاتصال (TIC)، تماشيا وزوال هذه الصفة بعد تسويق أول حاسوب عُرف باسم (ALTAIR).[1]

أولا: تعريف تكنولوجيات الإعلام والاتصال: يستعمل هذا المصطلح في عدة تخصصات، مثل الرياضيات، الإعلام الآلي، الاتصال، الأدب، علم الاجتماع، علم النفس، الفلسفة وغيرها من العلوم، فهو مصطلح متعدد المعنى والتخصص.[2]

وللوصول إلى تعريف دقيق لهذه التقنية، لابد من الإحاطة بكل عنصر من عناصرها (التكنولوجيا، الإعلام، الاتصال، تكنولوجيا الإعلام، تكنولوجيا الاتصال):

01- تعريف التكنولوجيا (Technology)

أ- لغة: يرجع أصل كلمة تكنولوجيا (Technology) إلى اليونانية، وتتكون من شقين أولهما (Techno) وتعني التشغيل الصناعي، والثاني (Logos) وتعني العلم أو المنهج، وبالجمع بينهما يكتمل المعنى "علم التشغيل الصناعي".[3]

ب- اصطلاحا: تعرف التكنولوجيا حسب معجم (Webster) بأنها: "اللغة التقنية والعلم التطبيقي والطريقة الفنية لتحقيق غرض عملي، فضلا عن كونها مجموعة الوسائل المستخدمة لتوفير كل ما هو ضروري لمعيشة الناس ورفاهيتهم"،[4] وتعرف كذلك بأنها: "عملية أو مجموعة من العمليات

---

[1]- أحمد داودي، تأثير تكنولوجيا المعلومات في تحسين صورة المؤسسة (دراسة ميدانية)، المركز الأكاديمي للنشر، الإسكندرية، 2022، ص: 17.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 62.

[3]- غسان قاسم اللامي، إدارة التكنولوجيا، ط1، دار المناهج، عمان، الأردن، 2006، ص: 22.

[4]- محمد الصيرفي، إدارة تكنولوجيات المعلومات، ط1، دار الفكر الجامعي، الإسكندرية، 2009، ص: 13.

تسمح من خلال طريقة واضحة للبحث العلمي بتحسين التقنيات الأساسية، وتطبيق المعارف العلمية، من أجل تطوير الإنتاج الصناعي".[1]

02- تعريف الإعلام (l'information):

أ- لغة: الإعلام مشتق من العِلم، يقول العرب: اسْتَعْلَمه الخبر فأعْلَمَه إيّاه، بمعنى صار يعرف الخبر بعد أن طلب معرفته، فيكون معناه نقل الخبر.[2]

ب- اصطلاحا: عرفه الأستاذ حامد زهران بأنه: "عملية نشر وتقويم معلومات صحيحة وحقائق واضحة، وأخبار صادقة، وموضوعات دقيقة، ووقائع محددة، وأفكار منطقية، وآراء وحجج للجماهير، خدمة للصالح العام"،[3] فيما عرفه الأستاذ حمزة عبد المطلب بأنه: "تزويد الناس بالأخبار الصحيحة والمعلومات السليمة والحقائق الثابتة التي تساعدهم على تكوين رأي صائب في واقعة معينة، أو مشكلة، بحيث يعتبر هذا الرأي تعبيرا موضوعيا عن عقلية الجماهير وميولاتهم".[4]

03- تعريف الاتصال (Communication)

أ- لغة: كلمة مشتقة من مصدر الفعل وصل، وتعني الربط بين كائنين أو شخصين، إذ ورد في لسان العرب: "الوصل ضد الهُجْران، وخِلاف الفصْل"،[5] وكلمة (Communication) مشتقة من الأصل اللاتيني (Communis)، وتعني المشاركة وتكوين العلاقة، فهو إذا عملية تتضمن المشاركة والتفاهم حول فكرة أو موضوع لتحقيق هدف أو برنامج.[6]

---

[1]- Jean-Luk Charon, Sabine Sépari, Organisation et gestion de l' entreprise, éprouve n° 3, 2éme édition, Paris, 2001, P: 374.

[2]- زهير احدادن، مدخل إلى علم الإعلام والاتصال، ديوان المطبوعات الجامعية، الجزائر، 1993، ص: 13.

[3]- خير الدين علي عويس، عبد الرحيم عطا حسن، الإعلام الرياضي، ج 1، ط1، مركز الكتاب للنشر، القاهرة، 1998، ص: 20.

[4]- عبد المطلب حمزة، الإعلام والدعاية، دار الفكر العربي، القاهرة، 1984، ص: 60.

[5]- ثريا تيجاني، القيم الاجتماعية والتلفزيون في المجتمع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2011، ص: 15.

[6]- مي العبد الله، نظريات الاتصال، ط2، دار النهضة العربية، بيروت، 2010، ص: 23.

ب- اصطلاحا: عرّف قاموس أوكسفورد (Oxford Dictionary) الاتصال بأنه: "نقل وتوصيل أو تبادل الأفكار والمعلومات بالكلام أو الكتابة أو الإشارة"،[1] وعرفه بعض الفقه بأنه: "فن نقل المعلومات والأفكار والمواقف من شخص إلى آخر"،[2] فهو يدل على تبادل الأفكار والمعلومات بين طرفين أو أكثر عن طريق أساليب ووسائل مختلفة.

وبدوره عرَف المشرع الجزائري الاتصالات الإلكترونية بأنها: "أي تراسل أو إرسال أو استقبال لعلامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية".[3]

ج- الفرق بين الإعلام والاتصال: رغم اتفاق العمليتين من حيث نقل المعلومة إلى الفرد أو المجتمع، إلا أنهما يختلفان في بعض الجوانب، أهمها:

* تتضمن عملية الإعلام عنصرين أساسين؛ هما المرسل والمستقبل دون وجود تفاعل بينهما عكس عملية الاتصال التي تتطلب قيام المستقبل بدور إيجابي يتفاعل من خلاله مع المرسل عن طريق تبادل الأفكار والمعلومات.[4]

* اعتناء الإعلام أساسا بالخبر والوسيلة والجمهرة، وينطبق ذلك على الصحيفة والمجلة والإذاعة والتلفزيون، بينما تغيب الجمهرة في وسائل الهاتف والفاكس والتلكس، بما يجعلها وسائل اتصال لا وسائل إعلام.[5]

الأمر الذي يتضح من خلاله أن مفهوم الاتصال أعم وأشمل من مفهوم الإعلام، فهذا الأخير جزءٌ لا يتجزأ من الاتصال.

---

[1]- يحيى عطوة الزنط، المرجع السابق، ص: 70.

[2]- عصام سليمان الموسى، مدخل إلى الاتصال الجماهيري، ط 6، إثراء للنشر، عمان، الأردن، 2008، ص: 6.

[3]- راجع المادة 02 من القانون رقم 09-04.

[4]- علي فلاح الضلاعين وآخرون، مقدمة في الإعلام، دار الإعصار للنشر والتوزيع، الأردن، 2015، ص: 15.

[5]- كمال عايد، تكنولوجيا الإعلام والاتصال وتأثيراتها على قيم المجتمع الجزائري، أطروحة دكتوراه، كلية العلوم الإنسانية والاجتماعية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2016-2017، ص: 32.

وقد عرفت وسائل الاتصال ثورة ساهمت في تطويرها، بدءا بالاتصالات السلكية واللاسلكية مرورا إلى التلفزيون، ثم الاعتماد على الأقمار الصناعية والألياف البصرية، وصولا إلى الاتصالات الحديثة،[1] ولا يزال أفقها غير محدد.

04- تكنولوجيات الإعلام: وهي تقنيات تسمح بصنع أو إنتاج المعلومة، وتحوي كلمة إنتاج (حجز ومعالجة وتخزين ونشر).[2] أو هي: "مدًى واسع من القدرات والمواد التي تُستخدم لإنتاج وتخزين ونشر واسترجاع المعلومات".[3]

عرفت وزارة التجارة والصناعة البريطانية تكنولوجيا الإعلام بأنها: "الحصول على البيانات ومعالجتها وتخزينها وتوصيلها وإرسالها في صورة معلومات مصورة أو صوتية أو مكتوبة أو في صورة رقمية، بواسطة توليفة من الآلات الإلكترونية وطرق المواصلات السلكية واللاسلكية".[4]

05- تكنولوجيات الاتصال: عرفتها هيئة الأمم المتحدة بأنها: "الوسائل الإلكترونية التي تقوم بمعالجة وتوصيل المعلومات التي توفر أو تدعم الأنشطة الاقتصادية وتطبيقاتها، باستخدام أجهزة الكمبيوتر والبرمجيات والاتصالات السلكية واللاسلكية، ولذلك يرتبط لفظ الاتصالات بالمعلومات".[5]

كان الاتصال في المرحلة البدائية يتم بنقل الأخبار من شخص لآخر عن طريق الكلام، ثم استعمل الفرد علامات يقع الاتفاق عليها مسبقا، كإشعال النار وصوت الدف، للإشعار بالخطر أو الفرح، غير أن ارتباط هذه الوسائل بحاستي السمع والبصر جعلها لا تغير كثيرا من نوعية الاتصال وطابعه الشخصي، إلى غاية ظهور الكتابة والورق، ثم الطباعة، فأصبح الخبر يُكتب ويُوزع على جهات عديدة عن طريق الصحافة، وصارت الأحداث تُسجل وتُحفظ وتُنقل بين الأجيال، وتحول الاتصال إلى طابع جماعي، لتأتي مرحلة العصر الحديث الذي شهد استعمال

---

[1]- الاتصالات الحديثة: "وتعني كافة الأنشطة والوسائل المتعلقة بعملية التبادل الالكتروني للمعلومات بين حاسبات آلية مرتبطة ببعضها"، العياشي زرزار، كريمة غياد، المرجع السابق، ص: 26.

[2]- Robert Reix, Système d'information et management des organisations, Vuibert , France, 4éme éd, 2002, p: 66.

[3]- مصطفى عليان ربحي، إيمان فاضل السامرائي، تسويق المعلومات، دار الصفاء للطباعة والنشر، عمان، الأردن، 2004، ص: 21.

[4]- قوي بوحنية، الاتصالات الإدارية داخل المنظمات المعاصرة، ديوان المطبوعات الجامعية، الجزائر، 2010، ص: 86.

[5]- يحيى عطوة الزنط، المرجع السابق، ص:68.

وسائل أخرى أكثر سرعة لنقل المعلومة، كالراديو والتلفاز والهاتف، ثم ظهر الحاسب الآلي لتسجيل المعلومات وحفظها ونقلها عبر شبكات تغطي العالم وتقرب القارات لتجعلها بمثابة قرية صغيرة".[1]

وتتجلى أهمية الاتصال في كونه وسيلة لنقل وتداول المعلومات بين مختلف الأفراد والفئات، رغم ما تتميز به كل فئة من مفردات لغوية ورموز مختلفة، ولضمان نجاح هذه العملية لابد من تحقيق التفاهم والتعاون بين المتصلين مهما اختلفت بيئاتهم، إذ تمثل هذه العملية أحد العناصر الأساسية في الاجتماع والتفاعل الإنساني بصفة عامة.

06- تكنولوجيات الإعلام والاتصال: وهي مجموعة التكنولوجيات المتقدمة التي أتاحتها الحاسبات الإلكترونية الدقيقة والاتصالات السلكية واللاسلكية المتطورة بواسطة الأقمار الصناعية والمحطات الأرضية والبحرية للاتصالات، وشبكات بنوك المعلومات الإلكترونية، وما تستخدمه من وسائل اتصال متطورة، مباشرة وغير مباشرة،[2] أو كما عرفها الدكتور محمد فتحي عبد الهادي: "دمج تكنولوجيا التخزين والاسترجاع مع تكنولوجيا الاتصال، فهي علم قائم بذاته، يهتم بمعالجة وتوصيل المعلومات باستخدام وسائل الاتصال لنقلها إلى المستفيد".[3]

برزت تكنولوجيات الإعلام والاتصال كمزيج بين تكنولوجيات معالجة البيانات وتكنولوجيات الاتصالات السلكية واللاسلكية، فالأولى تمنح القدرة على معالجة وتخزين المعلومات، أما الثانية فهي الحامل لتوصيلها، هذا المزيج تم إحداثه بفضل المكونات الإلكترونية الدقيقة وتجهيزاتها المعقدة.

وتجدر الإشارة إلى أن مصطلح "تكنولوجيا الإعلام والاتصال" أشمل وأدق من الترجمة المتداولة "تكنولوجيا المعلومات والاتصال"، فالإعلام ينطوي على مجموعة أنشطة من بينها نشاط نقل المعلومات وتداولها، فهو إذًا يشمل المعلومات، وبالمقابل فإن المعلومات لا تشمل الإعلام.

---

[1]- العياشي زرزار، كريمة غياد، المرجع السابق، ص: 36.

[2]- محمد الهوش أبو بكر، تقنية المعلومات ومكتبة المستقبل، مكتبة الإشباع، الجماهيرية العظمى، 1996، ص: 222.

[3]- أحمد داودي، المرجع السابق، ص: 22.

ثانيا: خصائص تكنولوجيات الإعلام والاتصال: تتميز تكنولوجيات الإعلام والاتصال بعدة خصائص، أهمها:

01- التفاعلية: وتعني إمكانية تبادل الأدوار بين المرسل والمستقبل، فلا يقف دور المستقبل عند حدود التلقي السلبي للرسالة، بل يصبح مشاركا متفاعلا في عملية الاتصال، يُرسل ويَستقبل المعلومات في الوقت ذاته،[1] وهو ما يسمح بخلق جو من التفاعل بين الأفراد والمؤسسات، ويؤدي إلى إمكانية تعدد المشاركين في عملية الاتصال.

02- الشيوع والانتشار: تخطى الربط بين وسائل الاتصال الحديثة الحدود الإقليمية وصار عالميا، أين أصبح بالإمكان الاتصال عن طريق الهاتف المحمول بأي مكان في العالم، كما تعددت قنوات البث التلفزيوني الفضائي.[2]

03- اللاَتزامنية: وتعني إمكانية إرسال المعلومات بين أطراف عملية الاتصال دون شرط تواجدهم وقت إرسالها، مما يمكنهم من استقبال المعلومات في الجهاز ثم تصفحها وقت الحاجة، ففي نظام البريد الإلكتروني مثلا يستطيع منتج الرسالة أن يرسلها مباشرة في أي وقت دون الحاجة لتواجد مستقبلها على الخط.[3]

04- اللاَجماهيرية: لم تعد وسائل الاتصال تعتمد على مخاطبة الجماهير من خلال رسائل عامة فحسب، بل صار بإمكانها توجيه رسائل إلى فرد محدد أو أو فئة معينة تبعا لاهتماماتها الخاصة، فتحولت بذلك من نطاق العمومية إلى نطاق خصوصية الرسالة حسب حاجة مستقبلها.[4]

---

[1]- ربيحة نبار، تكنولوجيا المعلومات والاتصالات (الخصائص والتأثيرات)، مجلة الباحث في العلوم الإنسانية والاجتماعية، مجلد 9، عدد 2، 2018، ص:91.

[2]- رحيمة الطيب عيساني، الوسائط التقنية الحديثة وأثرها على الإعلام المرئي والمسموع، الرياض، 2010، ص: 30.

[3]- ربيحة نبار، المرجع السابق، ص: 92.

[4]- محمد دفون، تكنولوجيا الإعلام والاتصال واستخداماتها، مجلة التراث، جامعة الجلفة، العدد 16، الجزائر، 2014، ص: 219.

05- قابلية التحويل: وتعني قدرة وسائل الاتصال على نقل المعلومات من وسيط لآخر باستعمال تقنيات التحويل الإلكترونية، مثل تحويل رسالة مسموعة إلى رسالة مطبوعة أو العكس.[1]

06- قابلية الحركة: وتعني إمكانية بث المعلومات واستقبالها من أي مكان إلى أي مكان آخر أثناء حركة المرسل، دون الحاجة إلى تواجده في مكان ثابت.[2]

07- تقليص الوقت: تسمح تكنولوجيات الإعلام والاتصال بالنقل المباشر للمعلومات والمعطيات، وتتيح قواعد البيانات الضخمة الوصول إلى المعلومات المخزنة بيُسر وسُهولة، وفي أقل وقت.[3]

08- اقتصادية: تتجلى اقتصادية وسائل الإعلام والاتصال في أكثر من مستوى، فهي تحقق الاقتصاد في الوقت والتكلفة المادية، إذ تلعب تكنولوجيات الإعلام والاتصال أدوارا فعّالة لإنجاز الكثير من المهام بتكاليف منخفضة، فتكلفة البريد الإلكتروني مثلاً لا تُذكر إذا ما قورنت بتكلفة البريد العادي، وتكلفة الكتاب الإلكتروني أقل بكثير من تكلفة نظيره العادي.[4]

الفرع الثاني: شبكات الإعلام والاتصال

بعد التعرف على الحاسوب وتكنولوجيات الإعلام والاتصال وجب علينا التطرق لشبكات الاتصال، إذ بواسطتها ترتبط الحواسيب مع بعضها سواء على المستوى المحلي أو العالمي.

ولمساهمة الإنترنت بشكل لا نظير له في صناعة المعلومات وثورتها بحكم أنها أحد العناصر الرئيسية التي ترتكز عليها تكنولوجيات الإعلام والاتصال، سنحاول التعرف على شبكات المعلومات وأنواعها، ثم على شبكة الإنترنت باعتبارها أكبر شبكة معلوماتية.

أولا: تعريف شبكات الإعلام والاتصال وأنواعها: ترتبط شبكات الحاسوب ببعضها عن طريق شبكات محلية موجودة في الموقع نفسه، أو عن طريق حواسيب تفصل بينها مسافات واسعة.

---

[1]- نوال مغيزلي، تكنولوجيا الإعلام والاتصال في الجزائر (دراسة للمؤشرات وتشخيص للعقبات)، المجلة الجزائرية للأمن والتنمية، العدد 12، 2018، ص: 173.

[2]- أحمد داودي، المرجع السابق، ص: 25.

[3]- المرجع نفسه، ص: 25.

[4]- محمد دفون، المرجع السابق، ص: 220.

01- تعريف الشبكة: هي ربط لجهازين أو أكثر من أجهزة الحاسوب بواسطة خطوط سلكية أو لا سلكية، من أجل تناقل البيانات وتبادل المعلومات فيما بينها.[1]

وقد عرفت المادة الأولى من القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات الشبكة بأنها:[2] "مجموعة من النقاط التي تمثل عناصر كهربائية أو عناصر إلكترونية أو نهايات طرفية، أو حاسبات يتصل بعضها بوصلات، كما في الشبكات الكهربائية وشبكات الحاسب الآلي وشبكات الاتصال"، كما عرفت الوسيط الإلكتروني بأنه: "ارتباط بين أكثر من وسيلة لتقنية المعلومات الحديثة للحصول على البيانات والمعلومات الإلكترونية وتبادلها، ويقصد به شبكة الحاسب الآلي أو الإنترنت أو أي شبكة الكترونية أخرى".

02- أنواع شبكات الإعلام والاتصال: نتج عن تطور العلوم في مجال الحواسيب وتكنولوجيا المعلومات، وما رافقهما من تطور في الحاجات والمواصفات المرغوبة لأداء الأعمال ظهور نوعين رئيسيين من الشبكات، هما:

أ- الشبكة المحلية (Local Area Network): يرمز لها اختصارا بـ: (LAN)، وهي الشبكة التي تكون على مستوى مؤسسة واحدة أو عدة مؤسسات أو مباني متقاربة، لكنها وسط بيئة محلية واحدة، وتكون المسافة بين الحواسيب المرتبطة مع بعضها البعض قصيرة كالحرم الجامعي أو مركز الشرطة،[3] وذلك بهدف ضمان تدفق المعلومات والاتصالات داخل مباني تلك المؤسسة، إذ يستطيع هذا النوع من الشبكات نقل البيانات بسرعة عالية بين أجهزة موزعة في منطقة محدودة غالبا ما تكون في حدود 05 كلم^2،[4] وهناك نوعين من الشبكات المحلية:

---

[1]- سامي جلال فقي حسين، المرجع السابق، ص: 49.

[2]- تم اعتماد هذا المشروع إثر اجتماع مجلس الوزراء العرب في دورته 19 بالقرار رقم 490-د 19، بتاريخ: 08-10-2003، ثم مجلس وزراء الداخلية العرب في دورته الـ 21، أنظر: عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، ط1، منشورات الحلبي الحقوقية، لبنان، 2007، ص: 140.

[3]- جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002، ص: 5.

[4]- عامر ابراهيم قنديلجي، علاء الدين عبد القادر الجنابي، نظم المعلومات الإدارية، ط1، دار الميسرة، الأردن، 2005، ص: 313.

* **شبكة الخادم والعملاء:** وتتميز بوجود حاسب يسمى (Server) يقدم الخدمات من الشبكة إلى حواسيب أخرى ترتبط معه تسمى العملاء (Clients).

* **شبكة نظير لنظير:** وفي هذه الشبكة تكون كل الأجهزة متساوية ومتكافئة، وبإمكان أي جهاز فيها أن يكون خادما أو عميلا في الوقت نفسه، أي لا وجود لجهاز مميز عن غيره.[1]

ب- الشبكة الواسعة (Wide Area Network): يرمز لها اختصارا بـ: (WAN)، وهي شبكة تتكون من مجموعة كبيرة من الحواسيب موزعة في مناطق مختلفة، سواءً على مستوى القطر الواحد أو على المستوى العالمي، تستخدم هذه الشبكة عادةً الأقمار الصناعية في عملها، وتتميز برامجها ومعلوماتها بالتوسع واللاَمحدودية.[2]

وانطلاقا من تسميتها، تمتاز هذه الشبكة بتغطيتها لمساحة جغرافية واسعة، لذلك تُستخدم لاتصال المؤسسات المتباعدة جغرافيا باستعمال أجهزة وبرامج خاصة، إضافة إلى الوسائط المتعددة لنقل المعلومات، غير أن تشكيلها يحتاج إلى تكاليف باهظة.[3]

وتعتبر الإنترنت أكبر شبكة حواسيب واسعة النطاق، إذ تُغطي جميع أنحاء العالم، الأمر الذي يفرض علينا التطرق لها بشيء من التفصيل.

ثانيا: شبكة الإنترنت: كان لظهور شبكة الإنترنت أثر كبير في انتقال المعلومات وتداولها والاستفادة منها في وقت قياسي في أي مكان من العالم، كما ساهمت بشكل فعّال في صناعة المعلومات وإحداث ثورة رقمية، بما جعل منها أحد العناصر الرئيسية التي ترتكز عليها تكنولوجيا المعلومات، وأصبحت وسيلة للتعامل اليومي بين مختلف الطبقات والمجتمعات.

---

[1]- طارق الشدي، المرجع السابق، ص: 46.

[2]- أحمد كيلان عبد الله، المرجع السابق، ص: 24.

[3]- مزهر شعبان العاني، شوقي ناجي جواد، العملية الإدارية وتكنولوجيا المعلومات، ط1، إثراء للنشر والتوزيع، الأردن، 2008، ص: 202.

01- تعريف الإنترنت وتطورها التاريخي: أدى التطور الهائل في نظم المعلومات والاتصال إلى ظهور ما يعرف بشبكة الإنترنت، ومع ظهورها برزت أنماط جديدة من الجرائم التي ترتكب بواسطتها، وهي في تزايد مستمر بالموازاة مع تنامي التطور التكنولوجي.

أ- **تعريف شبكة الإنترنت (Internet):**[1] هي كلمة إنجليزية مختصرة، تتكون من مقطعين (Inter) اختصارا لكلمة (International) وتعني دولي أو عالمي، و(Net) اختصارا لكلمة (Network) وتعني الشبكة، فهي شبكة عالمية ضخمة تربط بين الملايين من أجهزة الحواسيب الآلية حول العالم وتحتوي على الآلاف من شبكات الحاسب المحلية والواسعة، ورغم عالمية هذه الشبكة، إلا أنها لا تخضع لملكية فرد أو مؤسسة أو دولة، إذ يمكن لأي شخص أن يتواصل معها بمجرد توافر مستلزمات الاتصال لديه.[2]

فبعد أن كان استعمال الإنترنت حكرا على وزارة الدفاع الأمريكية، ثم المؤسسة القومية للعلوم، أدى تطورها إلى اختفاء مفهوم التملك، وحل محله ما يسمى بمجتمع الإنترنت الافتراضي،[3] فهي بذلك حصيلة جهود مشتركة لعدد كبير من المنظمات والمعاهد التي تساهم بأنظمتها الحاسوبية ومواردها المختلفة في خدمتها وصيانتها وتحديثها، مما جعل منها ملكية تعاونية للبشرية بقدر إسهاماتهم فيها، دون أن تكون لها إدارة مركزية،[4] لذلك يصفها بعض الفقه بأنها فوضى تعاونية، ذلك أن كل شبكة مشتركة في الإنترنت لها قواعدها الخاصة وهيكلها التنظيمي، غير أنه لا يمكن لهذه الشبكات الاتصال فيما بينها إلا إذا كان هناك تعاونا بينها.[5]

---

[1]- هناك فرق بين الإنترنت (Internet) التي سبق شرحها، والإنترانت (Intranet) التي تعني استخدام التكنولوجيا والإنترنت في وسط مغلق، مثل الشركة التي تقيم الربط بين فروعها المختلفة باستخدام تقنية تصميم صفحات الإنترنت، حيث يتم وضع لوائح العمل بالشركة أو أسعار بيع منتجاتها أو التطبيقات الخاصة بها، لكي يستفيد منها موظفو البيع، أو أي بيانات أخرى تريد اطلاع موظفيها عليها، ولا يمكن لأي شخص آخر الاطلاع على تلك الصفحات، علي عبود جعفر، المرجع السابق، ص: 59.

[2]- علي عبود جعفر، المرجع السابق، ص: 60.

[3]- رمضان مدحت، جرائم الاعتداء على الأشخاص والإنترنت، ط1، دار النهضة العربية، القاهرة، 2000، ص:5.

[4]- علي عبود جعفر، المرجع نفسه، ص: 61.

[5]- عبد الفتاح بيومي حجازي، الأحداث والإنترنت، ط1، دار الفكر الجامعي، الإسكندرية، 2002، ص: 20-21.

ب- التطور التاريخي لشبكة الإنترنت: تعود بداية ظهور شبكة الإنترنت إلى ستينيات القرن الماضي، عندما عهدت وزارة الدفاع الأمريكية سنة 1964 إلى وكالة مشاريع الأبحاث المتقدمة (ARPANET) مهمة بناء شبكة اتصال خاصة لا يمكن قطعها أو تدميرها في حالة نشوب حرب مفاجئة أو وقوع عمليات تخريب، وتكون قادرة على مكافحة الكوارث والاستمرار في العمل حال حصول هجوم نووي، فأنشأت الوكالة سنة 1969 شبكة مخصصة لهذا الغرض سميت (ARPANET)، وكانت في بدايتها تربط بين مختلف مراكز الحاسوب وأنظمة الراديو والأقمار الصناعية الخاصة بالولايات المتحدة الأمريكية في جميع أنحاء العالم.[1]

ورغم أن ظهور الشبكة كان لغايات عسكرية مثلما سبق بيانه، إلا أنه بعد مدة وجيزة تطور المشروع وأصبح متاحا للاستعمالات السلمية، فمع حلول سنة 1983 استخدمت شبكة (ARPANET) بكثافة كبيرة خصوصا من طرف الجامعات، إلى أن بدأت تعاني من ازدحام يفوق طاقتها بشكل صار معه من الضروري إنشاء شبكة أخرى، فظهرت شبكة (MILNET) التي خُصِّصت لخدمة المواقع العسكرية فقط، في حين تولت شبكة (ARPANET) الاتصالات المدنية مع بقائها موصولة بشبكة (MILNET) من خلال برنامج بروتوكول اسمه (IP).[2]

وفي سنة 1986 تم ربط خمس شبكات أطلق عليها اسم شبكة (NSFNET)، والتي أصبحت فيما بعد حجر الأساس لنمو وازدهار الإنترنت في أمريكا، وتولت المؤسسة القومية للعلوم في الولايات المتحدة الأمريكية (NSF) مسؤولية إدارتها، حيث قامت بشراء حواسيب عملاقة وتوزيعها على كل مناطق الولايات المتحدة الأمريكية، مكونة بذلك شبكة قومية تعمل مع بعضها البعض، ومع حلول عام 1990 قررت حكومة الولايات المتحدة الأمريكية وقف استثمار مواردها المالية في تطوير شبكة الإنترنت، لتفسح المجال أمام وسائل التمويل الأخرى لإكمال بناء هذه الشبكة، وبالفعل فإن الحاجة الماسة لاستخداماتها التجارية أدت إلى تطويرها، حيث ابتدع عدد من الشركات الكبرى شبكاتهم العالمية، إضافة إلى الإصدار الأول من شركة موزاييك (MOSAIC) وما

[1]- عيسى طوني، التنظيم القانوني لشبكة الإنترنت، ط1، المنشورات الحقوقية، 2001، ص: 62.

[2]- هلال البياتي، استخدام الحاسبات الفنية وحمايتها، بحث مقدم إلى ندوة القانون والحاسوب، بغداد، 1998، ص: 24-25.

تبعه من إصدارات لشركات (نتسكيب) و(مايكروسوفت)، كل هذه الأمور أدت إلى تطور شبكة الإنترنت بالصورة التي نراها عليها اليوم.[1]

أشار تقرير وكالة الأمم المتحدة المتخصصة في تكنولوجيا الاتصالات (ITU) الصادر في ديسمبر 2021، إلى وجود نمو عالمي قوي في استخدام الإنترنت بلغ 4.9 مليار شخص من إجمالي عدد سكان العالم المقدر بـ: 7.89 مليار شخص نفس السنة، وهو ما يعكس اتصال 62% من السكان بشبكات الإنترنت، بينما نسبة 37% المتبقية (ما يمثل 2.9 مليار شخص) لم يستخدموا الانترنت قط، أغلبهم (96%) في البلدان النامية، وأضاف التقرير بأن 71% ممن تتراوح أعمارهم ما بين 15 و24 سنة على مستوى الصعيد العالمي يستخدمون الإنترنت، مقارنة بـ 7% من جميع الفئات العمرية الأخرى، ورجح التقرير أن السكان في المناطق الحضرية يستخدمون الإنترنت مرتين أكثر ممن يقطنون في المناطق الريفية، أي بنسبة 76% في المناطق الحضرية مقابل 39% في المناطق الريفية.[2]

وفي الجزائر، كشف بيان لوزارة البريد والمواصلات السلكية واللاسلكية أن عدد المشتركين بالإنترنت الثابت بلغ 4.5 مليون مشترك خلال شهر أكتوبر 2022، مبرزا وجود ارتفاع في عدد المشتركين مقارنة بإحصائيات السنوات السابقة، على النحو التالي:

- 3.7 مليون مشترك سنة 2020.
- 4.2 مليون مشترك سنة 2021.
- 4.5 مليون مشترك سنة 2022.

[1]- علي جعفر عبود، المرجع السابق، ص: 63.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 212

وأضاف البيان بأن الأهداف المرحلية لتنفيذ مخطط عمل القطاع تتمثل في توصيل ثلثي الأسر بالإنترنت الثابت نهاية سنة 2024، وأن الهدف المسطر نهاية هذه السنة (2022) يتمثل في بلوغ 4.7 مليون مشترك.[1]

02- استخدامات شبكة الإنترنت: تتعدد استخدامات الإنترنت في مجالات مختلفة لا يسع المجال لذكرها، لذلك سنكتفي باستعراض بعض الخدمات التي لها علاقة بموضوعنا، ومن بينها:

أ- **البريد الإلكتروني (E.MAIL):**[2] هو نظام للتراسل باستخدام شبكات الحاسب الإلكترونية يستطيع الأشخاص من خلاله إرسال أو استقبال الرسائل الإلكترونية صورة وصوتا، مما يغني عن إرسالها بطريقة تقليدية، وفي ذلك اختصار للوقت والتكاليف، كما يحتفظ فيه كل فرد بسرية مراسلاته، باعتبار أن لكل بريد إلكتروني كلمة سر يعلمها صاحبها الذي يقوم بإنشاء هذا البريد على الإنترنت دون سواه.[3]

يعتبر البريد الإلكتروني من أقدم وأشهر الخدمات التي تقدمها شبكة الإنترنت، ورغم فوائده العديدة، إلا أنه يمكن أن يتحول إلى قنبلة مدمرة لحياة الأفراد في حالة اختراقه وفضح أسرار صاحبه، إضافة إلى ما يمكن أن يرده من فيروسات مخربة ورسائل مزعجة.

ب- شبكة العنكبوت العالمية (WWW): تسمى أيضا بشبكة الويب العالمية، وهي اختصار لكلمة (The World Wide Web) وتعني (النسيج عالمي الانتشار)، والويب عبارة عن نظام فرعي من الإنترنت مؤلف من كم هائل من النصوص والصور والعينات الصوتية ولقطات الفيديو، وغيرها، يمكن للمستخدم أن يتصفح محتوياته من خلال برنامج يسمى متصفح أو مستعرض، وأن يختار المواقع التي يرغب في زيارتها، إضافة إلى القيام بنشاطات أكاديمية كالبحث العلمي، أو اجتماعية

---

[1]- جريدة البلاد، الرابط الإلكتروني: https://.elbilad.net/s@gz4ovcar109356، تاريخ الاطلاع: 16-10-2022، الساعة: 15:20.

[2]- E.MAIL: اختصار لكلمة (Electronic Mail)، وتعني البريد الإلكتروني.

[3]- جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، 1992، ص: 15.

كالتعارف والتخاطب والتراسل، أو ترفيهية كالألعاب وقراءة الصحف والمجلات، أو اقتصادية كالتسوق وشراء الأسهم وغيرها، ولكل موقع من مواقع الويب عنوان خاص به.[1]

ويعود سبب تسميتها بشبكة العنكبوت العالمية إلى تداخل الروابط العديدة بين الوثائق التي تشكل مواقع هذه الشبكة المنتشرة عبر العالم بطريقة تشبه تداخل شبكة العنكبوت، فهي تجمع كافة الموارد المتعددة التي تحتوي عليها شبكة الإنترنت، للبحث عن كل ما في الشبكات المختلفة وإحضارها نصا وصورة وصوتا.[2]

ت- التواصل عن بعد (Telnet): هو خدمة تسمح للمستخدم بالاتصال عبر حاسوبه مع أي شخص في العالم باستعمال شبكة الإنترنت، وهو ما شجع العاملين على إنجاز أعمالهم عن بعد.[3]

وفي الوقت الراهن تعتبر مواقع التواصل الاجتماعي أهم وسيلة للتواصل بين الأفراد على مختلف شرائحهم،[4] وبصور متعددة كالرسائل أو الصور أو المقاطع المرئية أو الصوتية ...إلخ.

ث- التجارة الإلكترونية: تعتبر شبكة الإنترنت سوقا مفتوحا للبيع والشراء، إذ يمكن لأي تاجر الإعلان عن سلعته صورة وصوتا، كما يمكن للزبون أن يختار البضاعة التي تناسبه ويسدد قيمتها عن طريق الدفع الإلكتروني.[5]

ج- المجموعات الإخبارية: هي مساحات تغطي مواضيع يصعب حصرها، سواء أكانت علمية أم ثقافية أم رياضية، وغيرها، حيث يتحاور المستخدمون فيما بينهم حول مواضيع مختلفة.[6]

---

[1]- حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، 2009، ص: 24.

[2]- محمد المنشاوي، جرائم الإنترنت في المجتمع السعودي، أكاديمية نايف العربية للعلوم الأمنية، 2003، ص: 33.

[3]- علي حسن الطوالبة، المرجع السابق، ص: 36.

[4]- "بدأت مواقع التواصل الاجتماعي في الظهور سنة 2004 وازدادت أعدادها فيما بعد، أشهرها وأكثرها انتشارا واستخداما في العالم موقع فيس بوك، المسنجر، الانستغرام، الواتس آب، الفايبر وتويتر"، بهاء المري، المرجع السابق، ص: 39.

[5]- أحمد كيلان عبد الله، المرجع السابق، ص: 27.

[6]- محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، ط1، دار النهضة العربية، القاهرة، 2003، ص: 124.

ح- محركات البحث (Search Engines): هي برامج حاسوبية تساعد في الحصول على المعلومات المخزنة على شبكة الإنترنت، من خلال إخبار محرك البحث باسم الموضوع الذي يهم المستخدم فيزوده المحرك بقائمة المواقع التي تتطابق مع موضوعه، توجد عدة محركات بحث أشهرها Google، Yahoo.[1]

خ- الألعاب: تحتوي شبكة الإنترنت على العديد من الألعاب التي يمكن أن يشترك فيها أشخاص من جميع أنحاء العالم، مثل لعبة الشطرنج بين شخصين في بلدين مختلفين، أو الألعاب القتالية التي تؤثر سلبا على سلوك الأطفال والمراهقين.[2]

د- الخدمات المالية والمصرفية: هي خدمات تتيح للعملاء استعمال شبكة الإنترنت لإدارة حساباتهم وإنجاز أعمالهم المصرفية من داخل منازلهم أو مكاتبهم، وفي الوقت الذي يختارونه مثل القيام بالتحويلات المالية من حساب إلى آخر.

ذ- خدمة تحويل أو نقل الملفات (File Transfer Protocol): تعتبر إحدى الطرق التي تستخدم في تحميل ونقل الملفات بين أجهزة الحاسوب المتصلة بالشبكة، إذ يمكن للمستخدم من خلالها نسخ الملفات من حاسوب إلى آخر، وهي بذلك تساعد الباحثين في الحصول على أحدث الأبحاث العلمية من مختلف الجامعات ومراكز البحث العلمي في وقت قصير.[3]

بعد أن تعرفنا على الجانب التقني للجريمة الالكترونية، أين اتضح دور الحاسوب المحوري فيها، يتبادر إلينا التساؤل حول معنى هذه الجرائم، وما تنفرد به من سمات تميزها عن غيرها من الجرائم التقليدية، وما يتميز به مجرموها وضحاياهم عن نظرائهم في الجرائم العادية، وهو ما سنتطرق له من خلال المبحث الموالي.

[1]- هلال البياتي، المرجع السابق، ص: 30-31

[2]- علي حسن الطوالبة، المرجع السابق، ص: 37

[3]- علي جعفر عبود، المرجع السابق، ص: 70.

المبحث الثاني

مفهوم الجريمة الإلكترونية

تعد الجريمة الإلكترونية أهم مظاهر الاستخدام السلبي لتكنولوجيات الإعلام والاتصال، وقد تعددت الدراسات لتحديد مفهومها، واختلف رجال الفقه والقانون في وضع تعريف موحد لها نتيجة تطورها المتسارع، حتى قيل بأنها: "جريمة تقاوم التعريف".[1]

وفضلا عمَا لهذه الجريمة من خصائص تميّزها عن غيرها من الجرائم التقليدية، فإن مرتكبيها يشكلون طائفة جديدة من المجرمين لهم صفات خاصة، اصطلح على تسميتهم بمجرمي المعلوماتية، الذين يتخذون من ضحاياهم عبر الفضاء الرقمي أهدافا لهم.

ولشرح ذلك بشيء من الاستفاضة، ارتأينا تقسيم هذا المبحث إلى مطلبين كالآتي:

المطلب الأول: تعريف وخصائص الجريمة الإلكترونية.

المطلب الثاني: أطراف الجريمة الإلكترونية.

المطلب الأول

تعريف وخصائص الجريمة الإلكترونية

تختلف الجرائم الإلكترونية عن نظيرتها التقليدية في عدة جوانب، سواء من حيث الخصائص العامة، أو من حيث الباعث إلى تنفيذها، وحتى طريقة تنفيذها في حد ذاتها، الأمر الذي أظهر تحديا قويا أمام رجال القانون للإحاطة بمختلف جوانب هذه الجريمة المستحدثة، وهو ما ستناوله بالدراسة والتحليل خلال هذا المطلب.

[1]– هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1992، ص: 29.

الفرع الأول: تعريف الجريمة الإلكترونية

تباين تعريف الفقهاء للجريمة الإلكترونية تبعا لاختلاف المعيار المعتمد، فبعضهم عرّفها بالنظر إلى موضوع الجريمة، والبعض الآخر عرّفها استنادا إلى الوسيلة المستعملة لارتكابها،[1] ومنهم من استند في تعريفها إلى إلمام مرتكبها بالتقنية المعلوماتية، في حين دمج بعضهم عدة تعريفات في تعريف واحد، لذلك عرفت هذه الجريمة مسميات كثيرة: جرائم الحاسب الآلي، جرائم الإنترنت، جرائم تقنية المعلومات، الجرائم الإلكترونية، الجرائم المعلوماتية، جرائم الغش المعلوماتي، الجرائم السيبرانية، وغيرها.

أولا: التعريف الفقهي: تُعرّف الجريمة بوجه عام في إطار الفقه الجنائي بأنها: "سلوك إيجابي أو سلبي يُجَرمه القانون، ويُقَرر له عقوبة أو تدبير أمن، باعتباره يشكل اعتداءً على مصالح فردية أو اجتماعية يحميها القانون الجنائي".[2]

ويعرفها فقهاء الشريعة الإسلامية بأنها: "إتيان فعلٍ محرَم معاقب على فعله أو تركه، له جزاء عاجل في الدنيا، وجزاء آجل في الآخرة".[3]

أما الجريمة الإلكترونية، فقد اختلفت بشأنها التعريفات الفقهية بين ضيق وموسع، تبعا للمعيار الذي يستند إليه كل رأي.

01- التعريف الضيق: اختلف أصحاب هذا الرأي في تعريف الجريمة الإلكترونية، فمنهم من استند في تعريفها إلى معيار الوسيلة كأداة لارتكابها، ومنهم من استند إلى المحل الذي تستهدفه ومنهم من استند إلى إلمام الجاني بتقنية المعلومات.

أ- التعريف الذي يستند إلى وسيلة ارتكاب الجريمة: يستند أنصار هذا الرأي في تعريف الجريمة الإلكترونية إلى وسيلة ارتكابها، إذ يشترطون وجوب ارتكابها بواسطة جهاز الحاسوب، فيُعرفها

---

[1]- رضا مهدي، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021، ص: 114.

[2]- عبد الله أوهايبية، شرح قانون العقوبات الجزائري (القسم العام)، موفم للنشر، الجزائر، 2011، ص: 62

[3]- محمد علي عياد، شرح قانون العقوبات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1997، ص: 93.

الفقيه MERWE بأنها: "فعل غير مشروع يتورط في ارتكابه الحاسب الآلي"،[1] ويعرفها الفقيه LESLIE DE BALL بأنها: "فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية"،[2] فكلا التعريفين استوجب ارتكاب هذه الجريمة باستخدام الحاسب الآلي كأداة رئيسية.

غير أن هذا الرأي تعرض للنقد، لأن الأخذ به سيؤدي إلى توسيع مفهوم الجريمة الإلكترونية لتندمج ضمنه جرائم أخرى لا علاقة لها بالحاسوب، الذي لا يتعدى أن يكون محلا تقليديا في بعض الجرائم، مثل سرقته في حد ذاته، أو سرقة الأسطوانات الممغنطة أو الأقراص، باعتبار أن عدم اختلاف المكونات المادية للحاسوب عن الأموال المادية الأخرى يضفي على الجرائم التي تقع عليها الطابع التقليدي، كما أن المتعارف عليه أن الوسيلة التي تُرتكب بها الجريمة لا تدخل في تعريفها، فالمسدس والسكين يستويان في القدرة على القتل، لكنهما لا يدخلان في تعريف جريمة القتل.[3]

ب- التعريف الذي يستند إلى فاعل الجريمة: إذا كان أصحاب الرأي السابق قد أخذوا بمعيار الوسيلة (الحاسب الآلي) لتعريف الجريمة الإلكترونية، فإن أنصار هذا الرأي استندوا في تعريفها إلى معيار الفاعل أو الشخص الذي يستعمل الوسيلة في ارتكابها، انطلاقا من أن ما يميز الجريمة الإلكترونية عن غيرها من الجرائم هو معرفة مرتكبها بتقنيات الإعلام والاتصال، فلا مجال لارتكاب هذا النوع من الجرائم دون توافر هذه المعرفة.

وفي هذا الصدد عرف الفقيه DAVID THOMPSON الجريمة الإلكترونية بأنها: "أي جريمة يتطلب اقترافها إحاطة فاعلها بالمعرفة بتقنية الحاسوب"،[4] وعرفها الفقيه STEINSCHJQLBERG

[1]- Merwe (Van Der), Computer crimes and other crimes against information technology in south Africain, R.I.D.P, 1993, p: 554.

[2]- محمد خليفة، المرجع السابق، ص: 78.

[3]- المرجع نفسه، ص: 79-80.

[4]- خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص: 30.

بأنها: "كل فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر أساسية لارتكابه والتحقيق فيه وملاحقته قضائيا".[1]

ولم يسلم هذا الرأي بدوره من النقد، لأن هذا الشرط وإن تحقق في بعض الجرائم الإلكترونية فهو لا يتحقق في كثير منها، إذ يستطيع الفاعل ارتكاب جريمته دون معرفة كبيرة بتقنيات الإعلام والاتصال، فإرسال رسالة تحمل فيروسا لا يتطلب سوى معرفة بسيطة بهذه التقنيات.[2]

ت- التعريف الذي يستند إلى موضوع الجريمة: على العكس من الرأيين السابقين، لم يركز أصحاب هذا الرأي اهتمامهم على الوسيلة المستخدمة في الجريمة الإلكترونية، ولا على ما يجب أن يتوفر في فاعلها من صفات، بل ركّزوا على موضوع الجريمة في حد ذاتها.

وفي هذا السياق، عرف الباحث "ROSENBLATT" الجريمة الإلكترونية بأنها: "نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التي تحول عن طريقه"،[3] ومن أنصار هذا الاتجاه لدى الفقه العربي الدكتورة هدى حامد قشقوش، التي عرفت الجريمة الإلكترونية بأنها: "كل سلوك غير مشروع أو غير مسموح به فيما يتعلق بالمعالجة الآلية للبيانات أو نقل هذه البيانات"،[4] فالجريمة الإلكترونية وفقا لهذا الرأي هي جرائم الاعتداء على الأموال المعلوماتية المتمثلة في الأدوات المكونة للحاسب الآلي وبرامجه ومعداته.

غير أن هذا الرأي لم يسلم أيضا من الانتقادات، على أساس أنه يضيق من مفهوم الجريمة الإلكترونية من خلال حصرها فيما يقع على النظام الإلكتروني أو داخله فقط، بشكل يجعلها أشبه بالخرافة،[5] ويُخرج من نطاقها جانبا كبيرا من الأفعال غير المشروعة.

---

[1]- Donn B Parker, Nycm (S), Aura (S), Computer abuse, Stanford Research Institute, 1989, p: 517.

[2]- نائلة عادل محمد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي الحقوقية، بيروت، 2005، ص: 29.

[3]- محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط1، دار الثقافة للنشر والتوزيع، عمان، 2009، ص: 16.

[4]- خالد عياد الحلبي، المرجع السابق، ص: 28.

[5]- محمد عبد الرحمن عنانزه، القصد الجرمي في الجرائم الإلكترونية، ط1، دار الأيام للنشر والتوزيع، عمان، الأردن، 2017، ص: 63.

02- التعريف الموسع: أمام قصور التعريفات المبنية على معيار واحد، سعى البعض إلى تعريف الجريمة الإلكترونية بالاعتماد على أكثر من معيار، على غرار الفقيه الفرنسي (MASS) الذي عرفها بأنها: "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"،[1] وكذلك الخبير الأمريكي (DONN.B.PARKER) الذي عرفها بأنها: " أي فعل متعمد مرتبط بأي وجه بالحاسبات، يتسبب في تكبد أو إمكانية تكبد المجني عليه لخسارة، وحصول أو إمكانية حصول مرتكبه على مكسب".[2]

ويرى الفقيهان (Michel and Credo) أن الاستخدام السلبي للحاسوب يشمل استخدامه كأداة لارتكاب الجريمة، إضافة إلى حالات الولوج غير المصرح به إلى حاسوب المجني عليه أو بياناته، والاعتداءات المادية الماسة بالحاسوب أو بمعداته، وحتى الاستخدام غير المشروع لبطاقات الائتمان، وتزييف المكونات المادية والمعنوية للحاسوب، فضلاً عن سرقة جهاز الحاسوب في حد ذاته، أو أي مكون من مكوناته.[3]

وكغيره من الآراء السابقة لم يسلم هذا الرأي من النقد بسبب توسعه في تعريف الجريمة الإلكترونية، لأن مجرد مشاركة الحاسب الآلي في النشاط الإجرامي يضفي عليه وصف الجريمة الإلكترونية،[4] وهو الأمر الذي من شأنه أن يسقط وصف هذه الجريمة على أفعال أخرى بمجرد استعمال الحاسب.

ثانيا: التعريف القانوني: بين تباين التشريعات المقارنة في تعريفها للجريمة الإلكترونية، وإحجام بعضها عن ذلك تاركة المجال للفقه والقضاء، سنحاول التطرق للتعريفات الواردة في قوانين بعض المنظمات الدولية والإقليمية وبعض الدول العربية، وصولا إلى موقف المشرع الجزائري.

---

[1]- Michel Mass, la droit pénal spécial ne de l'informatique, in informatique et droit pénal travaux de l'institute de sciences criminelles de poitiers, 1981, p: 23.

[2]- Donn B Parker, Combatre la criminalité informatique, ed oras, 1985, p: 18.

[3]- محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004، ص: 09.

[4]- محمد عبد الرحمن عنانزة، المرجع السابق، ص: 64.

01- تعريف المنظمات الدولية والإقليمية: ورد في توصيات مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد بفيينا سنة 2000 أنه: "يقصد بالجريمة الإلكترونية أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي، وتشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية"،[1] وعرفتها منظمة التعاون الاقتصادي والتنمية الأوروبية (OCDE) بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية".[2]

أما مشروع القانون العربي النموذجي المُوحد لمكافحة جرائم تقنية المعلومات، فقد عرفها في مادته الأولى بأنها: "كل فعل مؤثم يتم ارتكابه عبر أي وسيط الكتروني".

02- تعريف بعض التشريعات العربية: اختلفت تشريعات الدول العربية بين من تناول تعريف الجريمة الإلكترونية كالمشرعين الكويتي والسعودي، وبين من عزف عن ذلك كالمشرع المصري.

أ- تعريف المشرع الكويتي: أورد المشرع الكويتي ضمن المادة الأولى من قانون مكافحة جرائم تقنية المعلومات رقم: 63 لسنة 2015 تعريفا للجريمة الإلكترونية بأنها: "كُل فعل يرتكب من خلال استخدام الحاسب الآلي أو الشبكة المعلوماتية، أو غير ذلك من وسائل تقنية المعلومات بالمخالفة لأحكام هذا القانون".[3]

ب- تعريف المشرع السعودي: تطرق المشرع السعودي من خلال نظام مكافحة الجرائم المعلوماتية في الفقرة الثامنة من مادته الأولى إلى تعريف الجريمة الإلكترونية بأنها: "أيُّ فعلٍ يُرتكب متضمنا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام".[4]

---

[1]- خالد عياد الحلبي، المرجع السابق، ص: 30.

[2]- هشام محمد فريد رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، العدد 17، 1990، ص: 110، ص: 111.

[3]- قانون رقم: 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ: 07 يوليو 2015، الجريدة الرسمية للكويت، العدد: 1244، الصادرة بتاريخ: 12-07-2015.

[4]- نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بموجب المرسوم الملكي رقم: م/17 بتاريخ: 08-03-1428 الموافق لـ: 27-03-2007.

وبذلك يمكن القول أن المشرعين الكويتي والسعودي كان لهما السبق في تعريف الجريمة الإلكترونية مقارنة بالتشريعات العربية الأخرى، خاصة أن تعريفها في صلب النص يعد نقطة مهمة في التشريع، لما يشكله من تكريس لمبدأ الشرعية وتجسيد لإلزامية التقيد بها من جهة، وتعزيز التعاون الدولي لمكافحة هذه الجرائم من جهة أخرى.

03- تعريف المشرع الجزائري: رغم تطرق المشرع الجزائري للجريمة الإلكترونية من خلال القانون 04-15 المعدل والمتمم لقانون العقوبات،[1] باستحداثه للقسم السابع مكرر المتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات (المادة 394 مكرر إلى المادة 394 مكرر7)، إلا أنه اكتفى بعرض صور هذه الجريمة دون التطرق لتعريفها، آخذا في عرضه لها بالمعنى الضيق الذي يعتمد على المعيار الموضوعي (موضوع الجريمة)، الأمر الذي أدى إلى حصر نطاقها في جرائم الاعتداء على النظام المعلوماتي، واستثناء الجرائم التقليدية المرتكبة باستعمال الحاسب الآلي، لتبقى بذلك خاضعة للنصوص العامة بشكل جعل الكثير منها يفلت من العقاب.

واستدراكا لما سبق، أعاد المشرع تنظيم هذه الجرائم مرة أخرى من خلال القانون رقم 09-04، المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرّفها في مادته الثانية بأنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأيُّ جريمة أخرى تُرتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"، جامعا بذلك بين الجرائم المعلوماتية البحتة (جرائم المساس بأنظمة المعالجة الآلية للمعطيات)، ونظيرتها المرتكبة بواسطة وسائل إلكترونية، إلا أن حصره لوسيلة ارتكابها في منظومة معلوماتية أو نظام للاتصالات الإلكترونية، أبقي المجال مفتوحا لخروج أصناف أخرى من دائرة التجريم في حالة ارتكابها باستعمال وسيلة إلكترونية أخرى غير الوسيلتين المذكورتين.

[1]- القانون رقم 04-15 المؤرخ في 10-11-2004 المعدل والمتمم قانون العقوبات، الجريدة الرسمية لسنة 2004، العدد 71.

ليعيد المشرع النظر مرة أخرى في هذه الجرائم من خلال الأمر: 21-11،[1] بسبب التطور الرهيب للجريمة الإلكترونية نتيجة استغلالها لأحدث التقنيات الناتجة عن اندماج تكنولوجيات الإعلام مع تكنولوجيات الاتصال، واستغلالها عبر الوسائط الإلكترونية لشن الحملات العدائية ضد الوطن، ونشر الفتنة بين أفراد المجتمع، مُعرفا إياها بأنها: "أيُّ جريمة ترتكب أو يسهل ارتكابها استعمال منظومة معلوماتية أو نظام للاتصالات الإلكترونية، أو أي وسيلة أخرى أو آلية ذات صلة بتكنولوجيات الإعلام والاتصال".[2]

وحسن فعل المشرع الجزائري حين أخذ بالمعنى الواسع للجريمة الإلكترونية، الذي يجمع فيه بين المعيار الموضوعي الذي يشمل الجرائم الماسة بالنظام المعلوماتي، والمعيار المادي الذي يشمل الجرائم المرتكبة باستعمال تكنولوجيات الإعلام والاتصال، دون حصره لتقنية محددة، وهو ما من شأنه أن يتيح التصدي لجميع أنواع الإجرام الإلكتروني.

الفرع الثاني: خصائص الجريمة الإلكترونية

انطلاقا من تعريفات الجريمة الإلكترونية المتعددة وفقا لمعايير مختلفة، وما صاحب التطور التكنولوجي الذي أحدثته الثورة الرقمية من ظهور لبعض الفئات التي سعت إلى تحويل هذه التقنية إلى وسيلة للإجرام، والتي ساهمت شبكات الاتصال في إعطائها بُعدًا عالميا جعل أثرها يمتد من النطاق الوطني إلى نظيره الدولي، يتبادر إلى الأذهان التساؤل حول الخصائص التي تميز هذه الجريمة، ومدى اختلافها عن غيرها من الجرائم التقليدية، وهو ما سنوضحه من خلال:

أولا: الخصائص المشتركة مع الجرائم الأخرى: تتميز الجرائم الإلكترونية على غرار بعض الجرائم التقليدية الأخرى كجرائم الإرهاب والاتجار بالمخدرات، والجرائم المنظمة العابرة للحدود الوطنية بالخصائص الآتية:

[1]- الأمر رقم 21-11 المؤرخ في 25-08-2021 المتمم للأمر رقم 66-155 المتضمن ق إ ج، الجريدة الرسمية لسنة 2021، العدد 65.

[2]- راجع الفقرة الأخيرة من المادة: 211 مكرر 22 ق إ ج.

01- خطورة الجريمة الإلكترونية: تنطوي الجرائم الإلكترونية على خطورة بالغة، لمساسها بفكر الإنسان وحياته الخاصة، وبالأمن الداخلي للدول، وحتى باقتصاد المؤسسات والشركات.[1]

فالجرائم الإلكترونية تُخَلف خسائرَ باهظة في شتى المجالات، بحكم أنها تطال المعلومات التي تشكل النسق العلمي والثقافي والاقتصادي للمجتمعات، وتنتهك الحياة الخاصة للأفراد من خلال الإطلاع على خصوصياتهم وكشف أسرارهم، رغم الحماية الموضوعية التي كفلتها المنظومات القانونية وطنيا ودوليا لهذا الحق الشخصي، كما تهدد أمن الدول، وتُوَلّد مخاطرَ متعددة تؤثر على عامل الثقة بالتقنية، فضلا عن تهديدها للملكية الفكرية، وقتْل روح الإبداع الإنساني،[2] مثلما تخلف خسائرَ اقتصادية باهظة، كحال سرقة المبالغ المالية من الأرصدة.[3]

02- الجريمة الإلكترونية عابرة للحدود: أفرزت تقنيات الاتصال الحديثة مجتمعا افتراضيا يتجاوز تفاعل أفراده الإلكتروني جميع الحدود الجغرافية، بشكل أعطى للجريمة الإلكترونية بعدا عالميا، إذ لا يقتصر أثرها على مكان وقوعها، فقد تتأثر في آن واحد أماكن متعددة عبر دول مختلفة بالجريمة الواحدة،[4] مثلما قد يكون المجرم في بلد والمجني عليه في آخر، ولذلك فهي لا تخضع لضوابط الزمان، ولا لقيود المكان.

وفي هذا الصدد، تمكن أحد الهواة في أوروبا من فك شفرة أحد مراكز المعلومات في البنتاغون (وزارة الدفاع الأمريكية)، وأصبح المجال أمامه مفتوحا للعبث ببياناته، وكذلك الحال بالنسبة لإنتاج الفيروسات ونشرها عبر مختلف أنحاء العالم وما تخلفه من أضرار وخسائر.[5]

ثانيا: الخصائص التي تنفرد بها عن الجرائم الأخرى: تتميز الجرائم الإلكترونية عن غيرها من الجرائم التقليدية بعدة خصائص، أهمها:

---

[1]- محمود أحمد عبابنة، المرجع السابق، ص: 32.

[2]- جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، مرجع سابق، ص: 17.

[3]- محمد عبد الرحمن عنانزه، المرجع السابق، ص: 66.

[4]- نائلة عادل محمد قورة، المرجع السابق، ص: 47.

[5]- محمود أحمد عبابنة، المرجع نفسه، ص: 34.

01- خصوصية مجرمي المعلوماتية: إذا كانت الجرائم التقليدية لا تتطلب مستوى معرفي وعلمي من أجل ارتكابها، فإن الأمر يختلف بالنسبة للجرائم الإلكترونية، باعتبار أنها جرائم تقنية لا يرتكبها عادة إلا ذوو الخبرة في مجال المعلوماتية ولو بحد أدنى من المعرفة باستعمال جهاز الحاسوب والتعامل مع شبكة الإنترنت.[1]

فمرتكب الجريمة الإلكترونية إضافة إلى امتلاكه للمعرفة والوسيلة، والسلطة والباعث، هو شخص يمتاز بالمهارة التي يكتسبها عن طريق الدراسة المتخصَصة في مجال تكنولوجيا المعلومات، أو من خلال تراكم خبرات احتكاكه بالآخرين،[2] كما أنه يعتمد على ذكائه في تنفيذ جريمته دون الحاجة إلى الاستعانة بقوته الجسدية إلا بالقدر اليسير، عكس المجرم العادي.[3]

وتتناسب خطورة الجرائم الإلكترونية مع المعرفة التقنية للحاسب الآلي وشبكات الاتصال تناسبا طرديا، فكلما تقدمت المعرفة التقنية لدى الفرد كلما زادت احتمالية توظيفها بشكل غير مشروع، وغالبا ما تتيح هذه المعرفة فرصا للجاني لإعاقة الجهة المكلفة بالتحري عن الدليل الرقمي،[4] وذلك باتخاذ تدابير فنية واقية تزيد من صعوبة التفتيش، كتشفير البيانات، أو إضافة كلمات السر وغيرهما، مما يتطلب أساليب متطورة تستطيع مواجهة هذا الإجرام.

02- صعوبة اكتشاف الجريمة الإلكترونية: عكس الجرائم التقليدية التي عادة ما يجد فيها جهاز التحقيق الجنائي الآثار الدّالة على مرتكبيها، أو خطوات ومراحل تنفيذها، فإنه يواجه صعوبة في اكتشاف الجرائم الإلكترونية، نتيجة عامل الطبيعة الرقمية لمسرح الجريمة، وعنصر الزمن الذي يمكن معه للمجرم الإلكتروني في ظرف قياسي -قد يكون جزءا من الثانية- أن يعبث ببيانات

---

[1]- نهلا عبد القادر المومني، المرجع السابق، ص: 59.

[2]- Benson Carl، Andrew Jablon، Paul kaplan، Mara Rosenthal، Computer crimes، Americain law review ، 1997, p: 410.

[3]- محمد خليفة، المرجع السابق ، ص: 33.

[4]- لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، ط1، دار الحامد للنشر والتوزيع، الأردن، 2015، ص: 28.

الحاسب وبرامجه عن طريق نبضات الكترونية لا تُرى بالعين المجردة، أو يقوم بمحوها قبل أن تصلها يد العدالة.[1]

كما ساهمت أيضا شبكات الحاسوب الدولية في خلق تقنيات تساعد على إخفاء شخصية مرتكبي هذا الصنف من الجرائم، بدءا من خدمات إرسال البريد المجهول، وإخفاء الرقم، أو استخدام أجهزة الوصول المجانية لمزودي خدمة الإنترنت، وصولا إلى ما توفره برمجيات الحاسوب والاتصالات من إمكانية التشفير (Encryption)؛ أي ترجمة البيانات إلى شفرة سرية وإخفائها (Data Hiding) من خلال إدخالها بصفتها جزءا لا يتجزأ من باقي البيانات لتبدو وكأنها بيانات بريئة، على غرار اختزال الصور لإخفاء المعلومات والاتصالات بعيدا عن الرقابة، فالتقنية الحديثة ساعدت الجناة كثيرا في التغلب على نظم الرقابة المتطورة،[2] وشكلت بذلك عاملا إضافيا في صعوبة اكتشاف هذا النوع من الجرائم.

لذلك يبقى الجانب الإحصائي لهذه الجرائم نسبيا لا يعكس حجمها الحقيقي، لكن رغم بقائه مجهولا فإنه بالتأكيد رقم كبير، وقد عبر عن ذلك الأستاذ توم فوريستر قائلا: "يعتقد العديد من الخبراء أن 15% من الجرائم الإلكترونية هي التي يعلن عنها من قبل الشركات، وأن العديد منها تمر دون الكشف عنها كليا، ونادرا ما تتم محاكمة الحالات التي يتم الكشف عنها".[3]

03- صعوبة إثبات الجريمة الإلكترونية: أضفت عوامل صعوبة اكتشاف الجريمة الإلكترونية خاصية فريدة عليها من حيث آثارها المادية، إذ أن تعلق محلها بالمعطيات والبيانات التي تُعد من قبيل الأشياء غير المادية يجعل مرتكبيها في غالب الحالات لا يُخلِّفون أثرا ماديا يدل عليهم، إن لم ينعدم ذلك أصلا، نتيجة ما يتعرض له محلها من تغيير أو محو أو إتلاف، بشكل يزول معه أي أثر مرئي أو ملموس يمكن الاستعانة به لإقامة الدليل على ارتكاب الجريمة.[4]

---

[1]- خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012، ص: 24.

[2]- عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011، ص: 181.

[3]- محمود أحمد عبابنة، المرجع السابق، ص: 38.

[4]- محمد عبد الرحمن عنانزه، المرجع السابق، ص: 68.

وترجع صعوبة إثبات الجرائم الإلكترونية إلى عدة أسباب، أهمها:[1]

أ- اعتماد الجريمة الإلكترونية على الذكاء والمهارة في ارتكابها.

ب- الاحترافية الفنية العالية اللازمة من أجل الكشف عنها، وهذا ما يعرقل عمل المحقق الذي تعود التعامل مع الجرائم التقليدية.

ت- صعوبة الاحتفاظ بآثارها إن وجدت.

ث- غياب الإطار التشريعي الموحد بين الدول، وضعف التعاون الأمني فيما بينها، مما يترك المجال مفتوحا لتنفيذ العديد من الجرائم الإلكترونية الدولية، مثل جرائم تبييض الأموال، والاتجار بالمخدرات، والاعتداء على قواعد البيانات.

ج- تعقيدات الجرائم الإلكترونية، مثل استخدام الجناة لعناوين مجهولة وأجهزة تشفير تجعل الوصول إلى الأدلة الرقمية أمرا في غاية الصعوبة.

ح- تنازع الاختصاص القضائي الدولي في حالة وقوع الفعل والنتيجة في أكثر من دولة، وتمسك كل دولة باختصاصها، مما يجعل من اعتقال الجناة ومحاكمتهم أمرا صعبا للهيئات القضائية.

لذلك تعتبر مسألة إثبات الجريمة الإلكترونية أحد أهم التحديات التي تواجه جهاز التحقيق الجنائي، خاصة أمام التطور المتزايد لتكنولوجيات الإعلام والاتصال، الذي تتطلب مواكبته مستوى عال من الخبرة التقنية.

04- الجرائم الإلكترونية هادئة ومغرية للمجرمين: فتنفيذها لا يتطلب عنفا، بل يكفيه توافر القدرة على التعامل مع الحاسب الآلي بمستوى تقني يوظف للقيام بالأفعال غير المشروعة، على نقيض الجرائم التقليدية التي كثيرا ما تتجلى في صور ممارسة العنف، كما هو الحال في جريمة القتل والاختطاف، أو صورة التسلق والكسر وتقليد المفاتيح في جريمة السرقة.[2]

[1]- عادل عزام سقف الحيط، المرجع السابق، ص: 182.

[2]- محمد سيد علي السيد، الجرائم الإلكترونية، دار التعليم الجامعي، الإسكندرية، 2020، ص: 28.

فالمجرم الإلكتروني لا يستخدم قوته الجسدية أو العضلية لتنفيذ جريمته، بل يعتمد على قدراته المعرفية وأساليبه الاحترافية، وقد تُلحق جريمته خسائر فادحة بالمجني عليه رغم أنها لا تُرى دائما بالعين المجردة، وفي بعض الأحيان قد لا تتطلب سوى كبسة زر واحدة على لوحة المفاتيح لنقل ملايين الدولارات من مكان لآخر،[1] لذلك فإن نعومة هذه الجرائم وما تدره من أرباح جعلها من الجرائم المغرية والجذابة للمجرمين.

المطلب الثاني

أطراف الجريمة الإلكترونية

هناك طرفان في الجريمة التقليدية، أحدهما مُجْرِم يقوم بإتيان الفعل المقترن بالجزاء فينال العقاب، والآخر ضحية يلحقه ضرر فيستحق جبره، وهما نفس أطراف الجريمة الإلكترونية من حيث الأصل، غير أنهما يختلفان عنهما بسبب اختلاف البيئة التي يقع فيها الإجرام وأسلوب ومتطلبات الجريمة.

الفرع الأول: المجرم الإلكتروني

أدى تراوح استغلال التطور التكنولوجي سلبا وإيجابا إلى جعله سلاحا ذو حدين، فبقدر ما أفرز ذكاء صناعيا يطمح إلى أفق أوسع في شتى المجالات، أفرز صنفا جديدا من المجرمين يتسمون بالمهارة والإلمام بالجوانب التقنية ذات الصلة بالحاسب الآلي وشبكاته، ويسعون إلى تحقيق غايات غير مشروعة تستهدف الأفراد والمؤسسات وحتى الدول، وهو مكمن خطورة الجريمة الإلكترونية.

أولا: تعريف المجرم الإلكتروني وسماته

01- تعريف المجرم الإلكتروني: يسمى أيضا بالمجرم المعلوماتي، أو الهاكر كما يفضل خبراء أمن المعلوماتية تسميته،[2] وهو شخص يتمتع بمهارات تقنية، أو دراية بأنظمة الحواسيب الآلية

[1]- لينا محمد الأسدي، المرجع السابق، ص: 29.

[2]- مصطفى محمد موسى، المرجع السابق، ص: 143.

وأساليب استخدامها، والقدرة على تجسيد قصده الإجرامي في شكل أفعال رقمية تكنولوجية لتحقيق غاياته، كاختراقه للرموز السرية من أجل تغيير المعلومات، أو تقليد البرامج، أو التحويل من الحسابات عن طريق استخدام الحاسوب نفسه.[1]

فالمجرم الإلكتروني فرد من المجتمع، يؤدي وظائفه بشكل طبيعي، سواء أكان مختصا في ميدان الإعلام الآلي أم هاو، أم مجرد مستعمل لجهاز الحاسوب، كما يقوم بواجباته ويمارس حقوقه الاجتماعية والسياسية دون أي عائق، غير أنه إنسان يتمتع بقدر كبير من الذكاء.[2]

02- سمات المجرم الإلكتروني: يتمتع المجرم الإلكتروني بعدة سمات تميزه عن المجرم التقليدي يساعد فهمها على فهم طبيعة التنظيمات الإجرامية التي تقف خلف تلك الأفعال، وكشف أساليب عملها، ومن أبرز هذه السمات:

أ- الذكاء: هدوء الجريمة الإلكترونية ونعومتها يعكس اتسام مرتكبيها بالذكاء، فانتقال الجريمة من العالم الواقعي إلى العالم الافتراضي جعل الإجرام الحديث يوصف بأنه إجرام الأذكياء، بالنظر إلى استغلال الذكاء البشري في جميع مراحل تنفيذ الجريمة إلى غاية تمامها، بالإضافة إلى طمس معالمها وأدلتها، على غرار اختراق أنظمة الحواسيب أو القرصنة الإلكترونية،[3] فالمجرم الإلكتروني يوظف قدراته العقلية لتحقيق غاياته دون أي عنف أو إتلاف المادي.

والجامع بين محترفي الجرائم الإلكترونية أنهم يتمتعون بقدر عال من الذكاء والمعارف العلمية، والإلمام الجيد بالتقنية العالية، وينتمون إلى التخصصات المتصلة بالحاسوب من الناحية الوظيفية، وهي الصفات التي تتشابه كثيرا مع صفات مجرمي ذوي الياقات البيضاء.[4]

---

[1]- هدى حامد قشقوش، المرجع السابق، ص: 27.

[2]- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، الجزائر، 2018، ص: 61-62.

[3]- رامي وسام أبو ملحم، المجرم والضحية المعلوماتيين على ضوء علم الإجرام، المؤسسة الحديثة للكتاب، لبنان، 2022، ص: 29.

[4]- "مصطلح ذوي الياقات البيضاء حديث نسبيا، أطلقه عالم الاجتماع Suter Land على الجرائم المرتكبة من قبل الطبقة الراقية في المجتمع، ذوو المناصب الإدارية الكبيرة، وتشمل أنواعا مختلفة من الجرائم كغسيل الأموال وتجارة الرقيق الأبيض وغيرها من الجرائم التي يرتكبونها وهم جالسون في مكاتبهم الفخمة"، نهلا عبد القادر المومني، المرجع السابق، ص: 76.

ب- المهارة: من أبرز سمات المجرم الإلكتروني تمتُّعه بمهارة ذهنية عالية في استخدام التقنية المعلوماتية، لأن تحديد الأسلوب الذي يرتكب به الجاني جرائمه يتوقف على مستوى خبرته ومهارته، والتي يكتسبها سواء من خلال الدراسة المتخصصة في مجال تكنولوجيا المعلومات،[1] أو من تراكم الخبرات والتجارب العملية.

يرى الباحث دون باركر (DONN.B.PARKER) أن المهارة هي أبرز سمات مجرمي المعلوماتية، فتنفيذ جريمة إلكترونية يتطلب قدرا من المهارة يكتسبها الجاني عن طريق الدراسة المتخصصة في هذا المجال، أو من خلال الخبرة المكتسبة، أو بمجرد التفاعل الاجتماعي مع الآخرين.[2]

ت- المعرفة: إن الإحاطة بظروف الجريمة المراد تنفيذها وإمكانيات نجاحها أو فشلها ميزة أخرى أضفتها طبيعة الجرائم الإلكترونية على مرتكبيها، إذ يدفعهم مسرح الجرائم التي يقدمون على ارتكابها، والمتمثل في نظام الحاسوب الشامل، إلى التخطيط من أجل تكوين تصور كامل عن الجريمة، بما في ذلك المحاكاة، كتنفيذ الجريمة على أنظمة مماثلة لأنظمة الجريمة التي يستهدفها تفاديا لأي عقبات من شأنها أن تعيقهم أو تسهل اكتشافهم.[3]

غير أن ذلك لا يعني بالضرورة أن يكون المجرم الإلكتروني على قدر كبير من الذكاء والمعرفة في هذا المجال، أو أن تكون لديه خبرة فنية كبيرة، فقد أثبت الواقع العملي أن أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة عن طريق التعليم، أو من الخبرة المكتسبة في العمل في هذا المجال، كما نرى أن الجرائم الإلكترونية التي لا تستهدف نظام المعلومات الإلكتروني لا تتطلب سوى قدر بسيط من المهارة لدى المجرم.[4]

---

[1]- محمد عبد الرحمن عنانزه، المرجع السابق، ص: 73.

[2]- Benson Carl، Andrew Jablon، Paul kaplan، Mara Rosenthal، Computer crimes، Americain law review ، 1997، p: 410.

[3]- نائلة عادل محمد قورة، المرجع السابق، ص: 52.

[4]- علي عبود جعفر، المرجع السابق، ص: 108.

ث- السلطة: وتتمثل في العلاقة التي تربط المجرم الإلكتروني بالنظام المعلوماتي وما تخوله له من حقوق أو مزايا تُسهل ارتكاب جرائمه، فكثير من مجرمي المعلوماتية لديهم سلطة مباشرة أو غير مباشرة على المعلومات محل الجريمة، قد تتمثل هذه السلطة في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على المعلومات، بما يُمَكِّن الفاعل من مزايا متعددة كفتح الملفات وقراءتها وكتابتها ومحو المعلومات أو تعديلها، وقد تتمثل في الحق في استعمال الأنظمة المعلوماتية أو إجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التي تحتوي على هذه الأنظمة، مثلما قد تكون السلطة التي يتمتع بها الجاني غير حقيقية، كما في حالة استخدام شفرة الدخول الخاصة بشخص آخر.[1]

ج- ذو طابع اجتماعي: صعوبة اكتشاف الجريمة الإلكترونية وإثباتها جعلت مرتكبها يحافظ على سماته ذات الطابع الاجتماعي، ويخرج عن نطاق النظريات البيولوجية أو النفسية أو الاجتماعية التي تناولت المجرم التقليدي بالدراسة، إذ أنه يعيش وسط بيئته ويتفاعل مع بقية الأفراد، ويحظى بالثقة في مجال عمله،[2] فهو إنسان قادر على التوافق والتصالح، بعيد عن الدخول في عداء مع محيطه الاجتماعي.

ولعل شعور المجرم الإلكتروني بأنه محل ثقة هو ما يدفعه إلى التمادي في ارتكاب جرائمه التي قد لا تُكتشف، وإن اكتُشِفت فإنها تواجه صعوبة الإثبات ونقص الأدلة والخبرة لدى المحققين.

ح- عدم الشعور بتجريم أفعاله: كان المجرم التقليدي في نظر علم الإجرام محدد الغاية التي يسعى لتحقيقها من وراء جريمته، وغالبا ما تكون دوافع مالية أو ابتزازية، وكان يعلم بأنه يرتكب جريمة معنوية وأخلاقية في حق الطرف الآخر، أما اليوم فتطور هذا المفهوم، وأصبح الإجرام المعلوماتي نوعا من الأفعال التي تتيح للمجرم فرصة الظهور أمام المجتمع بمظهر الذكي المتحكم في تقنيات المعلوماتية.[3]

---

[1]- نائلة عادل محمد قورة، المرجع السابق، ص: 58.

[2]- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مرجع سابق، ص: 62.

[3]- David Johnson, Electronic privacy, stodder,Canada, 1997, p: 66.

فذكاء المجرم الإلكتروني وحفاظه على طابعه الاجتماعي وصعوبة اكتشاف جرائمه من شأنه أن يولد لديه الشعور بالتفوق، والاعتقاد بأن ما يقدم على فعله لا يتصف بالتجريم وعدم الأخلاقية، خاصة في الحالات التي تنصرف فيها أفعاله إلى قهر نظام الحاسوب وتخطي حمايته المفروضة دون قصد إيذاء الغير، إذ يُفرق مرتكبو هذه الجرائم بين حالة الإضرار بالأشخاص التي يعتبرونها أمرا لا أخلاقيا، وحالة الإضرار بمؤسسة باستطاعتها اقتصاديا تحمل نتائج تلاعبهم، فيرونه أمرا عاديا.[1]

ويبدو أن تزايد استخدام أنظمة المعلوماتية، وتباعد الأشخاص دون وجود احتكاك مباشر بينهم أنشأ مناخا نفسيا ملائما لتصور استبعاد فكرة الخير والشر، فكثيرا ما يقوم موظفو المؤسسات باستخدام أجهزة الحاسوب لأغراض شخصية بوصفه سلوكا شائعا بين الجميع، لا بوصفه فعلا إجراميا، وفي هذا الصدد يرى الباحث دون باركر (DONN.B.PARKER) أن أغلب مجرمي المعلوماتية غير قادرين على اقتراف الجرائم التقليدية، خاصة تلك التي تتطلب مواجهة مع المجني عليه، فالمجرم الإلكتروني وإن كان لا يستطيع أن يعتدي على المجني عليه مباشرة، إلا أنه لا يرى مانعا في أن يكون هذا الاعتداء عن طريق وسائل التقنية الحديثة.[2]

ثانيا: أصناف المجرم الإلكتروني ودوافع إجرامه

01- أصناف المجرم الإلكتروني: انعكس التطور الرهيب للتكنولوجيا الحديثة على الجرائم الإلكترونية، فأصبحنا أمام جرائم سريعة التطور، يبدع مرتكبوها في ابتكار أحدث الأساليب لخرق الحواجز الأمنية في العالم الرقمي، مستغلين في ذلك خبراتهم ومهاراتهم الذهنية والعقلية، وهو ما صعَب من وضع تصنيف ثابت لهم، ومع ذلك سنتطرق لبعض هذه الأصناف وفقا لما توصلت إليه الدراسات والأبحاث، مع الإشارة إلى أن ذلك لا يعني أن كل مجرم إلكتروني يندرج تحت فئة محددة دون غيرها من الفئات الأخرى، بل يمكن أن يكون المجرم الواحد مزيجا بين فئتين أو أكثر.

أجرى الباحثون (DAVID ICOVEK ET WILIAM VONS TORCH ET KARL SAGER) دراسة توصلوا من خلالها إلى تصنيف مجرمي المعلوماتية إلى ثلاث طوائف رئيسية:

[1]- نائلة عادل محمد قورة، المرجع السابق، ص: 54 .

[2]- علي عبود جعفر، المرجع السابق، ص: 111.

الطائفة الأولى: المتطفلون والمخترقون (HACKERS & CRACKES)

أ- **المتطفلون أو الهواة (HACKERS):** أُطلق مصطلح الهاكرز لأول مرة في ستينيات القرن الماضي على مجموعة طلبة صغار السن في الجامعات الأمريكية، يتميزون بقدرٍ عالٍ من الكفاءة التقنية، ويتفاخرون بإلمامهم بعلوم الحاسوب وقدرتهم على اختراق شبكاته بجهدهم الذاتي دون الاستعانة بأي تعليمات من أي مصدر،[1] وقد أطلق الدكتور محمد سامي الشوا على هذه الفئة تسمية "صغار نوابغ المعلوماتية"، أي الشباب المفتون بالمعلوماتية والحاسبات الآلية،[2] أما الأستاذ توم فوريستر فأطلق عليهم تسمية "المتلعثمين".[3]

فالهاكرز متطفلون يتحدون إجراءات أمن النُّظم والشبكات دون أن تتوافر لديهم دوافع حاقدة أو تخريبية، لذلك تشكل تسمية الهاكرز مرادفا لهجمات التحدي، غير أن ذلك لا يعني أن أفعالهم لا تشكل ضررا على الغير، إنما يفتقدون فقط لنية إحداث الضرر.[4]

وقد ساهم توسع نقاط الاتصال بالشبكة والتعلق بها، وانتشار البرامج المجانية سهلة الاستعمال، في يسر استخدام أنظمة الإعلام الآلي من قبل مختلف الفئات، لاسيما المراهقين، حتى صاروا يعرفون بالجيل الرقمي (Génération Nintendo)،[5] وساعد ذلك على انتشار ظاهرة القرصنة الإلكترونية في السنوات الأخيرة.

ومن أمثلة هذا الصنف قيام أحد المتخصصين في تقنية المعلومات باختراق أحد الأنظمة الأمنية لشبكة الإنترنت البريطانية لمجرد كشف فجواتها الأمنية، وقد نجح في الحصول على أسماء

[1]- علاء مغايرة، الأوجه الحديثة للجرائم المعلوماتية، رسالة ماجستير، جامعة الحكمة، بيروت، 2000، ص: 13.

[2]- محمد سامي الشوا، المرجع السابق، ص: 13.

[3]- توم فوريستر، مجتمع التقنية العالية، قصة ثورة تقنية المعلومات، ترجمة ونشر مركز الكتاب الأردني، عمان، الأردن، 1989، ص: 401.

[4]- رامي وسام أبو ملحم، المرجع السابق، ص: 62.

[5]- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مرجع سابق، ص: 73.

وعناوين وكلمات السر والمعلومات الخاصة بالبطاقات الائتمانية لأكثر من 24 ألف شخص، من بينهم خبراء عسكريون وموظفون حكوميون وكبار مديري الشركات.[1]

والحقيقة التي لا يمكن إخفائها أن الهواة ساهموا في كشف الفجوات الأمنية للأنظمة الإلكترونية في المؤسسات المالية وغيرها، الأمر الذي ساعد على تطوير نُظم الأمن ضد الاختراقات، غير أنه ينبغي الانتباه لهذه الفئة، فلاشيء يمنع من تحول الشغف بالحاسوب وتحدي الأنظمة الإلكترونية إلى احتراف الجريمة الإلكترونية.

ب- المخترقون (CRACKERS): وهم الهاكرز ذوو النوايا الإجرامية، وأغلب أفراد هذه الطائفة من الشباب الذين تجاوزوا سن الخامسة والعشرين، ويتميزون بالتخصص العالي في مجال الحاسب الآلي والمعرفة التقنية والذكاء، فاعتداءاتهم تعكس ميولاتهم الإجرامية، وتدل على جانب كبير من خطورتهم، عكس طائفة الهواة (HACKERS)، ورغم أن هذا المعيار غير منضبط إلا أن الدراسات في مجال الجرائم الإلكترونية تعتمده.[2]

الطائفة الثانية: المحترفون

يتميز أفراد هذه الطائفة بسعة الخبرة والإدراك الواسع للمهارات التقنية، إضافة إلى التنظيم والتخطيط لأنشطتهم الإجرامية المرتكبة، وتهدف اعتداءاتهم أساسا إلى تحقيق كسب مادي، أو أغراض سياسية، أو للتعبير عن موقف فكري أو نظري أو فلسفي.[3]

كما يتسم أفراد هذه الطائفة بالتكتم خلافا للطائفة الأولى، إذ يعملون على تطوير معارفهم الخاصة، ويحاولون إخفاء طرقهم التقنية في ارتكاب الجريمة ما أمكن، دون تبادل للمعلومات بشأن أنشطتهم، وتشير الدراسات إلى أن الأعمار الغالبة على هذه الطائفة هي فئة الشباب الذين تتراوح أعمارهم بين (25-40) عاما.[4]

---

[1]- نهلا عبد القادر المومني، المرجع السابق، ص: 83.

[2]- محمود أحمد عبابنة، المرجع السابق، ص: 43.

[3]- علي عبود جعفر، المرجع السابق، ص: 116 .

[4]- علي حسن الطوالبة، المرجع السابق، ص: 64.

وينقسم محترفو الجريمة الإلكترونية إلى عدة مجموعات، سواء حسب تخصصهم في نوع معين من الجرائم، أو حسب الوسيلة المستعملة في ارتكاب جرائمهم، فمنهم محترفو التجسس الصناعي، الذين يوجَهون أنشطتهم إلى اختراق نظم الحاسوب التابعة للشركات الصناعية ومشاريع الأعمال قصد الاستيلاء على الأسرار الصناعية والتجارية، إما لحسابهم أو لحساب منافسين آخرين في السوق، ومنهم محترفي الاحتيال والتزوير، الذين يهدفون إلى الاستيلاء على أموال الآخرين وتحقيق الكسب المادي، وضمن هذه المجموعة قد نجد تقسيمات فرعية، مثل محتالي شبكات الهاتف، ومحتالي شبكة الإنترنت، وغيرهم.[1]

وتعكس الإحصائيات التي قام بها معهد (Stand For Research) دور محترفي الإجرام الإلكتروني في ارتكاب أفعال الغش المعلوماتي، فالمحللون يرتكبون ما نسبته 25%، فيما يرتكب المبرمجون ما نسبته 18%، وحتى المستخدمون الذين لديهم أفكار خاصة بنظم المعلومات بلغت نسبة ارتكابهم لها 17%، بينما يرتكب الشخص الأجنبي عن المكان الذي تتواجد فيه نظم المعلومات ما نسبته 12%، ويرتكب فنيو التشغيل ما نسبته 11%.[2]

وتعكس الإحصائيات التي قامت بها منظمة اتحاد صناعة البرمجيات والمعلومات SILA غايات محترفي الجرائم الإلكترونية، إذ بلغت الخسائر التي تسببت فيها القرصنة العالمية في مجال البرمجيات فقط حوالي 11 مليار دولار أمريكي، فيما توصل مجلس الشيوخ الأمريكي في دراسة حديثة له إلى أن العدوان على برامج الحاسب الآلي في الولايات المتحدة الأمريكية يشكل ما نسبته 27% من حركة تداول البرامج الحاسوبية في السوق الأمريكية، وتصل هذه النسبة إلى 90% في أسواق أخرى،[3] الأمر الذي دفع الدول المنتجة والمصدرة لهذه البرامج إلى مطالبة الدول المستهلكة بضرورة سن التشريعات والقوانين الكفيلة بإضفاء الحماية الفعالة لهذه البرامج من الاعتداء.

[1]– علي حسن الطوالبة، المرجع السابق، ص: 63-64.

[2]– محمود عبد الله حسين، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002، ص: 56.

[3]– محمد محمد الألفي، ندوة مكافحة الجريمة عبر الإنترنت على المستوى العربي، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، شرم الشيخ، مصر، 2008، ص: 91.

الطائفة الثالثة: الحاقدون

لا يسعى أفراد هذه الطائفة إلى إثبات قدراتهم ومهاراتهم، ولا إلى تحقيق مكاسب مادية أو سياسية، إنما يرتكبون أفعالهم الإجرامية بدافع الرغبة في الانتقام والثأر، كردة فعل على تصرف صاحب العمل معهم مثلا، أو بسبب تصرف المؤسسة المعنية تجاههم عندما يكونون غرباء عنها، ويغلب على نشاطهم استخدام تقنيات زراعة الفيروسات والبرامج الضارة، وتخريب النظام أو إتلاف كل معطياته أو بعضها، أو تعطيل الموقع المستهدف إن كان من مواقع الإنترنت.[1]

وهناك من يسمي أفراد هذه الطائفة بالمرتزقة، لأنهم يُستخدمون من طرف أفراد أو مؤسسات، وحتى حكومات، من أجل اقتحام برامج ونظم حواسيب محددة لتدميرها أو سرقة ما فيها أو تشويهها مقابل مبالغ مالية أو خدمات معينة، ويلاحظ أن أغلب أجهزة الأمن والاستخبارات تسعى إلى الاستفادة من مهارات هؤلاء الأفراد لصدَ الهجمات الإلكترونية، والتصنَت على الأفراد والمؤسسات والدول، الأمر الذي يعيق إيجاد وسائل ناجعة لمكافحة القراصنة المحترفين، لأن الأجهزة التي تريد خدماتهم الإجرامية تحقيقا لأغراضها تتمتع بالقوة، بل إن بعضها يمثل الدولة نفسها.[2]

فبرنامج الجوسسة الإسرائيلي بيغاسوس (Pegasus)، الذي يعد أحد أخطر برامج التجسس وأكثرها تعقيدا، استخدمته عدة دول للتجسس على هواتف معارضين وسياسيين وصحفيين ومسؤولين حكوميين في الدولة، بل وحتى على رؤساء دول وحكومات أجنبية، إذ يتمكن بمجرد اتصاله بالهواتف الذكية من قراءة جميع المعلومات الشخصية، وإزالة الحواجز الأمنية عن طريق كسر حماية نظام التشغيل دون أن ينتبه المستخدم لذلك عادة.

كما يندرج ضمن هذه الطائفة، التنظيمات الإرهابية بتنوع إيديولوجياتها، إذ تستغل الفضاء الإلكتروني في عمليات التجنيد والتعبئة والدعاية وجمع المتطوعين والأموال، وتسعى إلى جمع

[1]– علي حسن الطوالبة، المرجع السابق ، ص: 65.

[2]– مصطفى محمد موسى، المرجع السابق، ص: 153.

المعلومات حول الأهداف المقصودة، رغم أنها لم تصل بعد إلى مرحلة القيام بهجوم إلكتروني حقيقي على منشآت البنية التحتية للدول.[1]

02- دوافع الإجرام الإلكتروني: يشكل الدافع أحد أهم ركائز الجريمة، ورغم تميز الجرائم الإلكترونية من حيث خصائصها، إلا أن لها دوافع عديدة لارتكابها، أهمها:

أ- السعي نحو الكسب: تعتبر الرغبة في تحقيق مكاسب مادية ضخمة خلال زمن قياسي أحد أهم الدوافع لارتكاب الجرائم الإلكترونية، فالمنفعة المادية الناتجة عنها أكثر إغراء وأوفر ربحا عما تُدِرُه الجرائم التقليدية،[2] فضلا عن نعومة الفعل وهدوئه، إذ يكفي استعمال بطاقة سحب آلي مزورة أو منتهية الصلاحية، أو المساومة على البرامج أو المعلومات المتحصلة بطريق الاختلاس من جهاز الحاسوب لتحقيق مكاسب مادية.

خلال سنة 2003 تعرضت شركة تجارية في الولايات المتحدة الأمريكية تقوم بعمليات التحويل المالية لشركات (فيزا، ماستر كارد، أمريكان اكسبرس) إلى سرقة أرقام تخص 8.000.000 بطاقة ائتمان في حادثة تعد الأكبر من نوعها، نتيجة تعرض نظام العمل للاختراق من طرف مجهول غير مصرح له بالدخول إلى النظام مثلما أقرت به الشركة، والتي اكتفت بإبلاغ عملائها بالواقعة، مقابل تصريح لمكتب التحقيقات الفيدرالي بأن الأمر رهن التحقيق.[3]

وقد أدت إجراءات الحجر الصحي التي تم اتخاذها للحد من انتشار فيروس كورونا (covid19) والمتمثلة في غلق الحدود وحظر الطيران والسفر، وغلق دور العبادة، وعزل الناس في منازلهم إلى تراجع نسبة الإجرام التقليدي، بشكل دفع مرتكبيه بحثا عن الكسب المادي إلى نقل إجرامهم إلى العالم الافتراضي، من خلال استغلال مواقع التواصل الاجتماعي للترويج للمواد المخدرة والمؤثرة عقليا، والتحريض على الفسق وفساد الأخلاق وغيرها.[4]

---

[1]- يحيى عطوة الزنط، المرجع السابق، ص: 139.

[2]- محمد عبد الرحمن عنانزة، المرجع السابق، ص: 76.

[3]- محمد محمد الألفي، المرجع السابق، ص: 107-108.

[4]- يحيى عطوة الزنط، المرجع نفسه، ص: 263.

ولم يعد الكسب المادي وحده الدافع لارتكاب هذه الجرائم، بل أصبح الكسب المعنوي كذلك محفزا عليها، إذ أفرزت الرغبة في اجتياز امتحانات شهادتي التعليم المتوسط والبكالوريا بنجاح خلال السنوات الأخيرة ظاهرة إجرامية تُستعمل خلالها تكنولوجيات الإعلام والاتصال تسهيلا للغش من أجل تحقيق الغاية المنشودة، الأمر الذي دفع المشرع الجزائري إلى تجريمها من خلال تعديل قانون العقوبات سنة 2020 باستحداث نصوص قانونية تعاقب كل من يساهم في المساس بنزاهة الامتحانات والمسابقات من خلال المواد 253 مكرر 6 إلى غاية 253 مكرر 12،[1] وهو ما تم تكريسه ميدانيا في العمل القضائي، أين تم معالجة العديد من قضايا الغش في الامتحانات باستعمال وسائل التواصل الاجتماعي، وتمت متابعة الجناة ومعاقبتهم على أفعالهم.[2]

ب- إثبات التفوق العلمي: يشكل اختراق الأنظمة الإلكترونية وكسر حواجزها الأمنية متعة كبيرة لمجرمي المعلوماتية، وتسلية تشغل أوقات فراغهم، فمجرد الشغف بالإلكترونيات والرغبة في قهر النظام الإلكتروني والتفوق على تعقيدات التكنولوجيات الحديثة قد يدفع إلى ارتكاب هذه الجرائم، إذ يسعى صغار نوابغ المعلوماتية إلى اكتشاف البرامج الجديدة، وإثبات تفوقهم العلمي بتخطي حواجز الحماية الأمنية لهذه البرامج دون نية الإضرار بالغير.[3]

ويميل مرتكبو هذه الجرائم إلى إظهار براعتهم لدرجة وصولهم إلى شغف الآلة، فمع ظهور أي تقنية جديدة يسعون لإيجاد الوسيلة المناسبة للتفوق عليها، ويزداد هذا الدافع أكثر لدى صغار السن، الذين يمضون وقتا طويلا أمام حواسيبهم الخاصة في محاولة لكسر حواجز الأمن لأنظمة الحاسوب وشبكات المعلومات، وإظهار تفوقهم على وسائل التقنية الحديثة.[4]

---

[1]- قانون رقم 20-06 المؤرخ في 28-04-2020 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية لسنة 2020، العدد 25.

[2]- مثال ذلك القرار الصادر عن مجلس قضاء باتنة، الغرفة الجزائية، بتاريخ: 02-07-2023 ، فهرس رقم: 7759/23، انظر ملحق رقم 01.

[3]- محمد عبد الرحمن عنانزة، المرجع السابق، ص: 76.

[4]- علي حسن الطوالبة، المرجع السابق، ص: 70-71.

ت- الرغبة في الانتقام: قد يُفصل بعض الأفراد تعسفا من مؤسسة أو إدارة أو بنك رغم امتلاكهم للمعرفة الكافية بخفايا هذه المؤسسة، فيرتكبون جرائمهم باستغلال هذه المعلومات من أجل تكبيد المؤسسة خسائر مالية، انتقاما لما ألحقته بهم من ضرر،[1] فاستياء مدير أنظمة الحاسوب من تعامل الشركة معه دفع به إلى اختراق نظامها، وإزالة قواعد بيانات هامة، مع تغييره لحسابات الزبائن، مُكَبِّدا إياها خسائر مادية تجاوزت 50.000 دولار، وأدى ذلك إلى إفلاسها.[2]

ث- دوافع سياسية: تعد الدوافع السياسية من أبرز الأسباب المحفزة لاختراق الشبكات الحكومية، فقد تُوَجه هذه الاختراقات ضد دولة معينة أو عقيدة أو مذهب من أجل تشويه صورته بنشر أخبار كاذبة، وقد أصبحت شبكة الإنترنت مجالا خصبا لنشر أفكار العديد من الأفراد والجماعات.[3]

وينصب هذا الدافع على الوقائع التي تجذب اهتمام الرأي العام، وتلفت الانتباه إلى مشكلة خطيرة، من أجل بناء وعي جماهيري يؤدي إلى حلها، ومن الشائع أن يتوارى مجرمو المعلوماتية وراء هدف سياسي معادٍ للحكومة، وذلك بتلفيق الأخبار والمعلومات الزائفة، وإثارة الفتن ونشر الشائعات، ولو بالاستناد إلى جزء بسيط من الحقيقة.[4]

مثال ذلك ما عرفته الجزائر خلال فترة جائحة كورونا (Covid 19) من نشر لأخبار زائفة عبر مواقع التواصل الاجتماعي، تمحورت حول ندرة مادة الأكسجين بالمستشفيات، ونقص بعض المواد الغذائية الأساسية كالدقيق والزيت، مما خلق اضطرابا في أوساط المجتمع، ودفع ذلك بالمشرع إلى استحداث نصوص قانونية تتضمن عقوبات رادعة ضد كل من يروج لمثل هذه الأخبار، سواء من خلال تعديل قانون العقوبات بموجب الأمر رقم 20-01،[5] الذي تضمن نصوصا تجرم وتعاقب على نشر معلومات باستعمال وسيلة إلكترونية قصد الإضرار بالمرضى

[1]- محمود ابراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2014، ص: 123-124.

[2]- علي عبود جعفر، المرجع السابق، ص: 117.

[3]- محمد سيد علي السيد، المرجع السابق، ص: 30-31.

[4]- يحيى عطوة الزنط، المرجع السابق، ص: 257 .

[5]- قانون رقم 20-01 المؤرخ في: 30 جويلية 2020 المعدل والمتم للأمر رقم 66-156 المتضمن قانون العقوبات الجريدة الرسمية لسنة 2020، العدد 44.

وأسرهم أو بالهياكل الصحية،[1] أو من خلال القانون رقم: 21-15،[2] الذي يعاقب على أفعال المضاربة غير المشروعة باستعمال وسيلة إلكترونية، ويقرر عقوبات جد قاسية لمرتكبيها.[3]

لقد أصبح الإرهاب وثيق الصلة بالتكنولوجيا لدرجة القول أن بث الإرهاب عبر الإنترنت أصبح من سمات الألفية الثالثة،[4] وتزداد خطورته في الدول المتقدمة التي تدار بنيتها التحتية بالحواسب الآلية والشبكات الإلكترونية، مما يجعلها هدفا سهل المنال، فبدلا من استخدام القنابل والمتفجرات تستطيع الجماعات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وإغلاق المواقع الحيوية، وشل أنظمة القيادة والاتصالات، أو قطع شبكات الاتصال بين الوحدات وقيادتها المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية،[5] مما يستدعي تكاثف الجهود الدولية لمواجهة هذا الإجرام الخطير.

ج- دوافع أخرى: إن كان ما سبق بيانه يشكل أبرز دوافع الإجرام الإلكتروني، فإن هناك دوافع أخرى، فأنشطة الإرهاب الإلكتروني وحروب المعلومات تحركها الدوافع الإيديولوجية، في حين أن أنشطة الاستيلاء على الأسرار التجارية تحركها دوافع المنافسة، والفعل الواحد قد يعكس دوافع متعددة، خاصة إذا اشترك فيه شخصين فأكثر، وانطلق كل منهم من دوافع خاصة تختلف عن دوافع غيره.

---

[1]- راجع المادة 149 مكرر 3 من الأمر رقم 20-01.

[2]- قانون رقم: 21-15 المؤرخ في 28-12-2021 المتعلق بمكافحة المضاربة غير المشروعة، الجريدة الرسمية لسنة 2021، العدد 99.

[3]- "اعتبر المشرع أن ترويج أخبار أو أنباء كاذبة أو مغرضة عمدا بين الجمهور بغرض إحداث اضطراب في السوق تعد صورة من صور المضاربة غير المشروعة، وقرر لها عقوبات قاسية تصل إلى ثلاثين سنة سجنا إذا ارتكبت خلال الحالات الاستثنائية أو الأزمات الصحية، أما إذا ارتكبت في إطار جماعة إجرامية منظمة، فإن العقوبة تصل إلى السجن المؤبد"، راجع المواد: 01، 14، 15 من القانون رقم 21-15.

[4]- محمود إبراهيم غازي، المرجع السابق، ص: 126.

[5]- المرجع نفسه، ص: 127.

كما توجد مجموعات ناشطة عبر فضاء الإنترنت، تطلق على نفسها مجموعات الكراهية تزدري كل القيم الدينية والأخلاقية والاجتماعية السائدة في المجتمعات، وبصفة خاصة تلك المرتبطة بالأسرة، فضلا عن نشاط بعض المواقع الإلحادية، التي تطالب بإلغاء الدين والدولة والأسرة، وتدعو إلى تحرير الإنسان مما تصفه بالقيود والأصفاد،[1] وهؤلاء جميعا قد يرتكبون جرائم إلكترونية تبدو حسب آرائهم ومعتقداتهم مشروعة وتهدف إلى تحسين العالم.

الفرع الثاني: الضحية الإلكتروني

لم يعد علم الإجرام يقتصر في دراسته للجريمة على المتهم باعتباره المؤثر الرئيسي فيها، بل أصبح للضحية مكانة هامة في الدراسات الحديثة بحكم أنه أحد عناصر الجريمة، وإذا كان للجريمة التقليدية طرفان أحدهما مجرم والآخر ضحية، فللجريمة الإلكترونية كذلك طرفان، سبق وأن تعرفنا على طرفها الأول، وسنحاول التعرف على طرفها الثاني، وهو الضحية الإلكتروني.

أولا: تعريف الضحية الإلكتروني: عرفت الجمعية العامة للأمم المتحدة الضحايا بصفة عامة بأنهم: "الأشخاص الذين أصيبوا بضرر فردي أو جماعي، بما في ذلك الضرر البدني أو العقلي أو المعاناة النفسية أو الخسارة الاقتصادية أو الحرمان بدرجة كبيرة من التمتع بحقوقهم الأساسية عن طريق أفعال أو حالات إهمال تشكل انتهاكا للقوانين الجنائية النافذة في الدول الأعضاء، بما فيها القوانين التي تحرم الإساءة الجنائية لاستعمال السلطة"،[2] فضحية الجريمة عموما هو: "كل شخص طبيعي أو اعتباري أصيب بخسارة أو بضرر أو بعدوان نتيجة ارتكاب جريمة، وينتج الضحية سواء من فعل أو امتناع عن فعل".[3]

أما ضحية الجريمة الإلكترونية فهو: "كل كيان أصابه ضرر مادي أو معنوي نتيجة الاستخدام غير المشروع لتقنية المعلومات"،[4] وهو ما يعني أن ضحية الجريمة الإلكترونية قد يكون

[1]– أحمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، القاهرة، ط1، 2003، ص: 24.

[2]– يحيى عطوة الزنط، المرجع السابق، ص: 257.

[3]– مصطفى محمد موسى، المرجع السابق، ص: 158.

[4]– يحيى عطوة الزنط، المرجع نفسه، ص: 258.

شخصا طبيعيا أو معنويا، عاما أو خاصا، يتم استهدافه نظرا لقلة معرفته باستغلال تكنولوجيات المعلومات والاتصال، التي صار يعتمد عليها في تسيير مصالح الأفراد وشؤون الدول.

ثانيا: تصنيف الضحية الإلكتروني: يمكن تصنيف ضحايا الإجرام الإلكتروني إلى فئتين رئيسيتين:

01-الأشخاص الطبيعية: إذا كان للمجرم الإلكتروني عوامل وأسباب تدفعه لارتكاب الفعل الإجرامي، فإن للضحية كذلك دور في ارتكابها، فالجريمة لا تخلق عند الجاني من العدم، إنما تكون نتيجة مجموعة من الإيحاءات والعوامل والصفات التي تجذبه لارتكابها، وعادة ما يكون للضحية دور أساسي أو ثانوي في هذه العوامل،[1] وتعد شبكة الإنترنت المجال الخصب لاصطياد الضحايا، لاسيما ما تعلق بحياتهم الخاصة وبياناتهم الشخصية.

وما يثير الانتباه أن الجرائم الإلكترونية تستهدف جميع الأشخاص الطبيعية دون استثناء ذكورا كانوا أم إناثا، أحداثا كانوا أم بالغين، وهو ما سجلته من خلال الإحصائيات التي استقيتها من المصلحة المركزية لمكافحة الإجرام السيبراني التابعة لقيادة الدرك الوطني، التي عالجت 2472 جريمة الكترونية خلال سنة 2023، بلغ منها عدد الجرائم التي استهدفت الذكور 1298، بمعدل يفوق ضعف الجرائم التي استهدفت الإناث (556)،[2] فيما بلغ عدد الجرائم التي استهدفت الأطفال 200 قضية خلال سنة 2021، و 193 قضية خلال سنة 2022،[3] ليصل العدد إلى 230 قضية خلال سنة 2023.[4]

وتشهد الجريمة الإلكترونية تطورا ملحوظا تبعا لازدياد أفراد العالم الافتراضي، وهو ما سجلته من خلال الإحصائيات المذكورة، إذ عالجت المصلحة 1245 جريمة إلكترونية خلال سنة 2019، ثم ارتفع العدد ليصل إلى 1620 جريمة خلال سنة 2020، وواصل ارتفاعه خلال سنة

[1] - Fawn T. Ngo, Raymond Paternoster, Cybercrime Victimization- An examination of Individual and Situational level factors, International Journal of Cyber criminology, Vol 5, 2011, p: 774.

[2] – بطاقة معلومات حول حصيلة المصلحة المركزية لمكافحة الإجرام السيبراني، ملحق رقم 02، ص:02.

[3] – فريد درامشية (رائد بقيادة الدرك الوطني، مختص في الإجرام السيبراني)، مداخلة عبر موقع الإذاعة الجزائرية، الرابط الإلكتروني: https://my.radioalgerie.dz/ar/node/11978، تاريخ الاطلاع: 12-03-2024، الساعة: 07:45.

[4] – انظر ملحق رقم 02، ص:01.

2021 ليصل إلى 2828 جريمة، فيما عرفت سنة 2022 انخفاضا طفيفا بتسجيل 2316 جريمة، لتعود الحصيلة مرة أخرى إلى الارتفاع بتسجيل 2472 جريمة خلال سنة 2023.[1]

وقد بينت هذه الدراسة أن الجنايات والجنح الإلكترونية المرتكبة ضد الأفراد التي عالجتها المصلحة المذكورة خلال سنة 2023 بلغ حد 1446 قضية،[2] وهو ما يشكل نسبة (58%) من مجموع الجرائم، احتلت منها جرائم المساس بحرمة الحياة الخاصة للأشخاص الحظ الأوفر بمجموع 999 قضية، أي بنسبة (40%)، ثم تأتي بعدها جرائم النصب والاحتيال والسرقة (371 قضية)، ثم جرائم الغش في امتحانات شهادة البكالوريا (327 قضية)، ثم جرائم المساس بأنظمة المعالجة الآلية للمعطيات (141 قضية)، وتليها جرائم انتحال الشخصية (107 قضية).[3]

02- الأشخاص المعنوية: إضافة إلى الأشخاص الطبيعية، فإن الأشخاص المعنوية أيضا عرضة لأن يكونوا ضحايا للإجرام الإلكتروني لأسباب متعددة، سواء كانت سياسية، أم اقتصادية، أم اجتماعية، وسواء كان الشخص المعنوي من أشخاص القانون الخاص كالشركات والبنوك وغيرها، أو من أشخاص القانون العام كالدولة والجماعات المحلية، والمؤسسات العمومية ذات الصبغة الإدارية.

وتبين من خلال دراسة الإحصائيات المذكورة أن 618 شخص معنوي كان ضحية إجرام إلكتروني خلال سنة 2023، وهو رقم معتبر إذا ما قورن بالرقم الإجمالي الذي عالجته المصلحة خلال نفس السنة (2472).[4]

أ- الأشخاص المعنوية العامة: لم تكن مؤسسات الدولة في الإجرام التقليدي عنصر جذب للمجرمين، إذ كانت الدولة قادرة على حماية ممتلكاتها باتباع أساليب أمنية ووقائية، لكن بعد

[1]- انظر ملحق رقم 02، ص 01.

[2]- انظر ملحق رقم 02، ص: 02.

[3]- انظر ملحق رقم 02، ص: 03.

[4]- انظر ملحق رقم 02، ص:01.

توجهها نحو نمط الإدارة الإلكترونية[1] تحسينا لخدماتها، صارت عرضة للهجمات الإلكترونية، التي تستهدف مواقعها الرسمية، ومنصات التواصل الاجتماعي ضربا لأمنها واستقرارها.

ولعل أبرز مثال على ذلك تسريبات ويكيليكس (Wikileaks)، التي نجح من خلالها جوليان أسانج (Julian Assange) سنة 2006 في الوصول إلى معلومات في أجهزة الكمبيوتر الخاصة بوزارة الدفاع الأمريكية، وقام بنشر ملايين الوثائق السرية للإدارة الأمريكية وقنصلياتها حول العالم مما أدى إلى خلق مشاكل دبلوماسية بين الولايات المتحدة الأمريكية وحلفائها.[2]

كما أظهر رصد المخاطر الأمنية السيبرانية أنها أخذت منحى أشد خطورة وتعقيدا منذ نهايات القرن العشرين وبدايات القرن الواحد والعشرين، حيث أصبحت تهدد الأمن الداخلي للدول باستهداف منشآتها الحيوية كمصادر الطاقة وغيرها، وأدّت إلى بروز ما يعرف بحروب الجيل الرابع والخامس، التي تعد الهجمات السيبرانية أهم أدواتها، وقد ترقى إلى مستوى الحروب السيبرانية الشاملة التي تستهدف الدول والأفراد على حد سواء.

ففي الجزائر مثلا، تعرض حساب تويتر الخاص بوزارة العدل خلال فترة الحرب الروسية الأوكرانية بتاريخ: 11-03-2022 لعملية اختراق، من أجل تشويه صورة الجزائر، لكن مصالح الوزارة تفطنت لذلك، وتصدت له في حينه.[3]

وفي نفس السياق، كشف كتاب صدر في باريس تحت عنوان "عبر واشنطن" عن قيام جهازي المخابرات الأمريكية والإسرائيلية باختراق جميع أجهزة الحاسوب في العالم بغرض الحصول على جميع المعلومات المتعلقة بالدول في شتى المجالات، وأشار الكتاب إلى أن الولايات المتحدة

---

[1]- يعتبر مصطلح الإدارة الإلكترونية من المصطلحات التي تم تداولها بعد الثورة التكنولوجية، نتيجة التطور المذهل الذي شهدته شبكات المعلومات والاتصال، وأنظمة الإعلام الآلي، مما انعكس إيجابا على تطوير وتحسن نوعية الخدمة التي تقدمها الإدارة، انظر: الطيب بلواضح، الخدمات الإلكترونية المتاحة في مجال عصرنة الإدارة الجزائرية، مجلة الدراسات القانونية والسياسية، المجلد 06، العدد 01، 2020، ص: 139.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 139.

[3]- بيان لوزارة العدل، الرابط الإلكتروني: https://n9.cl/hzc33r، تاريخ الاطلاع: 11-03-2022 على الساعة: 17:45.

الأمريكية تقوم بنصب كمائن للنظم المعلوماتية لدى أعدائها وحلفائها على حد سواء، وتصطاد المعلومات في مختلف المجالات.[1]

ونشير في هذا الصدد إلى أن الدولة تتحمل جزءا كبيرا من المسؤولية الناتجة عن تعرضها لهذه الجرائم، وذلك بسبب ضعف بنيتها التحتية الإلكترونية، وعجز أنظمة حماية أمنها الإلكتروني ويرجع ذلك أساسا إلى تخلفها عن مواكبة التطورات تكنولوجية، مما يجعلها محل استقطاب للإجرام الإلكتروني.

ب- الأشخاص المعنوية الخاصة: عادة ما يقع الإجرام الإلكتروني على شخص معنوي خاص لأسباب اقتصادية دون استبعاد الأسباب الأخرى، ويتعدد ضحاياه بين شركات محلية وأجنبية، أو متعددة الجنسيات، ويمارس هذا الإجرام بعدة أساليب، كالاعتداء على الملكية الفكرية، وسرقة البيانات والأسهم، وتحويل الأموال، وتخريب البيانات، وغيرها.[2]

وتعتبر المؤسسات المالية أحد الأهداف الرئيسية للجيل الجديد من مجرمي المعلوماتية وذلك لاعتمادها الكلي على أنظمة إلكترونية لنقل التمويل، فإذا كانت بنوك نيويورك وحدها تتناقل 200 بليون دولار يوميا فإن ذلك يدفعنا إلى التساؤل عما سيكون عليه الحال إذا استطاع المجرمون الوصول للرموز الإلكترونية المستخدمة، وكم من الأموال يمكن نقلها في ثوان معدودة خارج البلد؟[3]

ولعل ما يجعل الإجرام الإلكتروني الواقع على الشخص المعنوي الخاص أكثر خطورة، أنه يبقى سريّا في أغلب الحالات، حتى لو توصلت المؤسسة أو الشركة لمعرفة الجاني، وذلك حفاظا على سمعتها أمام الزبائن، وعدم لفت انتباه الرأي العام.

---

[1]- كامل عفيفي عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2007، ص: 311.

[2]- رامي وسام أبو ملحم، المرجع السابق، ص: 76.

[3]- المرجع نفسه، ص: 33.

خلاصة الفصل

خلاصة لهذا الفصل من هذه الدراسة، يمكن القول أنه ورغم ما يستلزمه الإدراك العميق للجريمة الإلكترونية من فهم جانبها التقني الذي يشكل ركنها المفترض، والمتمثل خصوصا في جهاز الحاسوب باعتباره وسيلة لارتكابها، إضافة إلى تكنولوجيات الإعلام والاتصال، إلا أن اتسامها بالتطور حال دون الاتفاق على تعريف موحد لها، إذ تنوعت المعايير المعتمدة في ذلك بين المادي (بالنظر إلى وسيلة ارتكابها)، والموضوعي (بالنظر إلى محلها)، والشخصي (بالنظر إلى مرتكبها).

أما المشرع الجزائري، وبعد أن أخذ في بداية الأمر بالمعيار الموضوعي من خلال القانون رقم: 04-15 حين حصرها في الجرائم الماسة بالنظام المعلوماتي، اضطره تطورها إلى إعادة تنظيمها بموجب القانون رقم: 09-04، ثم القانون رقم: 21-11 معتمدا على المعيارين المادي والموضوعي معا، أين أسماها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، لتشمل بذلك الجرائم التي تكون تكنولوجيات الإعلام والاتصال وسيلة لارتكابها، إضافة إلى جرائم المساس بالنظام المعلوماتي.

وتتميز هذه الجرائم بطابعها الفني، الناتج عن وقوعها وسط بيئة افتراضية تختلف عن البيئة المادية، فضلا عما يميزها من خطورة وعالمية، ويتميز مجرموها بالذكاء والمهارة في تنفيذ أفعالهم الإجرامية، وهو ما يصعب على جهاز التحقيق الجنائي اكتشاف هذا النوع من الجرائم.

الفصل الثاني

جهاز التحقيق الجنائي

في الجريمة الإلكترونية

الفصل الثاني

جهاز التحقيق الجنائي في الجريمة الإلكترونية

مجابهة لظاهرة الإجرام عبر العصور، ظهرت عدة نظم إجرائية، أقدمها النظام الاتهامي الذي برز في روما والعصور القديمة، وامتاز بمنح سلطة الاتهام للضحية (المجني عليه)، الذي له أن يرفع دعواه مباشرة إلى الجهة المختصة بالمحاكمة، مثلما يقع عليه عبء الإثبات، وبظهور الدولة المركزية برز نظام التحرّي والتنقيب، الذي امتاز بمنح سلطة الاتهام إلى النيابة العامة، وبرزت معه مرحلة التحقيق الابتدائي.[1]

غير أن ما طال النظامين من انتقادات، عجّل بظهور نظام إجرائي مختلط في العصر الحديث، أخذت به أغلب التشريعات، التي اتفقت على مرحلة التحقيق الابتدائي، وتباينت في تحديد الجهة المكلفة بها، فمنها من أسندته إلى قاضي التحقيق باعتباره سلطة مستقلة، مثلما أخذت به فرنسا وبعض الدول الإفريقية كالجزائر، ومنها من رأت الجمع بين سلطتي الاتهام والتحقيق وأسندته بذلك للنيابة العامة، كما هو الحال في إنكلترا، أمريكا، مصر واليمن.

وإذا كان التحقيق الجنائي اختصاصا أصيلا لقاضي التحقيق، فإن لجهاز الشرطة القضائية دور لا يمكن الاستغناء عنه، سواء من خلال تهيئة القضية عن طريق جمع الاستدلالات وتقديمها إلى القضاء، لاستكمال التحقيق فيها إن كان ناقصا، أو المحاكمة إن كان كافيا، أو من خلال القيام ببعض الأعمال التي تعد من صميم العمل القضائي.

ومجابهة لظاهرة الإجرام التي وصلت حد الاستعانة بأحدث تقنيات التكنولوجيا، استحدث القانون رقم: 09-04 الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كهيئة تقنية تعمل على مساعدة السلطات القضائية الوطنية والأجنبية من أجل التصدي لهذا الإجرام المستحدث.

ولإبراز هذه المسائل ارتأينا تقسيم هذا الفصل إلى المبحثين الآتيين:

[1]- محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، ط 4، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص: 5.

المبحث الأول: السلطة المختصة بالتحقيق في الجريمة الإلكترونية.

المبحث الثاني: الأجهزة المساعدة على التحقيق في الجريمة الإلكترونية.

المبحث الأول

السلطة المختصة بالتحقيق في الجريمة الإلكترونية

تحتاج المحاكمة إلى مرحلة تحضيرية من أجل تهيئة القضية وتقديمها وهي جاهزة للفصل تسمى بمرحلة التحقيق القضائي، يتم خلالها العمل على جمع الأدلة والقرائن من أجل توضيح معالم الجريمة، وكشف أهم عناصرها.

والتحقيق القضائي بمفهومه الاصطلاحي يتضمن نوعين؛ الأول ابتدائي يتوسط مرحلتي جمع الاستدلالات والمحاكمة، غايته تهيئة القضية قبل عرضها على جهة الحكم، يختص به قاضي التحقيق على مستوى المحكمة، وغرفة الاتهام على مستوى المجلس، وهو موضوع دراستنا، أما الثاني فهو نهائي يقوم به قاضي الحكم خلال جلسة المحاكمة من أجل تكوين قناعته لإصدار حكمه بالبراءة أو الإدانة، يفتقد لبعض مميزات التحقيق الابتدائي المستمدة من النظام التنقيبي، وهو خارج عن نطاق دراستنا.

وللإلمام بعناصر الموضوع ارتأينا تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: مفهوم التحقيق في الجريمة الإلكترونية.

المطلب الثاني: أحكام التحقيق في الجريمة الإلكترونية.

المطلب الأول

مفهوم التحقيق في الجريمة الإلكترونية

تتطلب مرحلة التحقيق الابتدائي تحقيق نوع من التوازن بين مقتضيات الكشف عن الحقيقة عند وقوع الجريمة وما تقتضيه من سرعة لجمع الأدلة، وبين ما يمكن أن يتخللها من إجراءات قد تمتد للمساس بحرية المتهم، التي يحفظها الدستور والقانون، وهو ما جعل المشرع الجزائري يسندها إلى سلطة قضائية محايدة.

ولعل ظهور صور مستحدثة للجريمة على غرار الجريمة الالكترونية أثار التساؤل حول كيفية التعامل معها أثناء مرحلة التحقيق مقارنة بالجرائم العادية، لاسيما من حيث توظيف أحدث

التقنيات التي تتماشى مع طبيعتها الخاصة، تفاديا لضياع الأدلة وإفلات مرتكبيها من العقاب، وهو الأمر الذي سيتم التطرق إليه بالدراسة خلال هذا المطلب.

الفرع الأول: تعريف التحقيق في الجريمة الإلكترونية

من أجل الوصول إلى تعريف دقيق للتحقيق الجنائي في الجريمة الإلكترونية، لا بد من تعريف التحقيق الجنائي أساسا، سواء من الناحيتين اللغوية والفقهية، أو من الناحية القانونية عند بعض التشريعات المقارنة عموما، والتشريع الجزائري خصوصا.

01- التحقيق الجنائي لغة: عرف ابن منظور التحقيق بأنه: "التصديق أو التأكيد أو التثبيت"، يُقال حقَق الأمر، بمعنى أكّده وثبّته،[1] ويقال حقّق الظنّ، وحقّق القول والقضية، وحقّق الثوب، أي أحكم نسجه، وحقّق مع فلان في قضية أي أخذ أقواله فيها، وجنى، جناية، بمعنى أذنب، فالتحقيق الجنائي لغة يعني: "إثبات التهمة على الجاني بإحكام".[2]

02- التحقيق الجنائي فقها: عرّفه بعض الفقه بأنّه: "مجموعة الأعمال والإجراءات المشروعة التي يتخذها المحقق الجنائي للكشف عن الحقيقة وجمع الأدلّة التي تؤدي إلى معرفة الجاني وشركائه"،[3] وعرفه آخرون بأنه: "المرحلة الأولى للدعوى الجنائية؛ وهي تلك المرحلة التي تسبق وتمهد لمرحلة المحاكمة، ويطلق عليها وصف التحقيق الابتدائي، وتعني كلمة ابتدائي أنه مجرد تحضير وتهيئة للدعوى من أجل عرضها على القضاء إن كان لذلك وجه".[4]

ورغم تعدد التعريفات الفقهية للتحقيق الجنائي، إلا أنها تتفق عموما حول كونه: "مجموعة من الإجراءات، تصدر عن سلطة عهد إليها القانون بالتحقيق، بهدف الكشف عن الحقيقة حول جريمة ارتكبت، وجمع أدلتها، قبل إحالتها على جهة الحكم للفصل فيها".

---

[1]- أبو الفضل جمال الدين ابن منظور، لسان العرب، دار صادر للطباعة والنشر، بيروت، بدون سنة نشر، ص: 24.

[2]- عبد الواحد إمام مرسى، التحقيق الجنائي علم وفن(بين النظرية والتطبيق)، دار الفكر الجامعي، القاهرة، 1998، ص: 11.

[3]- المرجع نفسه، ص: 9.

[4]- محمود ابراهيم غازي، المرجع السابق، ص: 682.

03- التحقيق الجنائي في التشريعات المقارنة: انقسمت التشريعات الدولية في إسناد التحقيق الجنائي إلى وجهتين، الأولى تتخذ من مبدأ الفصل بين سلطتي التحقيق الاتهام معيارا لها، فتُسنده بذلك إلى قاضي تحقيق مختص، والثانية تجمع بين سلطتي الاتهام والتحقيق، فتسنده إلى النيابة العامة، الأمر الذي يدفعنا إلى التطرق لنموذجين متمايزين من هذه التشريعات:

أ- **التحقيق الجنائي في مصر:** يعد التشريع المصري من بين التشريعات التي منحت النيابة العامة الاختصاص الأصيل في مباشرة التحقيق الابتدائي، في حين جعلت قاضي التحقيق صاحب سلطة احتياطية في ممارسته، لتصبح بذلك النيابة العامة مختصة بالاتهام (المادة الأولى من قانون الإجراءات الجنائية المصري)، ومختصة أيضا بمباشرة التحقيق الابتدائي في كل الجرائم (المادة 199 وما بعدها من قانون الإجراءات الجنائية المصري)، ما لم تندب قاض للتحقيق في جريمة معينة (المادة 64 وما بعدها من قانون الإجراءات الجنائية المصري).[1]

وتجدر الإشارة إلى أن مهام قاضي التحقيق في مصر ليست محصورة في ممارسة التحقيق الابتدائي فقط، فهو أحد قضاة الحكم، تتحدد ولايته للتحقيق بمقتضى قرار ندبه، ومن خلال ولاية الحكم التي يتمتع بها أصلا، والتي قد يزاولها في الوقت ذاته في غير الدعوى الجنائية التي يجري التحقيق بشأنها.[2]

وقد تعرض نظام الفصل بين سلطتي الاتهام والتحقيق لعديد الانتقادات، بحجة أن نشاط القاضي محدود بعدم كفاية علاقاته برجال الشرطة القضائية، فضلا عما كشف عنه العمل القضائي من أن سؤال الشهود أمام رجال الشرطة، ثم أمام النيابة العامة، ثم أمام قاضي التحقيق ثم أمام قاضي الحكم، فيه تشتيت للدليل، وخلق للثغرات، وأن إلغاء هذا النظام سيساعد على تبسيط الإجراءات، دون أن يؤثر على حسن سير العدالة،[3] لذلك تتجه أغلب التشريعات الأوروبية

[1]- قانون الإجراءات الجنائية المصري الصادر بالقانون رقم 150 لسنة 1950، المعدل بالقانون رقم 01 لسنة 2024، عدد 02 مكرر، الجريدة الرسمية الصادرة بتاريخ 16-01-2024.

[2]- أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1993، ص: 487.

[3]- محمود إبراهيم غازي، المرجع السابق، ص: 694-695.

إلى العدول عن فكرة منع الجمع بين سلطتي الاتهام والتحقيق، وتكليف النيابة العامة بمهمة التحقيق الابتدائي، على غرار تشريعات إيطاليا، ألمانيا، بولندا وبلجيكا.

ب- التحقيق الجنائي في فرنسا: أخذ التشريع الفرنسي بمعيار الفصل بين سلطتي الاتهام والتحقيق، إذ عهد بمباشرة التحقيق الابتدائي إلى قاضي تحقيق مستقل، انطلاقا من وجود تعارض بين وظيفة ملاحقة الجناة أمام القضاء "الاتهام"، ووظيفة جمع وتقدير الأدلة "سلطة التحقيق"، بما يقتضي عدم منحهما لجهة واحدة، حتى لا تكون خصما وحكما في الوقت نفسه، مما يهدد انتهاك الحريات الفردية، فأسند بذلك وظيفة الاتهام إلى النيابة العامة، في حين أسند مهمة التحقيق إلى قضاة التحقيق، سواء كان قاضي التحقيق على مستوى الدرجة الأولى، أو غرفة الاتهام على مستوى الدرجة الثانية.[1]

وإن كانت النيابة العامة تباشر بنفسها أو بواسطة رجال الشرطة القضائية إجراءات البحث والتحري عن الجريمة، إلا أنها ليست من إجراءات التحقيق بمعناه الضيَق، رغم تأثيرها الحاسم من الناحية العملية في مساره، في حين أن قاضي التحقيق لا يمكنه مباشرة إجراءات التحقيق إلا بعد إبلاغه من طرف وكيل الجمهورية، أو بعد اتصاله بشكوى مصحوبة بادعاء مدني من قبل المتضرر من الجريمة (المادة 51 قانون الإجراءات الجنائية الفرنسي).[2]

04- التحقيق الجنائي في التشريع الجزائري: لم يعرف المشرع الجزائري كغيره من القوانين المقارنة التحقيق القضائي، لكنه تعرض إلى مهام قاضي التحقيق من خلال بعض نصوص قانون الإجراءات الجزائية (المواد: 38 ،66، 67، 68، 163، 164، 166)، والتي يتبين منها بأن التحقيق الجنائي هو: "نشاط إجرائي تباشره سلطة قضائية مختصة بالتحقيق للبحث في مدى صحة الاتهام بشأن واقعة جنائية (جناية أو جنحة أو مخالفة)، معروضة عليها من طرف النيابة العامة،

[1]- محمود إبراهيم غازي، المرجع السابق، ص: 691.

[2]- قانون الإجراءات الجزائية الفرنسي رقم 1426/57 المؤرخ في: 31-12-1957، الجريدة الرسمية، عدد 20، الصادرة بتاريخ 08-01-1958، المعدل والمتمم بالقانون رقم 1109/2021 المؤرخ في 24-08-2021.

للبحث عن الأدلة المتعلقة بالتهمة، وعن المجرمين المتابعين بها، وهو مرحلة لاحقة لمرحلة البحث التمهيدي الذي تباشره الشرطة القضائية، وتسبق مرحلة المحاكمة التي يمارسها قضاة الحكم".[1]

وردت عبارة "التحقيق الابتدائي" في الفقرة الأولى من المادة 66 من قانون الإجراءات الجزائية الجزائري بالنص العربي، ويقابلها في نفس المادة بالنص الفرنسي عبارة " L'instruction Préparatoire"، ونفس العبارة استعملها المشرع الفرنسي في المادة 79 من قانون الإجراءات الجنائية، التي نقلت منها المادة 66، وترجمتها الصحيحة "التحقيق التحضيري"، لذلك يطلق على هذه المرحلة تسمية "التحقيق الابتدائي"، أو "التحقيق التحضيري".[2]

غير أن ما يعاب على ق إ ج هو الخلط بين مصطلحي "التحقيق الابتدائي" و"التحقيق الأولي"،[3] فنجد مثلا عنوان الباب الثالث من الكتاب الأول (المادة 66 وما يليها) هو (في جهات التحقيق)، ويقابله في النص الفرنسي (des juridictions d'instructions) وتعني "التحقيقات الابتدائية"، في حين نجد عنوان الباب الثاني من الكتاب الأول (في التحقيقات) ويقابله في النص الفرنسي (des enquêtes)، وتعني "التحريات"، ونفس الملاحظة بالنسبة لعنوان الفصل الثاني من نفس الباب (في التحقيق الابتدائي)، الذي يقابله في النص الفرنسي (de l'enquête préliminaire)، وتعني "التحريات الأولية".[4]

كما يظهر الخلط بين المصطلحين في اعتماد تسمية "التحقيق الابتدائي" ضمن الفقرة الأولى من المادة 65 مكرر 5 ق إ ج، رغم أنها تتعلق بمرحلة التحريات الأولية، الأمر الذي يُستشف من النص الفرنسي الذي استعمل مصطلح "Enquête préliminaire"، ومن صياغة النص العربي ذاته، بحكم أن هذه المادة نصت في فقرتها الأولى على اختصاص وكيل الجمهورية بمنح

---

[1]– عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015، ص: 378.

[2]– محمد حزيط، المرجع السابق، ص: 21–22.

[3]– التحقيق الأولي أو البحث التمهيدي أو الاستدلال أو البحث والتحري، وجميعها مصلحات لنظام قانوني واحد، وهي المرحلة تقوم عليها النيابة العامة بنفسها أو تكلف بها جهاز الشرطة القضائية للقيام بإجراءات البحث والتحري عن الجريمة، وهي مصطلحات واردة في ق إ ج، انظر: عبد الله اوهايبية، شرح قانون الإجراءات الجزائية، مرجع سابق، ص: 213.

[4]– المرجع والموضع نفسه.

الإذن لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور (خلال مرحلة التحقيق الأولي)، ثم تحدثت بعد ذلك –ضمن فقرتها الرابعة– عن انتقال هذا الاختصاص إلى قاضي التحقيق عند فتح تحقيق قضائي (خلال مرحلة التحقيق الابتدائي).[1]

ورغم تشابه التحقيق الابتدائي مع التحقيق الأولي في أنهما يكونان بعد وقوع الجريمة ويهدفان إلى كشف ملابساتها، والوصول إلى مرتكبيها، تمهيدا لتقديمهم أمام القضاء، إلا أنهما يختلفان في عدة مواضع، أهمها:

أ– التحقيق الأولي يختص به جهاز الشرطة القضائية، ويباشره بمجرد العلم بوقوع الجريمة سواء تلقائيا، أو بناء على تعليمات من وكيل الجمهورية،[2] بينما التحقيق الابتدائي تختص به السلطة القضائية، وتباشره بناء على طلب افتتاحي لإجراء تحقيق،[3] أو بموجب شكوى مصحوبة بادعاء مدني.[4]

ب– التحقيق الأولي يشكل مرحلة سابقة على تحريك الدعوى العمومية، بينما التحقيق الابتدائي يعتبر أحد مراحلها الأساسية.[5]

ت– التحقيق الأولي مجرد مرحلة لجمع المعلومات، لذلك فهو لا ينطوي على إجراءات القهر والإكراه،[6] عكس التحقيق الابتدائي الذي يمكن فيه لقاضي التحقيق أن يلجأ لوسائل القهر التي من شأنها أن تساعده في الوصول إلى الحقيقة.[7]

---

[1]– راجع المادة 65 مكرر 5 ق إ ج.

[2]– راجع المادة 63 ق إ ج

[3]– راجع المادة 67 ق إ ج.

[4]– راجع المادة 72 ق إ ج.

[5]– عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط 4، دار بلقيس، الجزائر، 2018–2019، ص: 69.

[6]– المرجع نفسه، ص: 69.

[7]– مثال ذلك ما نصت عليه المادة 109 ق إ ج: "يجوز لقاضي التحقيق حسب ما تقتضيه الحالة أن يصدر أمرا بإحضار المتهم أو بإيداعه السجن أو بإلقاء القبض عليه.

ث- أعمال الاستدلال لا تقطع التقادم في الدعوى العمومية لأنها لا تندرج ضمن إجراءات التحقيق أو المتابعة القضائية، عكس إجراءات التحقيق الابتدائي التي تقطعه.[1]

ج- المعلومات المستنبطة من محاضر الاستدلال المحررة أثناء مرحلة التحقيق الأولي لا تشكل أدلة بمدلولها القانوني، ولا يسوغ للقاضي أن يستند إليها وحدها لبناء حكمه؛[2] بسبب عدم توافر ضمانات الدفاع المتطلبة لنشوء الدليل باستثناء ما ورد فيه نص خاص،[3] عكس الأدلة المستخلصة خلال مرحلة التحقيق الابتدائي؛ التي تكفل الضمانات اللازمة لحقوق الدفاع،[4] بما يجيز للقاضي أن يبني حكمه على ما ورد من أدلة مستنبطة منها.

05- التحقيق في الجريمة الإلكترونية: يعرف التحقيق في الجريمة الإلكترونية بأنه: "علم وفن كشف غموض الجرائم المرتكبة بواسطة تقنيات وشبكات المعلومات ونظم الاتصالات، بغية استجلاء الحقيقة، وتحديد شخصية مرتكبها، وإثبات التهمة أو نفيها بما أمكن الحصول عليه من أدلة وفق إجراءات قانونية"،[5] أو هو: "مجموعة الإجراءات التي يقوم بها المحقق، وتؤدي إلى اكتشاف الجريمة ومعرفة مرتكبها، تمهيدا لتقديمه إلى المحاكمة كي ينال عقابه، قد تكون هذه الإجراءات عملية كالتفتيش، أو فنية كمضاهاة البصمات، أو برمجية كتحديد كيفية الدخول إلى المعطيات المخزنة في أجهزة الحاسوب".[6]

ويعد التحقيق في الجريمة الإلكترونية علما حديثا، تزايد الاهتمام به في الآونة الأخيرة بسبب زيادة الاعتماد على الأجهزة الإلكترونية في شتى مجالات الحياة، مثل الحاسبات وأجهزة الهواتف المحمولة الذكية، وغيرها من الأجهزة الرقمية الأخرى، ويُعنى بدراسة أمن نظم تشغيل الأجهزة الرقمية وشبكاتها، بغية معرفة كيفية ارتكاب الجريمة الإلكترونية، وسبل استخلاص أدلتها

[1]- تنص المادة 07 ق إ ج: "تتقادم الدعوى العمومية في مواد الجنايات بانقضاء عشر سنوات كاملة تسري من يوم اقتراف الجريمة إذا لم يتخذ في تلك الفترة أي إجراء من إجراءات التحقيق أو المتابعة".

[2]- تنص المادة: 215 ق إ ج: "لا تعتبر المحاضر والتقارير المثبتة للجنايات والجنح إلا مجرد استدلالات ما لم ينص القانون على خلاف ذلك".

[3]- راجع المواد: 216، 218 ق إ ج.

[4]- راجع المواد: من 100 إلى 105 ق إ ج.

[5]- يحيى عطوة الزنط، المرجع السابق، ص: 294

[6]- خالد عياد الحلبي، المرجع السابق، ص: 191.

الجنائية، وضبط مرتكبيها من أجل تقديمهم إلى الجهات القضائية، ليطال بذلك مجال دراسته كل جهاز باستطاعته حفظ ومعالجة واسترجاع المعلومات وتداولها، ويمكن أن يستخدم في ارتكاب جريمة بشكل مباشر أو غير مباشر".[1]

الفرع الثاني: خصائص التحقيق في الجريمة الالكترونية

إذا كانت غاية التحقيق الجنائي عموما هي الوصول إلى الحقيقة من خلال جمع الأدلة، فإن اختلاف الجريمة الالكترونية عن نظيرتها التقليدية يدفعنا إلى التساؤل حول مدى تأثير ذلك على تطابق خصائص التحقيق الجنائي في الجريمتين.

أولا: الخصائص العامة للتحقيق: يتميز التحقيق الابتدائي أو التحضيري باعتباره عملا قضائيا يسبق مرحلة المحاكمة بمجموعة من الخصائص، أهمها:

01- تدوين التحقيق: وهي خاصية لازمة حتى يكون التحقيق حجَة على الكافة، وتكون إجراءاته أساسا صالحا لما يبنى عليها من نتائج، فذاكرة المحقق وحدها لا تكفي لتوثيقه، فقد تخونه بعد فترة من الزمن، الأمر الذي يستلزم تدوينه من طرف أمين الضبط، فالتحقيق ليس غاية في حد ذاته، بل تكمن غايته في عرض ما تم التوصل إليه من نتائج أمام جهة الحكم،[2] بما يجعله مختلفا عن محضر الاستدلالات الذي يحرره ضابط الشرطة القضائية.[3]

وقد أوجبت المواد 94، 95، 108 ق إ ج تدوين إجراءات التحقيق بحضور أمين الضبط، سواء ما تعلق منها باستجواب المتهمين، أو سماع الشهود والضحايا، أو المواجهات، أو المعاينات والتفتيش، مع دعوة الشخص المعني إلى قراءة فحوى محضر سماعه، أو تلاوته عليه إن لم يكن ملمَا بالقراءة، إضافة إلى التوقيع على كل صفحة من صفحاته من طرف قاضي التحقيق وأمين الضبط، بمعية المتهم بالنسبة لمحاضر الاستجواب، والشاهد والضحية بالنسبة لمحاضر سماعهم،

[1]- يحيى عطوة الزنط، المرجع السابق، ص: 293.

[2]- محمد الطراونة، ضمانات حقوق الإنسان في الدعوى الجزائية (دراسة مقارنة)، ط 1، دار وائل للنشر والتوزيع، عمان، الأردن، 2003، ص: 82.

[3]- أحمد بسيوني أبو الروس، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، ط 2، المكتب الجامعي الحديث، الإسكندرية، 2008، ص: 27.

وإذا امتنع أحدهم أو تعذّر عليه ذلك وجب التنويه عنه في المحضر،[1] وتخلُّف خاصية التدوين تنزل بالإجراء إلى درجة العدم، وتفقده الحجية،[2] مع الإشارة إلى أن تنفيذ إجراءات التحقيق عن طريق الإنابة القضائية، يخول لضابط الشرطة القضائية تحرير المحاضر بنفسه أو عن طريق أحد مساعديه من الأعوان دون إلزامية الاستعانة بكاتب لتحريره.

كما تفرض خاصية تدوين إجراءات التحقيق خلو المحاضر المحررة من أي شطب أو تحشير حفاظا على حجيتها، ويتعين حال وجودها أن يتم التصديق عليها من قبل قاضي التحقيق والكاتب والشخص المعني على كل شطب أو تخريج فيها، تحت طائلة اعتبار التشطيبات أو التخريجات ملغاة، على غرار المحاضر غير الموقع عليها توقيعا صحيحا، أو الخالية من توقيع في أحد صفحاتها.[3]

وتتجلى أهمية الكتابة خلال مرحلة التحقيق الابتدائي، ووجوب اصطحاب كاتب التحقيق فيما يلي:

أ- تفرُّغ قاضي التحقيق من الناحية الذهنية والفكرية للعمل الفني المتمثل في التحقيق ذاته، من خلال انشغاله بالجانب الإجرائي، ومناقشة أطراف الدعوى، في حين يتولى كاتب التحقيق تدوين كل ما تم أمامه ضمن محضر التحقيق، وبذلك يسهل على القاضي تكوين قناعته، والتوصل إلى الأدلة التي يبني عليها أوامره دون أن تشغله عنها كتابة المحاضر.[4]

ب- تمكين أطراف الدعوى من الإطلاع على محاضر التحقيق، ومناقشة ما تم فيها من إجراءات حتى يتسنى لهم بذلك تحضير دفاعهم، إذ تنص المادة 105-4 ق إ ج: "يجب أن يوضع ملف الإجراءات تحت طلب محامي المتهم قبل كل استجواب بأربع وعشرين ساعة على الأقل، كما يجب أن يوضع تحت طلب محامي المدعي المدني قبل سماع أقواله بأربع وعشرين ساعة على الأقل".

---

[1]- راجع المادة 94 ق إ ج.

[2]- محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، القاهرة، 1995، ص: 523.

[3]- راجع المادة 95 ق إ ج.

[4]- عبد الله أوهايبية، شرح قانون الإجراءات الجزائية، مرجع سابق، ص: 390.

02- سرّية التحقيق بالنسبة للجمهور: تتسم إجراءات التحقيق الابتدائي بالسرَية التي تحول دون الاطلاع عليها إلا من قبل أطراف الدعوى ومحاميهم، ومن قد يساعد في التحقيق كالخبراء وأمناء الضبط والمترجمين، بحكم أنهم ملزمون بكتمان السر المهني تحت طائلة العقوبات المقررة قانونا،[1] الأمر الذي يجعل نطاق السرية ممتدا إلى غيرهم؛ أي الجمهور.

وتتجلى الحكمة من سرية التحقيق في الحفاظ على سمعة المتهم وشرفه، وعدم التشهير به قبل صدور حكم بإدانته،[2] فالتحقيق الابتدائي مجرد مرحلة سابقة على مرحلة الحكم، والأصل في الإنسان البراءة إلى أن يثبت العكس، كما أن منع إفشاء إجراءات التحقيق يساهم في حسن سير العدالة، لما في ذلك من حرص على سلامته من الآثار السلبية الناجمة عادة عن إفشائه، كمحاولة طمس الحقيقة، أو إخفاء الأدلة وأدوات الجريمة، وغيرها.[3]

غير أنه وتفاديا لانتشار معلومات غير صحيحة أو غير كاملة، أو من أجل وضع حد للإخلال بالنظام العام، أجاز المشرع لممثل النيابة أو لضابط الشرطة القضائية بعد الحصول على إذن مكتوب من وكيل الجمهورية، أن يُطلع الرأي العام بعناصر موضوعية مستخلصة من الإجراءات، دون أن تتضمن أي تقييم للأعباء المتمسك بها ضد الأشخاص المتورطين.[4]

03- علانية التحقيق بالنسبة للخصوم: بحكم أن للتحقيق طابع السرَية الذي لا ينصرف أثره إلى أطراف الدعوى الجنائية، فإنه يكون وجاهيا بالنسبة لهم، وحضور إجراءات التحقيق يعني كل ذي مصلحة فيه، سواء أكان متهما أم مدعيا مدنيا أم دفاعا أم نيابة، لما يحققه ذلك من رقابة على إجراءات التحقيق وضمانة لحقوق الدفاع، فضلا عمَا يمنحه من طمأنينة لأطراف الدعوى، وفرصة لتفنيد الأدلة أو تعزيزها.[5]

---

[1]- راجع المادة: 11 ق إ ج.

[2]- عبد الواحد إمام مرسى، المرجع السابق، ص: 20.

[3]- فوزي عمارة، قاضي التحقيق، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2009-2010، ص: 31- 32.

[4]- راجع المادة 3/11 ق إ ج.

[5]- أحمد بسيوني أبو الروس، المرجع السابق، ص: 23.

وتحقيقا لخاصية العلانية أوجب القانون إخطار أطراف الدعوى بمواعيد التحقيق، ومنح للمتهم الحق في اصطحاب محاميه قبل استجوابه، إذ أنه لا يمكن الفصل بين المتهم ومحاميه طبقا لنصوص المواد: 100، 102، 104، 105 ق إ ج، مثلما يحق لوكيل الجمهورية أيضا إعمالا لحقه في الإعلام والاطلاع حضور إجراءات التحقيق، وإبداء رأيه وتقديم طلباته بخصوصها.[1]

واستثناء من ذلك يمكن لقاضي التحقيق مباشرة الإجراءات في غياب الخصوم متى دعته إلى ذلك ضرورة، أو توافرت حالة من حالات الاستعجال،[2] على أن يسمح للأطراف بالإطلاع على الأوراق المثبتة لهذه الإجراءات، ويخضع تقدير حالة الاستعجال أو الضرورة للسلطة التقديرية لقاضي التحقيق حسب ظروف وملابسات كل قضية.

ثانيا: الخصائص الذاتية للتحقيق في الجريمة الإلكترونية: رغم تشابه التحقيق في الجرائم العادية مع التحقيق في الجرائم الإلكترونية من الناحية الإجرائية، إلا أن تمايز الجريمتين أوجب تطوير أساليب التحقيق في هذه الأخيرة بصورة تتلاءم مع خصوصيتها، ويتمكن معها المحقق من كشف ملابساتها والتوصل إلى مرتكبيها، فالتحقيق في هذا النوع من الجرائم يستدعي إلى جانب السرعة والدقة، الدراية الواسعة بتقنية المعلومات، باعتبار أن أغلب الإجراءات تتم في بيئة افتراضية سرعان ما تتغير ويذهب معها الدليل، الأمر الذي يتضح معه تميّز التحقيق في الجرائم الإلكترونية بعدة خصائص، أهمها:

01- التحقيق في الجريمة الإلكترونية علم: وتظهر هذه الصفة في قواعده الثابتة والراسخة، سواء القواعد القانونية، وما يميزها من ثبات تشريعي يعدم سلطة المحقق ويلزمه بالتطبيق الحرفي للنصوص القانونية، أو القواعد الفنية وما يميزها من مرونة تتيح للمحقق أن يضفي عليها الكثير من خبرته وفطنته.[3]

---

[1]- راجع المادة 106 ق إ ج.

[2]- تنص المادة 99 ق إ ج "إذا تعذر على شاهد الحضور انتقل إليه قاضي التحقيق لسماع شهادته، أو اتخذ لهذا الغرض طريق الإنابة القضائية".

[3]- عبد الواحد إمام مرسي، المرجع السابق، ص: 155.

02- التحقيق في الجريمة الإلكترونية فن: فالكشف عن غموض الجريمة الإلكترونية مقارنة بخصوصيتها وتعقيداتها التقنية، يتطلب توافر المدارك العلمية والخبرات العملية، واكتساب المهارات الإبداعية والقدرات الذهنية والعقلية، التي تساعد في الوصول إلى الأدلة القانونية لإسناد أو نفي اتهام جنائي قائم من جهة، ولمواجهة ذوي المهارات العلمية والتقنية العالية، وما يتمتعون به من ذكاء ومهارة عند ارتكاب جرائمهم، وسرعتهم في التخفي من جهة ثانية.[1]

فالتحقيق الجنائي في الجريمة الإلكترونية ليس استجوابا يقتصر على طرح الأسئلة وتلقي الأجوبة، بل يعتمد أيضا على الدراسة والمهارة والخبرة والفراسة، إذ أن أي قصور في التحقيق أو أي خطأ في إجراءاته أو في توقيته، من شأنه أن يؤدي إلى ضياع الحقيقة واندثار أدلتها.[2]

03- التحقيق في الجريمة الإلكترونية منظومة عمل متكاملة: نظرا لما تفرضه الخصائص الذاتية للتحقيق في الجريمة الالكترونية من نهج إجراءات سريعة ومشروعة للوصول إلى الأدلة الإلكترونية وحفظها في أقراص معدة لذلك قبل إتلافها، يتطلب الأمر وجود فريق عمل متكامل يجمع بين المعرفتين القانونية والتقنية؛ الأولى يتمتع بها رجال القضاء ضمانا لشرعية إجراءات التحقيق، والثانية يتمتع بها ذوو الخبرة والتخصص في مجال المعلوماتية، ولتطبيقهما معا أثر بالغ في فك التعقيدات التي تفرضها ظروف وملابسات هذا الإجرام الخطير.

فالتحقيق في الجريمة الإلكترونية منظومة عمل تتضافر فيها جهود السلطة القضائية، مع أعمال الشرطة القضائية، وخبرة أهل الاختصاص في مجال المعلوماتية، من أجل كشف غموض الجرائم والوصول إلى أدلتها في إطار القواعد القانونية المنظمة لذلك.[3]

---

[1]- يحيى عطوة الزنط، المرجع السابق، ص: 294-295.

[2]- عبد الواحد إمام مرسي، المرجع السابق، ص: 11.

[3]- يحيى عطوة الزنط، المرجع نفسه، ص: 294-295.

المطلب الثاني

أحكام التحقيق في الجريمة الإلكترونية

انطلاقا مما سبق بيانه، سواء بخصوص الطابع القضائي لمرحلة التحقيق الابتدائي تمييزا لها عن مرحلة التحقيق الأولي، أو بخصوص تعريف التحقيق الجنائي في الجريمة الإلكترونية، يتبادر السؤال عن الأحكام التي تحكم التحقيق في هذا النوع من الجرائم، سواء ما تعلق بالجهة التي تختص به، أو قواعد الاختصاص التي تنظمها، وهو الأمر الذي يشمله هذا المطلب.

الفرع الأول: جهة التحقيق في الجريمة الإلكترونية

يباشر عملية التحقيق بقصد البحث والتنقيب عن الحقيقة وما يرتبط بها من أدلة وأعباء قضاة يعينون لهذا الغرض، ويتم ذلك على درجتين؛ درجة أولى يمثلها قضاة التحقيق على مستوى المحاكم، ودرجة ثانية تمثلها غرفة الاتهام على مستوى المجلس.

أولا: التحقيق على مستوى الدرجة الأولى: أسند المشرع الجزائري مهمة التحقيق الابتدائي إلى قضاة يعينون خصيصا لهذا الغرض بموجب مرسوم رئاسي يصدره رئيس الجمهورية، بعد مداولة المجلس الأعلى للقضاء،[1] وتنتهي مهامهم بنفس الطريقة، فضلا عن أسباب أخرى كالوفاة، الاستقالة، فقدان الجنسية الجزائرية، الإحالة على التقاعد، العزل أو التسريح،[2] وتجدر الإشارة إلى أن قضاة التحقيق كان يتم تعيينهم بقرار من وزير العدل.[3]

يختص قاضي التحقيق بإجراءات التحقيق في القضايا المعروضة عليه، ويجمع في وظيفته بين أعمال الشرطة القضائية من تحري وبحث عن الجريمة، وأعماله كقاض يصدر مجموعة من

---

[1]– راجع المادة 03 من قانون العضوي رقم 04–11 المؤرخ في 06–09–2004 المتضمن القانون الأساسي للقضاء، الجريدة الرسمية لسنة 2004، العدد 57.

[2]– راجع المادة 84 من القانون الأساسي للقضاء.

[3]– مرَ قاضي التحقيق في تعيينه بثلاث مراحل، إذ كان يعين من بين قضاة المحكمة بقرار من وزير العدل طبقا للمادة 39 ق إ ج، ثم أصبح يعين بمرسوم رئاسي بعد تعديل المادة 39 بالقانون 01–08، ثم بموجب مرسوم رئاسي بناء على اقتراح من وزير العدل، وذلك بعد إلغاء المادة 39 بالقانون 06–22. أوهايبية عبد الله، شرح قانون الإجراءات الجزائية، مرجع سابق، ص: 382.

الأوامر ذات الطبيعة القضائية،[1] ولا يجوز له الفصل في قضايا سبق له أن حقَق فيها وإلا كان حكمه باطلا، [2] ولا أن يحقق في قضايا من تلقاء نفسه، بل يجب أن ترفع إليه الدعوى من قبل غيره، إما بواسطة طلب افتتاحي لإجراء تحقيق صادر عن وكيل الجمهورية،[3] أو عن طريق شكوى مصحوبة بادعاء مدني،[4] كما يمكن أن تعرض عليه بطرق أخرى كالأمر بالتخلي، أو إثر تنازع للاختصاص بين القضاة، وذلك تطبيقا لقاعدة الفصل بين وظيفتي المتابعة والتحقيق.[5]

وإذا كان قاضي التحقيق هو صاحب الاختصاص الأصيل في مباشرة إجراءات التحقيق، فإنه يمكن استثناء لرئيس محكمة الجنايات أن يتخذ أي إجراء من هذه الإجراءات إذا رأى بأن التحقيق غير واف، أو اكتشف عناصر جديدة بعد صدور قرار الإحالة،[6] كما يمكن لقاضي الجنح والمخالفات إجراء تحقيق تكميلي متى تبين لهم خلال جلسة المحاكمة عدم كفاية الأدلة، أو بقاء بعض المسائل غامضة، على أن يتم ذلك بحكم قبل الفصل في الموضوع، تحدد فيه المهمة المراد إنجازها، ويتبع في هذه الحالة نفس الأحكام الخاصة بالتحقيق الابتدائي،[7] مثال ذلك أن يندب قاضي الحكم أحد ضباط الشرطة القضائية لسماع شاهد معين، أو للاتصال بأحد متعاملي الهاتف النقال لتحديد هوية صاحب رقم هاتفي معلوم.

وبالنسبة للجرائم المرتكبة من قبل الأحداث، فيختص بالتحقيق فيها حسب تصنيفها كل من قاضي التحقيق المكلف بالتحقيق بالنسبة للجنايات، وقاضي الأحداث بالنسبة للجنح، وحتى المخالفات متى طلبه وكيل الجمهورية.[8]

---

[1]– راجع المواد: 68، 109، 163 ق إ ج.

[2]– راجع المادة: 38 ق إ ج.

[3]– راجع المادة 67 ق إ ج.

[4]– راجع المادة 72 ق إ ج.

[5]– راجع المادة 545 ق إ ج.

[6]– راجع المادة 276 ق إ ج.

[7]– راجع المواد: 276، 356، 401 ق إ ج.

[8]– راجع المواد:61، 64 من القانون رقم 15–12 المؤرخ في 15–07–2015 المتعلق بحقوق الطفل، الجريدة الرسمية لسنة 2015، العدد 39.

فقاضي التحقيق إذا، هو أحد أعضاء الهيئة القضائية للمحكمة، ينتمي بحكم وظيفته إلى القضاء الجالس، ويتمتع بما قرَره القانون لهم من ضمانات واستقلالية عن النيابة العامة وعن السلطة التنفيذية،[1] ولا يخضع إلا للقانون وضميره المهني، وتتجلى مظاهر استقلاليته في:

01- تعيينه بموجب مرسوم رئاسي: بعد أن كان يتم تعيين قاضي التحقيق وإنهاء مهامه بقرار من وزير العدل، وما انجر عن ذلك من خضوعه للسلطة التنفيذية، أصبح يعيَن بموجب مرسوم رئاسي، وذلك تجسيدا لمبدأ استقلالية القاضي المكرس دستورا.[2]

02- استقلاليته في اختيار طريقة عمله: إن خضوع قاضي التحقيق لسلطان القانون وضميره المهني يجعله مستقلا في اتخاذ ما يراه مفيدا للتحقيق من إجراءات، كالأمر بإجراء خبرة من عدمه أو سماع شاهد أو الاستغناء عن شهادته، أو مباشرة التفتيش بنفسه أو عن طريق إنابة ضابط شرطة قضائية، على غرار حرَيته في اتخاذ إجراء دون آخر، كإخضاع المتهم لالتزامات الرقابة القضائية بدل وضعه رهن الحبس المؤقت أو العكس، باعتبار أنه غير مقيد بطلبات الأطراف بما فيهم النيابة، شريطة أن يسبَب أوامره الفاصلة في طلباتهم بأمر قابل للاستئناف.[3]

ثانيا: التحقيق على مستوى الدرجة الثانية: تكريسا لمبدأ المحاكمة العادلة وحفاظا على حقوق وحريات الأشخاص، وضع المشرع الجزائري جهة تحقيق على مستوى الدرجة الثانية، تعمل على مراقبة أعمال قاضي التحقيق باعتباره درجة أولى، أطلق عليها تسمية غرفة الاتهام، وتأخذ تسميات أخرى، كقضاء الإحالة في الفقه، ودائرة الاتهام في التشريع التونسي، والغرفة الجنحة في التشريع المغربي، وغرفة التحقيق عند المشرع الفرنسي.[4]

توجد على مستوى كل مجلس قضائي غرفة اتهام أو أكثر بحسب ما تقتضيه ظروف العمل، تتشكل من رئيس غرفة ومستشارين يتم اختيارهم من بين قضاة المجلس القضائي، يعينون

---

[1]- عبد الرحمان خلفي، المرجع السابق، ص: 279-280.

[2]- تنص المادة 163 من الدستور الجزائري: "القضاء سلطة مستقلة، القاضي مستقل، لا يخضع إلا للقانون"، المرسوم الرئاسي رقم 14-442 المؤرخ في: 30-12-2020، المتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء 01-11-2020، الجريدة الرسمية لسنة 2020، العدد 82.

[3]- محمد حزيط، المرجع السابق، ص: 25.

[4]- عبد الرحمان خلفي، المرجع نفسه، ص: 362.

بقرار من وزير العدل،[1] ويمثل النيابة العامة أمامها النائب العام أو أحد مساعديه، مثلما يقوم بكتابة الضبط فيها أحد أمناء الضبط بالمجلس القضائي، تنعقد جلساتها باستدعاء من رئيسها، أو بطلب من النيابة العامة كلما دعت الضرورة لذلك.[2]

تتمتع غرفة الاتهام بجميع صلاحيات قاضي التحقيق؛ فيجوز لها اتخاذ جميع إجراءات التحقيق التي تراها ضرورية،[3] كما يجوز لها الأمر بحبس المتهم أو الإفراج عنه،[4] أو الأمر بألاَ وجه للمتابعة،[5] مثلما لها صلاحية إحالة الملف على الجهة القضائية المختصة، سواء أكانت محكمة الجنايات أم قسم الجنح أم قسم المخالفات،[6] وتختص كذلك بالنظر في الطعون المرفوعة ضد أوامر قاضي التحقيق،[7] فضلا عن مراقبة إجراءاته من حيث مدى قابليتها للبطلان،[8] والفصل والفصل في تنازع الاختصاص بين القضاة داخل نفس المجلس القضائي.[9]

الفرع الثاني: قواعد الاختصاص في الجريمة الإلكترونية

الاختصاص القضائي بمعناه العام يتمثل في معايير منح المحكمة أو الجهة القضائية صلاحية أو أهلية النظر في الدعوى،[10] ويدخل ضمن المفهوم الواسع للمحكمة (جهة الاتهام، جهة التحقيق، جهة الحكم).

وتعد مسألة تحديد الاختصاص القضائي من أهم العوائق التي أفرزتها الجريمة الإلكترونية كونها عابرة للحدود، قد تقع في دولة واحدة وقد تقع في عدة دول، وهو ما أربك السلطات القضائية

---

[1]– راجع المادة 176 ق إ ج.

[2]– راجع المواد: 177 ، 178 ق إ ج.

[3]– راجع المادة 186 ق إ ج.

[4]– راجع المواد من 186 إلى 192 ق إ ج.

[5]– راجع المادة 195 ق إ ج.

[6]– راجع المواد من 196 إلى 197 ق إ ج.

[7]– راجع المواد: 170، 171، 172 ،173 ق إ ج.

[8]– راجع المادة 191 ق إ ج.

[9]– راجع المواد: 545 ،546 ق إ ج.

[10]– عبد الرحمان خلفي، المرجع السابق، ص: 283.

عند تحديد الجهة التي يؤول إليها الاختصاص القضائي، لذلك سنتطرق إلى قواعد الاختصاص القضائي على المستوى الوطني، ثم على المستوى الدولي.

الفقرة الأولى: على المستوى الوطني

يتحدد اختصاص قاضي التحقيق عموما من خلال ثلاثة معايير، الأول شخصي بالنظر إلى مرتكب الجريمة، والثاني نوعي بالنظر إلى طبيعة الجريمة، والأخير محلي بالنظر إلى مكان ارتكابها أو محل إقامة مرتكبها أو مكان القبض عليه، وتعتبر هذه القواعد من النظام العام التي لا يمكن الاتفاق على مخالفتها.[1]

وإذا كان الاختصاص الشخصي للتحقيق في الجريمة الإلكترونية يخضع لنفس القواعد الإجرائية العامة، فإن الاختصاص النوعي والمحلي يتميزان ببعض الخصوصيات، الناتجة عن الطبيعة الخاصة للجريمة الإلكترونية، لذلك سنركز في دراستنا هذه على هذين النمطين الأخيرين.

أولا: الاختصاص النوعي: يتحدد الاختصاص النوعي في المادة الجزائية استنادا إلى المعيار الكمي؛ أي جسامة الجريمة، ويكون عادة بحسب تصنيفها (جناية، جنحة، مخالفة)، مثلما أخذ به المشرع الجزائري.[2]

لذلك يختص القضاء العادي في معظم الدول بالتحقيق في الجريمة الإلكترونية، غير أن نقص المهارة والخبرة التقنية للمحقق مقارنة بما يتمتع به مرتكبو هذه الجرائم من مهارات عالية في مجال المعلوماتية أدى إلى صعوبة اكتشافها، الأمر الذي جعل المشرع الجزائري يحيطه ببعض القواعد الخاصة.

01- التحقيق على مستوى المحاكم: يعد التحقيق الابتدائي لازما في مواد الجنايات، إذ لا يجوز إحالة المتهم مباشرة للمحاكمة حال متابعته بجناية إلا بعد إجراء تحقيق قضائي، وذلك لخطورة هذه الجرائم وشدة عقوباتها، أما في مواد الجنح فهو اختياري، يخضع لتقدير النيابة العامة، ويلجأ إليه

[1]- جمال نجيمي، دليل القضاة للحكم في الجنح والمخالفات، ج 1، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014، ص: 58.

[2]- عبد الرحمان خلفي، المرجع السابق، ص: 283.

عادة في القضايا المعقدة أو المرتبطة بجرائم أخرى، أو في حالات بقاء الجاني مجهولا أو فارا، بينما يجوز إجراؤه في مواد المخالفات متى طلبه وكيل الجمهورية،[1] وذلك لكونها أقل خطورة من الجنايات والجنح، وعقوباتها أقل قسوة.

02- التحقيق على مستوى الجهات القضائية ذات الاختصاص الموسع: ساير المشرع الجزائري التشريعات الدولية باستحداث أقطاب جزائية متخصصة لمعالجة بعض الجرائم الخطيرة، فأنشأ جهات قضائية متخصصة بموجب القانون رقم: 04-14 المعدل لقانون الإجراءات الجزائية، يعهد بها لقضاة تحقيق من ذوي الخبرة والتكوين المتخصص في المسائل المتعلقة بجرائم محددة على سبيل الحصر، من بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،[2] وتتميز الأقطاب الجزائية عن المحاكم العادية بكونها جهات قضائية متخصصة، رغم أنها تتشكل بدورها من قضاة تحقيق وحكم ونيابة، إضافة إلى أمناء ضبط، وتخضع الدعوى العمومية فيها لنفس القواعد الإجرائية العامة، مع مراعاة بعض الأحكام الخاصة بها.[3]

وقد حدد المرسوم التنفيذي رقم: 06-348 المؤرخ في: 05-10-2006،[4] المعدل بالمرسوم التنفيذي رقم: 16-267 المؤرخ في: 17-10-2016،[5] الجهات القضائية ذات الاختصاص الموسع بأربع محاكم موزعة على الجهات الأربع للوطن (سيدي امحمد، قسنطينة، وهران، ورقلة).

ورغم منح المشرع الجزائري الأقطاب الجهوية المتخصصة مهمة التحقيق الابتدائي في الجريمة الإلكترونية، إلا أنه لم ينزع اختصاص نظرها من المحاكم العادية، ما لم يتمسك النائب

---

[1]- راجع المادة 66 ق إ ج.

[2]- راجع المادة 40 ف 02 ق إ ج.

[3]- تنص المادة: 40 مكرر ق إ ج: "تطبق قواعد هذا القانون المتعلقة بالدعوى العمومية والتحقيق والمحاكمة أمام الجهات القضائية التي تم توسيع اختصاصها المحلي طبقا للمواد: 37 و40 و329 من هذا القانون، مع مراعاة أحكام المواد من 40 مكرر 1 إلى 40 مكرر 5".

[4]- مرسوم تنفيذي رقم: 06-348 المؤرخ في: 05-10-2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية لسنة 2006، العدد 63.

[5]- مرسوم تنفيذي رقم: 16-267 مؤرخ في: 17-10-2016 يعدل المرسوم التنفيذي رقم: 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية لسنة 2016، العدد 62.

العام لدى المجلس القضائي الواقع بدائرة اختصاصه القطب الجهوي بالاختصاص، أو من خلال تقديم طلب التخلي عن الملف لقاضي التحقيق بالقطب،[1] لذلك يعد اختصاص الأقطاب الجهوية اختصاصا تفضيليا وليس مانعا.

وفي هذا الصدد، وطالما أن المشرع الجزائري قد أخذ بالتعريف الموسع للجريمة الإلكترونية الذي يشمل الجرائم التي تستهدف النظام المعلوماتي (جرائم المساس بأنظمة المعالجة الآلية للمعطيات) إلى جنب الجرائم التي ترتكب باستخدام تكنولوجيات الإعلام والاتصال من جهة، وأمام تعدد مهام الأقطاب الجهوية التي لم تعد قادرة على مواجهة عدة جرائم خطيرة ومتنوعة، يحتاج كل صنف منها إلى تخصص معين بذاته من جهة أخرى، فإننا ندعو إلى استحداث أقطاب جهوية متخصصَة في مكافحة الجريمة الإلكترونية من أجل تحقيق الفعالية اللازمة لجهاز التحقيق والوصول إلى الغاية المنشودة.

03- التحقيق على مستوى القطب الوطني الإلكتروني: رغم أنه سبق للمشرع إنشاء أقطاب جزائية متخصصة للفصل في بعض الجرائم الخطيرة بموجب القانون رقم: 04-14، ومنها الجرائم الإلكترونية كما سبق ذكره، إلا أن تعدد اختصاص هذه الأقطاب في عدة جرائم مختلفة، تتطلب كل جريمة منها تخصصا معينا، حال دون فعاليتها، وهو ما جعل المشرع يتجه إلى إنشاء قطب وطني متخصص في مكافحة الجريمة الإلكترونية، بموجب الأمر رقم: 21-11،[2] أسماه بالقطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، ومنحه اختصاصا وطنيا من أجل تجاوز العوائق التي تواجهها جهات التحقيق.

وإن كانت مرحلتا الاتهام والتحقيق الابتدائي على مستوى القطب الإلكتروني تناطان إلى وكيل الجمهورية وقاضي التحقيق، كل حسب اختصاصه، إذ يباشر الأول منهما متابعة الجرائم الإلكترونية والجرائم المرتبطة بها، في حين يباشر الثاني التحقيق والتصرف في هذه الجرائم طبقا

[1]- راجع المادة: 40 مكرر 03 ق إ ج.

[2]- الأمر رقم 21-11 المؤرخ في: 25-08-2021، المتمم لقانون الإجراءات الجزائية، الجريدة الرسمية لسنة 2021، العدد 65.

للقانون،[1] إلا أن قاضي الحكم لدى القطب الإلكتروني يختص بنظر الجرائم الإلكترونية والجرائم المرتبطة بها حال وصفها بالجنح، أما الجرائم الموصوفة بالجنايات، والتي تم التحقيق فيها من طرف قاضي التحقيق لدى القطب الإلكتروني، فتخرج من ولايته وتخضع لاختصاص محكمة الجنايات بمجلس قضاء الجزائر.[2]

ثانيا: الاختصاص المحلي: الأصل في الاختصاص المحلي لقاضي التحقيق أنه يتحدد بدائرة إقليمية معينة، غير أنه يمكن تمديده في بعض الحالات ليشمل دوائر اختصاص محاكم أخرى، كما قد يمتد ليشمل كافة الإقليم الوطني، وهو ما سنتطرق له تباعا:

01- على مستوى المحكمة: نظم المشرع الجزائري الاختصاص المحلي لقاضي التحقيق ضمن المادة 40 ق إ ج، من خلال تقييده بثلاثة معايير؛ الأول مكان وقوع الجريمة، والثاني محل إقامة المتهم، والثالث مكان القبض عليه،[3] وهي قاعدة عامة تسري على جميع الجرائم، باستثناء بعض الحالات التي ينحصر فيها الاختصاص المحلي لقاضي التحقيق على مستوى القطب الوطني الإلكتروني دون سواه، والتي سنتطرق إليها في حينها.

غير أنه يجوز لقاضي التحقيق التنقل رفقة كاتبه إلى المحاكم المجاورة إذا تطلب التحقيق ذلك، بشرط إخبار وكيلي الجمهورية لدى محكمة دائرة اختصاصه والمحكمة التي سينتقل إليها وذكر أسباب انتقاله ضمن المحضر،[4] كما يتمتع قاضي التحقيق باختصاص وطني لاتخاذ بعض الإجراءات اللازمة مثل التفتيش، الحجز، وأساليب التحري الخاصة، في بعض الجرائم المحددة على سبيل الحصر، ومن بينها الجرائم المعلوماتية.[5]

02- على مستوى الجهات القضائية ذات الاختصاص الموسع: يتسع اختصاص قاضي التحقيق لدى الأقطاب الجهوية المتخصصة، ليشمل الاختصاص الإقليمي لمجالس قضائية أخرى.

---

[1]- راجع المادة 211 مكرر ف 1 من الأمر 21-11.

[2]- وهو ما نصت عليه صراحة الفقرة الثانية من المادة 211 مكرر 22 ق إ ج.

[3]- راجع المادة 40 ق إ ج.

[4]- راجع المادة: 80 ق إ ج.

[5]- راجع المادة 47 ف 3، 4 ق إ ج.

فاختصاص قاضي التحقيق لدى محكمة سيدي امحمد يمتد ليشمل النطاق الإقليمي للمحاكم التابعة للمجالس القضائية لكل من: (الجزائر، الشلف، الأغواط، البليدة، البويرة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس، تيبازة، وعين الدفلى).[1]

بينما يمتد اختصاص قاضي التحقيق لدى محكمة قسنطينة ليشمل اختصاص المحاكم التابعة للمجالس القضائية لكل من: (قسنطينة، أم البواقي، باتنة، بجاية، بسكرة، تبسة، جيجل، سطيف، سكيكدة، عنابة، قالمة، برج بوعريريج، الطارف، الوادي، خنشلة، سوق اهراس، وميلة).[2]

أما الاختصاص المحلي لقاضي التحقيق لدى محكمة ورقلة فيمتد بدوره ليشمل نطاق اختصاص المحاكم التابعة للمجالس القضائية لكل من: (ورقلة، أدرار، تامنغست، إليزي، تندوف، وغرداية).[3]

وكذلك الاختصاص المحلي لقاضي التحقيق لدى محكمة وهران يمتد ليشمل اختصاص المحاكم التابعة للمجالس القضائية لكل من: (وهران، بشار، تلمسان، تيارت، سعيدة، سيدي بلعباس مستغانم، معسكر، البيض، تيسمسيلت، النعامة، عين تيموشنت، وغليزان).[4]

03- **على مستوى القطب الوطني الإلكتروني:** نظرا لخصوصيات الجريمة الإلكترونية التي جعلت أجهزة التحقيق التقليدية تقف عاجزة عن ضبط أدلتها الرقمية، وسَع المشرع اختصاص هذا القطب وجعله وطنيا تبعا لما يزخر به من آليات وكفاءات تساعده على التصدي لهذه الجرائم، إذ يتمتع قاضي التحقيق لديه باختصاص وطني، على غرار كل من وكيل الجمهورية ورئيس القطب،[5] وذلك فق نمطين:

[1]- راجع المادة 02 من المرسوم التنفيذي رقم 06-348.
[2]- راجع المادة 03 من المرسوم التنفيذي رقم 16-267.
[3]- راجع المادة 04 من المرسوم التنفيذي رقم 16-267.
[4]- راجع المادة 05 من المرسوم التنفيذي رقم 16-267.
[5]- راجع المادة:211 مكرر 23 ق إ ج.

النمط الأول: الاختصاص الحصري

ينعقد الاختصاص للقطب الإلكتروني دون سواه في معالجة الجرائم الإلكترونية المرتكبة عبر كافة الإقليم الوطني في حالتين:

أ- **الجرائم المحددة قانونا والجرائم المرتبطة بها:** يختص قاضي التحقيق لدى القطب الوطني الإلكتروني بالتحقيق دون سواه عبر كافة الإقليم الوطني في الجرائم الإلكترونية التالية:[1]

* الجرائم الماسة بأمن الدولة أو بالدفاع الوطني.

* جرائم نشر وترويج أخبار كاذبة من شأنها المساس بالأمن أو السكينة العامة أو استقرار المجتمع.

* جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.

* جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.

* جرائم التمييز وخطاب الكراهية.

* جرائم الاتجار بالأشخاص أو الأعضاء البشرية أو تهريب المهاجرين.

كما يختص كذلك بمعالجة الجرائم المرتبطة بالجرائم الإلكترونية المذكورة، وتتمثل حالات الارتباط حسب أحكام المادة 188 ق إ ج في:

* ارتكاب الجرائم من طرف عدة أشخاص مجتمعين في وقت واحد.

* ارتكاب الجرائم من طرف عدة من أشخاص، وبموجب تدبير إجرامي سابق بينهم.

* ارتكاب الجناة لبعض هذه الجرائم بغرض الحصول على وسائل ارتكاب جرائم أخرى أو لتسهيل ارتكابها، أو إتمام تنفيذها، أو لجعلهم في مأمن من العقاب.

[1]- راجع المادة: 211 مكرر 24 ق إ ج.

* إخفاء الأشياء المنتزعة أو المختلسة أو المتحصلة من جناية أو جنحة.

ب- الجرائم المعقدة والجرائم المرتبطة بها: يختص أيضا قاضي التحقيق لدى القطب الإلكتروني بالتحقيق دون سواه في الجرائم الإلكترونية الأكثر تعقيدا والجرائم المرتبطة بها عبر كافة الإقليم الوطني.[1]

وقد عرفت المادة 211 مكرر 25 ق إ ج الجريمة الأكثر تعقيدا بأنها: "الجريمة التي بالنظر إلى تعدد الفاعلين أو الشركاء أو المتضررين، أو بسبب اتساع الرقعة الجغرافية لمكان ارتكاب الجريمة أو جسامة آثارها، أو الأضرار المترتبة عليها، أو لطابعها المنظم، أو العابر للحدود الوطنية، أو لمساسها بالنظام والأمن العموميين، تتطلب استعمال وسائل تحري خاصة، أو خبرة فنية متخصصة، أو اللجوء إلى تعاون قضائي دولي".

النمط الثاني: الاختصاص التفضيلي

يتمتع قاضي التحقيق لدى القطب الإلكتروني عند معالجته للجرائم الإلكترونية والجرائم المرتبطة بها التي تخرج من اختصاصه المانع باختصاص مشترك مع باقي الجهات القضائية المختصة أصلا، مع تمتعه بحق الأفضلية،[2] إذ يمارس اختصاصا مشتركا مع الجهة القضائية المختصة محليا طبقا للمادة 40 ق إ ج، غير أن لوكيل الجمهورية لدى القطب الإلكتروني كامل السلطة للمطالبة بالملف، بعد أخذ رأي النائب العام لدى مجلس قضاء الجزائر، وفي هذه الحالة يتم تفعيل الإجراءات المعمول بها بالنسبة للأقطاب الجزائية المتخصصة.

غير أنه إذا تزامنت المطالبة بالملف من طرف وكيل الجمهورية لدى القطب الإلكتروني مع المطالبة به من قبل وكيل الجمهورية لدى القطب الجهوي المتخصص، فإن الاختصاص يؤول وجوبا للقطب الوطني الإلكتروني،[3] أما إذا تزامن اختصاص هذا الأخير مع اختصاص القطب الوطني الاقتصادي والمالي، فإن الاختصاص يؤول لهذا الأخير،[4] ونفس الأمر في حالة تزامن

[1]- راجع المادة 211 مكرر 25 ف 1 ق إ ج.
[2]- راجع المادة 211 مكرر 27، ف 01 ق إ ج.
[3]- راجع المادة 211 مكرر 11 ف 01 ق إ ج.
[4]- راجع المادة 211 مكرر 28 ق إ ج.

اختصاص القطب الإلكتروني مع اختصاص محكمة مقر مجلس قضاء الجزائر، أين يؤول الاختصاص لهذه الأخيرة.[1]

ورغم أهمية هذا القطب في مكافحة الجرائم الإلكترونية، إلا أن تخصيص قطب وطني واحد من شأنه أن يؤدي إلى إبعاد العدالة عن المتقاضي، وإطالة أمد التقاضي مقارنة بالحجم الكمي للقضايا المطروحة أمامه، بما قد ينعكس سلبيا على نوعية الأحكام، الأمر الذي يجعلنا ندعو ثانية إلى إنشاء عدة أقطاب جهوية متخصصة في مكافحة هذا النوع الخطير من الإجرام.

الفقرة الثانية: على المستوى الدولي

في ظل ما تتميز به الجريمة الإلكترونية من بعد عالمي، فإن سلوكها المجرَم قد يرتكب في دولة معينة، وتتحقق نتيجته في دولة أخرى، وهنا تبرز مسألة تنازع الاختصاص بين الدول باعتبارها أحد أصعب العراقيل التي تعيق التحقيق الجنائي، ممَا يدفعنا إلى التساؤل عن الحالات التي ينعقد فيها الاختصاص للقضاء الوطني.

01- اختصاص القاضي الوطني وفقا لمبدأ الإقليمية: أخذ المشرع الجزائري على غرار باقي التشريعات بمبدأ إقليمية القوانين الجزائية، ومؤدَاه أن أي فعل يقع داخل إقليم الدولة ويشكل جريمة في قوانينها الجزائية، يعاقب مرتكبه بمقتضى قوانين تلك الدولة،[2] بغض النظر عن جنسية الجاني والمجني عليه، وعن المصلحة التي أهدرتها الجريمة، حتى ولو تعلقت بدولة أجنبية،[3] وأساس ذلك أن كل جريمة ترتكب في إقليم الدولة تعتبر مساسا بنظامها العام، لذلك لا يمكنها أن تتنازل عن اختصاصها لأي دولة أخرى،[4] كما أن الأخذ بهذا المبدأ فيه تعبير عن استقلال الدولة وتمتعها بالشخصية المعنوية داخل المجتمع الدولي،[5] فضلا عن أن محكمة مكان وقوع الجريمة أقدر على

---

[1]- راجع المادة 211 مكرر 29 ق إ ج.

[2]- أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 11، دار هومة للطباعة والنشر والتوزيع، 2012، ص: 88.

[3]- رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء القانون الجنائي الداخلي والدولي، ط1، دار الجامعة الجديدة، مصر، 2007، ص: 13.

[4]- عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام)،ج 1، ط 6، ديوان المطبوعات الجامعية، الجزائر، 2005، ص: 101-102.

[5]- منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر، الجزائر، 2006، ص: 108.

جمع الأدلة والإحاطة بجميع ظروفها، وأن محاكمة الجاني في بلد ارتكاب الجريمة يحقق الردع العام، ويقضي على الاضطراب الاجتماعي الذي أحدثته تلك الجريمة.[1]

وهو المنهج ذاته الذي كرسته الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، التي ألزمت الدول الأطراف باتخاذ ما يلزم من تدابير لتقرير اختصاص أجهزتها القضائية في متابعة ومحاكمة الجرائم التي تشملها الاتفاقية، خاصة إذا وقعت كلها أو أحد عناصرها في إقليم الدولة، أو تم الإعداد أو التخطيط أو الشروع في تنفيذها أو عند تحقق أحد صور المساهمة على إقليمها، فضلا عن امتداد آثار الجريمة إليه.[2]

كما حددت المادة 30-1 فقرة د من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المعايير التي يتعين اعتمادها من طرف الدول الأطراف لتقرير اختصاصها القضائي لمكافحة الجرائم الإلكترونية، ومن بينها: (حالة ارتكاب الجريمة في إقليم الدولة الطرف، أو على متن سفينة تحمل علم الدولة الطرف أو طائرة مسجلة تحت قوانينها).[3]

ومع ذلك، فإن تحديد مكان وقوع الجريمة ليس بالأمر السهل دائما، إذ أن إتيان السلوك المجرم في دولة معينة، وحدوث نتيجته في دولة أخرى، يقودنا إلى التساؤل عن تحديد مكان وقوع الجريمة، بين مكان حدوث السلوك الإجرامي، أو مكان تحقق نتيجته، حتى يتسنى إسناد الاختصاص لإحدى الدولتين، وهو ما يقودنا لمناقشة الحالات التالية:

أ- **وقوع أحد أفعال الجريمة في الجزائر:** إضافة إلى الحالة التي تُرتكب فيها الجريمة بجميع عناصرها في الجزائر،[4] تُعتبر كذلك كل جريمة تم أحد الأعمال المميزة لأركانها داخل إقليمها،[5]

---

[1]- محمود نجيب حسني، شرح قانون العقوبات اللبناني، المجلد الأول، ط3، منشورات الحلبي الحقوقية، بيروت، 1988، ص: 180.

[2]- نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، 2021-2022، ص: 217.

[3]- صادقت الجزائر على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ 21-12-2010 بموجب المرسوم الرئاسي رقم 14-252 المؤرخ في: 08-09-2014، الجريدة الرسمية لسنة 2014، العدد 57.

[4]- راجع المادة 03 ق ع.

[5]- راجع المادة: 586 ق إ ج.

فيكفي لانعقاد اختصاص القاضي الجزائري أن يُرتكب أحد عناصر الركن المادي للجريمة (الفعل أو النتيجة) في الجزائر، الأمر الذي يتضح معه أن أغلب الجرائم الإلكترونية لا يمكنها أن تفلت من المتابعة الجزائية.

وفي هذا الصدد، أكد الاجتهاد القضائي الفرنسي على تطبيق القانون الفرنسي في حالة نشر الصورة أو الرسالة موضوع الفعل الإجرامي على شبكة الإنترنت بفرنسا، مهما كان مصدر الإرسال عبر العالم،[1] واعتبر أن مجرد الاستقبال من طرف المستخدم على شبكة الإنترنت يعد عنصرا مشكلا للجريمة.

أما في الجزائر، فقد أصدرت المحكمة العليا قرارا بتاريخ: 29-12-2004، ملف رقم: 355105 ورد فيه: "ينعقد الاختصاص في جرائم القذف عن طريق الصحافة المكتوبة أو المسموعة أو المرئية، لكل محكمة قُرئت بدائرتها الصحيفة، أو سُمعت فيها الحصة الإذاعية، أو شُوهدت فيها الحصة المرئية"،[2] وفي ذلك تعزيز لهذا المبدأ.

ب- الاشتراك في الجريمة: يسري قانون العقوبات الجزائري أيضا على كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة ارتكبت في الخارج، حال تحقق الشرطين الآتيين:

* ازدواجية التجريم بين الجزائر والبلد الذي ارتكبت فيه الجريمة.

* ثبوت ارتكاب الجريمة الموصوفة بأنها جنحة أو جناية بقرار نهائي من الجهة القضائية الأجنبية.[3]

ت- ارتكاب الجريمة على متن السفن والطائرات: إضافة للمعايير السابقة، فإن القانون الجزائري يطبق على الجنح والجنايات التي ترتكب على متن الطائرات والسفن التي تحمل العلم الجزائري بغض النظر عن جنسية مرتكبها، أو مكان ارتكابها.[4]

---

[1]- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، مرجع سابق، ص: 89.

[2]- قرار صادر عن الغرفة الجنائية بالمحكمة العليا، بتاريخ: 29-12-2004، ملف رقم: 355105، مجلة المحكمة العليا، عدد خاص، الجزائر، 2019، ص: 641.

[3]- راجع المادة 585 ق إ ج.

[4]- راجع المواد 590 و 591 ق إ ج.

02- اختصاص القاضي الوطني وفقا لمبدأ الشخصية: ويقصد به: "تطبيق قانون العقوبات الوطني على الجاني الوطني الذي يرتكب جريمة في الخارج، ثم يعود لوطنه الذي يحمل جنسيته"،[1] وتتجلى أهميته في كونه وسيلة فعالة لمنع فرار المجرمين من العقاب إلى أوطانهم.

وقد تبنت الاتفاقية الأوروبية المتعلقة بمكافحة الجريمة الإلكترونية هذا المبدأ في مادتها 22-1، وحثت الدول الأطراف على تطبيق قانونها الداخلي على كل مواطن يرتكب جريمة على إقليم دولة أخرى يعاقب عليها القانون الداخلي،[2] كما تبنته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في مادتها 30-1، وبدوره ساير المشرع الجزائري هذه الاتفاقيات، وكرس هذا المبدأ في قانون الإجراءات الجزائية،[3] مانحا بذلك الاختصاص للقاضي الوطني للنظر في الجرائم الآتية:

أ- الجنايات والجنح المرتكبة من طرف جزائريين في الخارج: ينعقد اختصاص القاضي الجزائري للنظر في الجنايات والجنح -بما فيها الجرائم الإلكترونية- التي ارتكبها جزائري خارج إقليم الوطن متى توافرت الشروط الآتية:

* أن يكون الفعل المرتكب مجرما بوصفه جناية حسب القانون الجزائري،[4] أو جنحة طبقا لقانون البلد الذي وقع فيه فضلا عن القانون الجزائري.[5]

فاختصاص القاضي الوطني في نظر القضايا المرتكبة من قبل جزائريين في الخارج ينعقد متى كان تكييفها جنائيا حسب القانون الجزائري، بعض النظر عن موقف قانون مكان ارتكابها سواء ما تعلق بتجريمها أو تكييفها وعقوبتها،[6] أما إذا كان وصفها جنحيا، وارتكبت ضد الأفراد، فلا

---

[1]- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، المؤسسة الوطنية للفنون المطبعية، الرغاية، الجزائر، 2011، ص: 148.

[2]- وقعت 30 دولة على هذه الاتفاقية ببودابيست في 23-11-2001، من بينهم 26 دولة من مجلس أوروبا، إضافة إلى أمريكا وكندا واليابان وجنوب إفريقيا، في حين امتنعت 17 دولة أوروبية عن التوقيع، من بينها الدانمارك وايرلندا، دخلت الاتفاقية حيز التنفيذ عام 2004، انظر: سليمان قطاف، الآليات القانونية لمكافحة الجرائم السيبرانية في ضل اتفاقية بودابيست والتشريع الجزائري، المجلة الأكاديمية للبحوث القانونية والسياسية، المجلد 06، العدد 01، ص: 338.

[3]- راجع المواد: 582 و 583 ق إ ج.

[4]- راجع المادة 582 ق إ ج.

[5]- راجع المادة 583 ق إ ج.

[6]- راجع المادة: 582 ق إ ج.

فلا يختص القاضي الوطني بنظرها إلا بطلب من النيابة العامة بعد تلقيها لشكوى من الطرف المتضرر، أو بلاغ من سلطات البلد الذي ارتكبت فيه الجريمة.[1]

وبمفهوم المخالفة، فإنه ومتى كان محل هذه الجنح ممتلكات عمومية، فللنيابة أن تباشر الدعوى العمومية متى وصل إلى علمها وقوع الجريمة دون اشتراط شكوى المتضرر أو بلاغ سلطات الذي ارتكبت فيه، وفي ذلك تعزيز لحماية الممتلكات الوطنية في الخارج.

* أن يكون الجاني جزائري الجنسية، سواء أكانت أصلية أم مكتسبة،[2] حتى ولو اكتسبها بعد ارتكاب جريمته في الخارج.[3]

* أن يعود الجاني إلى أرض الوطن،[4] بغض النظر عن سبب عودته، لأن تطبيق القانون يستند على المصلحة العامة التي تبرَر العقاب، لا على رغبة الأشخاص.

* ألا يكون قد سبق الحكم على الجاني نهائيا في الخارج، أو استفاد من العفو، أو استنفذ العقوبة المحكوم بها، أو سقطت عنه بالتقادم، إذ لا يجوز محاكمة الشخص على واقعة واحدة مرتين.

وإن كان في تكريس هذا المبدأ تجسيد لسيادة الدولة على أفرادها، إلا أنه يثير إشكالا فيما يتعلق بالوصف الجنائي، وذلك لمَا يرتكب الفرد فعلا في الخارج، يعد مباحا في مكان ارتكابه، لكنه مجرم حسب قانون دولته، فتعاقبه على ذلك، الأمر الذي من شأنه أن يشكل مساسا بحق مكتسب استمده من مبدأ المشروعية الجنائية.

ب- الجنايات والجنح المرتكبة ضد الجزائريين: رغم أخذ المشرع الجزائري بمبدأ الشخصية مثلما سبق بيانه، إلا أنه قصر تطبيقه في بداية الأمر على الحالة التي يكون فيها الجزائريون جناة، بما

[1]- راجع المادة: 583 ف 03 ق إ ج.

[2]- راجع المادة 584 ق إ ج.

[3]- راجع المادة 584 ق إ ج.

[4]- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص: 151.

يشكل تطبيقا للمبدأ في جانبه الإيجابي فقط، دون السلبي حين يكون الجزائريون ضحايا،[1] باستثناء ما أوردته المادة 591 ق إ ج.[2]

غير أن تزايد انتشار الجرائم الماسة بحقوق مواطني الدولة، على غرار الجرائم الإلكترونية، وما خلفته من آثار سلبية، دفع بالمشرع إلى التراجع عن موقفه، والأخذ بمبدأ الشخصية السلبية، ليمنح بذلك القاضي الوطني ولاية النظر في الجرائم المرتكبة خارج الإقليم الوطني متى كان المجني عليه جزائريا، وهو ما تبنَاه من خلال تعديل ق إ ج سنة 2015،[3] وبعض النصوص القانونية الخاصة التي سارت على هذا المبدأ، على غرار قانون الوقاية من خطاب الكراهية والتمييز ومكافحتهما،[4] قانون الوقاية من جرائم اختطاف الأشخاص ومكافحتها،[5] قانون الوقاية من الاتجار بالبشر ومكافحته،[6] وهو موقف إيجابي يحسب للدولة الجزائرية في تعميم سيادتها على مواطنيها أينما تواجدوا ضمانا لحقوقهم وحرياتهم.

03- اختصاص القاضي الوطني وفقا لمبدأ العينية: ويقصد به عموما: "تطبيق القانون الجنائي الوطني على كل جريمة ترتكب في الخارج، وتمس بالمصالح الحيوية للدولة، بغض النظر عن مكان ارتكاب الجريمة وعن جنسية مرتكبها"،[7] ويعتمد الأخذ بهذا المبدأ على معيار أهمية المصلحة المعتدى عليها، إذ أن المساس بالمصالح الأساسية للدولة يجعلها تسعى إلى بسط سلطان قانونها بغية حمايتها من أي جريمة تطالها، خصوصا في حالة عدم تضرر الدولة التي وقعت بها الجريمة، هذا إن لم تكن من المستفيدين منها، أو كان لها ضلع في ارتكابها.

---

[1]- راجع المواد: 582، 583 ق إ ج.

[2]- راجع المادة 591 ق إ ج.

[3]- راجع الفقرة الأخيرة من المادة 588 ق إ ج.

[4]- راجع المادة 21 من القانون رقم:20-05 المتعلق بالوقاية من خطاب الكراهية والتمييز ومكافحتهما.

[5]- راجع المادة 14 من القانون 20-15 المتعلق بالوقاية من جرائم اختطاف الاختطاف ومكافحتها.

[6]- راجع المادة 26 من القانون رقم 23-04 الوقاية من الاتجار بالبشر ومكافحته.

[7]- عبد الله أوهايبية، شرح قانون العقوبات الجزائري، مرجع سابق، ص: 154.

وقد كرّست العديد من التشريعات المقارنة هذا المبدأ، كما تبنته الاتفاقية العربية لمكافحة الجريمة المعلوماتية، التي نصت في مادتها 30-1 على تطبيق القانون الوطني للدولة متى كانت الجريمة المرتكبة تمس أحد مصالحها العليا.

وإذا كان هذا هو مفهوم عينية النص الجنائي، فإن المشرع الجزائري حصره على حماية المصالح الأساسية والاقتصادية للدولة وأمنها و مقراتها الدبلوماسية من الجرائم التي تقع في الخارج من طرف الأجانب فقط دون المواطنين،[1] وهو ما يستشف من نصوص المواد 588، 589 ق إ ج التي قيدته بعدة شروط، تتمثل في:

أ- أن ترتكب الجريمة في الخارج.

ب- أن يكون الجاني أجنبيا.

ت- أن تكون الجريمة المرتكبة جناية أو جنحة تمس بأمن الدولة الجزائرية أو اقتصادها أو بمقراتها الدبلوماسية والقنصلية.

ث- أن يتم القبض على الجاني في الجزائر، أو يسلم لها وفقا لاتفاقيات تسليم المجرمين.

ج- ألاَ يكون قد سبق الحكم على الجاني نهائيا في الخارج، أو استفاد من العفو، أو استنفذ العقوبة المحكوم بها، أو سقطت عنه بالتقادم.

وحسن فعل المشرع الجزائري حين حصر نطاق هذا المبدأ على الأجانب، باعتبار أن المواطنين الجزائريين يخضعون في هذه الحالة لمبدأ الشخصية.

04- اختصاص القاضي الوطني وفقا لمبدأ العالمية: ويهدف هذا المبدأ إلى تطبيق القانون الجنائي للدولة على كل شخص ارتكب جريمة في الخارج وتم القبض عليه داخل إقليمها، بغض النظر عن جنسيته أو مكان ارتكاب جريمته، ورغم قلة التشريعات التي أخذت به على غرار المشرع البلجيكي، إلا أن تعدد الشكاوى ضد رؤساء الدول، وما سببه من حرج دبلوماسي أدى إلى

[1]- راجع المادة 588 ق إ ج.

تلطيف هذا المبدأ،[1] وإن كانت بعض التشريعات العربية قد أخذت به على غرار قانون العقوبات السوري،[2] إلا أن المشرع الجزائري لم يأخذ به.

يستمد هذا المبدأ أهميته من خطورة الإجرام الدولي الحديث، نظرا لما وفَرته سهولة الاتصالات من فرص لتكوين عصابات دولية، تتكون من مجرمين ينتمون إلى جنسيات متنوعة ويمتد نشاطهم الإجرامي إلى دول مختلفة، مما يستوجب تعاون الدول لمكافحته، وذلك بتولي كل واحدة عقاب المجرم الذي يضبط داخل إقليمها، دون الاكتراث بجنسيته أو مكان ارتكاب الجريمة، والدول إنما تفعل ذلك باعتبارها نائبة عن المجتمع الدولي.[3]

ورغم مساهمة هذا المبدأ في مكافحة الجريمة الإلكترونية، إلا أنه يثير عدة إشكالات، أهمها تنازع الاختصاص الإيجابي بين الدول، فضلا عن إمكانية جعل القاضي الداخلي مجرد دبلوماسي أو سياسي، خصوصا في ظل الصراعات والتكتلات الدولية وهيمنة المصالح الخاصة، أين تصبح المتابعات الجزائية متاحة للدول العظمى على حساب الدول الضعيفة، وتفاديا لما يثيره تطبيق هذا المبدأ من إشكالات برز مبدأ المساعدة القضائية الدولية عن طريق تبادل المعلومات والخبرات القضائية، مما يجعلنا ننادي بإمكانية الاستغناء عنه، والتوجه إلى تعزيز المساعدة القضائية للحد من هذه الجرائم.

---

[1]– أحسن بوسقيعة، الوجيز في القانون الجزائي العام، مرجع سابق، ص: 94.

[2]– تنص المادة: 23 من قانون العقوبات السوري، الصادر بالمرسوم التشريعي رقم 148 بتاريخ: 1949: "يطبق القانون السوري على كل أجنبي مقيم في الأرض السورية أقدم في الخارج، سواء كان فاعلا أو محرضا أو متدخلا على ارتكاب جناية أو جنحة غير منصوص عليها في المواد 19 و20 و21 إذا لم يكن استرداده قد طلب أو قبل".

[3]– جمال الدين عنان، عولمة القانون الجنائي (الآليات والمظاهر)، مجلة الدراسات والبحوث القانونية، المجلد 3، العدد 4، 2018، ص: 54.

المبحث الثاني

الأجهزة المساعدة على التحقيق في الجريمة الإلكترونية

بالنظر إلى بروز العديد من الجرائم الإلكترونية التي أضحت تهدد أمن المجتمعات واستقرارها، متأثرة بالتطور السريع الذي شهده العالم في مجال التكنولوجيا وأجهزة الاتصال الحديثة سارع المجتمع الدولي إلى دق ناقوس الخطر من أجل تعزيز أجهزة مكافحة هذه الجرائم، وتطوير آليات مكافحتها.

والجزائر كغيرها من الدول، سعت إلى تعزيز أجهزة مكافحة هذه الجرائم، سواء عن طريق الاستعانة بجهاز الشرطة القضائية، لاسيما من خلال تكوين فرق بحث متخصصة تعمل على مساعدة القضاء من خلال ما تجمعه من أدلة وما تنفذه من طلبات، أو من خلال استحداث هيئة وطنية تقنية، تهتم بتقديم المساعدة القضائية الوطنية والدولية لجهاز التحقيق الجنائي.

ولتوضيح دور هذين الجهازين في مسار التحقيق في الجريمة الإلكترونية ارتأينا تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: جهاز الشرطة القضائية.

المطلب الثاني: الهيئة الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها.

المطلب الأول

جهاز الشرطة القضائية

يضطلع جهاز الشرطة القضائية بإحكام سيادة القانون والسهر على عدم الإخلال به من خلال ممارسته لوظيفيتين متكاملتين؛ الضبط الإداري، والضبط القضائي.

فالضبط الإداري ذو طابع وقائي، غايته المحافظة على النظام العام بعناصره الثلاثة (الأمن العام، الصحة العامة، والسكينة العامة)، من خلال العمل على منع وقوع الجرائم باتخاذ تدابير الوقاية واحتياطات الأمن اللازمين، وهو خارج عن نطاق دراستنا التي تعنى بالتحقيق الذي يكون بعد وقوع الجريمة.

بينما يبدأ الضبط القضائي بعد وقوع الجريمة؛ أي منذ لحظة فشل الضبط الإداري في منع وقوعها ،[1] وهو بذلك يساعد القضاء في مسار التحقيق الجنائي، سواء قبل مرحلة التحقيق الابتدائي، أو خلالها، وهو موضوع دراستنا.

الفرع الأول: مفهوم الشرطة القضائية

سنتطرق من خلال هذا الفرع إلى تعريف الشرطة القضائية وتنظيمها، ثم نتعرف على الشرطة المتخصصة في مكافحة الجريمة الإلكترونية.

الفقرة الأولى: تعريف الشرطة القضائية وتنظيمها

أولا: تعريف الشرطة القضائية: تعددت المصطلحات التي أطلقت على هذا الجهاز حسب منظور كل نظام إجرائي، إذ يسميه التشريع الأردني "الضبطية العدلية"، ويسميه التشريع المصري "الضبطية القضائية"،[2] ونفس التسمية اعتمدها المشرع الجزائري إلى غاية تعديل ق إ ج بموجب القانون رقم 17-07، أين استبدلها بـ "الشرطة القضائية" على غرار التسمية المعتمدة من طرف المشرع الفرنسي (police judiciaire)، وللإلمام بمفهوم هذا الجهاز سنتطرق إلى مختلف تعريفاته:

01- **الشرطة لغة:** تعني: "حَفَظة الأمن في البلد الواحد، وهي جمع شرطي، نقول أَشْرَطَهُ؛ أي جعل له علامة تميّزه عن غيره".[3]

02- الشرطة اصطلاحا: وهي: "قوات نظامية رسمية، يناط بها تطبيق القوانين والمحافظة على النظام العام بجميع عناصره"،[4] وهو المصطلح الذي اعتمدته جامعة الدول العربية سنة 1972.[5]

---

[1]- نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2013، ص: 89.

[2]- كمال بلارو، الشرطة القضائية في التشريع الجزائري، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2020-2021، ص: 18.

[3]- المعجم الوسيط، مجمع اللغة العربية، الإدارة العامة للمجمعات وإحياء التراث، ط 4، مكتبة الشروق الدولية، مصر، 2004، ص: 479.

[4]- هبة شعوة، تطبيق الشرطة الجزائرية، مجلة المعيار،مجلد 02، عدد 22، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر،2018، ص: 238.

[5]- كمال بلارو، المرجع نفسه، ص: 18.

03- **تعريف الضبطية القضائية فقها:** عرفها بعض الفقه بأنها: "جميع الإجراءات التي تهدف إلى التحري عن الجريمة والبحث عن مرتكبيها، وجمع كافة العناصر والدلائل اللازمة للتحقيق في الدعوى الجنائية، للتصرف على ضوئها".[1]

04- تعريف المشرع الجزائري للشرطة القضائية: رغم أن المشرع الجزائري لم يورد تعريفا محددا للشرطة القضائية تاركا مهمة ذلك للفقه، إلا أنه باستقراء النصوص المنظمة لعملها لاسيما المواد: 12، 13، 15 ق إ ج، يمكن القول بأنها: "مجموعة من الموظفين منحهم القانون صفة الضبطية القضائية، وخول لهم بموجب هذه الصفة سلطات البحث والتحري عن الجرائم ومرتكبيها وجمع الاستدلالات عنها قبل فتح تحقيق قضائي، إضافة إلى تنفيذ طلبات جهات التحقيق بعد فتحه".

وهو التعريف الذي أخذ بمعيار أهمية الشرطة القضائية المتمثلة في البحث والتحري عن الجرائم من أجل تهيئة القضية وتقديمها للنيابة العامة، حتى يتسنى لها تقدير مدى إحالتها للمحاكمة حال كفاية الأدلة، أو للتحقيق بغية استكمال الأدلة حال نقصها.

غير أن ما يعاب على المشرع الجزائري، أنه ورغم تغييره لتسمية هذا الجهاز بموجب القانون رقم: 17-07، من "الضبطية القضائية" إلى "الشرطة القضائية"، إلا أنه مازال يجمع بين المصطلحين في العديد من المواضع.

ثانيا: تنظيم جهاز الشرطة القضائية: بالرجوع إلى أحكام المادة: 14 ق إ ج نجد أن الشرطة القضائية تشمل ثلاث فئات:

الفئة الأولى: ضباط الشرطة القضائية: وينقسمون حسب المادة: 15 ق إ ج إلى ثلاثة أقسام:

أ- **ضباط الشرطة القضائية بقوة القانون:** ويقصد بهم الأشخاص الذين يتمتعون بصفة الضبطية القضائية بموجب القانون، وهم: "رؤساء المجالس الشعبية البلدية، ضباط الدرك الوطني، الموظفون التابعون للأسلاك الخاصة للمراقبين، محافظي وضباط الشرطة للأمن الوطني".[2]

[1]- محمد زكي أبو عامر، الإجراءات الجنائية، منشورات الحلبي الحقوقية، لبنان، 2010، ص: 89.

[2]- راجع المادة 15 ق إ ج.

ب- ضباط الشرطة القضائية بموجب قرار وبموافقة لجنة خاصة: وهي الفئة التي لا تتمتع بصفة الضبطية القضائية إلا بموجب قرار مشترك بعد موافقة اللجنة الخاصة،[1] ويندرج ضمن هذه الفئة:

* ضباط الصف الذين أمضوا في سلك الدرك الوطني 03 سنوات على الأقل، وتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الدفاع الوطني.

* الموظفون التابعون للأسلاك الخاصة للمفتشين وحفاظ وأعوان الشرطة للأمن الوطني الذين أمضوا 03 سنوات على الأقل بهذه الصفة، وتم تعيينهم بموجب قرار مشترك صادر عن وزير العدل ووزير الداخلية.

ت- مستخدمو مصالح الأمن العسكري: ينتمي إلى هذه الفئة ضباط الجيش، ضباط الصف التابعين للمصالح العسكرية للأمن الذين تم تعيينهم خصيصا بموجب قرار مشترك صادر عن وزير الدفاع الوطني ووزير العدل، ولا يشترط في هذه الفئة أقدمية معينة، ولا موافقة لجنة خاصة.

الفئة الثانية: أعوان الشرطة القضائية: بحسب المادة 19 ق إ ج المعدلة بالقانون رقم: 19-09 المؤرخ في: 11-12-2019، فإنه يعد من أعوان الشرطة القضائية: "موظفو مصالح الشرطة وضباط الصف في الدرك الوطني، ومستخدمو المصالح العسكرية للأمن الوطني الذين ليست لهم صفة ضباط شرطة قضائية".

الفئة الثالثة: الموظفون والأعوان المكلفون ببعض مهام الشرطة القضائية: منح قانون الإجراءات الجزائية وبعض القوانين الخاصة صفة الضبطية القضائية لبعض الأعوان والموظفين في مجال محدد من الجرائم حسب وظيفتهم، ومن أمثلة ذلك:

أ- **رؤساء الأقسام والمهندسون والأعوان الفنيون والتقنيون المختصون في الغابات وحماية الأراضي واستصلاحها:** إذ منحهم القانون مهام البحث والتحري عن جنح ومخالفات الغابات وتشريع الصيد وتحرير محاضر بشأنها، إضافة إلى جميع الأنظمة التي عُينوا فيها بصفة خاصة،

[1]- تتشكل هذه اللجنة من ثلاثة أعضاء، عضو ممثل لوزير العدل رئيسا، وبعضوية ممثل لوزير الدفاع الوطني وممثل لوزير الداخلية، انظر المرسوم رقم 66-167 المؤرخ في 08-06-1966، المحدد لتأليف وتسيير اللجنة المكلفة بامتحان المترشحين لمهام ضباط شرطة قضائية، الجريدة الرسمية لسنة 1966، العدد 50.

غير أنه لا يمكنهم الدخول إلى المنازل إلا بحضور ضابط للشرطة القضائية، فضلا عن توافر باقي الشروط المحددة قانونا.[1]

ب- الولاة: منحهم القانون بعض مهام الضبطية القضائية بالنسبة للجنايات والجنح الماسة بأمن الدولة، إذ خول لهم اتخاذ الإجراءات الضرورية لإثبات هذه الجرائم في حالة عدم إخطار السلطة القضائية، وعند الاستعجال فقط.[2]

ت- أعوان الجمارك: وينحصرون في الأعوان الذين منحهم القانون صفة ضابط شرطة قضائية وخول لهم القيام ببعض مهامهم، مثل تحرير المحاضر، وتفتيش الأشخاص والبضائع.[3]

ث- مفتشي العمل: خول لهم القانون بعض مهام الشرطة القضائية، من خلال تكليفهم بمهام البحث والتحري وإثبات الجرائم التي ترتكب خرقا لتشريعات العمل.[4]

وكذلك الحال بالنسبة لأعوان البريد والمواصلات السلكية واللاسلكية،[5] حراس الشواطئ،[6] شرطة المياه،[7] أعوان قمع الغش،[8] مفتشو التعمير وأعوان البلدية المكلفين بالتعمير،[9] وغيرهم.

ونظرا لأهمية دور الشرطة القضائية لاسيما في ممارستها لوظيفة الضبط القضائي، فإنها تعمل تحت إدارة وكيل الجمهورية، وإشراف النائب العام لدى المجلس، وتخضع لرقابة غرفة الاتهام،[10] بما يعكس تبعيتها المطلقة للقضاء أثناء القيام بمهامها.

---

[1]- راجع المادة 21 ق إ ج.

[2]- راجع المادة: 28 ق إ ج.

[3]- راجع المادة: 241 من قانون الجمارك.

[4]- راجع المادة 14 من القانون 90-03 المؤرخ في 06-2-1990 المتعلق باختصاصات مفتشية العمل.

[5]- راجع المادة 121 من القانون 2000-03 المؤرخ في 05-08-2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية.

[6]- راجع المادة 65 من القانون رقم: 01-11 المؤرخ في 03-06-2001، المتعلق بالصيد البحري وتربية المائيات.

[7]- راجع المادة 161 من القانون رقم: 05-12 المؤرخ في 04-08-2005 المتضمن قانون المياه.

[8]- راجع المادة 25 من القانون" 09-03 المتعلق بحماية المستهلك وقمع الغش المعدل.

[9]- راجع المادة 76 مكرر من القانون رقم 04-05 المعدل والمتمم للقانون رقم 90-29 المتعلق بالتهيئة والتعمير.

[10]- راجع المادة 12 من ق إ ج.

الفقرة الثانية: الشرطة القضائية المختصة في مكافحة الجريمة الإلكترونية

بحكم أن جهاز الشرطة القضائية هو المكلف بالتحري عن الجريمة بشتى أنواعها، فإن تطور الأخيرة وامتدادها إلى العالم الافتراضي باستغلال التقنيات الحديثة، جعله يأخذ بفكرة التخصَص من خلال تشكيل وحدات متخصصة في البحث عن الجريمة الإلكترونية، سواء على المستوى الوطني أو الدولي، وهو ما سنتناوله فيما يلي:

أولا: على المستوى الوطني: في إطار تعزيز آليات مكافحة الجريمة الإلكترونية عملت الدولة الجزائرية على تكوين أجهزة متخصصة في مكافحة الجريمة الإلكترونية على مستوى جهازي الأمن والدرك الوطنيين كما يلي:

01- على مستوى جهاز الأمن الوطني: تعتبر الشرطة القضائية أحد أهم مديريات مصالح الأمن الوطني، بالنظر إلى دورها الهام في مجال مكافحة الجريمة، باعتبارها هيئة مركزية تتمتع باختصاصات ذات بعد إداري، وظيفي وعملياتي، من خلال وضع استراتيجية وطنية لمكافحة الجريمة، وتحسين أداء أعوانها عن طريق التكوين المتخصص، فضلا عن سهرها على تنفيذ الإنابات والأحكام القضائية.[1]

وحرصا على فعالية أدائها شهدت مديرية الشرطة القضائية تطورا مستمرا في إطار التصدي لمختلف أشكال الجريمة، من خلال استحداث مصالح مختلفة، منها نيابة مديرية القضايا الجنائية، نيابة مديرية القضايا الاقتصادية والمالية، ونيابة مديرية الشرطة العلمية والتقنية،[2] التي أُسندت إليها مهمة مكافحة الجرائم الإلكترونية، وتضم هذه الأخيرة عدة مصالح من بينها:

أ- المصلحة المركزية لمكافحة الجرائم السيبرانية: وتعتبر النواة الأمنية الأولى لمكافحة الجريمة الإلكترونية، تم تشكيلها على مستوى مديرية الشرطة القضائية المستحدثة سنة 2011، ليتم بعدها إنشاء المصلحة المركزية لمكافحة الجرائم الإلكترونية، وإلحاقها بالهيكل التنظيمي لمديرية الشرطة

[1]- المديرية العامة للأمن الوطني، "مديرية الشرطة القضائية: الحصن المنيع لصد الجريمة الإلكترونية"، مجلة الشرطة، المؤسسة الوطنية للاتصال والنشر، الرويبة، الجزائر، العدد 151، 2022، ص: 26.

[2]- المرجع والموضع نفسه.

القضائية في جانفي 2015، ومع تزايد حجم الجريمة الإلكترونية تم استحداث 48 فصيلة تابعة للمصالح الولائية للشرطة القضائية عبر أمن الولايات.[1]

تعمل هذه المصلحة على دعم التحريات التقنية والرقمية، ومساعدة التحقيقات القضائية حول الجرائم الإلكترونية، وتحليل التهديدات السيبرانية لوضع خطط الوقاية، كما تساهم في برامج تأمين الأنظمة المعلوماتية والفضاء الرقمي الوطني، وتعزيز قدرات مكافحة الجريمة الإلكترونية من خلال البحث العلمي والتقني في هذا المجال،[2] إضافة إلى تكفّلها باليقظة المعلوماتية، والبحث عبر الشبكات المفتوحة عن كل محتوى غير شرعي، فضلا عن مساهمتها في التكوين المتخصص لعناصر الشرطة الموزعة عبر فرق مكافحة الجريمة المعلوماتية بأمن الولايات.[3]

فخلال امتحانات التعليم المتوسط لدورة جوان 2019، وبعد ضبط أحد الممتحنين يقوم بتصفح حسابه الإلكتروني بمركز الامتحان مستعملا هاتفا ذكيا، تمكنت فرقة مكافحة الجريمة الإلكترونية لأمن ولاية عين الدفلى، بالتنسيق مع المصلحة المركزية لمكافحة الجرائم السيبرانية بمديرية الشرطة القضائية، وفي ظرف قياسي، من توقيف ثلاثة أشخاص من بين مجموعة متخصصة في نشر وتداول مواضيع وحلول الامتحانات عبر أحد التطبيقات واسعة الانتشار، أين تم تقديمهم أمام القضاء لمحاكمتهم طبقا للقانون.[4]

ب- **المخبر المركزي للشرطة العلمية:** ويعمل على تقديم الخبرات في عدة مجالات من بينها تحليل الصوت والأدلة المعلوماتية،[5] يحتوي هذا المخبر على دائرتين؛ الأولى تقنية، تتولى مهام البحث والتحقيق، وتحليل الأدلة الجنائية الناتجة عن الجرائم الإلكترونية، والجرائم التي تستعمل فيها

---

[1]- المديرية العامة للأمن الوطني، "المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية"، مرجع سابق، ص: 69.

[2]- المديرية العامة للأمن الوطني، "مديرية الشرطة القضائية: الحصن المنيع لصد الجريمة الإلكترونية"، مرجع سابق، ص: 27.

[3]- المديرية العامة للأمن الوطني، "المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية"، مرجع سابق، ص: 69.

4- المرجع والموضع نفسه.

5- المديرية العامة للأمن الوطني، "مديرية الشرطة القضائية: الحصن المنيع لصد الجريمة الإلكترونية"، مرجع سابق، ص: 27.

الأسلحة والقذائف بمختلف أنواعها، وكذا جرائم التزوير، والثانية علمية تتولى أعمال البحث والتحقيق وتحليل الأدلة المتصلة بالمجال البيولوجي، الطب الشرعي والكيمياء، المخدرات والتسمم، الحريق والمتفجرات، لتعالج كل جريمة منها على مستوى مخبر خاص.[1]

وتوسيعا لنشاطها أنشأت مديرية الشرطة القضائية خمسة مخابر جهوية تابعة للمخبر المركزي على مستوى ولايات: (وهران، قسنطينة، ورقلة، بشار، وتامنراست)، تعمل جميعها على إنجاز التحاليل والخبرات العلمية الضرورية لسير التحقيقات القضائية، بطلب من المحققين والسلطات المؤهلة، إضافة إلى توفير الدعم التقني الضروري في تسيير مواقع حدوث الجريمة.[2]

ت- **المكتب المركزي الوطني انتربول الجزائر:** يقوم هذا المكتب بمهام البحث عن المعلومات المطلوبة من المكاتب المركزية الدولية للانتربول، ويتقاسم معهم البيانات الجنائية، إضافة إلى دوره المساعد في التحقيقات والاعتقالات عبر الحدود، بالتنسيق مع أي مكتب مركزي آخر، كما يعمل على جمع المعلومات وتبادل الخبرات في التدخلات الناجحة ضد الجريمة في ثلاثة مجالات عالمية تعتبر الأكثر طلبا اليوم، وهي: الجريمة الإلكترونية، جرائم الإرهاب، والجريمة المنظمة.[3]

ويبرز دور مصالح الشرطة القضائية المختصة في مكافحة الجريمة الإلكترونية وحماية المواطن عبر الفضاء الافتراضي من خلال التزايد الملحوظ للجرائم التي تولَت تتبَعها، فبعد أن سجلت 567 قضية سنة 2015، ارتفع العدد إلى 3522 قضية خلال سنة 2018، منها 2627 قضية تم حلها، ما يعادل نسبته 74.27%، كما سبق لها معالجة ما نسبته 73.90% من القضايا خلال سنة 2017.[4]

---

[1]- حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016، ص: 178.

[2]- المادة 09 من القرار الوزاري المشترك المؤرخ في 14-04-2007 المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية لسنة 2007، العدد 15.

[3]- المديرية العامة للأمن الوطني، "مديرية الشرطة القضائية: الحصن المنيع لصد الجريمة الإلكترونية"، مرجع سابق، ص: 27.

[4]- المديرية العامة للأمن الوطني، "المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية"، مرجع سابق، ص: 70.

02- على مستوى جهاز الدرك الوطني: يعتبر هذا الجهاز قوة عسكرية مكلفة بمهام الأمن العمومي، يمارس مهام الشرطة الإدارية والقضائية وكذلك العسكرية عبر كامل التراب الوطني، إذ يعمل على محاربة الجريمة والجريمة المنظمة طبقا لأحكام قانون الإجراءات الجزائية، مستعينا في ذلك بوسائل التحري العلمية والتقنية، إضافة إلى خبرة الأدلة الجنائية.[1]

وحرصا على نجاعة هذا الجهاز في مكافحة الجريمة بعد ظهور أنماط جديدة تستغل أحدث التقنيات التكنولوجية، بما جعل مكافحتها من أولويات الدولة لضمان حفظ الطمأنينة والأمن العمومي في الفضاء الرقمي، تمّ إنشاء مركز للوقاية من جرائم الإعلام الآلي والجرائم الإلكترونية ومكافحتها، إلى جانب المعهد الوطني للأدلة الجنائية وعلم الإجرام.

أ- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها: وهو عبارة عن هيئة تقنية وظيفتها ضمان المراقبة الدائمة لشبكة الإنترنت ومختلف شبكات الاتصال الإلكترونية، من أجل مساعدة وحدات الدرك الوطني والجهات القضائية، وذلك بمعاينة الجرائم الإلكترونية، والبحث عن الأدلة الرقمية، والمشاركة في عمليات التحري والتسرب الإلكتروني، والتعاون مع مختلف مصالح الأمن والهيئات الوطنية من أجل قمع هذه الجرائم.[2]

فمنذ إنشائه سنة 2008، ساهم هذا المركز في تحليل معطيات وبيانات الجرائم الإلكترونية وتحديد هوية مرتكبيها،[3] إذ عالج خلال سنة 2014 ما يقارب 240 قضية إلكترونية، شملت جرائم: التهديد، المساس بالنظام العام، التحرش الجنسي بالقصر وتحريضهم على الفسق والدعارة، الاختراق، إهانة هيئات ورموز وطنية، النصب والاحتيال، والاعتداء على حرمة الحياة الخاصة.[4]

---

[1]- راجع المواد 02، 03، 07، 08 من المرسوم الرئاسي رقم: 09-143 المؤرخ في: 27-04-2009، المتضمن لمهام الدرك الوطني وتنظيمه، الجريدة الرسمية لسنة 2009، العدد 26.

[2]- حسين ربيعي، المرجع السابق، ص: 185.

[3]- سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد السابع، عدد 01 ، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، جوان ،2021، ص: 280-281.

[4]- المرجع نفسه، ص: 281.

ب- المعهد الوطني للأدلة الجنائية وعلم الإجرام: وهو مؤسسة عمومية ذات صبغة إدارية يتمتع بالشخصية المعنوية والاستقلال المالي، يقع مقره بمدينة الجزائر،[1] تم إنشاؤه بموجب المرسوم الرئاسي رقم: 04-183، يعمل على خدمة العدالة ودعم وحدات التحري في نطاق مهام الشرطة القضائية، ويختص بإجراء الخبرات والفحوص العلمية بغرض إقامة الأدلة التي تسمح بالتعرف على مرتكبي الجنايات والجنح، بناء على طلب من القضاء أو من السلطات المؤهلة، كما يقدم المساعدة العلمية أثناء التحريات المعقَّدة باستخدام مناهج الشرطة العلمية، ويشارك في الملتقيات والمحاضرات والندوات على الصعيدين الوطني والدولي لتطوير قدرات مستخدمي المعهد.[2]

ورغم الجهود المبذولة من طرف الشرطة القضائية، والنتائج المحققة في مجال مكافحة الإجرام الإلكتروني، إلا أن التطور الرهيب لأساليب الأخير، يستلزم تطوير أكثر لمختلف هياكل مكافحته ماديا وتقنيا، والسهر على التكوين المتخصَص والمستمر لعنصرها البشري، مع ضرورة تنسيقها الدائم مع باقي الأجهزة المماثلة على المستوى الإقليمي والدولي، حتى تكون سندا قويا للقضاء في كشف ملابسات الجرائم الإلكترونية المعقدة والتوصل إلى مرتكبيها.

ثانيا: على المستوى الدولي: ما تتميز به الجريمة الإلكترونية من عالمية وانتشار جعلها عابرة للحدود، بشكل أضحى معه التعاون الدولي ضروريا لجمع الأدلة والمعلومات عن مرتكبيها من أجل مكافحتها، ويعد التنسيق الأمني أو الشرطي أهم صور التعاون الدولي لمجابهة هذا النوع من الإجرام، وتجسَد ذلك في إنشاء مكاتب متخصصة في هذا الغرض، أبرزها:

01- المنظمة الدولية للشرطة الجنائية "INTERPOL": تم إنشاء هذه المنظمة سنة 1923 للتنسيق بين أجهزة الشرطة في الدول الأوروبية، تتخذ من فرنسا مقرا لها (خلال سنة 1946 تم نقل مقرها من فيينا إلى باريس، وخلال سنة 1989 تم نقله إلى مدينة ليون الفرنسية)، كانت تسمى باللجنة الدولية للشرطة الجنائية (La Commission Internationale de Police Criminelle) ثم توقف نشاطها بسبب اندلاع الحرب العالمية الثانية، ليعيد مؤتمر فيينا إحيائها سنة 1956 تحت تسمية

[1]- راجع المواد: 02 ، 03 من المرسوم رئاسي رقم 04-183، مؤرخ في 26-06-2004 المتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية لسنة 2004، العدد 41.

[2]- راجع المادة 04 من المرسوم الرئاسي رقم 04-183.

منظمة الشرطة الجنائية الدولية (Organisation Internationale de Police Criminelle)، يرمز لها اختصارا (OIPC)، كانت تضم 177 دولة عضو،[1] ثم ازداد عدد الدول المنتمية إليها ليصل إلى 195 دولة.[2]

تعمل "INTERPOL" على تمكين أجهزة الشرطة حول العالم من العمل سويا للوقاية من الجرائم العابرة للحدود ومكافحتها، وذلك من خلال وظيفتين أساسيتين؛ الأولى عن طريق جمع البيانات والمعلومات المتعلقة بالجريمة عبر مكاتبها الوطنية المتواجدة عبر أقاليم الدول الأعضاء، والثانية من خلال التعاون في مجال ضبط المجرمين الفارَين، وتسليمهم إلى الدولة التي تطلب تسليمهم،[3] وتركز اهتمامها في ست مجالات إجرامية أعطتها أولوية من بينها الإجرام المالي المرتبط بالتكنولوجيات المتقدمة.[4]

انضمت الجزائر إلى الأنتربول سنة 1963، وشغلت بها منصب نيابة رئاسة المنظمة لعهدتين متتاليتين من سنة 1971 إلى غاية 1981، فضلا عن رئاستها للعديد من لجانها، وشاركت بصفة منتظمة في جمعياتها العامة، بشكل ساهم في استفادة عديد موظفي الشرطة من تكوينات متخصصة من أجل تحسين مستواهم.[5]

وفي إطار التعاون مع الأنتربول شارك إطار من الإدارة المركزية لوزارة العدل في الاجتماع العاشر لفريق عمل الحوكمة للمنظمة، الذي يتكون من إطارات بجهاز العدالة وسلطات الشرطة الجنائية للدول الأعضاء في الفترة الممتدة من 18 إلى 20 جويلية 2023 بمدينة ليون الفرنسية.[6]

---

[1]– حسين ربيعي، المرجع السابق، ص: 148.

[2]– المديرية العامة للأمن الوطني، "الجزائر تدعم المسعى الدولي لمكافحة الجريمة المنظمة العابرة للحدود"، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، رويبة، الجزائر، العدد 150، 2022، ص: 05.

[3]– جميل عبد الباقي الصغير، مرجع سابق، ص: 76.

[4]- Malcom Anderson, Policing the world – Interpol the politics of International Police Cooperation, Carendon press, Oxford, 1989, p: 186-185.

[5]– المديرية العامة للأمن الوطني، "مصلحة التعاون الدولي: الإشعاع الدولي للشرطة الجزائرية"، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، الرويبة، العدد 151، 2022، ص: 38– 39.

[6]– بيان لوزارة العدل، الرابط الإلكتروني: https://n9.cl/fvp98، تاريخ الاطلاع: 16–07–2023، الساعة: 22:58.

وقد حققت هذه المنظمة إنجازات كبيرة في مجال مكافحة الجريمة الإلكترونية، أبرزها عملية (Cathédral)، التي قامت بها بالاشتراك مع المباحث الفيدرالية الأمريكية والشرطة الإنجليزية سنة 1998، أين تمكنت خلالها من تفكيك موقع منشور عليه أكثر من 75.000 صورة سلبية لدعارة الأطفال، وإلقاء القبض على 107 شخص عبر 12 دولة.[1]

إضافة إلى مساهمتها في عمليات التكوين من أجل تحسين المستوى والتدريب لمكافحة الإجرام بجميع أشكاله، على غرار تنظيمها لمؤتمر دولي خلال سنة 2005 لتكوين المحققين في الجريمة الإلكترونية، والذي عرف مشاركة 30 دولة.[2]

02- مركز الشرطة الأوروبية "EUROPOL": وهو جهاز أمني يقع بمدينة لاهاي (هولندا)، أنشأه المجلس الأوروبي بلوكسمبورغ سنة 1991، ونظمته اتفاقية ماستريخت (Maastricht) الأوروبية الصادرة في: 26-07-1995، غايته تسهيل الإجراءات لرجال الشرطة على مستوى الاتحاد الأوروبي من أجل التحري عن الجرائم المتعلقة ببلدانهم، عن طريق مدَهم بمختلف النشرات الأمنية والتقارير حول هوية المجرمين، والأدلة المحصلة خارج الحدود الإقليمية لبلدانهم.[3]

يختص "L'EUROPOL" بمكافحة الجرائم الإلكترونية التي تكون إحدى المنظمات الإجرامية الناشطة على مستوى الإقليم الأوروبي طرفا فيها،[4] ويعتبر من أكبر الهيئات الاستشارية حول العالم في مجال الإجرام الإلكتروني، إذ تم اختياره من قبل الاتحاد الدولي للأمن المعلوماتي لإنجاز مختلف الدراسات الخاصة بالجريمة الإلكترونية بهدف تحليل دوافعها، ووضع تصور مستقبلي لتطورها، وهو ما يفسَر الثقة التي وضعتها فيه اللجنة الأوروبية باختيارها له كمركز إعلام حول موضوع الجريمة الإلكترونية.[5]

[1]- نبيلة هبة هروال، المرجع السابق، ص: 155.

[2]- Mohamed Chawki, Combattre La Cybercriminalité, Edition de saint Amans, Paris, France, 2009, p: 343.

[3]- Myriam Quéméner, Joel Ferry , Cybercriminalité Défi mondial, Edition Economica, Paris, 2009, P: 238.

[4]- Ibid, p: 237.

[5]- Myriam Quéméner, Jean Paul Pinte, Cybersécurité, Edition Hermès science, Paris, 2013, p: 194-195.

03- الأوروجست (EUROJUST): وهو جهاز أسسه مجلس الاتحاد الأوروبي في: 28-02-2002، بهدف تقوية التصدي للإجرام الخطير، كما يعمل على تطوير آليات مكافحة الجريمة الإلكترونية من خلال تبادل المعلومات مع محاكم الاتحاد الأوروبي بصفة دورية.[1]

خلال سنة 2013 تقدَمت المفوضية الأوروبية أمام كل من البرلمان والمجلس الأوروبيين باقتراح يتضمن لائحة توفر إطارا قانونيا جديدا لهذا الجهاز، وبعد مفاوضات عديدة تم اعتمادها سنة 2018، ودخلت حيز التنفيذ في: 12-12-2019، أين صار بإمكان "l'eurojust" مكافحة مستويات متزايدة من الجرائم الخطيرة العابرة للحدود الوطنية، ومن بينها الجريمة الإلكترونية.[2]

وتتلخص نشاطات الأوروجست عموما في تنسيق التعاون بين السلطات القضائية للدول الأطراف، وتبادل المعلومات أو التبليغ عن الجرائم فيما بينهم، كما يمكنه أن يطلب من الجهات القضائية الوطنية إجراء تحقيقات أو ملاحقات،[3] خاصة أن له علاقة وثيقة مع جهاز الأوروبول الذي يمده بالتحليلات اللازمة للقيام بتحرياته في الجرائم المنظمة، ولذلك فهو بمثابة دعامة هامة لنجاعة التحقيقات القضائية الوطنية لاسيما ما تعلق منها بالأنشطة المرتبطة بالإجرام الإلكتروني.

04- آلية الاتحاد الإفريقي للتعاون في مجال الشرطة "AFRIPOL": يمكن القول أنه جهاز شرطي يؤدي مهامه في إطار الاحترام الكامل للتشريعات الوطنية للدول الأعضاء في الاتحاد الإفريقي، يقع مقره بمدينة بن عكنون بالجزائر، كانت فعاليات أشغال الجمعية العامة لهذا الجهاز المنعقدة بالجزائر أيام 14، 15، 16 ماي 2017 بمثابة الإعلان الفعلي لتأسيسه واعتماد نظامه الأساسي، مثلما تم خلالها انتخاب الجزائر لرئاسته لمدة عامين.[4]

ويهدف الأفريبول إلى وضع إطار للتعاون الشرطي على المستوى الاستراتيجي والعملياتي بين أجهزة الشرطة الإفريقية، وذلك بتدعيم قدراتها التحليلية من خلال برامج التكوين المتخصص

[1] - Myriam Quéméner, Jean Paul Pinte, l'ouvrage précité, p: 195.

[2]- حسين ربيعي، المرجع السابق، ص: 251.

[3]- نبيلة هبة هروال، المرجع السابق، ص: 160.

[4]- المديرية العامة للأمن الوطني، " أشغال الجمعية العامة الأولى لآلية أفريبول تتوج بقرارات هامة ستشكل خارطة طريق بالنسبة لقادة الشرطة الأفارقة"، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، الرويبة، الجزائر، العدد 136، 2017، ص: 35.

الذي يتلاءم مع واقع البيئة الإفريقية، كما يهدف إلى تحسين كفاءات وفعالية مؤسسات الشرطة ووسائلها من خلال تيسير التبادل في ميادين التدريب، التكوين، الخبرات والممارسات، لاسيما في مجال التحقيق والتحليل الجنائيين واستعمال التكنولوجيات الحديثة.[1]

ورغم حداثة هذا الجهاز، فإنه ينتظر منه أن يلعب دورا هاما في تطوير العمل الأمني وتعزيز التعاون الشرطي المشترك بين مختلف الدول الإفريقية، من خلال إيجاد الأساليب الفعالة للتحري عن الجرائم الخطيرة بما فيها الإلكترونية، وتسهيل تبادل المعلومات والخبرات، فضلا عن ضرورة تنسيقه مع الأجهزة المشابهة له على المستوى الإقليمي والدولي للاستفادة من خبراتهم.

الفرع الثاني: دور الشرطة القضائية في التحقيق في الجريمة الإلكترونية

رغم أن التحقيق الجنائي في الجرائم الإلكترونية اختصاص أصيل للقضاء، إلا أن الشرطة القضائية تلعب دورا لا يمكن الاستغناء عنه خلال هذه العملية الصعبة، سواء عن طريق ما تجمعه من معلومات من شأنها أن تساعد في كشف ظروف وملابسات الجريمة، وتسهيل الوصول إلى مرتكبيها،[2] لتنير بذلك الطريق أمام قاضي التحقيق لاستكمال ما تبقى من أدلة، أو من خلال الاستعانة بها على تنفيذ تفويضات السلطة القضائية بعد فتح التحقيق القضائي.[3]

الفقرة الأولى: دور الشرطة القضائية قبل فتح تحقيق قضائي

تتمثل المهمة الأساسية للشرطة القضائية في البحث والتحري عن الجرائم، بدءا بتلقي البلاغات والشكاوى بخصوصها، مرورا إلى الانتقال إلى مكان ارتكابها ومعاينته، فجمع مختلف الأدلة والقرائن المتعلقة بها، ثم سماع أقوال المشتبه فيهم، وصولا إلى تحرير محاضر تدون فيها كل الأعمال والإجراءات التي تم القيام بها.[4]

---

[1]– المديرية العامة للأمن الوطني، "أشغال الجمعية العامة الأولى لآلية أفريبول تتوج بقرارات هامة ستشكل خارطة طريق بالنسبة لقادة الشرطة الأفارقة"، مرجع سابق، ص: 35.

[2]– راجع المادة 12 ق إ ج.

[3]– راجع المادة 13 ق إ ج.

[4]– راجع المواد: 17 و 63 ق إ ج.

وتبدأ إجراءات البحث والتحري في بعض الجرائم الإلكترونية من خلال تحديد هوية مرتكب الجريمة عبر شبكة الإنترنت، وذلك عن طريق الاستعانة بعنوان المجرم على شبكة المعلومات (IP)، إذ يتم التعرف على خط الهاتف المتصل بالجهاز الإلكتروني المستخدم في ارتكاب الجريمة سواء أكان خطا هاتفيا ثابتا أم محمولا، ثم الاستعلام من مقدم الخدمة المعني عن اسم صاحب الخط، فضلا عن إمكانية تحديد النطاق الجغرافي لمرتكب الجريمة عبر الإنترنت.[1]

فاستخدام شبكة الانترنت يخضع لأسس وقواعد أمنية وإدارية تساعد على تحديد هوية المتعاملين عبرها، والوصول إلى مرتكبي الجرائم الواقعة عليها أو باستخدامها، ويعد بروتوكول الإنترنت (Internet Protocol)، الذي يعرف اختصارا بـ: (IP)، أبرز هذه الأسس، فهو عنوان رقمي مميز خاص بكل جهاز عند اتصاله بشبكة الإنترنت، سواء أكان هذا الجهاز حاسبا آليا، أم خادما، أم هاتفا محمولا ... إلخ، ولا يمكن أن يتكرر على أكثر من جهاز واحد، لذلك يعتبر العنوان الرقمي للجهاز أحد أهم الأدلة الإلكترونية لإثبات أو نفي الجرائم التي تقع عبر شبكة الإنترنت.[2]

طرحت قضية على القضاء الجزائري، مفادها تعرض فتاة للسب بعبارات نابية من قبل شخص يحمل اسما مستعارا، كانت قد تعرفت عليه عبر موقع التواصل الاجتماعي "فيسبوك"، مع تهديدها بنشر صورها تشويها لسمعتها، وفي إطار التحري تمكنت عناصر مكافحة الجريمة المعلوماتية بالمصلحة الولائية للشرطة القضائية بعد التحريات التي قامت بها من استرجاع عنوان (IP) الخاص بحساب صاحب الاسم المستعار، لتقوم بعدها بمراسلة مديرية اتصالات الجزائر من أجل تحديد هوية صاحب هذا العنوان، وكان الرد بأنه مرتبط بالرقم الهاتفي (06**.***.***) وهو الرقم المقيد باسم المشتبه فيه، الذي تمت متابعته من طرف القضاء ومعاقبته على جرمه.[3]

كما يمكن لرجال الشرطة القضائية خلال مرحلة البحث والتحري حول الجرائم الإلكترونية القيام بإجراء معاينات مادية، أو تسخير أهل الخبرة في مجال تكنولوجيات الإعلام والاتصال

[1]– بهاء المري، المرجع السابق، ص: 777.

[2]– عصام أبو العز، دور التقنيات العلمية الحديثة في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2020، ص: 27.

[3]– قرار صادر عن مجلس قضاء باتنة، الغرفة الجزائية، بتاريخ: 14-01-2024، فهرس رقم: 648/24، انظر ملحق رقم: 03.

للاستعانة بهم في بعض الجرائم المعقدة،[1] أو اللجوء إلى إجراءات التفتيش والحجز داخل منظومة معلوماتية، إضافة إلى استعمال آليات التحري المستحدثة أو الخاصة، مثل مراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها، التسرب الإلكتروني،[2] وذلك بعد الحصول على إذن مكتوب من السلطة القضائية، وهي الأساليب التي سنتناولها بشيء من التفصيل في حينها.

وتتميز أعمال البحث والتحري في الجرائم الإلكترونية بعدة خصائص، أهمها:

01- عدم النص عليها على سبيل الحصر: وضع المشرع الجزائري لضابط الشرطة القضائية قاعدة عامة تجيز له القيام بأي إجراء من شأنه الكشف عن الجريمة وجمع أدلتها، وتتبع مرتكبيها لتقديمهم أمام الجهة القضائية المختصة، شريطة أن يتحرَى المشروعية في كل أعماله.

02- تجرَد أعمال البحث والتحري من الإجبار والقهر: انطلاقا من تميز مرحلة التحقيق الأولي عن التحقيق الابتدائي بعدم انطوائها على إجراءات القهر والإكراه باعتبارها مرحلة لجمع المعلومات، فلا يمكن لضابط الشرطة القضائية القيام بأي إجراء قسري كتفتيش المساكن أو أجهزة الحاسوب أو التوقيف للنظر إلا بإذن من السلطة القضائية المختصة.[3]

03- تحرير محضر بأعمال البحث والتحري: عند انتهاء ضابط الشرطة القضائية من إنجاز محاضر الاستدلالات يقوم بإرسالها إلى وكيل الجمهورية طبقا للمادة 18 ق إ ج، ليقوم هذا الأخير باتخاذ ما يراه مناسبا بشأنها تطبيقا لمبدأ ملائمة المتابعة الجزائية.[4]

ففي حال وقوع جريمة إلكترونية مثلا عن طريق إرسال عبارات تشكل قذفا أو سبا أو تهديدا باستخدام جهاز هاتف محمول، يتعيّن على ضابط الشرطة القضائية أن يطَلع على الرسائل النصية أو صورها المقدمة من طرف الشاكي، ويقوم إما بتفريغ محتواها في محضر الاستدلالات أو إرفاق نسخ منها، مع إثبات رقم الهاتف الذي أُرسلت منه، وتوقيت وصولها إلى المجني عليه،

---

[1]- راجع المادة 49 ق إ ج.

[2]- راجع المادة: 03 من القانون 09-04.

[3]- عبد الرحمان خلفي، المرجع السابق، ص: 70.

[4]- حسين العيساوي، محاضرات في مقياس النيابة العامة لطلبة السنة أولى ماستر جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، السنة الدراسية: 2020-2021، ص: 23.

ليقوم بناء على ذلك باستدعاء الجاني إن كانت هويته معروفة، أو السعي إلى تحديدها بالتنسيق مع متعاملي الهاتف النقال، ومن ثم استدعائه ومواجهته بتصريحات الشاكي وسماعه بخصوصها.

الفقرة الثانية: دور الشرطة القضائية عند الانتداب للتحقيق الابتدائي

بعد الانتهاء من التحقيق الأولي الذي يعد من صميم أعمال الشرطة القضائية، تأتي مرحلة التحقيق الابتدائي التي يختص بها القضاء، إلا أن ذلك لا يعني بالضرورة انتهاء دور الشرطة القضائية، إذ أجاز المشرع الجزائري لجهة التحقيق أن تندب أحد ضباطها للقيام ببعض الإجراءات عن طريق الإنابة القضائية.[1]

والعمل بإجراء الإنابة القضائية أملته عدة اعتبارات؛ سواء أكانت قانونية كحصر اختصاص جهة التحقيق في نطاق إقليمي محدد مقارنة بامتداد نطاق الجريمة وطنيا وحتى دوليا، أم واقعية كتعدد المعاينات، أو سرعة القيام ببعض الإجراءات، ممَا يستلزم الاستعانة بضابط شرطة قضائية لتنفيذ ما عجزت جهة التحقيق عن القيام به بنفسها.

أولا: تعريف الإنابة القضائية: رغم عدم ورود نص تشريعي في ق إ ج يعرف الإنابة القضائية صراحة، إلا أنه يستشف من أحكام المادة 138 من هذا القانون بأنها:" تفويض جزئي من قاضي التحقيق إلى قاض آخر أو ضابط شرطة قضائية للقيام ببعض إجراءات التحقيق المحددة من أجل الوصول إلى الحقيقة"،[2] بينما عرفها القانون المدني –بصفته الشريعة العامة للقوانين– بأنها: "عقد بمقتضاه يفوض شخص شخصا آخر للقيام بعمل لحساب الموكل وباسمه".[3]

أما الفقه فقد عرفها بأنها: "قيام قاضي التحقيق في مجال اختصاصه بندب أحد القضاة أو ضباط الشرطة القضائية للقيام مقامه ونيابة عنه ببعض إجراءات التحقيق، عندما يتعذر عليه القيام بذلك بنفسه، على أن تكون الإنابة مكتوبة ومحددة المهام".[4]

---

[1]– راجع المادة 68–6 ق إ ج.

[2]– راجع المادة 138 ق إ ج.

[3]– راجع المادة 571 من القانون رقم 07–05 المؤرخ في 13–05–2007 المعدل والمتمم للأمر رقم 75–58 المؤرخ في 26–09–1975، المتضمن القانون المدني.

[4]– عبد الرحمان خلفي، المرجع السابق، ص: 110.

ولعدم ورود نص قانوني يحدد حصرا الإجراءات التي يمكن لجهة التحقيق أن تنيب غيرها للقيام بها، فإن اللجوء إليها يبقى حالة استثنائية مقترنة بما قد يعترض إجراءات التحقيق من عقبات قانونية أو واقعية، كحالة وجود شاهد يقيم خارج الاختصاص الإقليمي لقاضي التحقيق، أو عند ضرورة القيام بإجراء تفتيش أو معاينة في مكان يقع خارج الاختصاص، أو من أجل الاتصال بأحد متعاملي الهاتف النقال لتحديد هوية صاحب رقم هاتفي، وتحديد مكان تواجده خلال فترة معينة.[1]

ثانيا: شروط الإنابة القضائية: حتى تكون الإنابة القضائية صحيحة في إجراءاتها ومنتجة لآثارها يجب أن تتوفر فيها عدة شروط، يمكن تلخيصها فيما يلي:

01- شروط شكلية: نظرا لتعلق موضوع الإنابة القضائية بأحد الإجراءات المخولة أصلا للجهات القضائية، فقد قيَدها المشرع ضمانا لحقوق الأفراد وحرياتهم بعدة ضوابط، أهمها:

أ- أن تكون الإنابة مكتوبة، فلا يجوز أن تصدر شفاهة أو عن طريق الهاتف، وذلك لأن القواعد العامة في التحقيق تقتضي التدوين كما سبق توضيحه.

ب- أن تكون الإنابة واضحة ومحددة، إذ فضلا عن تضمنها نوع الجريمة محل التحقيق والأشخاص المتابعين بها، يجب تحديد المهمة المراد القيام بها ومدة إنجازها،[2] وفي ذلك ضمان لمراقبتها والتأكد من شرعيتها.

ت- أن تكون الإنابة مؤرخة وموقعة، وتحمل ختم قاضي التحقيق الذي أصدرها، كما يجب أن تتضمن الصفة القانونية لضابط الشرطة القضائية المنتدب،[3] دون وجوب ذكر اسمه، بحكم أن تنفيذها يصح من أي مندوب تتوافر فيه الصفة الواردة فيها.[4]

---

[1]- نموذج لإنابة قضائية من قاضي التحقيق إلى ضابط الشرطة القضائية للاتصال بمتعامل الهاتف النقال لتحديد هوية صاحب رقم هاتفي، ملحق رقم 04.

[2]- راجع المواد: 138 و 141 ق إ ج.

[3]- راجع المادة 138-02 ق إ ج.

[4]- عمارة فوزي، قاضي التحقيق، مرجع سابق، ص: 215.

02- شروط موضوعية: إضافة إلى الشروط الشكلية، يشترط لصحة الإنابة القضائية توافر عدة ضوابط موضوعية، يمكن تلخيصها فيما يلي:

أ- أن تصدر من جهة مختصة نوعيا ومحليا؛ أي من طرف قاضي التحقيق، فمن لا يملك التحقيق لا يملك التفويض، كما يجب أن يكون مختصا محلَيا، وإلا كانت إنابته باطلة.[1]

ب- أن تصدر لفائدة أحد ضباط الشرطة القضائية، فلا يجوز ندب أحد أعوان الشرطة القضائية للقيام بها.[2]

ت- يجب أن توجَه إلى ضابط شرطة قضائية يعمل بنفس دائرة الاختصاص الذي يمارس فيه قاضي التحقيق وظيفته،[3] غير أن ذلك لا يمنع من انتداب قاضي تحقيق آخر يعمل بأي محكمة عبر التراب الوطني، وله أن يوكل بدوره مهمة تنفيذ الإنابة إلى أحد ضباط الشرطة القضائية العاملين في دائرة اختصاصه في إطار ما يسمى بـ: "التفويض بعد الإنابة".[4]

ث- يجب أن تكون الإنابة خاصة، فتنصب على إجراء من إجراءات التحقيق أو بعض الأعمال التي لها علاقة مباشرة بالجريمة، ولا يمكن أن تنصب على أعمال التحقيق كلها وإلا كانت باطلة.[5]

ج- لا يجوز أن تتعلق الإنابة باستجواب المتهم أو مواجهته بغيره أو بسماع الطرف المدني،[6] وذلك بسبب أهمية هذه الإجراءات لكونها تعد وسيلة تحقيق ودفاع في آن واحد، الأمر الذي جعل المشرع يحيطها بعدة ضمانات، أهمها إسنادها لجهة محايدة ومستقلة.

---

[1]- عبد الرحمان خلفي، المرجع السابق، ص: 110.

[2]- راجع المواد: 68-6، 138 ق إ ج.

[3]- راجع المادة 138 ق إ ج.

[4]- محمد حزيط، المرجع السابق، ص: 127

[5]- تنص المادة 139 ف 01 ق إ ج" يقوم القضاة أو ضباط الشرطة القضائية المنتدبون بجميع السلطات المخولة لقاضي التحقيق ضمن حدود الإنابة القضائية، غير أنه ليس لقاضي التحقيق أن يعطي بطريق الإنابة القضائية تفويضا عاما".

[6]- راجع المادة 139 ف 02 ق إ ج .

ح- لا يجوز أن تتعلق الإنابة بالأوامر القسرية، كالأمر بالحبس المؤقت، أو الأمر بالقبض، أو الأمر بالضبط والإحضار، بحكم أنها إجراءات ذات طبيعة قضائية محضة.[1]

ثالثا: تنفيذ الإنابة القضائية: إن صدور أمر الإنابة القضائية مستوفيا لشروطه الشكلية والموضوعية، يخول لضابط الشرطة القضائية المكلف بتنفيذها كل السلطة المخولة لقاضي التحقيق الذي ندبه في حدود الإجراء المشمول بالإنابة، ويتعين عليه بناء على ذلك تنفيذ الإجراء المكلف به في حدود اختصاصه وفق الضوابط الآتية:

01- يجب على ضابط الشرطة القضائية المنتدب أن يتأكد من توافر اختصاصه المحلي والنوعي،[2] وفي غياب ذلك يتعين عليه رد الإنابة، مع ذكر أسباب الرد.[3]

02- يجب على ضابط الشرطة القضائية أن يتقيد بحدود الإنابة،[4] فحال تعلَق الإنابة بإجراء التفتيش مثلا يوجب التقيد بتفتيش المسكن المحدد دون سواه، تحت طائلة بطلان الإجراء.

03- يجوز لضابط الشرطة القضائية المنتدب لسماع الشهود أن يستدعيهم للحضور، وهم ملزمون بحلف اليمين وأداء الشهادة،[5] غير أنه لا يمكنه اللجوء إلى الوسائل القسرية لإجبارهم، ويبقى له أن أن يخبر القاضي المنيب الذي يمكنه تسخير القوة العمومية، أو توقيع عقوبة الغرامة.[6]

04- يجب أن ينفذ أمر الإنابة مرة واحدة، فلا يجوز لضابط الشرطة القضائية المنتدب استعمال أمر الإنابة القضائية مرة أخرى، لما يشكله ذلك من اغتصاب لسلطات غيره، ويلزمه بتحمل كامل مسؤولياته تأديبيا، جزائيا ومدنيا.[7]

---

[1]- راجع المواد: 68-6 ق إ ج و 138 ف 01 ق إ ج.

[2]- راجع المادة 138 ق إ ج.

[3]- أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص: 121.

[4]- راجع المادة 139 ق إ ج.

[5]- راجع المادة 140 ف 01 ق إ ج.

[6]- راجع المادة 140 ف 02 ق إ ج.

[7]- عبد الرحمان خلفي، المرجع السابق، ص: 112.

05- يتعين على قاضي التحقيق بمجرد تلقيه لنتائج الإنابة القضائية مراجعة الإجراءات المنجزة من طرف الضابط المنتدب،[1] ويمكنه أن يعيدها له لإتمامها إذا رأى أنها غير مكتملة.[2]

06- يجب على ضابط الشرطة القضائية أن يحرَر محضرا بأعماله، يرسله إلى قاضي التحقيق المنيب خلال المدة المحددة له، على أن لا تتجاوز مهلة 08 أيام من انتهاء الإجراءات المتخذة حال عدم تحديد الأجل.[3]

07- تكتسي المحاضر المحررة من قبل ضابط الشرطة القضائية بمناسبة تنفيذ أمر الإنابة القضائية نفس حجية محاضر التحقيق، باعتبارها امتدادا لأعمال قاضي التحقيق، عكس المحاضر المحررة أثناء التحقيق الأولي ذات الطابع الاستدلالي.[4]

وبالموازاة مع جهاز الشرطة القضائية وما يقدمه من خدمات، استحدث القانون رقم 09-04 جهازا آخر لتقديم المساعدة لسلطة التحقيق، أسماه بالهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وهو ما سنتناوله من خلال المطلب التالي.

المطلب الثاني

الهيئة الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها

أدى ازدياد الوعي العام لدى المواطنين وبحثهم عن الحقوق والحريات، وما صاحبه من تطور في وسائل الإعلام والاتصال، إلى ظهور السلطات الإدارية المستقلة من أجل تعزيز حقوق وحريات الأفراد أمام عجز الإدارة التقليدية عن ذلك في ضل هذه التطورات.[5]

---

[1]- راجع المادة 68 ف 6.

[2]- أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص: 122.

[3]- راجع المادة: 141 ف 05 ق إ ج.

[4]- عبد الرحمان خلفي، المرجع نفسه، ص: 113.

[5]- نادية ضريفي، محاضرات حول السلطات الإدارية المستقلة (لطلبة السنة الأولى ماستر)، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2019-2020، ص: 5.

لم تعرف المنظومة القانونية والإدارية الجزائرية هذا النوع من السلطات إلا مع مطلع تسعينيات القرن الماضي، حين ظهر المجلس الأعلى للإعلام سنة 1990،[1] ثم أعقبه بسلطات أخرى لاسيما في المجالين المالي والاقتصادي، مسايرة منه للتحولات المتسارعة في شتى المجالات وصولا إلى إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها كجهاز مساعد على التصدي للجرائم الإلكترونية، وأخضعها بالمقابل إلى رقابة القضاء ضمانة لحقوق الأفراد من التعسف، وهو ما سنتناوله بالدراسة والتحليل من خلال هذا المطلب.

الفرع الأول: النظام القانوني للهيئة

بعد أن تم إنشاء الهيئة بموجب القانون رقم: 09-04،[2] صدرت عدة مراسيم رئاسية منظمة لها، أولها المرسوم الرئاسي رقم: 15-261 ،[3] الذي أضفى عليها الطابع الإداري ومنحها الاستقلالية، وأخضعها لإشراف وزير العدل، إلا أن المرسوم الرئاسي رقم: 19-172 تراجع عن ذلك، واعتبرها مؤسسة عمومية ذات طابع إداري تشرف عليها وزارة الدفاع الوطني،[4] ليعيد المشرع مرة أخرى تنظيمها بموجب المرسوم الرئاسي رقم: 20-183،[5] معتبرا إياها سلطة إدارية مستقلة يشرف عليها رئيس الجمهورية، وهو النهج الذي حافظ عليه حتى بعد صدور المرسوم الرئاسي رقم: 21-439.[6]

[1]- راجع المادة 59 من قانون 90-07 المؤرخ في: 03-04-1990، المتعلق بالإعلام، الجريدة الرسمية لسنة 1990، العدد 14، الملغى بموجب القانون رقم 12-05 المؤرخ في 12-01-2012 المتعلق بالإعلام.

[2]- تنص المادة 13 من القانون 09-04: "تنشأ هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته".

[3]- مرسوم رئاسي رقم 15-261 مؤرخ في: 08-10-2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة، الجريدة الرسمية لسنة 2015، العدد 53.

[4]- مرسوم رئاسي رقم 19-172 مؤرخ في: 06-06-2019 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة، الجريدة الرسمية لسنة 2019، العدد 37.

[5]- مرسوم رئاسي رقم 20-183 مؤرخ في: 13-07-2020 يتضمن إعادة تنظيم الهيئة، الجريدة الرسمية لسنة 2020، العدد 40.

[6]- مرسوم رئاسي رقم 21-439 مؤرخ في: 07-11-2021 يتضمن إعادة تنظيم الهيئة، الجريدة الرسمية لسنة 2021، العدد 86.

أولا: تعريف الهيئة: يتبين من خلال النصوص القانونية المنشأة والمنظمة للهيئة، أنها: "سلطة إدارية مستقلة، تهدف إلى الحد من الجرائم الإلكترونية، من خلال تنسيق عمليات البحث والتحري بين مختلف الجهات الوطنية والدولية المختصة في هذا المجال".

يقع مقر الهيئة بمدينة الجزائر، ويمكن نقله إلى أي مكان آخر من التراب الوطني.[1]

ثانيا: الطبيعة القانونية للهيئة: اعتبر المشرع الجزائري الهيئة سلطة إدارية مستقلة، لذلك يمكن القول أن طبيعتها القانونية تتسم بـ:

01: الطابع الإداري: تتميز الهيئة بالطابع الإداري بنص القانون،[2] وهو يجعل منها مرفقا إداريا، ويخضع قراراتها لرقابة القضاء،[3] كما أن في إصباغ الطابع الإداري تمييز لها عن الهيئات القضائية.

02: الطابع السلطوي: تعتبر السلطات الإدارية المستقلة نمطا جديدا من أساليب ممارسة السلطة العامة، وتنظيما لم يكن معروفا في التقسيم الإداري التقليدي، الذي يقوم على تقسيم الإدارة العامة إلى إدارة مركزية وأخرى لا مركزية.

وانطلاقا من ذلك فإن مصطلح السلطة يعني "ممارسة سلطة القيادة واتخاذ القرار"،[4] فالطابع السلطوي للهيئة يخولها امتيازات السلطة العامة؛ ويمنحها سلطة اتخاذ القرار في مجال اختصاصها من أجل تحقيق غاية استحداثها بشكل فعَال، دون أن يجعل منها سلطة موازية للسلطات الثلاث.

---

[1]– راجع المواد: 02 و 03 من المرسوم الرئاسي رقم 21–439.

[2]– تنص المادة 02 من المرسوم الرئاسي رقم 21–439: "الهيئة سلطة إدارية مستقلة".

[3]– تنقسم دول العالم بشأن تنظيم عملية الرقابة على أعمال الإدارة إلى نظامين رئيسيين؛ هما النظام الأنجلوسكسوني الذي يقوم على أساس القضاء الموحد، والنظام اللاتيني حيث يوجد الإزدواج القضائي، انظر: فواز لجلط، خصائص الدعوى الإدارية ضمانة لمبدأ الشرعية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 01، 2016، ص 39.

[4]– نادية ضريفي، المرجع السابق، ص: 19–20.

03: طابع الاستقلالية: برزت السلطات الإدارية المستقلة كهيئات من الجيل الثاني، تمتاز عن باقي الأجهزة الإدارية بميزة الاستقلالية، وتعني: "عدم خضوعها لأي رقابة إدارية، رئاسية كانت أم وصائية، مع عدم تلقيها لأي تعليمة من أي جهة كانت".[1]

غير أن صفة الاستقلالية التي تتمتع بها الهيئة لا يعني ترك مجال عملها دون قيود، فهي ملزمة بممارسة مهامها في إطارها الشرعي درءا لأي تعسف، فضلا عن خضوعها لرقابة القضاء.[2]

وما يلاحظ على التشريع الجزائري هو عدم استقراره في تحديد الطبيعة القانونية للهيئة، إذ اعتبرها في بداية الأمر سلطة إدارية مستقلة، لكنه تراجع عن ذلك واعتبرها مؤسسة عمومية إدارية ثم أعاد تنظيمها من جديد، واعتبرها سلطة إدارية مستقلة، ولعل ذلك راجع إلى عدة عوامل وطنية ودولية، أبرزها الظروف الأمنية والسياسية التي كانت تشهدها البلاد آنذاك، بالموازاة مع الاضطرابات السياسية التي عرفتها بعض الدول العربية ومساهمة تكنولوجيات الإعلام والاتصال بشكل كبير في تأجيجها وانتشارها، الأمر الذي دفع المشرع إلى وضع هذه الهيئة تحت إشراف وزارة الدفاع الوطني، بالنظر إلى ما تمتلكه من إمكانيات تكنولوجية متطورة تمكنها من مواكبة الوضع وما قد ينجر عنه من سلبيات، غير أن عدم تناسب وصف المؤسسة العمومية مع طبيعة عمل الهيئة، والرغبة في إبعادها عن تدخل السلطة التنفيذية، جعل المشرع يستقر بعد تردد طويل على منحها الطابع السلطوي ويضفي عليها طابع الاستقلالية، حتى يتسنى لها المساهمة بصورة فعالة في مكافحة الجرائم الإلكترونية، وتعزيز التعاون الدولي تبعا لما تفرزه استقلاليتها من طمأنينة لدى بقية الدول بشكل يحول دون التردد في التعامل معها.

ثالثا: تشكيل الهيئة: رغم استحداث الهيئة بموجب القانون رقم: 09-04، إلا أنه لم يتم التطرق إلى تشكيلتها ولم يوضح آليات عملها، واكتفى المشرع بإحالة هذه المسائل على التنظيم، إلى أن

[1]- المرجع والموضع نفسه.

[2]- تنص المادة: 04 من المرسوم الرئاسي رقم: 21-439: "تمارس الهيئة المهام المنوطة بها تحت رقابة السلطة القضائية طبقا لأحكام قانون الإجراءات الجزائية".

صدر المرسوم الرئاسي رقم 21-439، الذي أعطى للهيئة تنظيما هيكليا يساعدها على القيام بمهامها بكل استقلالية وفعالية، وذلك من خلال تزويدها بمجلس للتوجيه ومديرية عامة.[1]

01: مجلس التوجيه: يرأسه الأمين العام لرئاسة الجمهورية، ويتولى أمانته العامة المدير العام للهيئة،[2] يجتمع في دورة عادية مرة في السنة، ويمكنه أن يجتمع في دورة استثنائية بناء على استدعاء من رئيسه، أو بطلب من أحد أعضائه، أو من المدير العام للهيئة.[3]

ويقوم مجلس التوجيه بعدة مهام، أهمها:[4]

أ- توجيه عمل الهيئة ومراقبته والإشراف عليه.

ب- التقرير حول الإستراتيجية الوطنية للوقاية من الجرائم الإلكترونية ومكافحتها.

ت- دراسة المسائل التي تدخل في نطاق اختصاص الهيئة، لاسيما تلك المتعلقة بإجراء المراقبة الوقائية للاتصالات الإلكترونية، والتأكد من توافر شروطه.

ث- تقييم حالة التهديد في مجال الجرائم الإلكترونية، حتى يمكن تحديد مضمون العمليات الواجب مباشرتها، والأهداف المنشودة بدقة.

ج- اقتراح الأنشطة المتصلة بالبحث، وتقييم الأعمال المباشرة في مجال الوقاية من الجرائم الإلكترونية ومكافحتها.

ح- البت في مسائل التعاون مع المؤسسات والهيئات الوطنية والأجنبية المعنية بالجرائم الإلكترونية.

---

[1]- راجع المادة 05 من المرسوم الرئاسي رقم 21-439.

[2]- راجع المادة 06 من المرسوم الرئاسي رقم 21-439.

[3]- راجع المادة 09 من المرسوم الرئاسي رقم 21-439.

[4]- راجع المادة 07 من المرسوم الرئاسي رقم 21-439.

02- المديرية العامة: يديرها مدير عام يعينه رئيس الجمهورية،[1] تسهر على حسن سير الهيئة، وتتولى في هذا المجال: [2]

أ- اقتراح بنود الإستراتيجية الوطنية للحد من الجرائم الإلكترونية، والسهر على تنفيذها.

ب- تمثيل الهيئة أمام القضاء والسلطات والمؤسسات الوطنية والدولية.

ت- تنسيق أعمال هياكل الهيئة ومراقبتها ومتابعتها.

ث- إخطار رئيس الجمهورية بكل حادثة مرتبطة بالأعمال الإرهابية أو التخريبية، أو من شأنها تهديد أمن الدولة.

ج- إخطار رئيس أركان الجيش الوطني الشعبي بالمسائل المتعلقة بالدفاع الوطني.

ح- إعداد تقرير سنوي يتضمن نشاطات الهيئة، ورفعه إلى رئيس الجمهورية.

وتضم المديرية العامة بدورها عدة مديريات فرعية، هي:

أ- مديرية المراقبة الوقائية واليقظة الإلكترونية: تعمل على تنفيذ عمليات المراقبة الإلكترونية للكشف عن الجرائم السيبرانية ومرتكبيها، وجمع الأدلة الرقمية المتعلقة بها وحفظها من أجل تزويد السلطات القضائية ومصالح الشرطة القضائية بذلك، كما تعمل على تنفيذ طلبات المساعدة القضائية الأجنبية في مجال اختصاصها، فضلا عن تنظيم أنشطة للتوعية حول استعمال تكنولوجيات الإعلام والاتصال ومخاطرها، ولها في سبيل القيام بمهامها على أكمل وجه أن تقوم بتفتيش أي مكان أو جهاز يحوز أو يستعمل وسائل وتجهيزات موجهة لمراقبة الاتصالات الإلكترونية، باستثناء تلك التابعة لوزارة الدفاع الوطني.[3]

---

[1]- تنص المادة 09 من المرسوم الرئاسي رقم 21-439: "يدير المديرية العامة مدير عام يعين بموجب مرسوم رئاسي وتنهى مهامه حسب الأشكال نفسها".

[2]- راجع المادة 10 من المرسوم الرئاسي رقم 21-439.

[3]- راجع المادة 14 من المرسوم الرئاسي رقم 21-439.

إضافة إلى ذلك، تقوم هذه المديرية بتوفير الأجهزة التقنية الضرورية على مستوى المنشآت القاعدية لمتعاملي ومقدمي خدمات الاتصالات الإلكترونية، الذين يتعين عليهم بدورهم تقديم المساعدة الضرورية لها لممارسة مهامها في إطار أحكام قانون الإجراءات الجزائية.[1]

ب- مديرية الإدارة والوسائل: تسهر هذه المديرية على تسيير الموارد البشرية والوسائل المادية والمالية للهيئة، وصيانة العتاد والمنشآت، كما تتولى الإسناد التمويني والتقني للهيئة.[2]

ت- مصلحة الدراسات والتلخيص: تُكلَف هذه المصلحة بإعداد مشروع عمل الهيئة بالتشاور مع بقية الهياكل، وتقوم بالدراسات والبحوث المتعلقة بأعمالها، فضلا عن مراقبة الإجراءات المتعلقة بالطلبات القضائية، وإعداد التقارير والحصيلة السنوية لنشاطاتها.[3]

ث- مصلحة التعاون واليقظة التكنولوجية: وهي مصلحة مكلفة بالتعاون مع باقي الشركاء من أجل تنفيذ عمليات الوقاية من الجرائم الإلكترونية، واليقظة الدائمة في متابعة تكنولوجيات الإعلام والاتصال الخاصة بنشاطات الهيئة.[4]

ج- الملحقات الجهوية: تسهر مديرية المراقبة الوقائية واليقظة الإلكترونية على وضع الملحقات الجهوية قيد الخدمة، من أجل تنفيذ عمليات المراقبة الوقائية للاتصالات الإلكترونية في إطار الكشف عن الجرائم المعلوماتية، بناء على إذن مكتوب من السلطة القضائية، وتحت مراقبتها.[5]

ومن أجل مساعدة الهيئة في تأدية مهامها، يمكنها أن تنتدب قضاة وضباط وأعوان شرطة قضائية مؤهلين، سواء من المصالح العسكرية للأمن، أو مصالح الدرك والأمن الوطنيين، وكذا من

[1]- راجع المادة 15 من المرسوم الرئاسي رقم 21-439.
[2]- راجع المادة 14 من المرسوم الرئاسي رقم 21-439.
[3]- راجع المادة 17 من المرسوم الرئاسي رقم 21-439.
[4]- راجع المادة 18 من المرسوم الرئاسي رقم 21-439.
[5]- راجع المادة 19 من المرسوم الرئاسي رقم 21-439.

مستخدمي الدعم التقني والإداري للمصالح العسكرية للأمن المختصة،[1] كما لها أن تستعين بأي خبير أو شخص يستطيع مساعدتها في أعمالها،[2] بل ويمكنها توظيف فئات أخرى عند الحاجة.[3]

الفرع الثاني: مهام الهيئة

تضطلع الهيئة من خلال هياكلها بدورين أساسين؛ الأول وقائي بالنسبة لجرائم الإرهاب والتخريب والمساس بأمن الدولة، والثاني مساعد للتحقيق بالنسبة للجرائم الإلكترونية الأخرى.

أولا: الدور الحصري في الوقاية والكشف عن الجرائم الإرهابية والتخريبية والماسة بأمن الدولة: إذ أنها الجهة المُكلَّفة حصرا في هذه الحالة بمراقبة الاتصالات الإلكترونية، والعمل على تجميع وتسجيل محتواها في حينها، تحت سلطة قاض تابع للهيئة، وتبعا لذلك فإن دورها الحصري يتمثل في:

01- المراقبة الوقائية للاتصالات الإلكترونية: عرّف الفقه المراقبة الإلكترونية للاتصالات بأنها: "وضع تقنيات لازمة لتجميع وتسجيل محتوى الاتصالات الإلكترونية، بما فيها تلك التي تتم على الشبكة العنكبوتية أو الهاتف أو الفاكس، أو أي وسيلة الكترونية أخرى تنقل المعلومات، على أن يتم هذا التجميع والتسجيل في حينه، أي أثناء إجراء الاتصال، أما إذا تم الاطلاع على هذه المعلومات في وقت لاحق فإن ذلك يعد تفتيشا لا مراقبة"،[4] في حين عرف التشريع الأمريكي هذا الإجراء بأنه: "عملية الاستماع لمحتويات أسلاك، أو أي اتصالات شفوية عن طريق استخدام جهاز إلكتروني، أو أي جهاز آخر".[5]

أما المشرع الجزائري، فلم يقدم تعريفا صريحا لإجراء مراقبة الاتصالات الإلكترونية، واكتفى بالإشارة إلى ذلك ضمن المادة 03 من القانون: 09-04، حين أجاز للهيئة وضع ترتيبات تقنية

[1]- راجع المادة 20 من المرسوم الرئاسي رقم 21-439.

[2]- راجع المادة 32 من المرسوم الرئاسي رقم 21-439.

[3]- راجع المادة 21 من المرسوم الرئاسي رقم 21-439.

[4]- سامي جلال فقي حسين، المرجع السابق، ص 284.

[5]- ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2009، ص: 138.

لمراقبة الاتصالات وتجميع وتسجيل محتواها في حينها متى دعت إلى ذلك مقتضيات النظام العام، أو مستلزمات التحريات أو التحقيقات القضائية الجارية، مضفيا بذلك طابعا وقائيا على هذا الإجراء من خلال وجوب القيام به قبل حدوث أي جريمة تفاديا لوقوعها.

وقد عددت المادة 04 من القانون: 09-04 الحالات التي يُسمح فيها بالمراقبة الإلكترونية كأصل عام،[1] فيما حددت المادة 25 من المرسوم الرئاسي رقم: 21-439 الحالة التي يمكن فيها اتخاذ هذا الإجراء كأسلوب وقائي؛ وذلك تفاديا لوقوع جرائم الإرهاب أو التخريب أو المساس بأمن الدولة.[2]

وإن تشابه هذا الإجراء مع إجراء اعتراض المراسلات وتسجيل الأصوات، فإنه يختلف عنه من حيث أنه يمكن استخدامه كتدبير احترازي للوقاية من جرائم الإرهاب أو التخريب أو الماسة بأمن الدولة، أو كإجراء تحري في بقية الجرائم الإلكترونية، عكس اعتراض المراسلات وتسجيل الأصوات الذي يعد إجراء تحري يلجأ إليه في بعض الجرائم المحددة على سبيل الحصر.

ونظرا لخطورة هذا الإجراء ومساسه بسرية المراسلات والاتصالات، فقد أخضعه المشرع لإشراف ورقابة القضاء، فلا يمكن مباشرته إلا بإذن منه،[3] ولا ينفذه إلا أعوان الهيئة المؤهلين تحت إدارة ومراقبة قاض تابع لها، مع وجوب التزامهم بواجب السر المهني،[4] فضلا عن عدم استخدام المعلومات التي تجمعها الهيئة لأغراض أخرى، غير تلك المتعلقة بالوقاية من الجرائم.[5]

02- التفتيش والحجز الوقائيين في الأنظمة المعلوماتية: تتمتع الهيئة باختصاص حصري لإجراء التفتيش الإلكتروني والحجز في الأنظمة المعلوماتية، قصد الوقاية من جرائم الإرهاب أو

---

[1]- تنص المادة 04 من القانون رقم 09-04:" يمكن القيام بعمليات المراقبة المنصوص عليها في المادة03 في الحالات التالية:أ- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، ب-في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، ج-لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول على نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية، د- في إطار تنفيذ طلبات المساعدة القضائية".

[2]- راجع المادة 25 من المرسوم الرئاسي رقم 21-439.

[3]- راجع المادة 04 من القانون رقم 09-04.

[4]- راجع المادة 23 من المرسوم الرئاسي رقم: 21-439.

[5]- راجع المادة 29 من المرسوم الرئاسي رقم: 21-439.

التخريب أو الماسة بأمن الدولة، مع ضرورة حصول ضباط الشرطة القضائية على إذن مكتوب من النائب العام لدى مجلس قضاء الجزائر،[1] وهي الإجراءات التي سنتناولها بشيء من التفصيل في حينها.

ثانيا: الدور المساعد في مكافحة الجريمة الإلكترونية: أجاز المشرع للهيئة مساعدة السلطات القضائية وجهاز الشرطة القضائية في التحريات التي يباشرونها، مثلما أجاز لها تبادل المساعدة القضائية مع نظرائها في الخارج في إطار التعاون الدولي.

01- تقديم المساعدة القضائية الوطنية: تعمل الهيئة على مساعدة السلطات القضائية الوطنية ومصالح الشرطة القضائية في تحرياتهم بشأن الجرائم الإلكترونية، من خلال جمع المعلومات وتزويدهم بها، فضلا عن إنجاز الخبرات القضائية،[2] كما يمكنها القيام بإجراء المراقبة الإلكترونية بطلب من الجهات القضائية المختصة في الحالات التالية:

أ- حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو الاقتصاد الوطني أو مؤسسات الدولة: إذ أن السلطات القضائية بمجرد تلقيها لمعلومات تحمل تهديدا للنظام العام، أو الدفاع الوطني، أو الاقتصاد الوطني، أو مؤسسات الدولة، يمكن لها أن تستعين بالهيئة، وتطلب مساعدتها للقيام بهذا الإجراء من أجل كشف الجريمة ومرتكبيها باعتبارها هيئة تقنية متخصصة، بشرط الحصول على إذن مكتوب من السلطة القضائية المختصة.[3]

ب- لمقتضيات التحريات والتحقيقات القضائية: يتم اللجوء إلى إجراء المراقبة الإلكترونية في هذه الحالة بعد ارتكاب الجريمة، وذلك بسبب فشل الإجراءات التقليدية في الكشف عنها نتيجة

[1]- راجع المادة 04 من القانون 09-04، والمادة 25 من المرسوم الرئاسي رقم 21-439 .

[2]- راجع المادة 04 من المرسوم الرئاسي رقم 21-439.

[3]- راجع المادة 04 من القانون رقم 09-04.

تعقيداتها، فيتم الاستعانة بالهيئة بحكم تخصَصها للقيام بهذا الإجراء، بشرط أن يقدم لها طلب المساعدة، وأن تتحصل على إذن مكتوب من السلطة القضائية المختصة.[1]

02- تقديم المساعدة القضائية الدولية: يمكن للهيئة في إطار التعاون الدولي تقديم المساعدة القضائية للسلطات الأجنبية من خلال تبادل المعلومات في إطار جمع الأدلة الرقمية المفيدة في كشف الجرائم الإلكترونية، قصد الوصول إلى مرتكبيها، وتحديد أماكن تواجدهم.[2]

[1]- تنص المادة 04 من القانون رقم: 09-04:"لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية".

[2]- راجع المادة 14 من قانون 09-04

خلاصة الفصل

اتفقت التشريعات المقارنة على أن التحقيق الجنائي هو المرحلة التي تسبق مرحلة المحاكمة وتمهَد لها، لكنهم اختلفوا في تحديد الجهة المختصة به، فمنهم من أسنده إلى قاض محايد، أخذا بمبدأ الفصل بين سلطة التحقيق وسلطة الاتهام، ومنهم من أسنده إلى النيابة العامة أخذا بمبدأ الجمع بين السلطتين.

أما المشرع الجزائري فقد أسنده إلى قاضي التحقيق على مستوى الدرجة الأولى وغرفة الاتهام على مستوى الدرجة الثانية، مثلما خوله استثناء لقضاة الحكم في المواد الجزائية حال تبين لهم عدم اكتمال الأدلة.

ويؤدي جهاز الشرطة القضائية دورا لا يمكن الاستغناء عنه في مسار التحقيق، سواء من خلال المعلومات التي يجمعها أثناء مرحلة التحريات الأولية، أو من خلال الاستعانة به لتنفيذ أعمال من صميم العمل القضائي حين تنفيذه للإنابة القضائية.

وأمام تطور الجريمة الإلكترونية سعى المشرع الجزائري إلى تعزيز أجهزة مكافحتها من خلال استحداث هيئة تقنية متخصصة بموجب القانون رقم: 09-04، منحها السلطة والاستقلالية لتحقيق الفعالية المرجوَة، وضمان استمرارية التعاون الدولي.

الباب الثاني

أساليب التحقيق الجنائي

في الجريمة الإلكترونية

الباب الثاني

أساليب التحقيق الجنائي في الجريمة الإلكترونية

ترتبط الجرائم الإلكترونية بأنماط ودرجات عالية من التكنولوجيا، مما يتطلب قواعد وتقنيات مماثلة لها، تتماشى مع التطور التكنولوجي، ولا تقتصر على أساليب التحقيق التقليدية.

ومن أجل التصدي لهذه الجرائم استحدث المشرع الجزائري أساليب تحقيق تعتمد على استخدام نفس التقنية التي يستخدمها المجرم الإلكتروني، وتضمن في الوقت ذاته احترام خصوصية الإنسان وحرمة حياته الخاصة،[1] بدءا بتعديل قانون الإجراءات الجزائية سنة 2006، وتكريس أساليب تحري خاصة لم تكن معروفة قبل ذلك، مرورا إلى استحداث القانون رقم 09-04، وبعض القوانين الخاصة التي أضافت أساليب أخرى.

وبما أننا بصدد دراسة موضوع التحقيق في الجريمة الإلكترونية وما يثيره من إشكالات إجرائية، فسنقتصر في دراستنا على الأساليب التي لها علاقة بالتقنية الرقمية التي تنصب على الأشياء، دون التطرق لغيرها من الإجراءات التي تتم في مواجهة الأشخاص، كالاستجواب والمواجهة، وسماع الشهود، والتي تخضع لنفس القواعد في الجرائم التقليدية.

ومن أجل الإلمام بهذه الإجراءات، ارتأينا تقسيم هذا الباب إلى الفصلين الآتيين:

الفصل الأول: الأساليب التقليدية للتحقيق في الجريمة الإلكترونية.

الفصل الثاني: الأساليب الحديثة للتحقيق في الجريمة الإلكترونية.

[1]- تنص المادة 47 من الدستور الجزائري: "لكل شخص الحق في حماية حياته الخاصة وشرفه".

الفصل الأول

الأساليب التقليدية للتحقيق في الجريمة الإلكترونية

الفصل الأول

الأساليب التقليدية للتحقيق في الجريمة الإلكترونية

نظمت مختلف التشريعات الجنائية طرق الحصول على أدلة الجريمة، بدءا باتخاذ إجراءات تتبعها، وصولا إلى تحقيق الغاية المنشودة، وهي إثبات الجريمة ومعرفة مرتكبها، وتستخدم هذه الإجراءات لجمع الدليل في مختلف الجرائم سواء التقليدية أو المستحدثة.

ورغم التقدم العلمي الذي أدى إلى توظيف وسائل علمية حديثة في نظام الإثبات الجنائي لتجنب تضليل المتهم للعدالة، وكشف ما يقوم به من محو لآثار الجريمة، إلا أنه يبقى للدليل المادي دور أساسي في كشف ملابساتها.

فمهما حاول الجاني إخفاء الحقيقة، إلا أنه وفي النهاية لابد وأن يترك أثرا، وذلك نتيجة الحالة النفسية والانفعالات التي تصاحبه عند ارتكاب جريمته،[1] لذلك يبقى للإجراءات التقليدية دور مهم في جمع الدليل الجنائي، فتغير طريقة المعاينة والتفتيش مثلا لا يعني أنهما لم يصبحا من الإجراءات التقليدية.

وعلى هذا الأساس ارتأيت أن أتحدث على الإجراءات التقليدية من خلال المبحثين الآتيين:

المبحث الأول: المعاينة والخبرة في الجريمة الإلكترونية.

المبحث الثاني: التفتيش والحجز في الجريمة الإلكترونية.

[1]– ابراهيم صادق الجندي، حسين حسن الحسيني، تطبيقات البصمة الوراثية في التحقيق والطب الشرعي، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002، ص: 9.

المبحث الأول

المعاينة والخبرة في الجريمة الإلكترونية

تعتبر المعاينة والخبرة من طرق الإثبات المباشرة، وذلك لاتصالهما اتصالا ماديا بالواقعة محل الإثبات، إذ تثبت المعاينة حالة الأماكن والأشياء والأشخاص، ولها أهمية بالغة في الكشف عن مرتكبي الجريمة الإلكترونية، وتوفر الخبرة عملا فنيا خاصا لا يتوافر لدى المحقق الجنائي، لذلك أجاز القانون الاستعانة بأهل المعرفة والتخصص متى تطلب التحقيق ذلك.

ولا خلاف لدى الفقه والقضاء على مشروعية الخبرة والمعاينة في الكشف عن أدلة الجريمة قصد إظهار الحقيقة، غير أنهما تعتبران من بين عقبات التحقيق، نظرا لورودهما على مسرح جريمة افتراضي، يختلف عن مسرح الجريمة التقليدي.

ولدراسة ما سبق عرضه من نقاط يتعين تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: المعاينة في الجريمة الإلكترونية.

المطلب الثاني: الخبرة في الجريمة الإلكترونية.

المطلب الأول

المعاينة في الجريمة الإلكترونية

يعد إجراء المعاينة أحد سبل التحقيق للكشف عن ملابسات الجريمة، لذلك أجاز القانون للمحقق الجنائي التنقل إلى مكان وقوع الجريمة لإثبات حالتها، وضبط الأشياء و الأدوات التي ارتكبت بها، فهي دليل من أدلة الدعوى.

الفرع الأول: مفهوم المعاينة

تلعب المعاينة في الجريمة الإلكترونية دورا مهما في الكشف عن الدليل الرقمي الذي يمكن أن يتوافر وسط بيئة رقمية، نظرا لما تشتمل عليه من صفحات إلكترونية، وحسابات بريد إلكتروني ومواقع للتواصل الاجتماعي، وغرف محادثة، ولوحات إعلانية، ومنتديات وغيرها.

أولا: تعريف المعاينة: لم يتطرق المشرع الجزائري لتعريف المعاينة، في حين عرفها بعض الفقه الجنائي بأنها: "إجراء ينتقل بموجبه المحقق إلى مكان وقوع الجريمة، ليشاهد بنفسه ويجمع الآثار

المتعلقة بالجريمة وكيفية وقوعها، وجميع الأشياء المفيدة في كشف الحقيقة"،[1] وعرفها البعض الآخر بأنها: "إجراء يستهدف أمرين؛ الأول وهو جمع الأدلة التي تخلفت عن الجريمة، وحصر ما بجسم الجريمة من آثار، والثاني هو إعطاء فرصة للمحقق ليطّلع بنفسه على مسرح الجريمة، حتى يمكنه تمحيص مدى صدق الأقوال التي أبديت حول كيفية وقوعها".[2]

وتتم المعاينة المادية بأي حاسة من الحواس، سواء عن طريق اللمس أو السمع أو البصر أو الشم أو الذوق،[3] وتتنوع بتنوع محلها، فتكون معاينة شخصية إذا تعلقت بشخص المجني عليه وتكون معاينة مكانية إذا تعلقت بالمكان الذي تمت فيه الجريمة ووضعيات الشهود والمتهم والمجني عليه، وتكون معاينة عينية إذا تعلقت بالأشياء أو الأدوات المستخدمة في الجريمة.

وأيا كان تعريف المعاينة، فهي تتطلب الانتقال إلى مكان وقوع الجريمة ووضع وصف شامل له، سواء بالكتابة أو بالرسم التخطيطي أو بالتصوير لإثبات حالته بالكيفية التي تركها عليه الجاني، كما تشمل فحص جسم الجاني والمجني عليه، وبيان ما يوجد بهما من آثار تخلفت عن الجريمة.

ورغم إمكانية اللجوء إلى المعاينة في جميع الجرائم، إلا أنها ليست دائما مجدية، فهناك بعض الجرائم لا تتطلب هذا الإجراء، لذلك يترك تقدير لزومها إلى جهة التحقيق، فهي ليست إجراء تلقائيا، بل إجراء هادف للكشف عن أدلة الجريمة.

ثانيا: تعريف المعاينة في الجريمة الإلكترونية: وتعني: "معاينة الآثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت، وتشمل الرسائل المرسلة منه، أو التي يستقبلها، وكافة الاتصالات التي تمت من خلال جهاز الحاسب الآلي والشبكة العالمية"،[4] أو هي: "معاينة البيئة الافتراضية المكونة من البرمجيات والمكوّنات المادية وشبكة الإنترنت، أين يوجد الدليل الرقمي لجريمة وقعت".[5]

---

[1]– محمود ابراهيم غازي، المرجع سابق، ص: 716.

[2]– بهاء المري، المرجع السابق، ص: 811.

[3]– أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص: 86.

[4]– خالد ممدوح ابراهيم، المرجع السابق، ص: 165.

[5]– بهاء المري، المرجع نفسه، ص: 817.

والملاحظ هو أن الآثار المعلوماتية المستخلصة من أجهزة الكمبيوتر ثرية بالمعلومات، مثل صفحات المواقع المختلفة، ومواقع البريد الإلكتروني، والفيديوهات الرقمية، وغرف الدردشة والمحادثة، والملفات المخزنة في الكمبيوتر الشخصي، وغيرها.

ثالثا: خصائص مسرح الجريمة الإلكتروني: إذا كانت معاينة المسرح التقليدي للجريمة تتطلب التنقل المادي للمحقق، فالأمر مختلف بالنسبة لمسرح الجريمة الإلكتروني، إذ يستطيع المحقق أن يقوم بهذه العملية من خلال الحاسوب وهو جالس في مكتبه، لذلك يتميز مسرح الجريمة الإلكتروني عن مسرح الجريمة التقليدي بعدة خصائص، أهمها:[1]

01- ذو طبيعة مركبة: فهو يجمع بين البيئة المادية التقليدية لأجهزة الحاسب الآلي وملحقاته وبين البيئة المعنوية المتمثلة في البيانات والمعلومات المحملة على أجهزة الحاسب الآلي وشبكات المعلومات بمختلف أنواعها.

02- عابر للحدود: وذلك عند النظر إليه من زاوية الشبكات المفتوحة المتصلة بأجهزة الحاسب الآلي، والكم الهائل للمواقع الإلكترونية المتصل بها، ويستمد مسرح الجريمة هذه الخاصية من طبيعة الشبكة الدولية العابرة للحدود.

03- ديناميكي ومتنوع: فهو مسرح حركي وسريع التغيير، سواء من حيث أدواته أو وسائله، وذلك لارتباطه بمعدلات التطور والتغير الدائم في أنظمة المعلومات وأجهزتها وشبكاتها ومواقعها.

04- علمي وتقني ومتخصَص: إذ تعتمد عملية استخلاص الأدلة الجنائية الرقمية على الإحاطة بعلوم مختلفة؛ قانونية وجنائية وهندسية، إضافة إلى علوم الحاسب الآلي وشبكاته.

05- معقَّد ومتشابك: حيث تتداخل فيه الكيانات المادية للحاسب الآلي مع الكيانات المعنوية، فلا يمكن فصل إحداها عن الأخرى، ولا فصلهما عن الحيز المكاني المحيط بهما، مما يتطلب توافر معارف علمية وخبرات فنية عند التعامل مع الأدلة الرقمية.

رابعا: أهمية المعاينة في الجريمة الإلكترونية: يعتبر إجراء المعاينة عموما صورة من صور الحصول على الإيضاحات، وقد خصها المشرع بالنص عليها لأهميتها، ويقتضي إجراؤها الانتقال إلى مكان الجريمة وإثبات حالته، وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى مرتكبها.

[1]- يحيى عطوة الزنط، المرجع السابق، ص: 322.

وتكتسي المعاينة في الجريمة الإلكترونية أهمية خاصة في مجال التحقيق الجنائي من الناحيتين القانونية والعلمية، فهي تترجم ما قام به الجاني من أفعال، وعلى ضوئها يتأكد وقوع الجريمة أو نفيها، وصدق أو كذب أطراف الدعوى، وبيان ركن الخطأ أو العمد في الواقعة، كما تكتسي أهمية في تحديد الوصف القانوني للواقعة، وتساعد القاضي على تكوين عقيدته واقتناعه.[1]

فإذا وقعت جريمة إلكترونية باستخدام هاتف محمول مثلا، سواء كان الاتصال بهاتف آخر أو بشبكة الإنترنت، مثل إرسال عبارات تشكل قذفا أو سبا أو تهديدا، أو كان وسيلة لارتكاب سلوك غير مشروع، فإنه يمكن للمحقق معاينته، ومن خلاله يستطيع معاينة الصفحة التي اتصل بها الجاني بشبكة الإنترنت لمعرفة محتوى هذا السلوك، كاطلاعه على الرسائل أو الصور أو التهديدات، وتفريغ محتواها في محضر، أو نسخها عن طريق طابعة وإرفاق صور منها بالمحضر، مع إثبات رقم الخط الهاتفي المستعمل في عملية الإرسال، وساعة وصولها إلى المجني عليه، أو ساعة نشرها على موقع التواصل الاجتماعي، أو إرسالها إلى البريد الإلكتروني للمجني عليه أو لغيره.[2]

ونظرا لما تتميز به الجريمة الإلكترونية من تعقيدات، فيمكن للمحقق أن يستعين بأصحاب المعرفة للفحص وإبداء الرأي الفني في الأمور التي يصعب عليه فهمها وتفسيرها، حتى يمنع أي تشكيك في صحة الدليل المستمد من معاينته.

ورغم أهمية المعاينة في كشف غموض الجريمة الإلكترونية وضبط أدلتها، إلا أن دورها لا يرق إلى نفس الدرجة في كشف الجرائم التقليدية، وذلك راجع للأسباب التالية:[3]

01- قليلا ما تخلف الجرائم الإلكترونية آثارا مادية عند ارتكابها، فما ينتج عنها غالبا من أدلة هو بيانات غير مرئية.

---

[1]- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مرجع سابق، ص: 59-60.

[2]- بهاء المري، المرجع السابق، ص: 815.

[3]- هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، (دراسة مقارنة)، مكتب الآلات الحديثة، أسيوط، مصر، 1994، ص: 57.

02- تردد العديد من الأشخاص على المسرح الافتراضي للجريمة خلال الفترة الزمنية الممتدة بين تاريخ ارتكابها وتاريخ اكتشافها، مما يفسح المجال لحدوث إتلاف أو تغيير أو عبث بآثار الجريمة ويدخل الشك على الدليل المستمد من المعاينة.

03- إمكانية تلاعب الجاني بالبيانات عن بعد، لذلك ينبغي وضع عقوبات جنائية لكل من يقوم بإحداث تغييرات أو محو في المعلومات المسجلة في ذاكرة الحاسوب، أو في وسائط التخزين، أو في بنك المعلومات، أو في قاعدة البيانات، قبل انتقال جهة التحقيق للمعاينة.

04- مشكلة السرعة في ضياع الدليل الإلكتروني الذي يمكن تعديله أو محوه في بضع ثوان، لذلك أجاز المشرع الأمريكي لعضو النيابة العامة أن يعجل بإجراء المعاينة خشية ضياع الأدلة، وذلك بإرسال رسالة إلى مزود خدمة الإنترنت يلزمه فيها بتتبع السجلات المطلوبة إلى حين صدور أمر المحكمة باتخاذ هذا الإجراء أو غيره، وقد كرَس المشرع الجزائري بدوره هذا الإجراء، وهو ما سنتعرف عليه بالتفصيل في حينه.

الفرع الثاني: قواعد المعاينة الإلكترونية ونطاقها

يعتمد المحقق الجنائي عند إجراء المعاينة بحثا عن الأدلة الإلكترونية على فحص مكونات الحاسب الآلي التي لها علاقة بالجريمة وشبكات الاتصال، لذلك سنتطرق إلى قواعد المعاينة في الجريمة الإلكترونية، ثم نتعرف على نطاقها.

أولا: قواعد المعاينة في الجريمة الإلكترونية: حتى تكون المعاينة مفيدة في كشف ملابسات الجريمة الإلكترونية، ويطمئن القضاء للأخذ بها كدليل في الدعوى، فإنه يتعين أن يكون المحقق ملما بالقواعد الفنية التي تسهل له الوصول إلى أدلة تتواجد وسط بيئة رقمية معقدة وحجزها دون خطأ، فضلا عن إدراكه بالقواعد القانونية التي تمكنه من ضبط هذه الأدلة في إطارها الشرعي.

01- القواعد الفنية للمعاينة الإلكترونية: نظرا لصعوبة المعاينة في الجريمة الإلكترونية بسبب ما تتطلبه من ولوج إلى الحاسب الآلي عن طريق بعض البرامج، أو إجرائها عبر شبكة الإنترنت، فإنه يتعين اتباع قواعد فنية أبرزها:

أ- توفير معلومات مسبقة عن مكان وقوع الجريمة ونوع وعدد الأجهزة المتوقع مداهمتها وشبكات الاتصال المرتبطة بها.

ب- إعداد فريق تفتيش يتكون من محققين وخبراء وفنيين ممن لهم تكوين متخصص في مجال مكافحة الجريمة الإلكترونية، خصوصا عندما يتعلق الأمر ببعض الجرائم الإلكترونية المعقدة.[1]

ت- توفير الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل، مثل برنامج معالجة الملفات، وبرنامج النسخ، وبرنامج (ENCASE) الذي ينتج صورا مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفيدرالية الأمريكية، ويسميه الخبراء "حقيبة الأدلة الرقمية".[2]

ث- تصوير جهاز الكمبيوتر وسائر ملحقاته والأجهزة الطرفية المتصلة به، والمحتويات والأوضاع العامة بمكان تواجده بدقة، ويراعى وقت وتاريخ ومكان التقاط كل صورة.[3]

ج- أن يعمل المحقق الجنائي على الوصول إلى الملفات التي تحمل معلومات عن مختلف الاتصالات، وتحديد جهة صدورها والقائم بإجرائها، مع ضرورة إلمامه بالحالات التي يجب عليه أن يتحفظ فيها على جهاز الحاسوب، أو يأخذ نسخة من أسطواناته الصلبة، والحالات التي يستخدم فيها برامج استعادة المعلومات التي تم إلغاؤها.[4]

ح- فحص سلة المهملات لمعرفة الملفات التي تم حذفها، بالإضافة إلى استخدام برامج استرجاع الملفات المحذوفة نهائيا.

خ- الحرص على عدم إتلاف أي بيانات استخرجت من الحاسوب، والتأكد من وجود نسخة منها داخل الجهاز نفسه، مع ضرورة الفحص الدقيق لجميع الملفات للتعرف على العمليات التي قام بها مستخدم الجهاز، والمواقع التي زارها عبر شبكة الإنترنت، وكذا معرفة أسماء حساباته في مواقع التواصل الاجتماعي، وكلمات المرور الخاصة به.[5]

---

[1]- محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، أكاديمية نايف للعلوم الأمنية، العدد 30، 2000، ص: 357.

[2]- محمود إبراهيم غازي، المرجع السابق، ص: 723.

[3]- محمد أبو العلا أبو عقيدة، التحقيق وجمع الأدلة في الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للمعاملات الإلكترونية، دبي، 2004.

[4]- محمود إبراهيم غازي، المرجع نفسه، ص: 726.

[5]- أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2015، ص: 134-135 .

د- عدم نقل المعلومات خارج مسرح الجريمة إلا بعد التأكد من خلو المحيط الخارجي للحاسب من مجالات القوى المغناطيسية –الممرات المغناطيسية- التي قد تتسبب في محو البيانات، ولن يتأتى ذلك إلا بمعرفة خبراء الحاسب الآلي.[1]

ذ- تدوين المعاينة باعتبارها إجراء من إجراءات التحقيق، يسري عليها ما يسري على باقي الإجراءات، لذلك يمكن تدوينها كتابة ورسما وتصويرا.[2]

02- القواعد القانونية للمعاينة الإلكترونية: يتمتع قاضي التحقيق بسلطة تقدير ملائمة اللجوء للمعاينة خلال فترة التحقيق الابتدائي، إذ أجاز له القانون الانتقال إلى مكان وقوع الجريمة لإجراء المعاينات اللازمة متى رأى ذلك مفيدا للتحقيق، سواء كان ذلك بطلب من أطراف الدعوى، أو من تلقاء نفسه، مع ضرورة إخطار وكيل الجمهورية في الحالة الأخيرة حتى يتمكن من مرافقته إذا رغب في ذلك.[3]

وقد تتطلب المعاينة التنقل خارج الاختصاص المحلي لقاضي التحقيق، وحينها يتعين عليه أن يخطر وكيل الجمهورية الذي يعمل بدائرة اختصاصه، والذي يمكنه مرافقته، إضافة إلى إخطار وكيل الجمهورية الذي يعمل بالإقليم الذي ستجرى فيه المعاينة.[4]

وتجدر الإشارة إلى أن القانون 06-22 المعدل والمتمم لقانون الإجراءات الجزائية أجاز للمتهم وللطرف المدني ومحاميهما التقدم بطلب إجراء معاينة أمام قاضي التحقيق،[5] ويتعين على هذا الأخير في حالة رفض الطلب أن يصدر أمر مسببا قابلا للاستئناف أمام غرفة الاتهام.[6]

وقد أجاز المشرع الجزائري المعاينة في أي محل سكني أو غير سكني، وفي كل ساعة من ساعات الليل أو النهار، عندما يتعلق الأمر ببعض الجرائم، ومن بينها الجرائم الماسة بأنظمة

---

[1]- نبيلة هبة هروال، المرجع السابق، ص: 220.

[2]- خالد ممدوح إبراهيم، المرجع السابق، ص: 164.

[3]- راجع المادة 79 ق إ ج.

[4]- راجع المادة 80 ق إ ج.

[5]- راجع المادة 69 مكرر ق إ ج.

[6]- راجع المادة 172 ق إ ج.

المعالجة الآلية للمعطيات،[1] ليستثني بذلك تطبيق هذه الضمانة على هذا النوع من الجرائم تغليبا للمصلحة العامة للمجتمع في تحقيق العدالة، على مصالح الأفراد في حرمة حياتهم الخاصة.

ومع ذلك، يجب أن تنحصر المعاينة على الحيز المكاني للجريمة باعتباره موقعا مارس فيه الجناة أنشطتهم الإجرامية، دون أن تمتد إلى مستودع الأسرار، وإلاَ دخلت نطاق إجراء آخر من إجراءات التحقيق، وهو التفتيش بما له من أحكام وقيود ينفرد بها عن المعاينة.[2]

إضافة إلى ذلك، فقد عمد المشرع إلى تجريم المساس بمسرح الجريمة من طرف أي شخص ليست له صفة، وذلك بهدف المحافظة عليه من كل تغيير يؤدي إلى طمس آثارها قبل قيام المحقق بمعاينته،[3] خاصة في مجال الجرائم الإلكترونية التي تتطلب سرعة التحرك لمنع المجرم من تعديل الدليل الرقمي أو تدميره.

وتجدر الإشارة إلى أن قاضي التحقيق لا يحتاج إلى إذن للقيام بالمعاينة كونها تدخل ضمن إجراءات التحقيق التي يملك ما هو أخطر منها،[4] ورغم ذلك يتعين عليه أن يصدرا أمرا مكتوبا عند قيامه بأي إجراء من إجراءات التحقيق، حتى يتسنى مراقبة أعماله، تكريسا لمبدأ الشرعية الإجرائية.

ويجب أن يقتصر عمل قاضي التحقيق خلال معاينته الميدانية على نقل صورة صحيحة وكاملة لمحل المعاينة دون إضافة أو حذف، ودون إدراج أي استنتاج توصل إليه، ويبقى له الحق في مناقشة ذلك حين استجواب أطراف الدعوى.

وطالما أن المعاينة إجراء من إجراءات التحقيق، فإنها تخضع لنفس القواعد التي تحكم إجراءاته الأخرى، بما فيها إخطار الخصوم بمكان المعاينة وزمانها لتمكينهم من الحضور أثناء إجرائها.[5]

---

[1]– راجع المادة 47 ق إ ج.

[2]– برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية، دار النهضة العربية، القاهرة، 2006، ص: 175.

[3]– راجع المادة 43 ق إ ج.

[4]– عبد الرحمان خلفي، المرجع السابق، ص: 302

[5]– محمود ابراهيم غازي، المرجع السابق، ص: 718.

وبمجرد انتهاء قاضي التحقيق من إجراء المعاينة، يقوم أمين الضبط الذي يصاحبه بتحرير محضر يذكر فيه تاريخها ومكانها، مع سرد مفصل لجميع الأعمال التي قام بها قاضي التحقيق، حتى يسهل فهمه من طرف قضاة الحكم عند مناقشة الدليل.[1]

أما المعاينة التي يجريها رجال الشرطة القضائية خلال مرحلة التحريات الأولية، فنميز فيها بين المعاينة التي تتم في مكان عام، والتي لا تحتاج إلى إذن أو ندب من السلطة القضائية طالما أنها تدخل ضمن اختصاصهم الأصيل، وهو التحري عن الجريمة، وبين المعاينة التي تتم في مكان خاص، والتي تستلزم لصحتها إذنا مسبقا من القضاء.[2]

ثانيا: نطاق المعاينة في الجريمة الإلكترونية: تتم المعاينة في الجريمة الإلكترونية كأي جريمة أخرى عن طريق الانتقال إلى محل الواقعة الإجرامية باعتباره مكمن الآثار والأدلة المادية، أين يقوم المحقق الجنائي بفحص مكونات الحاسب الآلي الخاصة بالجاني والمجني عليه، وأنظمة الاتصال بشبكة الإنترنت بحثا عن الأدلة الإلكترونية، فهي تشمل:

01- معاينة مكونات الحاسوب: تعتبر الحواسيب الآلية مصدرا غنيا بالأدلة الإلكترونية، خاصة الحواسيب الشخصية التي تعد بمثابة أرشيف لسلوك الفرد ونشاطاته، إذ أن فحصها يعد نقطة بداية في الكشف عن خطوات الجريمة، باعتبار أن هذه الأجهزة وسيلة تنفيذها أو محل وقوعها، لذلك ينبغي التمييز عند معاينة جهاز الحاسوب بين المعاينة التي تنصب على مكوناته المادية وتلك التي تنصب على مكوناته المعنوية.

أ- معاينة المكونات المادية: وهي أقرب ما تكون إلى معاينة مسرح أي جريمة تقليدية يترك فيها الجاني آثارا أو بصمات، مثل معاينة أشرطة الحاسب أو مفاتيح التشغيل أو الأقراص أو شاشة العرض، وغيرها من المكونات المادية، فلا صعوبة في معاينة هذه المكونات ووضع الأختام عليها، وحجز كل ما استعمل في ارتكاب الجريمة والتحفظ عليه.[3]

---

[1]- راجع المادة 79 ق إ ج.

[2]- حسين طاهري، إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية، دار العلا للطباعة والنشر، أم البواقي، الجزائر، 2023، ص: 18.

[3]- تنص المادة 84 ف 2 ق إ ج: "ويجب على الفور إحصاء الأشياء والوثائق المضبوطة ووضعها في أحراز مختومة".

ب- معاينة المكونات المنطقية: يفترض في القائمين بهذه المعاينة الإلمام الجيد بأجهزة الحاسب الآلي وبرامجه، لأنها تستهدف ما يحتويه من برامج من أجل ضبط كل ما يفيد في الكشف عن الحقيقة.[1]

02- معاينة أنظمة الاتصال: قد لا تكفي معاينة مكونات الحاسب الآلي دائما لاستخلاص الدليل الرقمي، وهو ما يتطلب من المحقق معاينة أنظمة اتصال شبكة الإنترنت، وذلك بفحص مسار الشبكة والنظام الأمني والخادم،[2] ومن خلالها يمكنه معرفة البريد الإلكتروني للجاني وحسابه على مواقع التواصل الاجتماعي، ثم الاطلاع على ما نشره من أفكار متطرفة، أو إشاعات كاذبة أخلَت بالسلم والأمن الاجتماعيين.[3]

وتواجه المعاينة في الجريمة الإلكترونية إشكالات عديدة تتعلق بامتداد نطاقها المكاني خصوصا عندما يستعمل الجاني أو الجناة عدة حواسيب أو عدة شبكات لاقتراف الجريمة، وقد تتواجد هذه الأجهزة بمكان واحد، كما قد تتواجد بأماكن متفرقة، وفي صورة أخرى أكثر تعقيدا قد يتواجد بعضها أو كلها خارج إقليم الدولة، وقد يتوزعون على عدة دول، مما يصعب الوصول إليها.

لذلك ورغم الدور الذي تلعبه المعاينة في الكشف عن أدلة الجريمة الإلكترونية، إلا أنها قد تعجز عن تحقيق هدفها المنشود بسبب الذكاء الذي يتميز به مجرمو المعلوماتية، مما يدفع بالمحقق الجنائي إلى الاستعانة بأهل المعرفة والتخصص في هذا المجال، وهنا نكون أمام إجراء آخر من إجراءات التحقيق يتمثل في الخبرة، وهو ما سنتعرف عليه من خلال المطلب الموالي.

---

[1]- حازم محمد خلفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2017، ص: 56.

[2]- جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، ص: 64.

[3]- حازم محمد خلفي، المرجع نفسه، ص: 56.

المطلب الثاني

الخبرة في الجريمة الإلكترونية

تعتبر الخبرة القضائية من أهم أدلة الإثبات في الجريمة الإلكترونية، وذلك لما توفره من عمل فني لا يتوافر لدى المحقق الجنائي، إذ يستطيع أهل الخبرة بحكم تخصصهم التقني مواجهة هذه الجرائم التي تعتمد على التقنية المعلوماتية، سواء من حيث أساليب ارتكابها، أو من حيث سرعة محو وإخفاء أدلتها.

وسوف نتطرق للخبرة القضائية باعتبارها آلية من آليات التحقيق بالقدر الذي يفيدنا في بحثنا، تاركين التفصيل التقني لأهل البحث الفني في الجريمة الحديثة، وهو علم له أصوله وقواعده التي لا يسع المقام لذكرها.

الفرع الأول: الأحكام العامة للخبرة القضائية

تساهم الخبرة الفنية في تحقيق العدالة، وذلك بتنوير القاضي في الوصول إلى الحقيقة من خلال توفير الدليل العلمي في المسائل التقنية التي تقصر معارفه عن إدراكها، غير أن دور الخبير يقتصر على تحقيق الواقعة في الدعوى، وإبداء رأيه في المسائل الفنية، دون التطرق للمسائل القانونية التي تعتبر عملا أصيلا للقاضي.

أولا: تعريف الخبرة: يقصد بالخبرة عموما: "المهارة المكتسبة في تخصَص معين، سواء بحكم العمل في ذلك التخصص لمدة زمنية طويلة، أو نتيجة دراسات خاصة، أو نتيجة الاثنين معا، أي العمل والدراسة، ومن هنا يطلق على ذوي المهارات الخبراء"،[1] أو هي: "استشارة فنية يستعين بها القاضي لتقدير المسائل التي يحتاج تقديرها إلى معرفة فنية أو دراية علمية لا تتوافر لديه بحكم تكوينه".[2]

فالخبرة القضائية إجراء من إجراءات التحقيق، تتعلق بوقائع يستلزم بحثها أو تقديرها إبداء رأي فني أو علمي لا يتوافر لدى المحقق، فيعهد بها إلى شخص مختص يسمى "الخبير".[3]

---

[1]– خالد ممدوح إبراهيم، المرجع السابق، ص: 283.

[2]– أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص: 112.

[3]– محمود جمال الدين زكي، الخبرة في المواد المدنية والتجارية، مطبعة جامعة القاهرة، مصر، 1990، ص: 11.

وتتميز الخبرة عن غيرها من إجراءات التحقيق الأخرى كالمعاينة والتفتيش في إبداء الخبير لرأيه الفني في كشف الدلائل أو تحديد دورها في الإثبات، وهو الأمر الذي يتطلب معارف علمية أو فنية خاصة لا تتوافر لدى المحقق الجنائي.

ثانيا: موضوع الخبرة القضائية: تجيز المادة: 143 ق إ ج لقاضي التحقيق عندما تعرض عليه مسألة ذات طابع فني أن يندب خبيرا فنيا، سواء أكان ذلك من تلقاء نفسه، أو بطلب من النيابة العامة أو أطراف الدعوى.

إن دواعي اللجوء إلى الخبرة الفنية كثيرة، وهي في تزايد مستمر نتيجة للمستجدات على الساحة العلمية، خصوصا بعد لجوء الجناة إلى استخدام وسائل تقنية متطورة في ارتكاب جرائمهم التي صار يصعب الكشف عنها دون مساعدة أشخاص يتمتعون بالمهارة التقنية، ولعلَ ما يزيد من الحاجة إلى الخبرة الفنية هو طبيعة تكوين قضاة التحقيق الذي يغلب عليه طابع العمومية لا التخصَص.

وتتنوع مجالات الخبرة، فقد تشمل الأطباء الشرعيين الذين يتلقون إضافة إلى علم الطب دراسات تخصصية في مجال الفحص الطبي والتشريح من أجل توضيح أسباب الإصابة، أو الوفاة وتحديد كيفية وقوعها، ونوع الأداة المستخدمة، كذلك يوجد ما يسمى بخبراء البصمات الذين يقومون بالكشف عن آثار البصمات التي تركها الجاني في مكان الجريمة، ومقارنتها مع بصمات أخرى من المشتبه بهم ومعتادي الإجرام، ويوجد أيضا خبراء الأسلحة الذين يتولون فحص الأسلحة وتحديد نوعها، ونوع العيار المستعمل في الطلق الناري، أو تحديد الوضعية التي كان عليها الجاني والمجني عليه وقت إطلاق النار، إضافة إلى خبراء الحرائق المتخصصين في كشف المكان وبيان المواد المستخدمة في إشعال النار، والقول إن كان الحريق متعمدا، أو كان نتيجة شرارة كهربائية مثلا، وغيرهم في مجالات مختلفة.[1]

وتتميز مهمة الخبير بخاصيتين؛ فنية وقضائية، فهي مهمة فنية لما تتطلبه من اعتماد الخبير على معلوماته العلمية أو الفنية، وتبعا لذلك لا يعتبر خبيرا من كلفه القاضي بمعاينة يعتمد فيها على حواسه فقط، ولكن يعتبر خبيرا من كلفه القاضي بأن يجري معاينة، ويأتي بنتائج

[1]– خالد ممدوح ابراهيم، المرجع السابق، ص: 289

ملاحظته متى كانت المعاينة والملاحظة تتطلبان تطبيق أساليب علمية أو فنية،[1] وهي مهمة قضائية كونه لا يمكن للخبير أن يمارس مهمته إلا بندب قضائي، ويظل تحت إشراف القضاء إلى غاية الانتهاء من مهمته، أين يقوم بإعداد تقرير يضمنّه خلاصة عمله، ويودعه لدى أمانة ضبط قاضي التحقيق الذي انتدبه،[2] غير أن ذلك لا يعني أن ترد الخبرة على مشكلة قانونية، فالقاضي يعلم القانون وليس بحاجة إلى معونة الخبير في هذه المسألة.

كما تتميز مهمة الخبير بأنها محددة، فهو مقيد بمهام مبينة في أمر ندبه، يتعين عليه إنجازها، وفي بعض الحالات توضع له أسئلة واضحة ليجيب عنها، لذلك لا يمكن أن تكون مهمة الخبير عامة تمتد لإبداء رأيه في الدعوى، فهو مساعد للقاضي يقدم له معونته في بعض المسائل الفنية فقط.

ثالثا: إجراءات سير الخبرة القضائية: تتم الخبرة القضائية وفقا للقواعد الإجرائية المحددة في قانون الإجراءات الجزائية، سواء ما تعلق بندب الخبير وتحديد مهامه، أو بأداء اليمين القانونية، أو بمراقبة الخبرة ومدة إنجازها وإيداعها.

وقد أجاز القانون لقاضي التحقيق ندب خبير أو أكثر،[3] من أجل استجلاء غموض وقائع تحتاج إلى تفسير فني،[4] كما تتمتع غرفة الاتهام باعتبارها درجة ثانية للتحقيق بهذه المكنة، فهي تملك سلطات التحقيق، فضلا عن صلاحياتها في مراجعة التحقيق الذي تم على مستوى الدرجة الأولى،[5] ويجوز كذلك لقاضي الحكم اللجوء إلى هذا الإجراء في إطار التحقيق التكميلي.[6]

[1]– بهاء المري، المرجع السابق، ص: 724.

[2]– المرجع نفسه، ص: 724.

[3]– راجع المادة 147 ق إ ج.

[4]– راجع المواد: 143، 147 ق إ ج

[5]– راجع المادة 186 ق إ ج.

[6]– راجع المادة 356 ق إ ج.

يؤدي الخبير بمجرد قيده بجدول الخبراء اليمين القانونية أمام نفس المجلس المعين به بالصيغة المنصوص عليها في المادة 145 ق إ ج،[1] ولا يجدد القسم في كل مرة يتم تعيينه فيها.

يتم اختيار الخبير من جدول الخبراء بعد استطلاع رأي النيابة العامة،[2] ويجوز لقاضي التحقيق بصفة استثنائية وبأمر مسبب تعيين خبير غير مقيد بجدول الخبراء، غير أنه يتعين على هذا الأخير تأدية اليمين القانونية أمام قاضي التحقيق قبل مباشرة مهامه.[3]

يقوم الخبير بأداء مهمته تحت مراقبة قاضي التحقيق،[4] وإذا استعصت عليه مسألة خارجة عن اختصاصه فيمكنه أن يطلب من قاضي التحقيق ضم فنيين آخرين إليه، وفي هذه الحالة يؤدي الفنيون المنتدبون اليمين القانونية بنفس الصيغة التي يؤديها الخبير.[5]

وكثيرا ما يعاني قضاة التحقيق من طول مدة إنجاز الخبرة، مما يؤثر على السير الحسن للتحقيق، وهو ما دفع بالمشرع إلى التدخل، وإلزام قاضي التحقيق بتحديد مدة لإنجازها، ويبقى للخبير المطالبة بتمديدها إذا اقتضت ظروف عمله ذلك، على أن يكون هذا التمديد بقرار مسبب.[6]

وإذا تعدد الخبراء ولم يجمعوا في تقريرهم على رأي واحد، أو كانت لبعضهم تحفظات حول النتائج المشتركة، فإنه يتعين على كل واحد منهم توضيح رأيه أو تحفظاته، مع تعليل وجهة نظره.[7]

وبعد أن يكمل الخبير مهمَته ينجز تقريرا مفصلا لما قام به من أعمال، وما توصل إليه من نتائج تتضمن إجابات عن المهام الموكلة له، ثم يوقع عليه،[8] ويودعه أمانة ضبط الجهة التي أمرت بالخبرة، ويثبت هذا الإيداع بموجب محضر.[9]

---

[1]– تنص المادة 145 ق إ ج: " يحلف الخبير المقيد لأول مرة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتي بيانها: أقسم بالله العظيم بأن أقوم بأداء مهمتي كخبير على خير وجه وبكل إخلاص، وأن أبدي رأيي بكل نزاهة واستقلال".

[2]– راجع المادة 144 ق إ ج.

[3]– راجع المادة 145 ق إ ج.

[4]– راجع المادة 143 ف 04 ق إ ج

[5]– راجع المادة 149 ق إ ج.

[6]– راجع المادة 148 ق إ ج.

[7]– راجع المادة 153 ف 02 ق إ ج.

[8]– راجع المادة 153 ف 01 ق ا ج.

[9]– راجع المادة 153 ف 03 ق إ ج.

ويتعين على القاضي الذي أمر بالخبرة أن يستدعي أطراف الدعوى منذ إيداع تقرير الخبرة بأمانته، لتبليغهم بنتائجها، وتلقي أقوالهم بشأنها، ثم يحدد لهم أجلا لإبداء ملاحظاتهم أو تقديم طلباتهم حولها لاسيما ما تعلق بإجراء خبرة تكميلية أو مضادة.[1]

الفرع الثاني: خصوصية الخبرة في الجريمة الإلكترونية

تعد الخبرة الفنية من أقوى مظاهر التعامل القضائي مع ظاهرة تكنولوجيا المعلومات والاتصال، لما تؤديه من دور متميز يغطي نقص المعرفة القضائية بشبكة الإنترنت، وهو ما نلمسه جليا في الصعوبة التي تعترض جهات التحقيق عند جمع الأدلة الرقمية، بل إن المحقق في بعض الأحيان يدمر الدليل الفني نتيجة خطأ منه أو جهل في التعامل معه.[2]

أولا: أهمية الخبرة في الجريمة الإلكترونية: إذا كان للخبرة أهمية في الجرائم التقليدية، فإن أهميتها تزداد في الجريمة الإلكترونية، بل وتصبح حتمية عندما يتعلق الأمر ببعض الجرائم المعقدة، فإجرام الذكاء والفن لا يكشفه إلا ذكاء وفن مماثلين.

ويلعب الخبير دورا مهما في جمع الأدلة الإلكترونية، خصوصا وأن هذه الأخيرة لا تظهر بسهولة على الحاسب الشخصي للمتهم أو هاتفه المحمول، أو عبر حسابه الخاص، أو عبر حساب المجني عليه، أو بريده الإلكتروني، فالدخول إلى هذه المواقع يتطلب معرفة بالحواسيب الآلية وتقنية المعلوماتية، وكذلك الأمر عند فحص الأقراص الصلبة على الأجهزة الإلكترونية الحديثة لإظهار ما خفي أو حذف منها.[3]

وتتجلى أهمية الخبرة في الجريمة الإلكترونية فيما يلي:[4]

01- تساهم في الكشف عن الدليل الرقمي.

02- تساهم في تحديد الخصائص الفريدة للدليل الرقمي.

03- تساهم في إصلاح الدليل الرقمي، وإعادة تجميعه من المكونات المادية للكمبيوتر.

---

[1]- راجع المادة 154 ق إ ج.

[2]- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، درا الجامعة الجديدة، الإسكندرية، 2015، ص: 139.

[3]- بهاء المري، المرجع السابق، ص: 824.

[4]- خالد ممدوح إبراهيم، المرجع السابق، ص: 302-303.

04- تساهم في إعداد نسخة أصلية من الدليل الرقمي، للتأكد من عدم وجود معلومات مفقودة أثناء عملية استخلاصه.

05- يستخدم الخبير الخوارزميات للتأكد من عدم العبث بالدليل.

06- تساهم في تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية، مثل المستند الرقمي والبرامج والتطبيقات والاتصالات والصور والأصوات وغيرها.

07- يقوم الخبير بإجراء الاختبارات التكنولوجية والعلمية على الدليل الرقمي لاختباره والتحقق من أصالته ومصدره كدليل يمكن تقديمه للجهات القضائية.

08- يقوم الخبير بتحليل الدليل الرقمي للتأكد بأنه أصيل وموثوق ويمكن إدراجه ضمن سلسلة الأدلة المقدمة في الدعوى.

ثانيا: مجالات الخبرة في الجريمة الإلكترونية: تتعدد العمليات الإلكترونية، فنجد استخداماتها في الأعمال المصرفية، وفي الإدارة الإلكترونية، وفي التجارة الإلكترونية، وداخل مؤسسات الدولة والشركات الخاصة، لذلك يمكن تصور تنوع الجرائم التي تقع على هذه العمليات وفقا لتنوع الوسائل المستخدمة في ارتكابها.

ولا يمكن من الناحية العملية حصر مجالات الخبرة، فهي مطلوبة في جميع المسائل التي تحتاج لاستخراج الدليل الإلكتروني بطريقة علمية صحيحة وسليمة، وعادة ما يتم اللجوء إليها في الجرائم المعقدة، مثل جرائم تبييض الأموال عن طريق تعدد المبادلات الإلكترونية، جرائم دعارة الأطفال، جرائم التسلل داخل نظام محمي لبنك وتحويل الأموال إلى حسابات أخرى، جرائم التزوير الإلكتروني، جرائم التخريب باستعمال الفيروسات، وغيرها.[1]

ثالثا: تقنيات إنجاز الخبرة الإلكترونية: إن عالم تكنولوجيات الإعلام والاتصال متعدد الشعب والتخصصات من حيث البرامج والوسائل، وهو ما يستوجب مراعاته من طرف جهات التحقيق عند اختيار الخبير، فيتعين أن تتوافر لديه الإمكانات والقدرات العلمية والفنية في المجال الذي يتطلبه بحثه، ولا يكفي في ذلك حصوله على درجة علمية معينة، بل يجب أن تتوافر لديه أيضا الخبرة العملية التي تمكنه من اكتساب كفاءة فنية عالية.

[1]- يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، دار الخلدونية، الجزائر، 2021، ص: 328.

وبالنظر إلى الطبيعة العلمية والفنية للخبرة المطلوبة في هذه الجرائم، فإنه يتعين أن يحيط الخبير بالمعارف والمهارات التالية:[1]

أ- الإلمام بتركيب جهاز الحاسوب وصناعته ونظم تشغيله، وملحقاته، وكلمات المرور أو السر ورموز التشفير.

ب- معرفة طبيعة البيئة التي يعمل فيها الحاسوب، من حيث إدراك كيفية عمل أنظمة المعالجة الآلية للمعطيات، وتحديد أماكن التخزين، والوسائل المستخدمة في ذلك.

ت- قدرته على إتقان مهمته دون تدمير الأدلة المتحصَلة من الأنظمة المعلوماتية.

ث- التمكن من نقل أدلة الإثبات غير المرئية وتحويلها إلى أدلة مقروءة، أو المحافظة على دعاماتها إلى غاية القيام بمهمته دون أن يلحقها تدمير أو إتلاف، مع إثبات أن المخرجات الورقية لهذه الأدلة تتطابق مع ما هو مسجل على دعائمها الممغنطة.

رابعا: جهود المشرع الجزائري لتسهيل إجراء الخبرة في الجريمة الإلكترونية: أدرك المشرع خصوصية الجريمة الإلكترونية وصعوبة التحقيق فيها، فوضع نصوصا قانونية تسهل إجراء الخبرة وسط مسرح افتراضي، ويظهر ذلك من خلال:

01- المرونة في تعيين الخبراء: كما رأينا سلفا، فإن المشرع ترك المجال مفتوحا أمام جهة التحقيق للاستعانة بخبير استشاري حتى ولو كان خارج جدول الخبراء، وذلك بعد إدراكه لأهمية التطور التكنولوجي السريع، ناهيك عن إمكانية عدم توفر خبراء أكفاء مقيدين في جدول الخبراء أحيانا،[2] ويستوي أن يكون الخبير شخصا طبيعيا أو معنويا، ذلك أن العبرة في الاختيار تكون بتوافر المعرفة العلمية والخبرة اللازمتين في تخصص تكنولوجيات الإعلام والاتصال التي تتطور بصورة مذهلة.

[1]- علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، عدد: 01، الإمارات العربية المتحدة، 2003، ص: 35.

[2]- راجع المادة 144 ق إ ج.

كما أجاز المشرع لجهات التحقيق أثناء تفتيش منظومة معلوماتية أن تستعين بأي شخص له دراية بعمل هذه المنظومة،[1] دون تحديد لطبيعة هذا الشخص، فقد يكون شخصا طبيعيا أو معنويا، خبيرا معتمدا أو شخص محترف يتمتع بمهارات وقدرات عالية في مجال المعلوماتية.

02- إنشاء هيئات متخصصة في مجال الخبرة الإلكترونية: أنشأت الدولة الجزائرية هيئات مجهزة بهياكل مادية متطورة، ومعززة بإطارات بشرية مؤهلة، تهتم بإنجاز الخبرة المتعلقة الجرائم الإلكترونية بصورة علمية وسليمة، ومن بينها:

أ- **المعهد الوطني للبحث في علم التحقيق الجنائي:** ويحتوي على 05 مخابر جهوية، كل مخبر منها يحتوي على مصلحة تقنية تضم بدورها 06 مخابر، من بينها مخبر الأدلة المعلوماتية وجرائم الكمبيوتر، إضافة إلى مخبر استغلال الهواتف المحمولة.[2]

ب- مركز مكافحة الجريمة المعلوماتية للدرك الوطني: ويعمل على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة وتحديد هوية أصحابها، وتأمين الأنظمة المعلوماتية.

ت- المعهد الوطني للأدلة الجنائية وعلم الإجرام: يقدم المعهد خدمة أساسية في مجال خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية، وتعد مهمة إنجاز الخبرات العلمية بطلب من القضاء من أجل كشف حقيقة الجرائم الإلكترونية بالأدلة العلمية أحد مهامه الأساسية.

ث- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها: والتي أسندت لها مهمة تقديم المساعدة القضائية لجهاز التحقيق الجنائي عن طريق إنجاز الخبرات المتعلقة بالجريمة الإلكترونية.[3]

ورغم كل ما بذله المشرع الجزائري من جهود لتسهيل إجراء الخبرة في الجريمة الإلكترونية إلا أن ذلك وحده لا يكفي أمام التطور التكنولوجي الدائم، وما يصاحبه من تطور في أساليب الإجرام، لذا لابد من الاهتمام بالتكوين المستمر والتدريب العملي للمكلفين بمهمة التحقيق في هذا

[1]- راجع المادة 05 من القانون رقم 09-04.

[2]- قرار وزاري مشترك مؤرخ في 14-04-2007، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية لسنة 2007، العدد 36.

[3]- راجع المادة 05 من المرسوم 21-439.

النوع الحساس من الجرائم، قصد تجديد المعارف وتحسين المستوى، واكتساب المهارات التقنية اللازمة، والاستفادة من خبرات الدول الرائدة في هذا المجال.

خامسا: تقدير الخبرة الإلكترونية: يترتب على قاعدة الاقتناع الحر للقاضي أن رأي الخبير غير ملزم له، إذ يظل محتفظا بسلطته في تقدير الخبرة،[1] فرأي الخبير ليس في حقيقته سوى رأي استشاري،[2] للقاضي أن يأخذ به أو يستبعده، أو يأمر بإجراء خبرة تكميلية، أو خبرة مضادة، غير أنه يتعين عليه تسبيب استبعاد نتائج الخبرة.[3]

ومهما بلغت كفاءة الخبير، فإن الكلمة الأخيرة ترجع إلى القاضي الذي ينظر إلى تقرير الخبرة كوسيلة إثبات مثلها مثل الأدلة الأخرى، وهذا ما أكدته المحكمة العليا،[4] غير أنه وفي المسائل ذات الصبغة الفنية البحتة لا يمكن للقاضي أن يحل محل الخبير ويجزم برأيه الفني، بل عليه الرجوع إلى تعيين خبير آخر مختص في هذه المسألة.[5]

والأمثلة على أخذ القضاء الجزائري بالدليل الإلكتروني المستمد من الخبرة كثيرة، نذكر منها أنه بتاريخ: 11-09-2014 تقدمت مسيرة نشاط تجاري بشكوى ضد أحد العمال بمحلها التجاري الكائن بالمركز التجاري بباب الزوار، وصرحت بأن محلها الخاص بالمأكولات يحتوي على حاسوب يشرف عليه المشتكى منه، العامل لديها منذ 03 سنوات، وقد لاحظت بأن مقابل المبيعات اليومية تراجع خلال فترة عمله، مما جعلها تراجع حساباتها المالية، فتبين لها بأن المبلغ الإجمالي للمبيعات المدون على الفاتورة اليومية الإجمالية أقل من المبلغ الحقيقي للمبيعات، وعند رجوعها إلى الفاتورة اليومية لاحظت أنه يتم تغيير المبلغ الإجمالي بتخفيضه عن المبلغ الحقيقي وأخذ الفارق، وقدرت المبلغ المختلس من شهر جانفي 2012 إلى غاية 12-09-2014 بـ

---

[1]- عبد الله سليمان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، بن عكنون الجزائر، 1999، ص: 477.

[2]- تنص المادة 144 من قانون الإجراءات المدنية والإدارية: " يمكن للقاضي أن يؤسس حكمه على نتائج الخبرة، القاضي غير ملزم برأي الخبير، غير أنه ينبغي عليه تسبيب استبعاد نتائج الخبرة".

[3]- قرار صادر عن الغرفة المدنية، المحكمة العليا، ملف رقم: 806311، بتاريخ: 21-06-2012، مجلة المحكمة العليا، العدد 01، الجزائر، 2013، ص: 143.

[4]- عبد الله سليمان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، مرجع سابق، ص: 477.

[5]- عمر زودة، الإثبات في المواد الجزائية، ط2، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021، ص: 154.

(3515.434.00 دج)، وكون العملية تمت بواسطة جهاز الإعلام الآلي فقد وضعت الشاكية تحت تصرف مصالح الشرطة حاسوبين، كما قدمت فواتير الحساب والوصولات المستخرجة من طرف المشتكى منه وبقية العمال.

وتوصلت الخبرة المنجزة من طرف مخبر الشرطة العلمية إلى أن الفاعل قام بتحويل فاتورة من برامج الكمبيوتر إلى القرص الصلب، وعند فتحها يستطيع تغيير المعطيات، وبعد تتبع عمليات الكمبيوتر تبين بأن الفارق في المبلغ الإجمالي يخص الوصولات المستخرجة من قبل المتهم.

وبتاريخ 09-03-2015 أصدرت محكمة الحراش حكما قضى بإدانة المتهم بجنحة اختلاس أموال خاصة، ومعاقبته بعام حبس نافذ و 100.000 دج غرامة نافذة، مع إلزامه بتعويض الطرف المدني، وهو الحكم الذي أيدته الغرفة الجزائية لمجلس قضاء الجزائر.[1]

[1]- يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، مرجع سابق، ص: 340.

المبحث الثاني

التفتيش والحجز في الجريمة الإلكترونية

حتى نصل لإثبات الجريمة الإلكترونية لابد من اتخاذ سلسلة من الإجراءات التي من شأنها الكشف عن الجريمة ومرتكبيها، ومن بينها التفتيش والحجز وسط بيئة افتراضية، وهو ما يصعب المأمورية، باعتبار أن فضاء الإنترنت نظام مفتوح يستطيع أن يلجه أي شخص.

ويعتبر التفتيش في ظل التشريع الإجرائي وسيلة إثبات لا غاية في حد ذاته، فهو إجراء يستهدف ضبط أدلة الجريمة، وتكمن غايته في حجز الأدلة الرقمية التي تفيد في الوصول إلى الحقيقة.

ويختلف إجرائي التفتيش والحجز في الجريمة التقليدية عنهما في الجريمة الإلكترونية من حيث المحل، فهما يردان على أشياء ذات طبيعة معنوية في هذه الأخيرة.

ولمعالجة الموضوع ارتأينا تقسيم هذا المبحث إلى مطلبين:

المطلب الأول: التفتيش الإلكتروني.

المطلب الثاني: الحجز الإلكتروني.

المطلب الأول

التفتيش الإلكتروني

يعد التفتيش الالكتروني أحد أخطر الإجراءات في مسار التحقيق الجنائي في الجريمة الإلكترونية، وذلك لمساسه بحرمة الحياة الخاصة للأفراد، لذلك أحاطه المشرع بجملة من الضوابط حتى تكون ضمانا لهذه الحريات.

ورغم سعي التشريعات الحديثة لوضع انسجام بين القواعد الكلاسيكية في الإجراءات والتكنولوجيات الحديثة، إلا أن إبقاء المشرع لمصطلح "التفتيش" دليل على تمسكه باستخدام الأساليب القسرية، وإشارة منه إلى أن الغاية المنشودة من هذا الإجراء مماثلة لتلك المرجوة من التفتيش الكلاسيكي، وهو ما سنحاول إبرازه في هذا المطلب.

الفرع الأول: مفهوم التفتيش الإلكتروني

يعد التفتيش في الجريمة الإلكترونية من أصعب إجراءات التحقيق، وذلك لما تتميز به هذه الجرائم من خصوصيات انعكست بدورها على هذا الإجراء.

أولا: تعريف التفتيش: قبل التطرق لتعريف التفتيش الإلكتروني لابد من التعرف على المعنى العام للتفتيش.

01- التفتيش بوجه عام: لم تتطرق مختلف التشريعات لتعريف التفتيش تاركة هذه المهمة للفقه والقضاء، وبالرجوع إلى الفقه القانوني فإنه يقصد بالتفتيش عموما: "البحث عن أشياء تفيد في الكشف عن جريمة وقعت ونسبتها إلى المتهم"،[1] فيما عرفه الترزي بأنه: "إجراء قانوني من إجراءات التحقيق، تقوم به سلطة التحقيق أو من تندبه لذلك، للبحث عن أدلة وقوع الجريمة ونسبتها إلى المتهم"،[2] وعرفه البعض الآخر بشيء من التوسع بأنه: "بحث بوليسي أو قضائي عن عناصر الدليل لجريمة ما، ينفذ وفقا لقواعد قانونية خاصة في مسكن أي شخص، أو أي مكان آخر يمكن أن توجد فيه أشياء يكون اكتشافها مفيدا في إظهار الحقيقة".[3]

أما التشريع الجزائري، فقد كرس التفتيش كإجراء من إجراءات التحقيق دون تعريفه، إذ تنص المادة 79 ق إ ج على أنه: "يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء المعاينات اللازمة أو للقيام بتفتيشها..."، وتنص المادة 81 من ذات القانون على أنه: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة".

وقد ساهم القضاء بدوره في تحديد مدلول التفتيش، فعرَفته محكمة النقض المصرية بقولها: "هو إجراء رخص بموجبه المشرع بالتعرض لحرمة الشخص بسبب جريمة وقعت أو ترجح وقوعها، تغليبا للمصلحة العامة على مصالح الأفراد الخاصة، واحتمال الوصول إلى دليل يكشف الحقيقة".[4]

---

[1]- نزيم محمد الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلس أندلس للعلوم الاجتماعية والإنسانية، مجلد 15، العدد 19، أفريل 2017 ، ص: 321.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 316.

[3]- Serge Guinchard, Thierry Debard, L'exique des termes juridiques, terme "perquisition", 2017-2018, 25e ed, Dalloz, France, 2018,

[4]- محمود محمد محمود جابر، الأحكام الإجرائية للعلوم الناشئة عن استخدام الهواتف النقالة، المكتب الجامعي الحديث، مصر ، 2018، ص: 163.

وعموما فإن التفتيش لا يخرج في مفهومه العام عن كونه معاينة مادية، غير أنه ينصب على شيء له حرمة خاصة مثل المسكن والمعلومات.

02- التفتيش الإلكتروني: لا يختلف التفتيش الإلكتروني في مدلوله القانوني عن التفتيش في مدلوله العام، غير أنه يهدف إلى الوصول على أدلة معنوية ليس لها أي مظهر مادي محسوس لذلك يتطلب الأمر خبرة ومهارات خاصة، فهو يستند على الركيزتين القانونية والتقنية معا.

عرف بعض الفقه التفتيش الإلكتروني بأنه: "الاطلاع على محل منحه القانون حماية خاصة باعتباره مستودع سر صاحبه، ويستوي في ذلك أن يكون هذا المحل جهاز حاسب آلي أو أنظمة أو شبكة انترنت"،[1] فيما عرفه البعض الآخر بأنه: "إجراء قانوني من إجراءات التحقيق، تقوم به سلطة التحقيق أو من تندبه لذلك من أصحاب المعارف والخبرات العلمية والعملية في مجال نظم تكنولوجيا المعلومات والاتصالات، للبحث عن أدلة جريمة إلكترونية وقعت، ونسبتها إلى المتهم"،[2] فيما عرفه المجلس الأوروبي بأنه: "إجراء يسمح بجمع الأدلة المخزنة أو المسجلة بشكل إلكتروني".[3]

وقد كرس المشرع الجزائري التفتيش الإلكتروني للتحقيق الجنائي في الجريمة الإلكترونية بموجب القانون رقم 09-04،[4] ثم أتبعه ببعض النصوص القانونية الخاصة على غرار القانون المتعلق بمكافحة التزوير واستعمال المزور.[5]

ويجب التنويه إلى أن بعض الفقه يرى أن المصطلح الأدق لعملية البحث عن الأدلة وسط البيئة الرقمية هو "الولوج" أو "النفاذ"، أما مصطلح التفتيش فهو مصطلح تقليدي أكثر يعني التفحص والتدقيق.[6]

---

[1]- نزيم محمد الترزي، المرجع السابق، ص: 320-321.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 316.

[3]- يزيد بوحليط، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 48، ديسمبر 2016، ص: 84.

[4]- راجع المادة: 05 من القانون: 09-04.

[5]- راجع المادة 16 من القانون رقم 24-02 المؤرخ في 26-02-2024، المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية لسنة 2024، العدد 15.

[6]- نبيلة هبة هروال، المرجع السابق، ص: 224.

ثانيا: خصائص التفتيش الإلكتروني وغايته: يهدف التفتيش الإلكتروني إلى البحث عن أشياء متصلة بجريمة وقعت، تفيد في كشف الحقيقة، ويتميز عن غيره من إجراءات التحقيق كونه ينصب على مواطن السرَ التي تكفلها مختلف المواثيق الدولية والدساتير.

01- خصائص التفتيش الإلكتروني: يتميز التفتيش الإلكتروني عن غيره من إجراءات التحقيق بعدة خصائص أهمها:

أ- المساس بحق الخصوصية:[1] يقال في الفقه أن تفتيش الشخص يعد قيدا على حصانته أو حرمته الذاتية، وتفتيش المسكن يعد قيدا أو استثناء يرد على حرمة المسكن، بمعنى أن التفتيش هو مساس بقاعدة الحرمة المكفولة للشخص ذاته أو مسكنه أو رسائله.[2]

تعد أجهزة الحاسوب في نظر أغلب الناس المساحات الأكثر خصوصية، فغالبا ما يكون الحاسوب الشخصي مستودع المعلومات الخاصة التي لا يريد مالك الجهاز أن يطلع عليها غيره، لذلك ينطوي التفتيش على تعرض قانوني لحرمة حياته الخاصة، وأسراره الموجودة على جهاز الكمبيوتر ذاته، أو على برامج خاصة منه، أو على مستوى بريده الإلكتروني.

ب- الجبر والإكراه: يقتضي تفتيش مستودع أسرار المتهم الحد من حريته الشخصية بالقدر اللازم لتنفيذه، أي أن القهر لا غنى عنه لتنفيذ هذا الإجراء،[3] فهو تعرض قانوني لحرية المتهم بغير إرادته، فالقانون يوازن بين حق المجتمع في العقاب دفاعا عن مصالحه التي تنتهك بارتكاب الجرائم، وبين مدى تمتع الفرد بحريته أمام هذا الحق، فيبيح إجراء التفتيش جبرا على صاحب الشأن متى توافرت وروعيت ضمانات معينة.[4]

---

[1]- يعرف الفقيه Martin الحق في الحياة الخاصة أو الحق في الخصوصية بأنه: "الحق في الحياة الأسرية والشخصية والداخلية والروحية للشخص عندما يعيش وراء بابه المغلق"، ويعرفها الفقيه Neoism بأنه: "حق الشخص في الاحتفاظ بأسرار يتعذر على العامة معرفتها إلا بإرادته، وتتعلق بصورة أساسية بحقوقه الشخصية"، أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، ط3، 1994 دار النهضة العربية، القاهرة، 1994، ص: 12.

[2]- سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، ط1، دار النهضة العربية، مصر، 1972، ص: 40-41.

[3]- قرار محكمة النقض المصرية، الطعن رقم 757 بتاريخ 19-06-1967، أنظر: إيهاب عبد المطلب، تفتيش الأشخاص والأماكن، ط1، المركز القومي للإصدارات القانونية، مصر، 2009، ص: 14.

[4]- سامي حسني الحسيني، المرجع السابق، ص: 38-39.

ت- يمتاز التفتيش الإلكتروني بأنه وسيلة بحث عن الأدلة المادية والمعنوية للجريمة وضبطها بما يفيد في الكشف عن الحقيقة.

02- غاية التفتيش الإلكتروني: يهدف التفتيش الإلكتروني إلى البحث عن الأدلة المتعلقة بالجريمة الإلكترونية، وضبط مرتكبيها لتقديمهم أمام القضاء، لذلك يعد أحد إجراءات تقوية الدليل وإثبات إسناد الوقائع للمتهم أو نفيها عنه، فالعثور على أدلة الجريمة يعزَز الاتهام ويمنع إفلات المجرم من العقاب.[1]

ويستطيع المحقق الجنائي كشف ملابسات الجريمة على ضوء عملية التفتيش الإلكتروني من خلال:[2]

أ- تحديد زمان ومكان ارتكاب الجريمة، فقد تأخذ الجريمة الإلكترونية وقتا كبيرا لحين اكتشافها خاصة وأنها من الجرائم العابرة للحدود.

ب- تحديد شخصية الفاعل الأصلي للجريمة وشركائه، ودور كل واحد منهم وعلاقته بالضحية وروابط الاتصال بينهم.

ت- الحصول على الآثار والأدلة الجنائية الدالة على المجرم.

ث- التعرف على الأساليب الإجرامية التي يتبعها الجناة في ارتكاب جرائمهم الإلكترونية.

ج- التعرف على الثغرات الإلكترونية والأمنية التي استعملها الجاني ومكنته من ارتكاب جريمته ودور الضحايا في تسهيل ارتكابها.

الفرع الثاني: ضوابط التفتيش الإلكتروني

يرى بعض رجال القانون أن القواعد التقليدية للتفتيش تطبق على كافة الجرائم، سواء التي يكون محلها برامج الحاسوب كالسرقة أو الإتلاف، أو في حال استعمال هذه البرامج كأداة في ارتكاب الجريمة كالتزوير أو التلاعب في البيانات، أو الإتلاف الفني للأنظمة المعلوماتية، وأن

[1]- عادل عزام سقف الحيط، المرجع السابق، ص: 230.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 317.

هذه القواعد كافية لمواجهة الجرائم مهما كانت الوسيلة المستخدمة في ارتكابها، سواء تعلق الأمر بالجرائم العادية أم غلب عليها الطابع الفني.[1]

ويرى البعض الآخر عكس ذلك، إذ يعتبرون أن التفتيش وضبط الأدلة المادية لا ينطبق على بيانات الحاسوب غير المحسوسة، وأن هناك قصورا في التشريع، يستلزم إضافة نصوص تتعلق بالمواد المعالجة عن طريق الحاسوب وبياناته، حتى يمكن شملها بقواعد التفتيش،[2] فالتفتيش عن أدلة الجريمة الإلكترونية أمر مختلف، لأن الجاني يمكنه التخلص من البيانات عن طريق إرسالها عبر نظام معلوماتي من مكان إلى آخر، ومن أجل الوصول إلى هذه البيانات لابد من الكشف عن الرقم السري للمرور إلى ملف البيانات، وهذا الرقم لا يعرفه إلا المتهم، لذلك فإن النصوص التقليدية ليست كافية لإجراء التفتيش عن الأدلة الرقمية، ويدعون إلى تعديل القانون حتى تسهل عملية التفتيش أمام السلطات المختصة، ومنحهم صلاحيات أكبر لإنجاز مهامهم.[3]

ونظرا لخطورة التفتيش الإلكتروني ومساسه بحرمة الحياة الخاصة للأفراد،[4] فقد حرصت جل التشريعات الإجرائية على ضرورة إحاطته بمجموعة من الضوابط التي تضمن التوازن بين الحرية الفردية، وتحقيق الفاعلية المطلوبة من جهاز التحقيق الجنائي لكشف غموض الجريمة وضبط مرتكبيها، بما في ذلك الدستور الجزائري.[5]

أولا: الضوابط الموضوعية للتفتيش الإلكتروني: ويمكن حصرها في ثلاث قواعد أساسية:

01-سبب التفتيش: كون التفتيش إجراء من إجراءات التحقيق فلا يمكن مباشرته إلا بعد ارتكاب جريمة بوصفها جناية أو جنحة، وإسنادها إلى شخص معين بصفته فاعلا أصليا أو شريكا، مع

---

[1]- كامل عفيفي عفيفي، المرجع السابق، ص: 344.

[2]- عبد الله حسين محمود، إجراءات جمع الأدلة في مجال الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 2003، ص: 604.

[3]- وليد عاكوم، التحقيق في جرائم الحاسوب، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 2003، ص: 529.

[4]- تنص المادة 47 من الدستور الجزائري "لكل شخص الحق في حماية حرمة حياته الخاصة".

[5]- تنص المادة 48 من الدستور الجزائري "تضمن الدولة حرمة المنزل، لا تفتيش إلا بمقتضى القانون وفي إطار احترامه".

ضرورة توافر أدلة وقرائن كافية لانتهاك حرمة حياته الشخصية،[1] وذلك عملا بمبدأ المشروعية الذي يقتضي أن لا جريمة ولا عقوبة إلا بنص،[2] فقبل وقوع الجريمة وتوجيه الاتهام إلى شخص معين يكون التفتيش باطلا لانتفاء السبب الذي يبرره.

لذلك، وحتى يكون التفتيش الالكتروني مشروعا لابد من توافر العناصر التالية:

أ- ارتكاب جريمة إلكترونية: يشترط لإجراء التفتيش الالكتروني كقاعدة عامة أن تكون هناك جريمة الكترونية ارتكبت بشكل فعلي، سواء كانت جناية أو جنحة، ومن ثم تستبعد المخالفات من نطاق هذا الإجراء لضآلتها، فهي لا تصل إلى حد انتهاك حرمة الحياة الخاصة للأشخاص، كما لا يجوز التفتيش من أجل جريمة محتملة الوقوع، حتى ولو كانت هناك مؤشرات جدية على احتمال وقوعها.[3]

غير أنه واستثناء من ذلك أجاز المشرع الجزائري للنائب العام لدى مجلس قضاء الجزائر أن يأذن لضباط الشرطة القضائية المنتمين للهيئة اللجوء إلى التفتيش الالكتروني كإجراء وقائي لتفادي جرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، أو في حال توافر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية بشكل يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، وذلك حفاظا على المصلحة العليا للبلاد.[4]

ب- إسناد الجريمة الإلكترونية إلى شخص معين: لا يمكن مباشرة التفتيش بمجرد وقوع جريمة إلكترونية، بل لابد من نسبتها إلى شخص معلوم، سواء كان فاعلا أصليا أم شريكا، ويتحقق ذلك بتوافر دلائل كافية تدعو إلى الاعتقاد بأنه ارتكب الجريمة أو ساعد على ارتكابها، ويقصد بالدلائل الكافية مجموعة المظاهر أو الأمارات القائمة على العقل والمنطق والخبرة الفنية للمحقق، التي ترجح إسناد الجريمة إلى شخص معين باعتباره فاعلا أصليا أو شريكا.[5]

---

[1]- الشهاوي قدري عبد الفتاح، ضوابط التفتيش في التشريع المصري والمقارن، منشاة المعارف، الإسكندرية، 2005، ص: 53.

[2]- راجع المادة 01 ق ع.

[3]- رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد محمد لخضر، الوادي، العدد 5، جوان 2012، ص: 161-162.

[4]- راجع المواد 04 و 05 من القانون رقم 09-04.

[5]- جمال براهيمي، المرجع السابق، ص: 39.

ت- توافر أدلة أو قرائن على وجود أجهزة أو معدات معلوماتية تفيد في كشف الحقيقة: لا يكفي لقيام سبب التفتيش ارتكاب جريمة إلكترونية معاقبا عليها قانونا وإسنادها إلى شخص معين، بل يجب كذلك أن تتوافر أدلة أو قرائن كافية على وجود أجهزة إلكترونية استخدمت في الجريمة، أو أشياء متحصلة منها، أو مستندات رقمية لها فائدة في استجلاء الحقيقة.[1]

02- الجهة المكلفة بالتفتيش الإلكتروني: لا يعتبر التفتيش صحيحا ومنتجا لآثاره إلاَ إذا قام به من هو مخول قانونا بذلك، وقد اختلفت التشريعات الإجرائية في هذا الشأن، فمنهم من أسنده إلى النيابة العامة وضباط الشرطة القضائية، ومنهم من أسنده إلى قاضي التحقيق، وذلك حسب النظام القضائي المتبع في كل دولة.

وبالنسبة للتشريع الجزائري فإن التفتيش عموما يعد عملا من أعمال التحقيق يجريه قاضي التحقيق بنفسه،[2] أو بندب أحد ضباط الشرطة القضائية خلال مرحلة التحقيق الابتدائي،[3] كما يجريه ضباط الشرطة القضائية خلال مرحلة التحريات الأولية بعد حصولهم على إذن من السلطة القضائية المختصة، سواء تعلق الأمر بالجرائم العادية،[4] أو الجرائم المتلبس بها،[5] ونفس القول ينطبق على التفتيش الإلكتروني الذي أخضعه المشرع للقواعد العامة،[6] المكرسة بنصوص المواد: 44، 45، 46، 47 ق إ ج.

وبالنظر إلى ما تنفرد به الجرائم الإلكترونية من خصوصيات، فإنه يمكن للمحقق الجنائي الاستعانة بالهيئة للقيام بهذا الإجراء، شريطة أن يقدم لها طلب المساعدة بوصفها هيئة تقنية متخصصة، وأن تتحصل على إذن مكتوب من الجهة القضائية المختصة.[7]

---

[1]- طارق ابراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، مصر 2009، ص: 405.

[2]- راجع المواد: 81 و 82 و 38 ق إ ج.

[3]- راجع المادة 79 من ق إ ج.

[4]- راجع المادة 64 ق إ ج.

[5]- راجع المادة 44 ق إ ج.

[6]- راجع المادة 03 من القانون 09-04.

[7]- تنص المادة: 04 من القانون رقم: 09-04: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية".

كما يمكن للقائم بالتفتيش الإلكتروني أن يستعين بأي شخص له معرفة بعمل النظم المعلوماتية، وبالتدابير اللازمة لحماية المعطيات التي تتضمنها، وذلك بهدف تزويده بالمعلومات الضرورية لإنجاز مهمته،[1] إذ يقوم هذا الشخص بتقديم التوضيحات الكافية حول كيفية تشغيل الأنظمة الآلية، وطريقة النفاذ إليها، أو إلى المعطيات المخزنة أو المعالجة أو المنقولة بشكل يسهل فهمه.

ورغم أن القانون لم يمكن المتهم والمدعي المدني صراحة من الحق في المطالبة بإجراء التفتيش خلال فترة التحقيق الابتدائي، إلا أننا نستشف ذلك من المادة 69 مكرر ق إ ج كون التفتيش لا يخرج في مفهومه العام عن كونه معاينة.

03- محل التفتيش الالكتروني: يقع التفتيش بوجه عام على المحل الذي يحتوي على مستودع الأسرار الخاصة قصد الحصول على أدلة متعلقة بالجريمة وطريقة ارتكابها، وقد يكون المحل إمَا شخصا أو مسكنا أو محلا ألحقه القانون بحكم المسكن.[2]

ويعتبر محل التفتيش الالكتروني بمثابة المستودع الذي يحتفظ فيه الشخص بالأشياء التي تتضمن سرَه،[3] ويتكون هذا المحل من جهاز الحاسوب بمكوناته المادية والمعنوية، وشبكات الاتصال الخاصة به أو المتعلقة بالوسائل الالكترونية، إضافة إلى الأشخاص الذين يستخدمون الحاسب الآلي محل التفتيش، والأماكن التي توجد بها تلك الأشياء.[4]

ولا يكون المحل في الجرائم الإلكترونية قائما بذاته، بل يكون مقترنا إما بمكان معين كمسكن المتهم، أو بشخص معين بصفته مالكا أو حائزا له، كما هو الشأن في الحاسب المحمول أو الهاتف النقال، لذلك فإنه يتعين قبل مباشرة إجراء التفتيش مراعاة طبيعة المكان الذي تتواجد فيه

---

[1]- تنص المادة 05 الفقرة الأخيرة من القانون 09-04: "يمكن السلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

[2]- خالد ممدوح ابراهيم، المرجع السابق، ص: 180.

[3]- ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر، الوادي، العدد 16، جوان 2017، ص: 429.

[4]- أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، 2013، ص: 99.

الأجهزة الالكترونية المراد تفتيشها، والضمانات القانونية المحاطة به، لأن حكم تفتيش هذه الوسائل يتوقف غالبا على طبيعة المكان الذي تتواجد فيه.[1]

وعموما فإن التفتيش الإلكتروني ينصب على:

أ- **المكونات المادية:** أي تفتيش المكان الذي يوجد فيه الحاسب الآلي، والتفتيش هنا لا يكون داخل النظام المعلوماتي، وإنما يكون في أي جهاز له صلة بالحاسب، مثل المخرجات الورقية التي تم طبعها، أو الطابعة المتصلة به لاسيما إذا كانت ممَا يخزن المعلومات، أو الأقراص المدمجة، أو وسائط التخزين.[2]

إن تفتيش المكونات المادية لا يعني البحث عن البصمات والآثار المادية كما هو الحال في الجرائم التقليدية، وإنما يعني البحث عن الأجهزة والملحقات المرتبطة بالحاسب الآلي نفسه لإثبات قيامه بالجريمة من خلال تلك الأجهزة من عدمه، كالبحث عن جهاز ROUTER كدليل على دخوله للإنترنت، ووجود ماسح ضوئي SCANNER أو جهاز طابعة كقرينة على قيامه باستخدام جهاز الحاسب في تزوير وطباعة العملات النقدية، وما إلى ذلك من أجهزة وملحقات خاصة بالجهاز.[3]

ولا خلاف حول خضوع المكونات المادية للحاسوب للقواعد العامة للتفتيش الذي ينصب على الأشياء المادية الملموسة، مع مراعاة الجانب الفني للتفتيش من أجل ضمان عدم تلف الأجهزة والمعدات.[4]

ب- **المكونات المعنوية:** وينصب تفتيش هذه المكونات على البيانات المخزَنة التي جرى التلاعب بها أو تغييرها، وهنا يثور إشكال حول مدى صلاحية هذه المكونات للتفتيش؟

ثار جدل فقهي كبير حول مدى صلاحية المكونات المعنوية لأن تكون محلا للتفتيش باعتبار أن البيانات الالكترونية أو البرامج في حد ذاتها تفتقر إلى مظهر مادي محسوس في

[1]- جمال براهيمي، المرجع السابق، ص: 35.

[2]- بهاء المري، المرجع السابق، ص: 789.

[3]- حازم محمد خلفي، المرجع السابق، ص: 277.

[4]- رحيمة لدغش، ضوابط تفتيش الحاسب الآلي، مجلة الحقوق والعلوم الإنسانية، المجلد 1، العدد 25، ص: 139.

المحيط الخارجي، مما يجعلها تتعارض مع الهدف الذي يصبو إليه التفتيش، وهو البحث عن الأدلة المادية.

وفي هذا الصدد، ذهب جانب من الفقه إلى القول بصلاحية هذه المكونات للتفتيش كونها تتناسب مع الغاية المنشودة منه، وهي ضبط الأدلة التي تفيد في الكشف عن الحقيقة، فهذا المفهوم يجب أن يمتد ليشمل البيانات المنطقية، أي تمكين المحقق من القيام بأي شيء يكون ضروريا لجمع وحماية الدليل، وذلك تفسيرا لعبارة "شيء"[1] التي تشمل جميع البيانات، بما فيها المخزنة في الذاكرة الداخلية.[2]

في حين يرى جانب آخر أن هذه المكونات لا تصلح أن تكون محلا للتفتيش، فهي تختلف عن الأشياء المادية الملموسة، ومن ثم لا تخضع للنصوص العامة للتفتيش، وإنما تتطلب استحداث قواعد جديدة تتماشى مع طبيعتها الخاصة، أو تعديل النصوص المتعلقة بالتفتيش بشكل يجعل أحكامها متوافقة مع متطلبات هذه التقنية.[3]

أما المشرع الجزائري فلم يكتف بالنصوص التقليدية، بل نص صراحة على جواز تفتيش المكونات المعنوية من خلال المادة 05 من القانون رقم 09-04، وأخضعه من حيث ضوابطه القانونية إلى القواعد العامة للتفتيش، وميَز في ذلك بين تفتيش منظومة معلوماتية متصلة بمنظومة آخر تقع داخل الوطن، وتفتيش منظومة معلوماتية متصلة بمنظومة أخرى تقع خارج الوطن على النحو التالي:

* **اتصال حاسوب المشتبه فيه أو المتهم بحاسوب آخر داخل الوطن:** نصت الفقرة الأولى من المادة 05 من القانون 09-04 على أنه: "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار ق إ ج، وفي الحالات المنصوص عنها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

---

[1]- تنص المادة 81 ق إ ج: "يباشر التفتيش في جميع الأماكن التي يمكن العثور فيها على أشياء يكون كشفها مفيدا لإظهار الحقيقة".

[2]- نورة طرشي، مكافحة الجريمة المعلوماتية، رسالة ماجستير في القانون الجنائي، كلية الحقوق، جامعة الجزائر1، 2011-2012، ص: 55.

[3]- أحمد هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، مرجع السابق، ص: 73.

– منظومة معلوماتية أو جزء منها،[1] وكذا المعطيات المعلوماتية المخزنة فيها.

– منظومة تخزين معلوماتية.

قد تكون الأنظمة المعلوماتية متصلة ببعضها، كأن تكون المعطيات المبحوث عنها غير محفوظة في المنظومة الأولى محل التفتيش، لكنه يمكن الوصول إليها عن طريقها، أو تكون محفوظة في جهاز مرتبط مباشرة بالمنظومة الأولى، أو مرتبطة بطريقة غير مباشرة عن طريق شبكة اتصال كشبكة الإنترنت، ففي هذه الحالة يمكن تمديد التفتيش إلى مكان تواجد المعطيات المبحوث عنها، أو القيام بعملية استرداد واسترجاع هذه المعطيات قصد تحويلها للمنظومة المعلوماتية الأولى، أو اللجوء إلى طرق التفتيش الكلاسيكية بصفة منظمة ومنسقة في كلا المكانين في حدود الإقليم الوطني.[2]

وقد يمتد التفتيش أحيانا من المنظومة الأولى إلى معطيات مخزنة في منظومة معلوماتية أخرى تقع خارج مكان التفتيش مهما كانت طبيعة الشبكة (داخلية أو خارجية أو انترنت)، وهو ما قصده المشرع بعبارة "ولو عن بعد"،[3] وهي موضوع الفقرة الثانية من المادة 05 التي تنص: "ويجوز تمديد التفتيش بسرعة إلى المنظومة المعلوماتية الموجودة إلى جهاز آخر متصل بالجهاز الأول، بعد إعلام السلطة القضائية المختصة مسبقا بذلك 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"، وذلك بشرط أن تتم هذه الإجراءات داخل الإقليم الوطني.

فمن أجل تسريع عملية التفتيش أجاز المشرع تمديد التفتيش إلى منظومة معلوماتية أخرى دون الحاجة لاستصدر إذن ثان، واكتفى بضرورة إعلام السلطات القضائية المختصة، وذلك خوفا من تلاشي الدليل أو إتلافه، لأن المجرم الإلكتروني له من الخبرة والاحترافية ما يجعله يعبث بالدليل قبل صدور الإذن بالتفتيش.

---

[1]– عرفت المادة 02/02 من القانون رقم 09–04 المنظومة المعلوماتية بأنها: "أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين".

[2]– يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، مرجع سابق، ص: 351.

[3]– المرجع نفسه، ص: 352.

* **اتصال حاسوب المشتبه فيه أو المتهم بحاسوب آخر خارج الوطن:** أي اتصال الحاسب الآلي "محل الواقعة" بحاسب آخر يوجد خارج الوطن، وتتجسَد هذه الصورة حين يقوم مرتكبو الجريمة الإلكترونية بتخزين بياناتهم في أنظمة معلوماتية خارج الوطن، وذلك باستغلال شبكات التواصل الاجتماعي والبريد الإلكتروني وغيرها، بهدف عرقلة سلطات التحقيق عن تقفي أثرهم.

إن الحصول على مثل هذه المعلومات دون مساعدة الدولة الأجنبية المعنية يعد انتهاكا لسيادتها، وخرقا لقوانينها الوطنية، وللاتفاقيات الدولية المتعلقة بالتعاون الدولي في مجال مكافحة الجرائم بوجه عام، والجريمة الإلكترونية على وجه الخصوص.

وفي هذا الصدد أجازت المادة 32 من (ا أ م ج إ) الدخول بغرض التفتيش والحجز في أجهزة الحاسب الآلي أو شبكات تابعة لدولة أخرى دون الحصول على إذنها في حالتين:[1]

- حالة التفتيش عن معلومات أو بيانات متاحة للعامة.
- حالة موافقة مالك أو حائز البيانات على هذا التفتيش.

كما تصدى المشرع الجزائري بدوره لهذه الإشكالية من خلال المادة 05 فقرة 03 من القانون 09-04، بحيث أجاز التفتيش الإلكتروني خارج حدود الدولة، على أن يتم ذلك بمساعدة السلطات الأجنبية المختصة، في إطار الاتفاقيات الدولية ذات الصلة وطبقا لمبدأ المعاملة بالمثل،[2] كما أنشأ هيئة وطنية تعمل على تبادل المعلومات مع نظرائها في الخارج في إطار المساعدة القضائية الدولية.[3]

ورغم الاتفاقيات الدولية المبرمة في هذا الشأن، إلا أن الواقع العملي يكشف عكس ذلك، إذ أن غالبية الدول غير مستعدة لتسهيل هذا الإجراء، كونها تعتبر التفتيش تهديدا لأمنها الداخلي خاصة إذا كان طابع الجريمة فيه مساس بأمن الدولة،[4] فضلا عمَا يمكن أن يخلَفه من ضرر في حالة استعماله كذريعة للتجسس الإلكتروني أو لإرسال فيروسات مدمَرة، وهو ما يصعَب من عملية

---

[1]- نص (ا أ م ج إ) على الرابط: https://rm.coe.int/budapest-convention-in-arabic/1680739173

2- راجع المادة 05 من قانون 09-04 ف 03.

3- راجع المادة 14 ف 03 من القانون 09-04.

[4]- أسامة بن غام العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، المجلد 29، العدد 58، جامعة نايف العربية للعلوم الأمنية، السعودية، 2013، ص: 39-94.

التفتيش في الجرائم ذات البعد الدولي، ويستدعي إلى جنب توحيد القوانين، تسهيل تزويد الدول بالمعلومات المطلوبة في الوقت اللازم لمساعدتها على إقامة الدليل.

ثانيا: الضوابط الشكلية للتفتيش الإلكتروني: أجاز القانون رقم 09-04 لجهاز التحقيق إجراء التفتيش الإلكتروني في إطار القواعد المحددة في ق إ ج، وهو ما يعني أن الإجراءات الشكلية للتفتيش الإلكتروني تخضع لنفس أحكام التفتيش العام، وهي:

01- وجود أمر مكتوب من السلطة القضائية: نظرا لخطورة التفتيش على حرمة الحياة الخاصة فقد أحاطه الدستور الجزائري بعناية خاصة، وذلك بمنع إجرائه دون الحصول على إذن مكتوب من السلطة القضائية،[1] وعلى هذا المبدأ سارت النصوص القانونية، إذ نصت المادة 44 ق إ ج على عدم جواز انتقال ضابط الشرطة القضائية في حالة الجناية أو الجنحة المتلبس بها إلى مسكن المشتبه فيه لإجراء تفتيش إلا بعد الحصول على إذن مكتوب صادر من وكيل الجمهورية أو قاضي التحقيق، مع وجوب استظهاره قبل الدخول إلى المسكن والشروع في عملية التفتيش.

وبالرجوع إلى أحكام القانون رقم 09-04 نلاحظ أن المادة 05 لم تشترط صراحة حصول ضابط الشرطة القضائية على إذن قضائي مسبق لمباشرة التفتيش الإلكتروني، كما هو الشأن بالنسبة لإجراء مراقبة الاتصالات الالكترونية،[2] غير أن ذلك لا يعني عدم اشتراط هذا القيد، إذ أنه ورد في مستهل هذه المادة أنه يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار ق إ ج الدخول بغرض التفتيش إلى منظومة معلوماتية أو جزء منها، وهو ما يوحي بأن التفتيش الإلكتروني يخضع لنفس القواعد العامة للتفتيش العادي، بما في ذلك الإذن القضائي المسبق.

ويجب أن يتضمن الإذن بالتفتيش تحت طائلة البطلان تاريخ وجهة إصداره، وبيان وصف الجرم موضوع البحث عن الدليل، وتحديد المحل المراد تفتيشه بدقة،[3] ويستوي بعد ذلك أن يذكر في الإذن اسم ضابط الشرطة القضائية المكلف بإنجازه أو ذكر صفته الوظيفية فقط، إذ يكفي أن

---

[1]- تنص المادة 48 من الدستور الجزائري: "لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

[2]- تنص المادة 04 من القانون 09-04: "لا يجوز إجراء عمليات المراقبة في الحالات المذكورة أعلاه إلا بإذن مكتوب من السلطة القضائية المختصة".

[3]- راجع المادة 44 ف 03 ق إ ج.

تتوافر فيه صفة ضابط الشرطة القضائية التي تؤهله للقيام بعملية التفتيش، مادام الإجراء يدخل ضمن اختصاصه الإقليمي.[1]

وتعتبر الكتابة بتوافر البيانات المذكورة ضمانة هامة للحيلولة دون الاعتداء على حرمة الحياة الخاصة للأفراد دون موجب من القضاء، فيتحقق الضمان القضائي بتمكين المحكمة من بسط رقابتها على صحة الإذن وتوافر دواعي التفتيش.

ومع ذلك فإن الواقع العملي يثير بعض التساؤلات، سواء ما تعلق بإمكانية تفتيش ضابط الشرطة القضائية للمنظومة المعلوماتية للمشتبه فيه بناء على رضائه الصريح؟ أو ما تعلق بمدى إمكانية امتداد الإذن الخاص بتفتيش المسكن إلى تفتيش الأجهزة الإلكترونية الموجودة داخله في إطار البحث عن أدلة الجريمة؟ وهو ما يجعلنا نثير النقاط التالية:

أ- التفتيش الإلكتروني بناء على رضا المشتبه فيه: إذا شاهد ضابط الشرطة القضائية بنفسه الجريمة الإلكترونية حال ارتكابها، أو أبلغ عنها فانتقل إلى مكان ارتكابها وعاين آثارها بنفسه، واستدعت تحرياته تفتيش المنظومة المعلوماتية للمشتبه فيه، فلا يجوز له القيام بهذا الإجراء إلا بعد حصوله على إذن مكتوب من وكيل الجمهورية أو قاضي التحقيق، حتى ولو قبل المشتبه فيه بعملية التفتيش، وهو ما يستشف من نص المادة 44 من ق إ ج،[2] باعتبار أن التفتيش الإلكتروني يخضع لنفس القواعد العامة للتفتيش كما سبق ذكره.

وإذا كان الأمر محسوما بالنسبة للجريمة المتلبس بها، فإن التفتيش الذي يجريه ضابط الشرطة القضائية في الجرائم العادية يشوبه بعض الغموض، إذ تنص المادة 64 ق إ ج:[3] "لا يجوز تفتيش المساكن ومعاينتها وضبط الأشياء المثبتة للتهمة إلا برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات، ويجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن

---

[1]- نموذج لإذن بالتفتيش الإلكتروني، انظر ملحق رقم 05.

[2]- كانت الصياغة القديمة لهذه المادة تجيز لضابط الشرطة القضائية عند ارتكاب جناية متلبسا بها تفتيش مسكن المشتبه فيه دون الحاجة للإذن من وكيل الجمهورية أو قاضي التحقيق. انظر أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، ط 3، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2017، ص: 277.

[3]- لم تكن المادة 64 ق إ ج قبل تعديلها بالقانون رقم 90-24 تحيل إلى المادة 44، وإنما كانت تحيل فقط إلى للمواد 45 و 47.

فإن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، ويذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه".

وفي هذا الصدد يرى الأستاذ عبد الله أوهايبية أن تفتيش المساكن في هذه الحالة يعد معاينة أكثر منه تفتيشا، لا يتقيد فيه ضابط الشرطة القضائية بالقيود المذكورة في المواد 44، 45 47 ق إ ج، ولا يلتزم من يعاين المسكن إلا بالمحافظة على السرَ المهني حسب المادة 46 من ذات القانون، ذلك أن رضا صاحب الحق بدخول مسكنه وتفتيشه من طرف الغير يغني عن وجود الالتزام بتلك القيود، بشرط أن يكون الرضا سليما وصريحا.[1]

ويرى الأستاذ نجيمي جمال أن الإذن القضائي لوكيل الجمهورية أو قاضي التحقيق لا يكون إلا في حالة رفض صاحب المسكن أو غيابه، وإلا فما فائدة الرضا إذا كان هناك إذن من النيابة؟ كما أن المادة 76 من قانون الإجراءات الجزائية الفرنسي المقابلة لنص المادة 64 ق إ ج تنص على رضا صاحب المسكن، وفي غيابه يكون الإذن من طرف قاضي الحرَيات بناء على طلب من وكيل الجمهورية.[2]

ويرى بعض الفقه العربي أن الرضا بتفتيش المسكن بناء على رضا المعني يفقد التفتيش حقيقته كإجراء أو عمل من أعمال التحقيق الغرض منه الحصول على الدليل، ليصبح مجرد اطلاع عادي أو معاينة متاحة لكل من أذن له صاحب المسكن بالدخول، سواء كان من السلطة أو من العامَة.[3]

ب- التفتيش الإلكتروني بناء على إذن بتفتيش المسكن: ذهبت بعض التشريعات إلى أنه يكفي الحصول على إذن بتفتيش المسكن، ليمتد نطاقه إلى كل الأجهزة الإلكترونية المتواجدة داخله، بما فيها الملفات والبيانات التي تحتويها تلك الأجهزة، إذ يرون أن مختلف الأجهزة الرقمية تمثل مجالا

[1]- عبد الله اوهايبية، شرح قانون الإجراءات الجزائية، مرجع سابق، ص: 326.

[2]- جمال نجيمي، قانون الإجراءات الجزائية على ضوء الاجتهاد القضائي، الجزء الأول، ط1، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015، ص: 138.

[3]- عبد الله أوهايبية، المرجع نفسه، ص: 324.

حيويا ضخما لتخزين ملايين الملفات والمعلومات، ولا يعقل إصدار إذن بالتفتيش حسب عدد الملفات التي يحتويها الجهاز الإلكتروني أمام هذه القدرة التخزينية الضخمة.[1]

وعلى خلاف ذلك اتجه المشرع الأمريكي إلى أن كل ملف في الحاسوب الآلي يعتبر حاوية مغلقة، ويتطلب إذنا خاصا بالتفتيش، وأساسه في ذلك أن الحاسب الآلي يمكن أن يحتوي على ملفات تتعلق بالحياة الخاصة لصاحبه لا علاقة لها بالجريمة، وأن فتح أحد هذه الملفات دون إذن بذلك يعتبر تعد على حق الخصوصية.[2]

وبالنسبة للتشريع الجزائري فإن الدستور حرص على حماية حرمة الحياة الخاصة للأفراد، إذ تنص المادة 47 منه على أنه: "لا يجوز المساس بحرمة الحياة الخاصة للأفراد وسرية مراسلاتهم واتصالاتهم الخاصة في أي شكل كانت إلا بأمر معلَل من السلطة القضائية، ويعاقب من ينتهك هذه الحقوق"، ونصت المادة 48 منه على أنه: "لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة".

لذلك نرى أنه لا يمكن تفتيش المنظومة المعلوماتية في أي حال من الأحوال دون الحصول على إذن مكتوب من السلطة القضائية، ويتعين على المشرع الجزائري التدخل لإيجاد موازنة تكفل من جهة حرمة الحياة الخاصة للأفراد، وتضمن من جهة أخرى سرعة الوصول إلى الأدلة الرقمية للجريمة قبل العبث بها.

02- حضور المعني بالتفتيش أو من يمثله عملية التفتيش: يعتبر هذا الشرط من أهم الشروط الشكلية التي يتطلبها القانون، وذلك لضمان الاطمئنان على سلامة إجراءات التفتيش لما فيه من اطلاع على أسرار الشخص، إذ تشترط المادة 45 ق إ ج حضور المشتبه فيه عملية التفتيش إذا حصل في مسكنه، وإذا تعذر عليه الحضور وجب على ضابط الشرطة القضائية دعوته إلى تعيين ممثل له، وإذا امتنع عن ذلك أو كان هاربا استدعى ضابط الشرطة القضائية شاهدين من غير الموظفين الخاضعين لسلطته لحضور هذه العملية.

[1]- جمال براهيمي، المرجع السابق، ص: 38.

[2]- المرجع نفسه، ص: 39.

غير أن التعديل الذي أدخله المشرع الجزائري على هذه المادة بموجب القانون رقم 06-22 جعله يستغني عن هذه الضمانة في جرائم معينة، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وذلك لإضفاء نوع من السرَية أثناء جمع الدليل الإلكتروني، خاصة وأنه ذو طبيعة خاصة من حيث سرعة تعديله والتلاعب فيه.

03- الميعاد الزمني للتفتيش: حظر المشرع إجراء عملية التفتيش خارج مجال زمني محدد حرصا منه على تضييق نطاق الاعتداء على الحريات الخاصة، فحصر ميقاته بين الساعة الخامسة صباحا والثامنة مساء، باستثناء بعض الجرائم الخطيرة، التي أجاز فيها عملية التفتيش في كل ساعة من ساعات الليل أو النهار، ومن بينها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات،[1] ليستثني بذلك تطبيق هذه الضمانة على هذه الجرائم تغليبا لمصلحة المجتمع في تحقيق العدالة على مصلحة الفرد في حرمة حياته الخاصة.

ولأن عملية التفتيش تقوم أساسا على المباغتة والمفاجأة، فمن غير المنطقي إخطار المعني بها مسبقا، وإلا فقدت قيمتها، إذ يكفي إعلامه عند بدئها.[2]

04- تحرير محضر التفتيش: يعتبر محضر التفتيش الشهادة التي يعلن بمقتضاها المحقق ما شاهده من وقائع، وما اتخذه من إجراءات، وما توصل إليه من نتائج، فهو الصورة المكتوبة للتفتيش، ولمَا كان التفتيش عملا من أعمال التحقيق فإنه يستلزم تحرير محضر يثبت جميع الإجراءات والأدلة، ولا يتطلب القانون شكلا معينا لتحريره سوى ما تستوجبه أو تفرضه الأسس العامة في تحرير المحاضر بشكل عام؛ وهي أن يكون مكتوبا باللغة الرسمية للدولة، وأن يحمل تاريخ تحريره وتوقيع الشخص أو الجهة التي قامت بتحريره، وأن يتضمن كافة البيانات المتعلقة بالتفتيش.[3]

ويختلف الأمر عما إذا كان التفتيش قد تم من طرف ضابط شرطة قضائية، فهو بذلك يخضع للقواعد العامة التي يجب أن تتضمنها المحاضر المحررة من طرف الشرطة القضائية، أو

---

[1]- راجع المادة 47 ق إ ج.

[2]- توفيق الشاوي، فقه الإجراءات الجنائية، ج 1، ط 2، دار الكتاب العربي، مصر، 1994، ص: 387.

[3]- أسامة بن غانم العبيدي، المرجع السابق، ص: 102.

كان قد أجري من طرف قاضي التحقيق، والذي يتعين أن يكون مصحوبا بكاتب يتولَى تحرير المحضر والتأشير عليه تحت طائلة البطلان.[1]

إضافة إلى هذه الضوابط، فإن التفتيش في الجرائم الإلكترونية المعقَّدة يتطلب إحاطة المحقق الجنائي بتقنيات المعلوماتية، وله في سبيل ذلك أن يستعين بأهل الخبرة والمهارة لمساعدته على تحرير محضر يغطي الجوانب الفنية للتفتيش، حتى يمكن للقضاء أن يطمئن إليه عند مناقشة أدلة الدعوى.

ثالثا: الجزاء المترتب على عدم احترام ضوابط التفتيش: نظم المشرع إجراء التفتيش ووضع له ضوابط وجب تتبعها صونا للحقوق والحريات، ورتب بالمقابل البطلان على مخالفتها تكريسا لمبدأ الشرعية الإجرائية، إذ تنص المادة 48 ق إ ج على أنه: "يجب مراعاة الإجراءات التي استوجبتها المادتان 45 و 47 ق إ ج ويترتب على مخالفتها البطلان"، في حين تؤكد المادة 44 من ذات القانون على بطلان التفتيش الذي يجريه عون لا يحمل صفة ضابط شرطة قضائية، أو حال إجرائه خارج نطاق اختصاصه الإقليمي.

وبالرجوع إلى أحكام المادة 05 من القانون رقم 09-04 التي أحالت بدورها إلى القواعد الإجرائية العامة، فإن أي كل مخالفة لضوابط التفتيش المذكورة يترتب عليها البطلان، فيصبح التفتيش كأن لم يكن، وتسقط الأدلة المستمدة منه، ولا يمكن للمحكمة الاستناد إليها في إثبات التهمة.

وأمام شيوع تشابك الحواسيب وانتشار الشبكات الدولية والداخلية، فإن عملية التفتيش قد تمتد إلى نظم أخرى غير النظام محل التفتيش، وقد يتم من خلالها الحصول على معلومات من جهات ليست محلا للاشتباه، لذلك نرى أنه يتعين سن القوانين التي تضبط هذه المسألة بأكثر دقة تفاديا للتفتيش العام، مع ضرورة توخي المحقق الجنائي الحيطة اللازمة عند القيام بمهامه واستعانته بأهل المعرفة الفنية متى تطلب الأمر حتى يحقق التفتيش غرضه، مع السعي دوما نحو تحقيق تعاون دولي حقيقي يمكن من خلاله تبادل الأدلة في إطارها الشرعي.

[1]– رضا هميسي، المرجع السابق، ص: 170.

المطلب الثاني

الحجز الإلكتروني

إن الهدف الذي يسعى إليه المحقق الجنائي من إجراء التفتيش هو حجز الأشياء التي تفيد في كشف الجريمة وفك غموضها، سواء استعملت في ارتكابها أو نتجت عنها، لذلك توصف عملية الحجز بأنها إحدى الآليات المخولة لجهاز التحقيق، مثلها مثل المعاينة والتفتيش، والتي عادة ما تنتهي بالحصول على الدليل الإلكتروني.

وطالما أن أدلة الإثبات الرقمية غير مرئية، فإنه من السهل على المجرمين تخريبها أو تغييرها أو تحويلها من مكان تنفيذها، مما يستوجب الحفاظ عليها حتى يمكن للقاضي أن يستأنس إليها عند فحص أدلة الدعوى، من أجل ذلك كرَس المشرع الجزائري إجراء الحجز الإلكتروني كآلية من آليات التحقيق الجنائي ضمن القانون رقم 09-04،[1] كما سبق تكريس هذا الإجراء من طرف (ا أ م ج إ) التي دعت الدول إلى ضرورة تبنيه ضمن قوانينها الداخلية.[2]

الفرع الأول: مفهوم الحجز الإلكتروني

إذا كان اكتشاف سلطة التحقيق للبيانات يعد تفتيشا، فإن النسخ الرقمي لهذه لبيانات يعد حجزا، فهو بذلك إجراء يمكنها من الحصول على نسخة من البيانات التي تحتفظ بها لاستعمالها في المستقبل كدليل جزائي.

أولا: تعريف الحجز الإلكتروني: يعرف الحجز عموما بأنه: "وضع اليد على الأشياء والمحافظة على محتوياتها لمصلحة التحقيق".[3]

---

[1]- راجع المواد 03 و 06 من القانون 09-04.

[2]- تنص المادة 3/19 من الاتفاقية الأوروبية المتعلقة بمكافحة الجريمة الإلكترونية:

"Chaque partie adopte les mesures législatives et autre qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes:

a- saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique.

b- réaliser et conserver une copie de ces données informatiques.

c- préserver l'intégrité des données informatiques stockées pertinentes .

d- rendre inaccessibles ou enlever ces données informatiques du système informatique consulté".

[3]- جيلالي بغدادي، التحقيق، الديوان الوطني للأشغال التربوية، ط 1 ، الجزائر، 1999، ص: 152.

ولعلَ ما يميز هذا الإجراء أنه غير معرَف في ق إ ج، وهو موزع بين عدة قوانين جزائية، إذ عرفه قانون الوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما بأنه: "فرض حظر مؤقت على تحويل الأموال أو استبدالها أو التصرف فيها أو نقلها، أو تولَي عهدة الأموال أو السيطرة عليها مؤقتا بناء على قرار قضائي أو إداري"،[1] ونفس التعريف أخذ به قانون الوقاية من الفساد ومكافحته.[2]

ويمتد المفهوم التقليدي للحجز ليشمل البيانات الإلكترونية وما تحتويه من ملفات وسجلات فيعرف الحجز الإلكتروني على أنه: "وضع اليد على الدعائم المادية المخزنة فيها البيانات الإلكترونية أو المعلومات التي تتصل بالجريمة الإلكترونية المرتكبة، والتي من شأنها أن تفيد في كشف الحقيقة عن الجريمة ومرتكبيها"،[3] وتبعا لذلك فإن الحجز يحصل بوضع اليد على كل ما يصلح أن يكون دليلا في إثبات الجريمة أو نفيها، من أجل تقديمه إلى القضاء.

ومع مرور الزمن ظهرت بعض مساوئ حجز البيانات الإلكترونية المتحصل عليها من جهاز الحاسوب وشبكاته، وذلك بسبب ما قد يلحق الأشخاص من ضرر بحكم حاجتهم إلى الأجهزة المادية طيلة فترة الحجز، وخاصة المؤسسات الاقتصادية التي تشل نشاطاتها.[4]

وفي إطار البحث عن حل لهذا الإشكال تم تبني مقاربة حديثة تتجاوب مع واقع التخزين الرقمي، وتعتمد على النسخ الرقمية للبيانات المستهدفة بالتفتيش، بحكم أن معظم عمليات التفتيش أصبحت تتم من خلال نسخ المواد المخزنة في نظم المعالجة الآلية للمعطيات بقصد تفتيشها لاحقا مع ترك الأجهزة المادية والنسخة الأصلية للبيانات بحوزة صاحبها، وهو ما يعتبر عنصرا من عناصر الموازنة بين حق المجتمع وحقوق الأفراد.

---

[1]– راجع المادة 04 من القانون رقم 05-01 المؤرخ في 06-02-2005 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم بالقانون رقم بالقانون 23-01 المؤرخ في 07-02-2023، الجريدة الرسمية لسنة 2023، العدد 08.

[2]– تنص المادة 02 بند ح من القانون 06-01 المتعلق من الوقاية من الفساد ومكافحته: "التجميد أو الحجز هو فرض حظر مؤقت على تحويل الممتلكات أو السيطرة عليها مؤقتا، بناء على أمر صادر عن محكمة أو سلطة مختصة أخرى".

[3]–نبيلة هبة هروال، المرجع السابق، ص: 266.

[4]– رابح لهوى، الشرعية الإجرائية للأدلة المستمدة من التفتيش، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2020-2021، ص: 91.

وقد تناولت (ا أ م ج إ) قواعد الحجز الإلكتروني من خلال المادة 19 سابقة الذكر، أين استعملت المصطلح التقليدي وهو الضبط (Saisir)، إضافة إلى استعمالها لمصلح "الحصول بأي طريقة مماثلة" (Obtenir d'une façon similaire)، وذلك للإشارة إلى أساليب أخرى للحجز وسط البيئة الرقمية.

ثانيا: الخلاف الفقهي حول الحجز الإلكتروني: إذا كان الحجز في الجرائم التقليدية لا يثير جدلا كونه يرد على أشياء مادية ملموسة، فإن الأمر مختلف في الجرائم الإلكترونية كونه يرد على أشياء ذات طبيعة معنوية كالمعطيات المعالجة إلكترونيا، مما أثار خلافا فقهيا حول مدى إمكانية حجز هذه المكونات؟

يرى جانب من الفقه أن المعطيات المعالجة لا تصلح لأن تكون محلا للحجز نظرا لانتفاء عنصرها المادي، لذلك لا يمكن حجزها إلا بعد ضبطها في دعامات مادية، كما لو كانت مطبوعة في مخرجات الحاسوب أو أي وعاء آخر للبيانات، أو في حالة التصوير الفوتوغرافي لشاشة الحاسوب، ويجد هذا الاتجاه تجسيده الفقهي في ألمانيا ولوكسمبورغ ورومانيا والبرازيل والمجر وفنلندا والشيلي.[1]

في حين يرى جانب آخر أنه لا مانع من أن يرد الحجز الإلكتروني على البيانات الإلكترونية في حد ذاتها مادامت مفيدة في الكشف عن الجريمة، ويجد هذا الاتجاه تجسيده الفقهي في كل من الولايات المتحدة الأمريكية وكندا وبلجيكا ومصر،[2] إذ أجاز المشرع المصري لمأموري الضبط القضائي بعد الحصول على إذن مكتوب ومسبب من جهة التحقيق المختصة ضبط أو سحب أو التحفظ على البيانات والأنظمة المعلوماتية وتتبعها أينما وجدت، مع الحرص على أن لا يؤثر ذلك على استمرارية أداء خدماتها، كما بينت المواد 53 و 55 و 91 من قانون الإجراءات الجنائية المصري بأن عملية الضبط تشمل كل ما يحتمل أن يكون قد استعمل في الجريمة أو نتج عنها.[3]

---

[1]– نبيلة هبة هروال، مرجع سابق، ص: 265.

[2]– المرجع نفسه، ص: 265.

[3]– خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2020–2021. ص: 104.

وبدوره أجاز المشرع الجزائري الحجز عموما من خلال المادة 84 ق إ ج، التي أتاحت لقاضي التحقيق حجز الأشياء والوثائق التي يرى أنها مفيدة لإظهار الحقيقة، ولا يقتصر الحجز على الأشياء التي ساعدت أو استعملت في ارتكاب الجريمة، بل يشمل أيضا تلك المخصصَة لارتكابها، والتي تحصلت منها، والتي استعملت لمكافأة مرتكبيها.[1]

ثم أتبعه بتكريس الحجز الإلكتروني من خلال القانون 09-04، أين أتاحت المواد 03 و 06 القيام بإجراءات الحجز داخل منظومة معلوماتية على دعامات تخزين إلكترونية قابلة للحجز ووضعها في أحراز وفقا للقواعد العامة.

والأمثلة على أخذ القضاء الجزائري بالأدلة الرقمية المستمدة من عملية الحجز عديدة، منها القرار الصادر عن الغرفة الجزائية لمجلس قضاء الجزائر، بتاريخ 08-06-2015 جدول رقم 15/02327، والذي اعتبر حجز القرص الصلب الذي يحتوي على برنامج القرصنة للموقع الإلكتروني للضحية دليلا لإثبات الجرائم المعلوماتية المنسوبة للمتهم.[2]

الفرع الثاني: نطاق الحجز الإلكتروني

تنص المادة 06 من القانون 09-04 على أنه: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز، وتوضع في أحراز وفقا للقواعد المقررة في ق إ ج.

يتبين من خلال هذا النص أن الأصل في عملية الحجز الإلكتروني هو حجز كامل المنظومة المعلوماتية، والاستثناء هو الاكتفاء بحجز المحتوى المجرم، وأنه يمكن إضافة إلى حجز المعطيات الأساسية حجز المعطيات اللازمة لفهمها، لذلك فإن عملية الحجز الإلكتروني تشمل ما يلي:

[1]- أحسن بوسقيعة، التحقيق القضائي، مرجع سابق، ص: 92.

[2]- يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، مرجع سابق، ص: 426.

01- حجز المعطيات الآلية: يمكن للمحقق الجنائي حال تواجد المنظومة المعلوماتية داخل التراب الوطني أن يحجز كل معطياتها المخزَنة المفيدة في الكشف عن الجرائم والوصول إلى مرتكبيها على دعامة تخزين إلكترونية، ويضعها في أحراز،[1] وإذا امتدت آثار الجريمة خارج الإقليم الوطني فيتعين عليه الاستعانة بالدولة التي تتواجد بها هذه الآثار، وذلك بتقديم طلب لحجزها في إطار المساعدة القضائية الدولية،[2] وأن نسخ هذه المعطيات دون إذن من هذه الدولة يعد خرقا لسيادتها.

والملاحظ أن المشرع الجزائري استعمل مصطلح دعامة تخزين الكترونية قابلة للحجز، مثل القرص المرن أو المضغوط أو الأشرطة المغناطيسية دون حصرها، ليترك المجال مفتوحا أمام ظهور تقنيات تخزين جديدة، باعتبار أنه لا يمكن التعامل مع تلك المعطيات في صورتها الأولية على شكل نبضات أو ذبذبات الكترونية إلا بعد نسخها على دعامات مادية.

02- حجز المعطيات اللازمة لفهم المعطيات الأساسية: إذا كان حجز المعطيات ذات المحتوى المجرم غير كاف لاستخدامه كدليل ما لم يقترن بحجز المعطيات اللازمة لفهمها، ففي هذه الحالة يمكن للمحقق الجنائي حجز المعطيات الأخيرة على دعامة إلكترونية قابلة للحجز،[3] ذلك أن حجز المعطيات المساعدة لفهم المعطيات الأساسية من شأنه توضيح الدليل المستمد منها، وبالتالي مساعدة قضاة الحكم على فهم المسائل التقنية للجريمة.

03- الحجز عن طريق منع الوصول إلى المعطيات: إذا استحال على المحقق الجنائي إجراء الحجز الإلكتروني لأسباب تقنية، وخشي من إتلاف أو نقل أو ضياع الأدلة التي توصل إليها خلال عملية التفتيش، فيمكنه اللجوء إلى استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.[4]

والملاحظ أن المشرع حصر إمكانية اللجوء إلى الحجز عن طريق منع الوصول في حالة وحيدة وهي استحالة الحجز لأسباب تقنية، دون ضبط هذه الأسباب، سواء تعلق الأمر بالمنظومة

[1]- راجع المادة 06 من القانون رقم 09-04.

[2]- راجع المادة 16 من القانون رقم 09-04

[3]- راجع المادة 06 ف 01 من القانون رقم 09-04.

[4]- راجع المادة 07 من القانون رقم 09-04.

المعلوماتية ذاتها، كاستحالة الدخول لوجود كلمة السر أو لصعوبة اختراق نظام الحماية، باعتبار أن نظم الحواسيب الحديثة تكون في الغالب جزءا من شبكات واسعة ومعقدة يصعب حجزها دون تعامل حقيقي من القائم على تشغيل النظام، أو تعلق بعملية نسخ المعطيات، وذلك بسبب التطور الدائم لتكنولوجيات الإعلام والاتصال،[1] لذلك أبقى المجال مفتوحا من أجل تمكين المحقق من اتخاذ تدابير احترازية تمنع المجرم الإلكتروني من العبث بالمعطيات المخزنة.[2]

ويتعين التنويه إلى أنه يجب على الجهة التي تقوم بالحجز الإلكتروني في جميع حالاته الالتزام بالقواعد العامة المقررة في ق إ ج،[3] وذلك باحترام ضمانات التحقيق، وخاصة سر المهنة وحقوق الدفاع.

كما يجب عليها السهر على سلامة المعطيات الموجودة بالمنظومة المعلوماتية التي يجرى بها التفتيش والحجز،[4] غير أن ذلك لا يمنعها من استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، بشرط ألاَ يؤدي ذلك إلى المساس بمحتواها.[5]

وبعد الانتهاء من عملية الحجز توضع النسخة المحجوزة تحت تصرف القضاء إلى حين انتهاء المحاكمة، لذلك يستحسن حفظ نسخة ثانية لدى الجهة القائمة بالتفتيش، حتى يمكن الرجوع إليها في حالة تلف أو ضياع النسخة الوحيدة الموضوعة تحت تصرف القضاء.

---

[1]– هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، 1994، ص: 98.

[2]– زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011، ص: 153.

[3]– راجع المادة 06 ف 1 القانون رقم 09-04.

[4]– تنص المادة 06 ف 02 من القانون 09-04 " يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية".

[5]– تنص المادة 06 ف 03 من القانون 09-04 "غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق، شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات".

ومن أجل صون الحريات الفردية والحفاظ على حرمة الحياة الخاصة للأفراد أثناء هذه العملية وضع المشرع حدودا لاستعمال المعطيات الآلية المتحصل عليها، إذ لا يجوز استعمالها خارج نطاق التحريات الأولية أو التحقيق القضائي.[1]

لكن ورغم كل ما بذله المشرع من جهود لتسهيل عملية الحجز الإلكتروني، إلا أنها تبقى عرضة لبعض العقبات، خاصة ما تعلق بالحجم الهائل للمعطيات المطلوب حجزها في الأنظمة المعلوماتية، كالبحث في النظام الإلكتروني لشركة متعددة الإقامة، أو في حالة تواجد هذه المعطيات في شبكات أو أنظمة معلوماتية تابعة لدولة أجنبية، في ضل إحجام بعض الدول عن تقديم المساعدة القضائية في حينها، هذا إن لم تكن طرفا في الجريمة.

[1]– راجع المادة 09 من القانون رقم 09-04.

خلاصة الفصل

يتضح جليا أن ما أفرزه امتداد ظاهرة الإجرام إلى العالم الافتراضي من ظهور نمط إجرامي جديد، فرض على جهاز التحقيق في سبيل مواجهتها الاستعانة بأساليبه التقليدية، إذ تم الاعتماد على المعاينة لما لها من دور في كشف غموض الجريمة الإلكترونية، وضبط أدلتها وإسنادها إلى مرتكبيها، غير أنها لم ترق إلى نفس الأهمية مقارنة بالجرائم العادية، وذلك بسبب ما يمكن أن يحدثه الجاني من عبث بالأدلة الرقمية.

ونظرا لما تتميز به الجريمة الإلكترونية من طابع تقني وفني، كان لزاما على المحقق الاستعانة بأهل الخبرة والاختصاص لفك غموضها، فإجرام الذكاء والفن لا يكشفه إلا ذكاء وفن مماثلين.

فضلا عن ذلك، تم الاستعانة بآلية التفتيش الإلكتروني للولوج داخل النظم المعلوماتية، الذي ورغم اتفاقه في مدلوله العام مع التفتيش العادي، إلا أنه يختلف عنه كونه ينصب على بيئة افتراضية، ويستهدف أدلة معنوية ليس لها أي مظهر مادي محسوس، الأمر الذي يستدعي الإلمام بالجانب التقني لهذه الجريمة، بالموازاة مع جانبها القانوني.

وطالما أنه من السهل على مجرمي المعلوماتية تخريب الأدلة الرقمية أو تعديلها، تم اللجوء إلى الحجز الإلكتروني كآلية للحفاظ عليها، سواء تعلق الأمر بالمنظومة المعلوماتية ككل أو بجزئها المجرَم فقط، مع الاستعانة في سبيل ذلك بالدولة التي تتواجد بها آثار الجريمة.

ورغم ما بذله المشرع من جهود لتطوير آليات التحقيق في الجريمة الإلكترونية، إلا أن التطور التكنولوجي المستمر، وأثره المباشر على تطور هذا النمط الإجرامي، حال دون فعالية الآليات التقليدية في مكافحتها، وفرض ضرورة البحث عن أساليب أخرى من شأنها أن تكفل ذلك.

الفصل الثاني

الأساليب الحديثة للتحقيق

في الجريمة الإلكترونية

الفصل الثاني

الأساليب الحديثة للتحقيق في الجريمة الإلكترونية

إن التطور الحاصل في مجال تكنولوجيات الإعلام والاتصال كان له أثر واضح على مبادئ الفكر القانوني لاسيما عناصر دليل الإثبات، باعتبار أن الدليل الذي يقوى على إثبات هذه الجرائم لابد وأن يكون من نفس طبيعتها التقنية، وهو ما جعل العديد من الدول تراجع قوانينها الداخلية بحثا عن أساليب أكثر فاعلية.

وقد ساير المشرع الجزائري هذه الثورة التقنية، فاستحدث آليات تعتمد على استغلال تكنولوجيات الإعلام والاتصال الحديثة، بدءا بتكريس أساليب التحري الخاصة من خلال تعديل قانون الإجراءات الجزائية سنة 2006، مرورا إلى تعزيز آليات المساعدة القضائية.

وللإحاطة بهذه العناصر، ارتأينا تقسيم هذا الفصل إلى المبحثين الآتيين:

المبحث الأول: أساليب التحري الخاصة.

المبحث الثاني: المساعدة القضائية.

المبحث الأول

أساليب التحري الخاصة

عزَز المشرع الجزائري إجراءات التحقيق بإضافة أساليب جديدة، تعرف عند الفقه الجنائي بأساليب التحري الخاصة، يمكن استغلالها في البحث عن بعض الجرائم الخطيرة، بما فيها جرائم المساس بأنظمة المعالجة الآلية للمعطيات.[1]

ومع ظهور أنماط جديدة من الجريمة، وجد المشرع نفسه مضطرا لتوسيع نطاق هذه الأساليب لتشمل جرائم أخرى، أكثر خطورة وأشد تعقيدا، خاصة تلك التي تعتمد في ارتكابها على تكنولوجيات الإعلام والاتصال، على غرار جرائم عصابات الأحياء،[2] جرائم اختطاف الأشخاص،[3]جرائم إفشاء المعلومات والوثائق الإدارية،[4] جرائم الاتجار بالبشر ومكافحته،[5] جرائم التزوير واستعمال المزور.[6]

وحتى نغطي هذه النقاط بالدراسة والتحليل ارتأينا تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: التسرب الإلكتروني.

المطلب الثاني: اعتراض المراسلات وتسجيل الأصوات والتقاط الصور.

---

[1]– راجع المادة 65 مكرر 5 ق إ ج.

[2]– راجع المادة 20 الأمر رقم 20–03 المؤرخ في: 20–08–2020، المتعلق بالوقاية من عصابات الأحياء ومكافحتها، الجريدة الرسمية لسنة 2020، العدد 51، الموافق عليه بالقانون رقم 20–12 المؤرخ في 22–10–2020

[3]– راجع المادة 16 من القانون رقم 20–15 المؤرخ في 30–12–2020 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها، الجريدة الرسمية لسنة 2020، العدد 81.

[4]– راجع المادة 27 من الأمر 21–09 المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية لسنة 2021، العدد 45.

[5]– راجع المادة 36 من القانون رقم 23–04 المؤرخ في 07–05–2023 المتعلق بالوقاية من الاتجار بالبشر ومكافحته، الجريدة الرسمية لسنة 2023، العدد 32.

[6]– راجع المادة 15 من القانون رقم 24–02 المؤرخ في 26–02–2024 المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية لسنة 2024، العدد15.

المطلب الأول

التسرب الإلكتروني

أمام التطور الرهيب للجريمة الإلكترونية، كان لزاما على الدول البحث عن أساليب أخرى قادرة على مواجهة خطر تفاقم هذه الظاهرة، من بينها تسلَل رجل الشرطة القضائية داخل المجموعة الإجرامية لكشف خططها، وهو ما يعرف قانونا بالتسرب.

لكن وقبل التفصيل في هذا الإجراء وجب علينا أن نعرَج على الجدل الفقهي الذي أثارته أساليب التحري الخاصة، نظرا لما تعتمده من أساليب غير مشروعة، وما تشكله من انتهاك لحرمة الحياة الخاصة للأفراد.

الفرع الأول: الجدل الفقهي حول مشروعية أساليب التحري الخاصة

انقسم الفقه بين مؤيد ومعارض لاستعمال هذه التقنيات، وذلك لما تحمله من انتهاك لحق الخصوصية، ولكل فريق حججه وأسانيده.

01- الرأي المعارض: يدعو جانب من الفقه إلى تجنب هذه الوسائل كونها تتم خفية دون علم المشتبه فيه، فهي تنتهك حرمة حياته الخاصة، التي تعد أبرز الحقوق والحريات التي تكفلها الشريعة الإسلامية والمواثيق الدولية ومختلف الدساتير.

ورد في القرءان الكريم ما يؤكد النهي عن التجسَس في قوله تعالى: "يَآأَيُّهَا الذِينَ ءامَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَب بَّعْضُكُم بَعْضًا"،[1] كما جاءت السنة النبوية مقررة لحق الإنسان في ستر خصوصياته، فعن أبي هريرة رضي الله عنه أن رسول الله صلى الله عليه وسلم قال: "إياكم والظَن، فإن الظَن أكذب الحديث، ولا تحسَسوا، ولا تجسَسوا، ولا تنافسوا، ولا تحاسدوا، ولا تباغضوا، ولا تدابروا، وكونوا عباد الله إخوانا كما أمركم".[2]

---

[1]- الآية 12 من سورة الحجرات.

[2]- أبي زكرياء محي الدين يحيى بن شرف النووي، رياض الصالحين من كلام سيد المرسلين، ط2، دار ابن الجوزي للنشر والتوزيع، مصر، 2014، ص: 375.

كما كرس الإعلان العالمي لحقوق الإنسان في العاشر من ديسمبر 1948، باعتباره أول وثيقة تتضافر فيها إرادة الدول لتحقيق كرامة الإنسان هذا الحق،[1] إذ تنص المادة 12 منه: "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة، أو في شؤون أسرته أو مسكنه أو مراسلاته ولا لحملات تمس شرفه وسمعته، ولكل شخص حق في أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات".

ويعد الفقيه هولمز HOLMEZ أبرز أنصار هذا الرأي، إذ وصف هذه الإجراءات بالعمل القذر، وقال بأنه يفضَل أن يفلت المجرم من العقاب خير له من أن يرى السلطة وهي تمارس هذا الدور غير الأخلاقي.[2]

ومن الانتقادات الموجهة لهذا الرأي أن هذه الإجراءات تباشر خفية دون علم ورضا المشتبه فيه، فهي بذلك تنتهك حرمة حياته الخاصة، وتهدم أهم ضمانات حقوق الإنسان، فضلا على أنها لا تعكس الحقيقة دائما، إذ يمكن تغيير أو حذف أي مقاطع أو صور عن بعضها، أو تركيبها بشكل يغير من حقيقتها، خاصة عندما يتعلق الأمر بالصوت أو الصورة، وفي بعض الأحيان قد يوجد تشابه بين الأصوات.[3]

02- الرأي المؤيد: شجَع جانب آخر من الفقه على تبني هذه الأساليب، وذلك لما تقدَمه من فوائد عملية خلال رحلة الكشف عن الجريمة والبحث عن المجرمين، فضلا عن اعتمادها من طرف الدول التي تنادي باحترام حقوق الإنسان،[4] وأن جل الاتفاقيات تدعو الدول إلى إدراج هذه الأساليب ضمن قوانينها الوطنية من أجل تقوية قدراتها على مواجهة تطورات الإجرام المنظم.[5]

[1] - Bettai M, Oliver Duhamel Laurent Geilsamer, la déclaration universelle des droits de l'homme, gallimard, 1999, p: 10.

[2]- ياسر الأمير فاروق، المرجع السابق، ص: 29.

[3]- محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي، ط1، دار الثقافة للتوزيع والنشر، عمان، الأردن، 2011، ص: 45.

[4]- عبد الرحمان خلفي، المرجع السابق، ص: 97.

[5]- ياسر الأمير فاروق، المرجع نفسه، ص: 199.

وتعد الولايات المتحدة الأمريكية من أوائل الدول التي أثير فيها النقاش حول مدى مشروعية هذه الأساليب، أين صدر القانون الفيدرالي الذي ينظم إجراءات مراقبة الاتصالات من قبل أجهزة الشرطة الفيدرالية أو المحلية بتاريخ: 19-06-1968، وأحاطها بعدة ضمانات تهدف إلى صون الحياة الخاصة.[1]

وبعد أحداث 11-09-2001 وما رافقها من تغييرات تراجعت الولايات المتحدة الأمريكية عن سياستها، وأصدرت قانونا يبيح التصنَت على المكالمات الهاتفية وتسجيلها، واعتراض المراسلات بجميع أنواعها، واعتبرته وسيلة وقائية ضد جرائم الإرهاب الدولي، دون أن يشكل انتهاكا للحق في الخصوصية.[2]

أما في مصر فقد أجاز المشرع لقاضي التحقيق أن يأمر بمراقبة المحادثات السلكية واللاَسلكية، وأن يجري تسجيلات لأحاديث تتم في مكان خاص، متى كان ذلك مفيدا في إظهار الحقيقة حول جناية أو جنحة معاقبا عليها بالحبس لمدة تزيد على ثلاثة أشهر.[3]

وتجدر الإشارة إلى أنه سبق الدفع بعدم دستورية التسرب أمام محكمة النقض الفرنسية، ليتم إحالة الدفع على المجلس الدستوري على أساس عدم توفير الضمانات الكافية لاحترام حق الدفاع، وانطوائها على انتهاك لمبدأ المساواة وحرمة الحياة الخاصة للأفراد، الذي تكفله المواد 1، 2، 6، 16 من الإعلان العالمي لحقوق الإنسان، وانتهت الدعوى إلى رفض هذا الدفع لعدم جدَيته، وجاء في تسبيبه بأن ضابط الشرطة القضائية حين يقوم بالبحث عن المجرمين في بعض الجرائم

[1]- فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة (دراسة مقارنة)، أطروحة دكتوراه، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2011-2012، ص 196.

[2]- كاظم عبد الله نزال المياحي، حجية المراقبة الإلكترونية للصوت والصورة في الإثبات الجنائي (دراسة في القانون العراقي والمقارن)، أطروحة دكتوراه، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2016، ص: 134.

[3]- تنص المادة 95 من قانون الإجراءات الجنائية المصري: "لقاضي التحقيق أن يأمر بضبط جميع الخطابات والرسائل والجرائد والمطبوعات والطرود لدى مكاتب البريد وجميع البرقيات لدى مكاتب البرق، وأن يأمر بمراقبة المحادثات السلكية واللاسلكية أو إجراء تسجيلات لأحاديث جرت في مكان خاص متى كان لذلك فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر".

المحددة بنص القانون، عن طريق اعتراض تبادل الرسائل باسم مستعار، دون التحريض على ارتكابها، فإن ذلك لا يشكل خرقا لحقوق الدفاع، ولا تدخلا في الحياة الخاصة، مادام الشخص حرَ في الإجابة على هذه الرسائل.[1]

الفرع الثاني: الأحكام القانونية للتسرب الإلكتروني

يعتبر التسرب أسلوبا من أساليب التحري الخاصة، كرسته المادة 20 من اتفاقية الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية، في إطار ما اصطلح عليه بالأعمال المستترة، وحثَت الدول الأطراف على تكريسه ضمن قوانينها الداخلية.[2]

ومواكبة لذلك اعتمد المشرع الجزائري هذا الإجراء بموجب القانون رقم 06-01 المتعلق بالوقاية من الفساد ومكافحته تحت تسمية "الاختراق"،[3] غير أنه لم يعرفه ولم يبيَن سبل تنفيذه، مما أبقى النص جامدا إلى غاية تعديل ق إ ج بموجب القانون رقم 06-22، الذي عرَفه وحدَد ضوابطه من خلال نصوص المواد (65 مكرر 11 إلى 65 مكرر 18)، ثم أتبعه بتكريس التسرب الإلكتروني من خلال بعض النصوص القانونية الخاصة.

أولا: تعريف التسرب: سنتطرق لتعريف هذا الإجراء من الجانب الغوي والفقهي والقانوني، وصولا إلى تعريف التسرب الإلكتروني، كما يلي:

---

[1]- يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، مرجع سابق، ص: 483-484.

[2]- صادقت الجزائر على اتفاقية الأمم المتحدة المتعلقة بمكافحة الجريمة المنظمة عبر الوطنية بتحفظ، بموجب المرسوم الرئاسي رقم 02-05 المؤرخ في: 02-02-2002 ، الجريدة الرسمية لسنة 2002، العدد 09.

[3]- تنص المادة 56 من الأمر 06-01 المتعلق بالوقاية من الفساد ومكافحته:"من أجل تسهيل جمع الأدلة المتعلقة بالجرائم المنصوص عليها في هذا القانون، يمكن اللجوء إلى التسليم المراقب أو اتباع أساليب تحري خاصة كالترصد الإلكتروني والاختراق، على النحو المناسب وبإذن من السلطة القضائية المختصة".

01- التسرب لغة: مشتق من الفعل: تسرَب، تسرَبا، أي دخل وانتقل خفية، ويعني: "الولوج والدخول بطريقة أو بأخرى إلى مكان أو جماعة"،[1] وللتسرَب تسمية أخرى توظف في العديد من المؤلفات القانونية وهي "الاختراق"، المشتق من الفعل: اخترق، اختراقا، بمعنى: "مشى وسطهم".[2]

02- التسرب فقها: عرف بعض الفقه التسرب بأنه: "عملية أمنية تفيد قيام أحد عناصر الشرطة القضائية بالتسلَل داخل جماعة إجرامية، أو التوغل في مكان أو تنظيم يصعب الدخول إليه، بشكل يجعله يتقرب من أعضائها، ويشعرهم بالانتماء إليهم بصفته شريكا أو خاف أو وسيط، وذلك بغرض مراقبة تحركاتهم قبل وخلال قيامهم بالعمل الإجرامي، ومن ثمة تحقيق حالة التلبس بالجريمة"،[3] وعرفه البعض الآخر بأنه: "التسلل والتوغل داخل مكان أو هدف، أو تنظيم الدخول إليه لكشف نوايا الجماعات الإجرامية".[4]

02- التسرب قانونا: نص عليه المشرع الجزائري في ق إ ج كترجمة لمصطلح **L'infiltration** ووضع له على غير العادة تعريفا من خلال نص المادة 65 مكرر 12 التي تنص: "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 لهم أو خاف".

فالتسرب إذا؛ تقنية تسمح لضابط أو عون الشرطة القضائية بالتوغل داخل جماعة إجرامية بهدف مراقبة أشخاص مشتبه فيهم، وكشف أنشطتهم الإجرامية، وذلك بإخفاء هويته الحقيقية، وتقديم نفسه على أنه فاعل معهم أو شريك.[5]

---

[1]- هدى زوزو، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، دفاتر السياسة والقانون، العدد 11، 2014، ص: 117.

[2]- علي بن هادية وآخرون، القاموس الجديد للطلاب، ط15، المؤسسة الوطنية للكتاب، 1984، الجزائر، ص: 20.

[3]- عبد الرحمان خلفي، المرجع السابق، ص: 104.

[4]- حمزة عبدلي، خصوصية إجراءات المتابعة وتوقيع الجزاء في جرائم الفساد، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 06، العدد 02، 2021، ص: 729.

[5]- عبد الرحمان خلفي، المرجع نفسه، ص: 103.

ويمكن تجسيد عملية التسرب الإلكتروني في ولوج ضابط أو عون شرطة قضائية إلى البيئة الافتراضية، واشتراكه مع أفراد الجريمة في محادثات غرف الدردشة أو ملفات النقاش حول قيام أحدهم باختراق شبكات أو بث فيروسات، مستخدما في ذلك أسماء وصفات مستعارة، يظهر من خلالها بمظهر طبيعي، حتى يتمكن من اكتشاف وضبط الجريمة.[1]

لم تنص الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، ولا الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على إجراء التسرب ضمن أحكامهما الإجرائية، فيما كرسته العديد من التشريعات الدولية، على غرار المشرع الفرنسي الذي أجازه لمعاينة بعض الجرائم الخطيرة بما فيها الجرائم المرتكبة بواسطة وسيلة اتصال إلكترونية.[2]

أما في الجزائر، فقد اعتمده المشرع كآلية للتحري عن بعض الجرائم الخطيرة، بما فيها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، وتناوله ضمن أحكام الفصل الخامس من الباب الثاني (المواد من 65 مكرر 11 إلى غاية 65 مكرر 18 ق إ ج)، لكنه لم يستعمل مصطلح "التسرب الإلكتروني" بصورة صريحة إلى غاية صدور بعض القوانين الخاصة، على غرار القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما،[3] والقانون رقم 20-15 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها،[4] والقانون رقم 23-04 المتعلق بالوقاية من الاتجار بالبشر ومكافحته،[5] والقانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور.[6]

ثانيا: ضوابط التسرب الإلكتروني: يعتبر إجراء التسرب من أخطر الإجراءات على الحقوق والحريات، حيث يستعمل المتسرب أساليب غير مشروعة لكشف ملابسات الجريمة، لذلك أحاطه المشرع بجملة من الضوابط القانونية تتمثل فيما يلي:

[1]- رشيدة بوكر، المرجع سابق، ص: 434.

[2]- يوسف مناصرة، الدليل الإلكتروني، مرجع سابق، ص: 481.

[3]- راجع المادة 26 من قانون الوقاية من التمييز وخطاب الكراهية ومكافحتهما.

[4]- راجع المادة 16 من قانون الوقاية من الاختطاف ومكافحته.

[5]- راجع المادة 32 من قانون الوقاية من الاتجار بالبشر ومكافحته.

[6]- راجع المادة 15 من قانون مكافحة التزوير واستعمال المزور.

01- نوع الجريمة: كان إجراء التسرب محصورا في بدايته على بعض الجرائم الخطيرة (جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف وجرائم الفساد)،[1] وهي جرائم سريعة الانتشار، عابرة للحدود الوطنية، تعتمد في تنفيذها على التخطيط والتنظيم، وآثارها وخيمة على المجتمع، كالهلاك الناجم عن تبادل المخدرات، والخسائر المالية التي تلحق الاقتصاد الوطني من جرائم الفساد.[2]

لكن تطوَر الجريمة دفع بالمشرع إلى توسيع نطاق هذا الإجراء، ليشمل جرائم أخرى أشد خطورة وأكثر تعقيدا، تعتمد في ارتكابها على أحدث تقنيات التكنولوجيا، مثل جرائم عصابات الأحياء، جرائم خطاب الكراهية، جرائم اختطاف الأشخاص، جرائم إفشاء المعلومات والوثائق الإدارية، جرائم الاتجار بالبشر ومكافحته، جرائم المخدرات، جرائم التزوير واستعمال المزور.

02- إعداد تقرير مسبق: يجب على ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب أن يعد تقريرا مسبقا ومفصَلا عن الجريمة، وذلك حتى يتسنى للقاضي المختص بمنح الإذن الاطلاع على ظروف القضية ومتطلباتها، وتقييم جدوى عملية التسرب.[3]

لذلك يتعين عليه جمع أكبر قدر ممكن من المعلومات حول الجريمة، وما تحتاجه من وسائل، ثم يعدَ تقريرا بذلك، يقدمه إلى وكيل الجمهورية أو قاضي التحقيق المختص، الذي يمنحه الإذن، أو يرفض ذلك متى تبين له وجود خطر يهدد حياة المتسرب أو الأشخاص المسخرين معه.

03- صفة المتسرب: يشترط في المتسرَب أن يكون ضابط شرطة قضائية، ويرجع ذلك أساسا إلى خبرته وكفاءته المهنية، ولا مانع من أن يكون عون شرطة قضائية، بشرط أن يباشر مهمته تحت مسؤولية ضابط شرطة قضائية.[4]

---

[1]- راجع المواد 65 مكرر 11 و65 مكرر 5.

[2]- هدى زوزو، المرجع السابق، ص: 121.

[3]- راجع المادة 65 مكرر 13 ق إ ج.

[4]- راجع المادة 65 مكرر 12 ق إ ج.

04- الإذن القضائي: تكريسا للمادة 47 من الدستور الجزائري، أوجب المشرع لمباشرة عملية التسرب ضرورة حصول ضابط الشرطة القضائية على إذن مكتوب من طرف وكيل الجمهورية، أو قاضي التحقيق المختص إقليميا بعد إخطار وكيل الجمهورية.[1]

ويجب أن يكون الإذن بالتسرب مكتوبا ومسبَبا تحت طائلة البطلان، وذلك بذكر نوع الجريمة، وهوية ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته، والمدة اللازمة لإتمامها والمحددة بأربعة أشهر قابلة للتجديد بنفس الشروط،[2] دون أن يحصر المشرع عدد مرات التجديد وهو ما يبقي المجال مفتوحا وفقا لمقتضيات التحقيق.

غير أنه وحفاظا على حياة المتسرب من أي خطر، أجاز القانون للقاضي الذي رخَص بالعملية أن يأمر بوقفها في أي وقت شاء،[3] كما لو وصلته معلومات عن اكتشاف العملية من طرف المجموعة الإجرامية، وجرَم بالمقابل أي فعل أو قول يؤدي إلى الكشف عن هوية المتسرب، وتمتد هذه الحماية لتشمل زوجته وأبنائه وأصوله، وتشدَد العقوبة إذا تعرض أحدهم للضرب أو الجرح أو الوفاة.[4]

ومن أجل الحفاظ على السرية اللازمة لنجاح هذه العملية، اشترط المشرع أن يبقى الإذن بالتسرب خارج ملف الإجراءات إلى غاية الانتهاء من التحريات،[5] كما منع سماع الضابط أو العون المتسرب كشاهد في القضية، غير أن ذلك لا يمنع من سماع الضابط المنسق للعملية الذي جرى التسرب تحت مسؤوليته.[6]

---

[1]- راجع المادة 65 مكرر 11 ق إ ج.

[2]- راجع المادة 65 مكرر 15 ق إ ج.

[3]- راجع المادة 65 مكرر 15 ف 04 ق إ ج.

[4]- راجع المادة 65 مكرر 16 ق إ ج.

[5]- تنص المادة 65 مكرر 15 ف 05: "تودع الرخصة في ملف الإجراءات بعد الانتهاء من عملية التسرب".

[6]- راجع المادة 65 مكرر 18 ق إ ج.

وينبغي التنويه هنا بأن القانون أجاز سماع الضابط المنسق لعملية التسرب بصفته شاهدا على العملية، في حين أنه مجرد ناقل لشهادة المتسرب، الذي عايش وسط الجريمة، وهو أدرى بتفاصيلها.[1]

وبعد الانتهاء من عملية التسرب يقوم ضابط الشرطة القضائية المكلف بتنسيق العملية بإعداد تقرير مفصل يشمل جميع الجوانب العملية، مع ذكر الأسماء والأزمنة والأماكن بدقة، وإبراز الأشياء المستعملة والأشياء ذات الصلة، والنتائج المتوصل إليها، يقدمه للقاضي الذي منحه الإذن للتصرف في الملف طبقا للقانون.

المطلب الثاني

اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

إن اعتراض المراسلات وتسجيل الأصوات والتقاط الصور هي عدة تسميات يمكن اختزالها في مصطلح واحد هو "المراقبة الإلكترونية"، والتي لا تخرج عن كونها رقابة مشروعة لشخص أو مكان أو حديث أو مراسلات مكتوبة أو مرئية، نتيجة الاشتباه في تصرفات غير قانونية، بصورة لا يحس معها الغير بمباشرتها نظرا لطابع السرية الذي يكتنفها.[2]

الفرع الأول: مفهوم اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

للتعرف على حقيقة هذه الأساليب، سنحاول التعرف على كل آلية منها، من خلال توضيح مدلولها وتقنياتها:

أولا: آلية اعتراض المراسلات: أجاز المشرع مراقبة المراسلات السلكية واللاَسلكية متى كان ذلك مفيدا في الوصول إلى كشف ملابسات الجريمة.

[1]– السعيد برابح، كمال بوبعاية، الأساليب المستحدثة ضمن استراتيجية الكشف عن الجرائم المستحدثة في التشريع الجزائري (التسرب نموذجا)، دفاتر البحوث العلمية، المجلد 09، العدد 01، 2021، ص: 250.

[2]– فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراء تحقيق قضائي في المواد الجزائية، مرجع سابق، ص: 236.

01- معنى اعتراض المراسلات: أغفل المشرع كعادته تعريف هذه العملية، واكتفى بتنظيمها من خلال المادة 65 مكرر 5 ق إ ج التي تنص على أنه: "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 الخاصة 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".

أما لجنة خبراء البرلمان الأوروبي المنعقدة بتاريخ: 06-10-2006 من أجل دراسة أساليب التحري التقنية وعلاقتها بالأفعال الإرهابية، فقد عرفت هذه العملية بأنها: "مراقبة سرية المراسلات السلكية واللاَسلكية في إطار البحث والتحري عن الجريمة، وجمع الأدلة والمعلومات حول الأشخاص المشتبه فيهم، أو في مشاركتهم في ارتكاب الجريمة".[1]

مع الإشارة إلى أنه ينبغي التفرقة بين عملية اعتراض المكالمات الهاتفية التي تتم دون علم المعني ودون رضاه، وعملية وضع الخط الهاتفي تحت المراقبة، التي تتم بطلب من صاحب الشأن، وتخضع لملائمة السلطة القضائية.[2]

02- تقنيات اعتراض المراسلات: تتم هذه العملية عن طريق الاعتراض أو التسجيل أو النسخ للمراسلات التي تكون على شكل بيانات قابلة للإنتاج أو التوزيع أو التخزين أو الاستقبال أو العرض، باستعمال وسائل اتصال سلكية كالهاتف الثابت، أو لا سلكية كالهاتف النقال والبريد

[1]- رشيدة بوكر، المرجع السابق، ص: 442.

[2]- سليم علي عبده، التفتيش في ضوء أصول المحاكمات الجزائية الجديد، ط1، منشورات زين الحقوقية، بيروت، 2006، ص: 93.

الإلكتروني،[1] ولا فرق في ذلك بين المراسلات الكتابية كالرسائل البريدية، أو الشفوية كالاتصالات الهاتفية،[2] وتعتبر المراسلات عبر البريد الإلكتروني[3] من أهم العمليات الإلكترونية التي يتم إخضاعها للمراقبة، كونها من أكثر وسائل الاتصال تداولا.

وتجدر الإشارة إلى أن المراسلات التي تكون محلا للاعتراض يجب أن تتسم بطابع الخصوصية، ولا يتحقق ذلك إلا بتوافر عنصرين أساسيين:

أ- **عنصر شخصي:** ويتجلى في اتجاه إرادة المرسل إلى تحديد المرسل إليه، ورغبته في عدم السماح لغيره بالاطلاع على مضمون الرسالة،[4] وهو ما أكدته المحكمة العليا الكندية بقولها: "إن الحالة الذهنية للمرسل هي الحاسمة في تحديد الصفة الخاصة أو العامة للاتصال".[5]

ب- **عنصر موضوعي:** ويتعلق بمضمون الرسالة في حد ذاتها، بمعنى أن تكون الرسالة ذات طابع شخصي وسرَي أو خاص فيما تخبر به.

03- الطبيعة القانونية لاعتراض المراسلات: كفل الدستور الجزائري حق الأفراد في سرَية مراسلاتهم مهما كان شكلها، إذا لا يمكن المساس بها إلا بأمر معلل من السلطة القضائية، وتحت طائلة العقوبات المقررة قانونا.[6]

---

[1]- نورة هارون، جريمة الرشوة في التشريع الجزائري (دراسة على ضوء اتفاقية الأمم المتحدة لمكافحة الفساد)، أطروحة دكتوراه، جامعة مولود معمري، تيزي وزو، الجزائر، 2017، ص: 280.

[2]- نصيرة بوحزمة، المرجع السابق، ص: 378.

[3]- البريد الإلكتروني: "هو نظام لتبادل الرسائل والصور وغيرها من المواد القابلة للإدخال الرقمي في صندوق الرسالة أو القابلة للتحميل الرقمي بصفتها ملحقات بالرسالة، كما يستخدم كمستودع خاص وشخصي للمستخدم، وهو محاط بحماية فنية"، زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى، الجزائر، 2011، ص: 159.

[4]- نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتي في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013، ص: 180.

[5]- عمر محمد بن يونس، أشهر المبادئ المتعلقة بالإنترنت في القضاء الأمريكي، دار النهضة العربية، القاهرة، 2004، ص: 582.

[6]- راجع المادة 47 من الدستور الجزائري.

وإذا كانت المراسلات التقنية والكلام المتفوه به بصورة سرية ليست سوى رسائل شفوية تنطبق عليها الحماية المقررة لحرمة الاتصالات المكفولة دستورا، فإنها أثارت جدلا كبيرا حول طبيعتها القانونية، إذ يرى جانب من الفقه بأنها تعتبر تفتيشا وتخضع لقيوده، واستند في ذلك إلى أن اعتراض المراسلات تهدف إلى البحث عن دليل الجريمة في مواطن السرَ، وهي نفس الغاية المتوخَاة من عملية التفتيش.[1]

في حين يرى جانب آخر بأن هذه العملية هي إجراء يهدف إلى الحصول على إقرار أو اعتراف غير قضائي، فهي صادرة بحرية صاحبها في غير مجلس القضاء، غير أنها تختلف عن الاعتراف القضائي فيما يتطلبه من ضرورة إحاطة المتهم علما بالتهمة الموجهة إليه، لذلك تعتبر إجراء من نوع خاص يماثل التفتيش، لكنه في الحقيقة مختلف عنه.[2]

ونميل بدورنا إلى الرأي الأخير، ومردّ ذلك أن إجراء التفتيش وإن كان يهدف إلى ضبط أدلة الجريمة –سواء المادية أو الرقمية– في مواطن السر، إلا أنه إجراء لاحق لارتكابها، في حين أن اعتراض المراسلات وتسجيل الأصوات والتقاط الصور هي عمليات مزامنة لها.

ثانيا: آلية تسجيل الأصوات: أجاز المشرع استراق السمع لأجل كشف غموض الجريمة وضبط الجناة عن طريق الاستعانة بتقنيات متطورة.

01- معنى تسجيل الأصوات: وهي النقل المباشر والآلي للموجات الصوتية من مصادرها، بنبراتها ومميزاتها الفردية وخواصها الذاتية بما تحمله من عيوب في النطق إلى شريط تسجيل يحفظ الإشارات الكهربائية على هيئة مخطط مغناطيسي، بحيث يمكن إعادة سماع الصوت والتعرف على مضمونه"،[3] أو هي: "حفظ الحديث على الأشرطة المخصصة لذلك لإعادة الاستماع إليه.[4]

[1]– رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجبل للطباعة، مصر، 1995، ص: 358.

[2]– عبد المهيمن بكر، إجراءات الأدلة الجنائية، ج 1، ط1، دار الفكر العربي، القاهرة، 1997، ص: 128.

[3]– سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة، الرياض، 2005، ص: 377.

[4]– محمود إبراهيم غازي، المرجع السابق، ص: 297

وبالرجوع إلى المادة 65 مكرر 5 ق إ ج نجد أنها أجازت وضع ترتيبات تقنية من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية دون موافقة المعنيين سواء كان ذلك في أماكن عمومية أو أماكن خاصة.

وتعد مراقبة المحادثات إجراء من نوع خاص يختلف عن باقي الأساليب، والدليل المستمد منها هو دليل علمي أو رقمي يحوز حجية في الإثبات متى كان مشروعا، ويجوز للمتهم أن يثبت عكسه.[1]

02- **تقنيات تسجيل الأصوات:** يلعب التطور العلمي دورا بالغ الأهمية في مجال مراقبة المكالمات الهاتفية، فهي عملية تشمل من جهة التصنَت على المكالمات أو الاستماع إليها خلسة، ويكون ذلك بالأذن وحدها دون الحاجة للاستعانة بأي جهاز أو أداة، وتشمل من جهة أخرى تسجيل الحديث على الأجهزة المخصصة لذلك قصد إعادة سماعه.[2]

ويتم التصنَت على المكالمات إما بصورة مباشرة أو غير مباشرة، إذ يتم التصنَت المباشر عن طريق الدخول على الخط المراد مراقبته بوضع سماعة يمكن توصيلها بسلك المشترك، وتعد هذه الطريقة من الطرق القديمة، التي يعيبها سهولة كشفها، بسبب التغييرات التي تطرأ على التيار حين يتداخل مع سلك المتصنَت، في حين يتم التصنَت غير المباشر بوضع سلك آخر بجانب سلك المشترك، بحيث يتداخل معه مغناطيسيا دون أن يتصل به، ويتم التقاط محادثته وتسجيلها.[3]

ومع انتشار الهواتف المحمولة طورت الشركات الألمانية نظاما يسمى (Schwarz Identity) يستطيع اصطياد جميع الإشارات الصادرة من الهواتف وقلبها إلى كلمات مسموعة، كما طوَرت جهازا إلكترونيا يمكنه استغلال مكبر الصوت الموجود على الهاتف لنقل جميع الأصوات.[4]

---

[1]- بهاء المري، المرجع السابق، ص: 747.

[2]- محمود ابراهيم غازي، المرجع السابق، ص: 297.

[3]- زين العابدين سليم، محمد ابراهيم زيد، الأساليب الحديثة في مكافحة الجريمة، المجلة العربية للدفاع الاجتماعي، العدد 15، 1983، ص: 110.

[4]- المرجع نفسه، ص: 51.

إن التطور التقني في مجال تكنولوجيات الإعلام والاتصال سمح بإنتاج أجهزة تصنَت على سرية الاتصالات الشخصية والمحادثات الهاتفية، وأصبح من الممكن اقتحام خلوة الإنسان وتجريده من كل أسراره وخصوصياته دون أن يشعر بشيء من ذلك.

ومن بين الإشكالات المطروحة في العمل القضائي، قيام بعض الأشخاص بتسجيل ما يدور بينهم من اتصالات تتضمن سبا أو قذفا أو تهديدا، أو تحرشا جنسيا، فيدفع المتهم ببطلان هذه التسجيلات التي تمت دون إذن من القضاء.

وفي هذا الصدد حسمت محكمة النقض المصرية النزاع، وقضت بأن ما يتطلب إذنا هو تسجيل الأحاديث التي لا يكون القائم بالتسجيل طرفا فيها، إذ ورد في قرارها: "إذا كان المشرع قد فرض وضع الهاتف تحت المراقبة في حالة دلائل قوية على أن مرتكب جريمة الإزعاج بالهاتف قد استعان في ارتكابها بجهاز هاتفي معين، فإن مفاد ذلك أن تلك الإجراءات فرضت لحماية الحياة الخاصة والأحاديث الشخصية للمتهم، ومن ثمَ لا تسري تلك الإجراءات على تسجيل ألفاظ الإزعاج أو المضايقة أو السب أو القذف من هاتف المجني عليه، الذي يكون له وحده بإرادته تسجيلها دون حاجة للحصول على إذن من رئيس المحكمة المختصة، وبغير أن يعتبر ذلك اعتداء على الحياة الخاصة، ومن ثم فلا جناح على المجني عليه إذا وضع على هاتفه الخاص جهاز تسجيل لضبط ألفاظ السباب أو الإزعاج الموجهة إليه توصلا إلى التعرف على الجاني".[1]

أما في الجزائر فإن القانون يعاقب كل من يتعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت، بما في ذلك التقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سرية بغير إذن صاحبها أو رضاه،[2] أي أن القانون يمنع تسجيل المكالمات الخاصة بغير إذن من السلطة القضائية، حتى ولو كان المجني عليه طرفا في المكالمة.

ونرى بدورنا أن جرائم المساس بشرف واعتبار الأشخاص باستغلال تكنولوجيات الإعلام والاتصال تفشت في المجتمع الافتراضي، وأصبحت خطرا يهدد سمعتهم، لذلك ندعو إلى مسايرة

[1]– بهاء المرَي، المرجع السابق، ص: 748–749.

[2]– راجع المادة 303 مكرر من قانون العقوبات المعدل والمتمم.

التشريع المصري في حصر التجريم على المكالمات الخاصة التي لا يكون المجني عليه طرفا فيها، باعتبار أن تسجيل الشخص لمكالمة يجريها مع شخص آخر لا يعد انتهاكا لخصوصية هذا الأخير متى تعدَت أقواله القانون، ووصلت حدود التجريم، وبذلك يتاح للضحية المجال للمشاركة في ضبط الدليل الرقمي، ويبقى للقضاء السلطة في تقدير هذا الدليل.

ثالثا: آلية التقاط الصور: لم يكتف المشرع بالسماح للمحقق بتسجيل الأصوات فحسب، بل مكّنه من مد عين الكاميرا إلى مواطن السر من أجل التقاط صور لشخص أو عدة أشخاص دون موافقتهم.[1]

01- معنى التقاط الصور: تعد عملية التقاط الصور استثناء على المبدأ العام الذي يمنع التقاط الصورة خلسة، باعتباره اعتداء على حرمة الحياة الخاصة للأفراد، ومع ذلك أجازه المشرع من أجل استبيان الجريمة وفك ملابساتها، لأن وصف الجريمة وقت ارتكابها مهما بلغت دقته لا يرقى إلى الدور الذي تقدمه الصورة الفوتوغرافية.

وقد عرَف القضاء الفرنسي هذه العملية بأنها: "وضع أجهزة تصوير صغيرة الحجم وإخفائها في أماكن خاصة لالتقاط صور تفيد في إجلاء الحقيقة وتسجيلها"،[2] فهي لا تعدو أن تكون مجرد معاينة مرئية لحالة الأشخاص على الوضعية التي كانوا عليها وقت التصوير، لتربط بذلك الزمان والمكان والأشخاص في وقت واحد.

02- تقنيات التقاط الصور: تقوم عملية التقاط الصور أساسا على استخدام الكاميرا أو أجهزة خاصة لالتقاط صورة للمشتبه فيه على الحالة التي كان عليها وقت التصوير، بغرض استخدام هذه الصورة كدليل مادي، باعتبار أن عدسة الكاميرا أصبحت من الأساليب العالمية المطلوبة لإثبات الحالة بما تنقله من صور حية وكاملة لمكان أو حدث أو واقعة معينة،[3] ومع التطور العلمي

---

[1]- راجع المادة 65 مكرر 5 ق إ ج.

[2]- عبد القادر مصطفاوي، أساليب البحث والتحري الخاصة وإجراءاتها، مجلة المحكمة العليا، العدد الثاني، الجزائر، 2009، ص: 71.

[3]- فوزي عمارة، اعتراض المراسلات وتسجيل الأصوات والتقاط الصور كإجراء تحقيق قضائي في المواد الجزائية، مرجع سابق، ص: 238.

ظهرت وسائل ذات جودة عالية تستطيع التقاط صور الأشخاص حتى في جنح الظلام بدقة ووضوح، وبشكل لا يجلب الانتباه.

وقد شاع في الوقت الراهن وضع كاميرات للمراقبة، سواء من طرف الأفراد أو المؤسسات وحدث في العديد من المرات أن عاينت مثل هذه الكاميرات وقوع جرائم واحتفظت بتسجيلاتها، مما يثير التساؤل على مدى مشروعية الصور الملتقطة؟ وحجيتها أمام القضاء؟

ذهب رأي من الفقه إلى القول أن استخدام هذه الأجهزة لا يثير أي اعتراضات بالنسبة لاحترام حريات الأفراد، وحجتهم في ذلك أن الصفة غير الاجتماعية للأعمال التي ترتكب لا يجب أن تجعل المتهم يتفاجأ حين يكتشف،[1] إلا أنهم يدعون إلى الإعلان عن استخدام هذه الوسائل قبل البدء بالعمل بها، فالتحذير أكثر فاعلية من القمع.[2]

في حين عارض جانب آخر استخدام هذه الأجهزة، وذهب إلى القول بأن العدالة لا تكون جديرة بهذا الاسم ما لم تكرس جميع الضمانات، وألا تحرم الإنسان من كرامته، ودعا إلى التصدي لهذه الوسائل بحزم.[3]

وفي هذا الصدد قضت محكمة تولوز الفرنسية في 26-02-1974 بأن جريمة انتهاك حرمة الحياة الخاصة المعاقب عنها بالمادة 368 من قانون العقوبات القديم، لا تنطبق في حالة تصوير أحد الأزواج في مكان عام.[4]

وفي الجزائر، ميَز المشرع الجزائري بين حالتين، الحالة التي تلتقط فيها صورة الشخص في مكان خاص بغير إذنه وبغير رضاه، وخصَها بالتجريم،[5] لذلك يمنع التقاط صور الأشخاص في أماكن خاصة دون إذن منهم أو من السلطة القضائية، تحت طائلة التجريم والعقاب.

[1] - Levasseur, les méthodes scientifiques de recherche de la vérité colloque d'abidijan 10-16, paris 1972, p: 345.

[2] – محمد أمين الخرشة، المرجع السابق، ص: 188.

[3] - Ancel, les problèmes poses par l'application des techniques scientifiques nouvelles au droit pénal et a la procédures pénal, rapport au journée franco-polonaises, 1960, p: 18.

[4] –محمد أمين الخرشة، المرجع نفسه، ص: 189-190.

[5] – راجع المادة 303 مكرر من قانون العقوبات.

أما التقاط الصور في الأماكن العمومية والأماكن المفتوحة للجمهور، فنرى أنها غير مقيدة بالإذن، ويستشف ذلك من عدم اشتراطه صراحة، كما هو الشأن بالنسبة للحالة السابقة، وعدم تجريم الفعل حال ارتكابه، إذ غلب المشرع في هذه الحالة المصلحة العامة للمجتمع في ضبط الدليل محاربة للجريمة، على مصلحة الأفراد في حرمة حياتهم الخاصة، لاسيما وأن هذه الخصوصية تتضاءل في الأماكن العامة، ومع ذلك ندعو إلى ضرورة الإعلام باستخدام هذه التقنية، لأنه من السياسة الحكيمة أن نجعل المتهم يسلك الطريق السليم خير من أن ينغمس في الفساد.

ويبقى للقاضي السلطة في تقدير الدليل المستمد من هذه العدسات وفقا لمبدأ اقتناعه الحر، فله أن يأخذ بها كدليل متى اطمأن إلى عدم العبث به أو أقر به المتهم، وله أن يستبعده متى راوده شك في عدم صحته أو عدم وضوحه، كما له أن يستعين بأهل الخبرة والاختصاص لفكَ ملابساته.

الفرع الثاني: الضوابط القانونية لاعتراض المراسلات وتسجيل الأصوات والتقاط الصور

حرص المشرع على إحاطة هذه العمليات ببعض الضوابط القانونية، نظرا لما تحمله من تهديد لحياة الأفراد الخاصة، وذلك بهدف تحقيق نوع من التوازن بين حق المجتمع في كشف الجريمة، وحق الفرد في صون خصوصيته، وتتمثل هذه الضوابط في:

01- حصر نطاق هذه الآليات: حدَد القانون الجرائم التي يمكن فيها استخدام آليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من خلال المادة 65 مكرر 5 ق إ ج، وهي: (جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبييض الأموال، جرائم الإرهاب، الجرائم الخاصة بالتشريع الخاص بالصرف وجرائم الفساد)، لكن وبعد انتشار الجرائم الإلكترونية الخطيرة، وسَع القانون من نطاقها لتشمل جرائم أخرى أخطر منها مثل: جرائم عصابات الأحياء، جرائم خطاب الكراهية، جرائم اختطاف الأشخاص، جرائم إفشاء المعلومات والوثائق الإدارية، جرائم الاتجار بالبشر ومكافحته، جرائم التزوير واستعمال المزور.

وما يلاحظ على التشريع الجزائري أنه لم يحصر الأماكن التي تتم فيها عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بل تركت على إطلاقها، إذ نصت المادة 65 مكرر 5 ق إ ج: "... في أماكن عمومية أو خاصة..."، لتسمح بذلك بالدخول إلى أي مكان من أجل وضع الترتيبات اللازمة لإنجاز العملية، فقد يكون المحل منزلا أو مقهى للإنترنت أو مقر شركة أو غيرها، كما خرج المشرع أيضا على قاعدة الآجال المنصوص عليها في المادة 47 ق إ ج،[1] كل ذلك من أجل نجاح هذه العمليات.

02- الإذن القضائي: تكريسا للمادة 47 من الدستور الجزائري، لا يمكن لضابط الشرطة القضائية مباشرة هذه الإجراءات إلا بعد حصوله على إذن من القضاء، يختص وكيل الجمهورية بمنحه خلال مرحلة التحريات الأولية،[2] وقاضي التحقيق خلال مرحلة التحقيق القضائي.[3]

وفي هذا الصدد، يرى الأستاذ أوهايبية عبد الله أن هذه العمليات تشكل خطرا على الحقوق والحريات خلال مرحلة البحث والتحري، لذلك يتعين ترك هذا الاختصاص لقاضي التحقيق، وسحبه من وكيل الجمهورية، ويبقى لهذا الأخير متى رأى ضرورة لاستخدام هذه التقنيات إحالة الملف إلى التحقيق القضائي، ثم تقديم طلباته أمام قاضي التحقيق.[4]

ولصحة الإذن الخاص بهذه العمليات، يجب تضمينه جميع العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها، كتحديد رقم الهاتف واسم المشترك، وتحديد الأماكن المقصودة بدقة، ونوع الجريمة التي تبرر اللجوء إلى هذا التدبير.[5]

03- تنفيذ العملية من طرف ضابط شرطة قضائية: نظرا لخطورة عمليات اعتراض المراسلات وتسجيل الأصوات والتقاط الصور على حريات الأشخاص وحرمة حياتهم الخاصة، فقد أناط

---

[1]- راجع المادة 47 ق إ ج.

[2]- راجع الفقرة 05 من المادة 65 مكرر 5 ق إ ج.

[3]- راجع الفقرة 05 من المادة 65 مكرر 5 ق إ ج.

[4]- عبد الله اوهايبية، شرح قانون الإجراءات الجزائية، مرجع سابق، ص: 333.

[5]- راجع المادة 65 مكرر 7 ف 01.

المشرع مهمة تنفيذها إلى ضابط شرطة قضائية،[1] الذي يمكنه بدوره تسخير أي عون مؤهل لدى هيئة مكلفة بالمواصلات السلكية واللاسلكية للتكفل بالجوانب التقنية لهذه العمليات.[2]

04- حصر المدة الزمنية: من الضوابط اللازمة لمشروعية هذه العمليات وجوب تضمين الإذن القضائي المدة اللاَزمة لتنفيذه، والمحددة بأربعة أشهر قابلة للتجديد وفقا لمقتضيات التحقيق، وبنفس الشروط التي صدر بها الأمر الأصلي،[3] غير أن ذلك لا يمنع القاضي الذي منح الإذن من توقيف العملية إذا لم تكن هناك ضرورة لاستمرارها.

05- تحرير تقرير عن العملية: بعد الانتهاء من عملية اعتراض المراسلات أو تسجيل الأصوات أو التقاط الصور، يحرر ضابط الشرطة القضائية محضرا يتضمن الترتيبات التقنية التي تم إعدادها، وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري، مع ذكر تاريخ وساعة بداية هذه العمليات وانتهائها،[4] ويمكن ترجمة المراسلات التي تتم باللغات الأجنبية، ويسجل كل ذلك في محضر يودع بملف القضية.[5]

06- كتمان السر المهني: من بين الضمانات المقررة كذلك وجوب التزام الأشخاص المكلفين بتنفيذ هذه العمليات بكتمان السر المهني،[6] فلا يجوز لهم الكشف عن المعلومات التي تحصلوا

[1]- راجع المواد 65 مكرر 8، 65 مكرر 9، 65 مكرر 10 ق إ ج.
[2]- راجع المادة 65 مكرر 8 ق إ ج.
[3]- راجع المادة 65 مكرر 7 ق إ ج.
[4]- راجع المادة 65 مكرر 09 ق إ ج
[5]- راجع المادة 65 مكرر 10 ق إ ج.
[6]- راجع المادة 65 مكرر 06 ق إ ج.

عليها إلاّ في إطار التحقيق، وذلك صونا لحريات الأشخاص من جهة، وتحقيقا للسير الحسن للعدالة من جهة أخرى.

إن أساليب التحري الخاصة وعلى قدر أهميتها فيما توفره من أدلة مستمدة من أجهزة الاتصالات السلكية واللاسلكية، ورغم نجاعتها في كشف ملابسات الجريمة الإلكترونية، إلا أنها تبقى أحد الإجراءات الخطيرة، كونها تنتهك حرمة الحياة الخاصة للأفراد وحرية مراسلاتهم، لذلك ينبغي التعامل معها بحذر شديد، وعدم الإفراط في استعمالها، والالتزام بضوابطها القانونية، وبذلك يمكن تحقيق موازنة بين حق المجتمع في مكافحة الجريمة وحق الفرد في صون حرياته الخاصة.

المبحث الثاني

المساعدة القضائية

إذا كان الوصول إلى الأدلة المادية سهل المنال، فإن الأمر مختلف حين يتعلق بالبحث عن أدلة رقمية وسط بيئة افتراضية، مما يستدعي تقديم المساعدة لجهاز التحقيق لبلوغ غايته المنشودة، وذلك باتخاذ تدابير احترازية للمحافظة على البيانات الإلكترونية المخزنة إلى غاية تقديمها أمامه، وهو التزام وضعه المشرع على عاتق مقدمي الخدمات.

ويزداد الأمر صعوبة عند تجاوز هذه البيانات لحدود الدولة، مما يتطلب مساعدة الدول التي امتدت إليها آثار الجريمة، وهو التزام دعت إليه جلَ الاتفاقيات الدولية.

ورغم اختلاف التشريعات، إلا أنها لا تكاد تخلو من عقبات تعترض مسار التحقيق، ويرجع ذلك أساسا إلى التطور المستمر لتكنولوجيات الإعلام والاتصال، وتأثيرها المباشر على تطور الجريمة الإلكترونية، مما ينبغي تشخيص هذه العقبات، بحثا عن حلول كفيلة بعلاجها.

وحتى نغطي هذه النقاط بالدراسة والتحليل، ارتأينا تقسيم هذا المبحث إلى المطلبين الآتيين:

المطلب الأول: أساليب المساعدة القضائية.

المطلب الثالث: عقبات التحقيق وسبل علاجها.

المطلب الأول

أساليب المساعدة القضائية

أدى تشعب الأدلة الرقمية عبر دول وقارات مختلفة إلى خلق صعوبات للجهة المكلفة بالتحري عن الجريمة الإلكترونية، مما جعلها تقف عاجزة عن تتبَعها، لذا دعت جلَ الاتفاقيات الدولية إلى مساعدتها على جمع أدلتها الرقمية، سواء كانت داخل إقليم الدولة أم خارجه.

الفرع الأول: مساعدة مقدمي الخدمات

قبل مباشرة التحقيق في الجريمة الإلكترونية يتطلب الأمر أحيانا اتخاذ بعض الإجراءات الوقائية من أجل المحافظة على البيانات الإلكترونية المخزنة وحمايتها من التلف أو التعديل، ويكون ذلك بإلزام مقدمي الخدمات بالتحفظ عليها إلى غاية إلى تقديمها أمام السلطات المكلفة بالتحريات القضائية، التي تستعين بها في تتبع مسار المجرم الإلكتروني.

الفقرة الأولى: مفهوم مقدمي الخدمات

تمت الإشارة إلى هذا الإجراء لأول مرة في لائحة الجمعية العامة لمنظمة الأمم المتحدة رقم 65-63 المؤرخة في 22-01-2001 المتعلقة بمكافحة إساءة استخدام تكنولوجيا المعلومات لأغراض إجرامية، إذ نصت في مادتها الأولى على ضرورة سماح الدول الأعضاء لجهاتها المكلفة بجمع الاستدلالات بأمر مزودي خدمات الاتصال بالحفظ السريع للمعطيات الإلكترونية المتعلقة بالتحقيقات الجنائية،[1] كما كرسته (ا أ م ج إ) في المواد د 16 و 17 و (ا ع م ج ت م) في مادتها 23.

وفي الجزائر، أتاح القانون رقم 09-04 للسلطة القضائية فرض التزامات على مقدمي الخدمات،[2] ثم عمّم هذا الإجراء في العديد من القوانين الخاصة، على غرار قانون الوقاية من التمييز وخطاب الكراهية ومكافحتهما،[3] القانون المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها ،[4] قانون حماية المعلومات والوثائق الإدارية ،[5] قانون الوقاية من الاتجار بالبشر ومكافحته،[6] قانون مكافحة التزوير واستعمال المزور.[7]

[1] -Bossan Jérome "le droit pénal confronté a la diversité des intermédiaires de l'internet", édition Dalloz, 2013, p: 302.

[2]- راجع المادة 10 من القانون 09-04.

[3]- راجع المادة 23 من القانون رقم 20-05 المتعلق بالوقاية من التمييز وخطاب الكراهية.

[4]- راجع المادة 15 من القانون رقم 20-15 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها.

[5]- راجع المادة 23 من الأمر 21-09 المتعلق بحماية المعلومات والوثائق الإدارية.

[6]-راجع المادة 31 من قانون رقم 23-04 المتعلق بالوقاية من الاتجار بالبشر ومكافحته.

[7]- راجع المادة 16 من القانون رقم 24-02 المتعلق بمكافحة التزوير واستعمال المزور.

أولا: تعريف مقدمي الخدمات: إن مزود خدمة الإنترنت (ISP) هو اختصار لكلمة (Internet Service Provider)، ويعني "الشركة التي توفر شبكة الإنترنت لعملائها"،[1] فمزود الخدمة هو الشخص الذي يقدم خدمة الاتصال، أو خدمة معالجة البيانات، أو خدمة تخزين البيانات، أو خدمة الاستضافة أو التخزين المؤقت أو الربط بالشبكات"،[2] في حين عرف المشرع الجزائري مقدمي الخدمات بأنهم: "أي كيان عام أو خاص يقدم لمستعملي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية، و/أو نظام للاتصالات، وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها".[3]

ثانيا: تصنيف مقدمي الخدمات: يمكن تصنيفهم حسب الخدمات التي يقدمونها إلى صنفين رئيسيين:

01- مقدم خدمة التوصيل (متعهد الوصول): وهو كل شخص طبيعي أو معنوي يقدم للعملاء خدمة الوصول إلى الإنترنت، حيث يقوم بتزويد العميل بمقتضى عقد اشتراك بالوسائل الفنية التي تمكنه من الوصول إلى الارتباط بالشبكة، والاطلاع على المواقع التي يريدها، فمهمته ذات طابع فني بحت يتمثل في توصيل المستخدم بالشبكة العنكبوتية.[4]

يخضع مقدمو الخدمات في أنشطتهم إلى دفتر شروط محدد من قبل سلطة الضبط للبريد والمواصلات، إذ توجد ثلاث شركات كبرى تهيمن على قطاع الاتصالات في الجزائر هي:

أ- **شركة اتصالات الجزائر:** وهي الشركة المالكة لشبكة موبيليس، تعمل على تقديم خدمات الاتصالات الهاتفية الثابتة والمحمولة، وتعد بمثابة الشركة الأم.

---

[1]- عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، المركز القومي للإصدارات القانونية، ط1، 2001، القاهرة، ص: 92.

[2]- أحمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، مصر، 2006، ص: 48.

[3]- راجع من خلال المادة 02-د من القانون 09-04

[4]- عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2003، ص: 126.

ب- شركة جيزي: وتعد شركة أوراسكوم تيليكوم أول شركة تقدم خدمات الهاتف المحمول بعد حصولها على رخصة تشغيله، وفي عام 2010 تقدمت الحكومة الجزائرية لشراء حصة 51% من أسهم الشركة، ليعلن الصندوق الوطني للاستثمار بتاريخ: 01-07-2022 عن شراء حصة فيمبلكوم الروسية، مما جعل الشبكة مملوكة بالكامل للدولة الجزائرية.

ت- **شركة أوريدو:** وهي شركة اتصالات قطرية، تقدم بدورها خدمات الهاتف المحمول، كانت تسمى سابقا بشركة نجمة.

02- متعهد الإيواء: وهو كل شخص طبيعي أو معنوي يعهد إليه بعرض صفحات شبكة الإنترنت على حاسباته الخادمة، وكأن المؤجر هو متعهد الإيواء، ومحل التأجير هو الموقع على شبكة الإنترنت، والمستأجر هو المستخدم الذي ينشئ ما يريده من نصوص أو صور أو تنظيم مؤتمرات للمناقشة، أو إنشاء روابط معلوماتية مع المواقع الأخرى.[1]

وتجدر الإشارة إلى أن سلطة ضبط البريد والمواصلات السلكية واللاسلكية منحت تراخيص لعدد كبير من مزودي خدمة الإنترنت لتغطية الطلب المتزايد على خدماتها، وبذلك تسهل للمستخدم الولوج إليها، وتمكن مزود الخدمة من تتبع جميع خطواته.[2]

الفقرة الثانية: التزامات مقدمي الخدمات والقيود الواردة عليهم

يلعب مقدمو الخدمات دورا لا يستهان به في مساعدة السلطات القضائية خلال تحريها عن الجريمة من خلال تتبعهم لمسار المجرم الإلكتروني، وصولا إلى تحديد هويته، وهو ما جعل أغلب التشريعات تعتمد هذه الآلية.

أولا: التزامات مقدمي الخدمات: ويمكن تقسيمها على ضوء القانون رقم 09-04 إلى:

[1]- محمد بعجي، التزامات مقدمي الخدمة عبر الانترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 01، العدد 01، 2019، ص: 37

[2]- يزيد بوحليط، المرجع نفسه، ص: 325.

01- التزامات عامة: إذا كان دور مقدم خدمة الإنترنت هو تمكين مستخدمها من الدخول إلى الشبكة، فإنه يستطيع مراقبة جميع الخطوات التي قام بها، والمواقع التي زارها، والمعلومات التي خزَنها، والاتصالات التي أجراها،[1] وبناء على ذلك يمكنه تحديد مصدر الإرسال، وعلى ضوئه تحدد هوية المجرم الإلكتروني،[2] لذلك يتعين على مقدمي الخدمات تقديم المساعدة لجهاز التحري من خلال:

أ- **التعجيل في حفظ المعطيات المتعلقة بحركة السير:** وذلك بالإسراع في جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات التي تسمح بالتعرف على مستعملي الخدمة، أو تلك المتعلقة بالتجهيزات المستعملة في الاتصال، وتاريخ وزمن ومدة كل اتصال، والمعطيات المتصلة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها، إضافة إلى المعلومات التي تسمح بالتعرف على المرسل إليه، وعناوين المواقع التي اطلع عليها وغيرها،[3] وقد تبنى المشرع الجزائري هذه الآلية من خلال المواد: 10 و 11 و 12 من القانون 09-04.

وينبغي التنويه بأن عملية الحفظ لا تمتد إلى جميع المعطيات الإلكترونية، وإنما تخص فقط معطيات حركة السير،[4] أو كما يسميها البعض بمعطيات المرور، والتي حصرتها المادة 11 من القانون رقم 09-04 في:

* المعطيات التي تسمح بالتعرف على مستعملي خدمة الإنترنت.

* المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال.

---

[1]- وسيمة مصطفى هنشور، النظام القانوني لمقدمي خدمات الإنترنت في التشريع الجزائري، مجلة البحوث القانونية والسياسية، العدد 05، ديسمبر 2015، ص: 113

[2]- تنص المادة 10 من القانون 09-04 على أنه :"في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها، وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه تحت تصرف السلطات المذكورة".

[3]- يزيد بوحليط، المرجع السابق، ص: 321

[4]- عرفت المادة 02 فقره هـ من القانون رقم 09-04 المعطيات المتعلقة بحركة السير بأنها: "أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزءا في حلقة اتصالات، توضح مصدر الاتصال، والجهة المرسل إليها، والطريق الذي يسلكه، ووقت وتاريخ وحجم ومدة الاتصال، ونوع الخدمة".

* الخصائص التقنية، وكذا تاريخ ووقت ومدة كل اتصال.

* المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها.

* المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال، وكذا عناوين المواقع المطلع عليها.

وإذا كان من السهل تحديد معطيات حركة السير المرتبطة بمقدم خدمة وحيد، فإن الأمر مختلف عندما يرتبط المستخدم بأكثر من مقدم خدمة، ويحتفظ كل واحد منهم بجزء من معطيات المرور، مما يجعل تحديد مصدر الاتصال ومنتهاه في غاية الصعوبة، لذلك يتم الحفظ العاجل لهذه المعطيات من طرف جميع مقدمي الخدمات، سواء بأمر منفصل لكل واحد منهم، أو بأمر واحد يشملهم جميعا.[1]

ب- التعجيل في الكشف عن المعطيات المتعلقة بحركة السير: كما تلزم سلطة التحقيق مقدمي الخدمات بالحفظ العاجل للمعطيات المتعلقة بحركة السير، فإنها تلزمهم كذلك بالإسراع بإفشاء هذه المعطيات لسلطات التحرّي، حتى يمكن استغلالها في تحديد مقدم الخدمة، والمسار الذي سلكه المجرم الإلكتروني في اتصالاته، وهي المعلومات التي تساعد في تحديد هوية المساهمين في الجريمة، لذلك يعتبر هذه الإجراء مكملا لإجراء الحفظ العاجل للمعطيات، وبدونه تبقى المعطيات المحفوظة دون فائدة.

أشار المشرع لهذا الإجراء من خلال المادة 10 من القانون رقم 09-04 بقوله: "وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 تحت تصرف السلطات المذكورة".

تهدف عمليتي الحفظ والإفشاء العاجل لمعطيات حركة السير إلى حمايتها من كل ما يمكن أن يتسبب في إتلافها أو تجريدها من صفتها أو حالتها الأصلية، مع الاحتفاظ بها لمقتضيات التحقيق في المستقبل، فقد تكون محلا للتفتيش أو الحجز، كما أنها ستشكل بنكا للمعلومات التي

[1]- أحمد هلالي عبد اللاّه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، مرجع سابق، ص: 208.

يمكن الرجوع إليها عند الحاجة، باعتبار أنه يصعب على المجرم الإلكتروني من الناحية الفنية اختراق هذه الأنظمة لمحو المعطيات المتعلقة باتصالاته.[1]

02- التزامات خاصة: يعدَ مقدم خدمة الإيواء من بين مقدمي خدمة الإنترنت، بل ويعتبر أهم الأشخاص الذين يمكنهم الاطلاع على المحتوى المخالف للقوانين الجزائية وللنظام العام والآداب العامة، ورغم أن المادة 12 من القانون رقم 09-04 لم تذكر مقدم خدمة الإيواء بنفس اللفظ، إلا أنه ورد بها: "زيادة على الالتزامات المنصوص عليها في المادة 11 يتعين على مقدمي خدمة الإنترنت ..."، وهي إشارة لمقدمي خدمة الإيواء،[2] الذين يتعين عليهم:

أ- التدخل الفوري لسحب المحتوى المعلوماتي المجرم: يتعين على مقدمي خدمة الإنترنت بمجرد علمهم بوجود محتوى غير مشروع أن يقوموا بسحبه وتخزينه،[3] على غرار المحتويات المتضمنة للممارسات الإباحية ضد الأطفال، أو الفيروسات والبرامج الضارة بالمعطيات، أو تزوير البطاقات البنكية، أو جرائم الاحتيال وغيرها.

ويتحقق علم مقدمي خدمة الإنترنت بعدم مشروعية المحتوى عن طريق إعذارهم من طرف الهيئة، أو بعد إخطارهم بالصفة الجرمية لهذا النشاط بموجب أمر أو حكم قضائي، وكل إخلال بهذا الالتزام يعرض مقدم الخدمة للمسائلة الجزائية.[4]

ب- وضع ترتيبات تقنية لمنع وصول الجمهور إلى الأنشطة المعلوماتية المجرمة: يتعين على متعهدي إيواء المواقع الإلكترونية حظر الدخول إلى مواقع الإنترنت والموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة، وذلك بوضع ترتيبات تقنية تمنع الوصول إليها، مع ضرورة إخطار المشتركين بذلك.[5]

---

[1]- يزيد بوحليط، المرجع السابق، ص: 323.

[2]- محمد بعجي، المرجع السابق، ص: 28.

[3]- راجع المادة 12 من القانون رقم 09-04.

[4]- راجع المادة 394 مكرر 08 ق ع.

[5]- راجع المادة 12 فقرة ب من القانون رقم 09-04.

وقد سبق النص على هذا الالتزام من خلال المادة 14 من المرسوم التنفيذي 98-257 (المعدل بالمرسوم التنفيذي 2000-307).[1]

ثانيا: القيود الواردة على مقدمي الخدمات: يقوم مقدمو الخدمات بدور فني بحت يتمثل في توصيل الزبون بشبكة الإنترنت، ولا علاقة لهم بمحتوى المادة التي ينشرها الزبون، لذلك ينبغي عليهم مراعاة الحدود والضمانات القانونية التي تكفل حقوق وحريات العملاء، وهي:

01- الإذن القضائي: حددت المواد 10، 11، 12 من القانون رقم 09-04 التزامات مقدمي الخدمات، وأحالت المادة 03 من ذات القانون بخصوص إجراءات تنفيذها إلى القواعد العامة الواردة في ق إ ج،[2] والتي تقتضي ضرورة الحصول على أمر مكتوب من الجهة القضائية المختصة كما سبق توضيحه في الإجراءات السابقة (وكيل الجمهورية خلال مرحلة التحريات الأولية، وقاضي التحقيق خلال مرحلة التحقيق الابتدائي).

ب- حصر مدة حفظ المعطيات: حصر المشرع المدة التي لا يمكن أن تتعداها عملية حفظ المعطيات المتعلقة بحركة السير بسنة من تاريخ تسجيلها،[3] وهي مدة تتجاوز المدة التي حددتها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات بـ 90 يوما قابلة للتجديد، ونرى بأنها مدة معقولة وكافية لإتمام التحريات.

ت- الالتزام بسرية العمليات ونتائجها: يقع على عاتق مقدمي الخدمات الالتزام بسرية العمليات التي ينجزونها والمعلومات التي يتوصلون إليها، سواء خلال عملية الحفظ أو بعدها، وذلك تحت طائلة العقوبات المقررة قانونا،[4] والحكمة من ذلك هي الحفاظ على السير الحسن للتحقيق، وصون حقوق الأفراد وحرياتهم الشخصية.

---

[1]- عادل بوزيدة، المسؤولية الجزائية لمتعهدي مواقع الإنترنت، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة تبسة، الجزائر، 2017، ص: 28.

[2]- راجع المادة 03 من القانون 09-04 .

[3]- راجع المادة 11 من القانون رقم 09-04.

[4]- راجع المادة 10 من القانون 09-04.

غير أنه بالرجوع إلى الواقع العملي نلاحظ عدم التزام مقدمي الخدمات بواجباتهم المهنية خصوصا ما تعلق بحجب المواقع التي تحتوي على معلومات مخالفة للنظام العام أو الآداب العامة، كما نلاحظ انتشار مقاهي الإنترنت التي توفر الخلوة لمستعمليها، لاسيما المراهقين منهم بعيدا عن مراقبة الأهل، وتخزن المواقع الإباحية سعيا منها لتحقيق الربح، بل ويجتهد بعضهم بتجهيز محلاتهم بالأضواء الخافتة، ووضع الحواجز بين الزبائن لتحقيق الخلوة، وهو ما يوفر المناخ المناسب لارتكاب الجريمة الإلكترونية.

الفرع الثاني: المساعدة القضائية الدولية

أقرَت العديد من الاتفاقيات الدولية نظام المساعدة القضائية الدولية كآلية لجمع أدلة الجريمة، على غرار اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، والاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، و الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، كما كرس المشرع الجزائري بدوره هذه الآلية من خلال ق إ ج والقانون رقم 09-04.

أولا: صور المساعدة القضائية الدولية

تعرف المساعدة القضائية الدولية بأنها: "قيام سلطة قضائية مختصة تابعة لدولة أجنبية باتخاذ إجراء أو أكثر من إجراءات التحقيق لحساب سلطة قضائية مختصة تابعة لدولة أخرى، من أجل الوصول إلى كشف الحقيقة في قضايا جزائية"،[1] وتأخذ المساعدة في مجال البحث عن الجريمة الإلكترونية عدة صور، أهمها:

01- تبادل المعلومات: يسهل تقاسم المعلومات المتعلقة بالجريمة الإلكترونية بين الدول مهمة السلطات الوطنية في التحرك المناسب لمواجهتها، وتبرز أهمية ذلك حين يلجأ مرتكبو الجريمة إلى التواري خلف شبكة الإنترنت عبر شخصيات وهمية، ويتبادلون نشاطهم الإجرامي عبر أكثر من دولة، وهو ما يتطلب تعاونا بين الدول التي تطالها الجريمة بغرض التعرف عليهم، وتحديد أماكن تواجدهم.

[1]- علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، (دكتوراه في الحقوق)، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، 2011، ص: 296.

ويقدم طلب المساعدة القضائية عموما من أجل الحصول على أي إعانة مفيدة في الكشف عن الجريمة وضبط مرتكبيها، مثل جمع الأقوال والشهادات، أو تحديد أماكن تواجد الأشخاص وتحديد هوياتهم، أو لتنفيذ عمليات التفتيش والحجز والتجميد، أو لفحص الأشياء والمواقع، أو لتقديم المعلومات والأدلة والتقييمات التي يقوم بها الخبراء، أو لتقديم أصول المستندات والسجلات ذات الصلة أو نسخ منها، أو لتبليغ المستندات القضائية، بشرط ألاّ يتعارض ذلك مع القانون الداخلي للدولة المطلوب منها،[1] وقد يمتد إلى السوابق القضائية للجناة.[2]

وقد دعت (ا ع م ج ت م) الدول الأطراف إلى مساعدة بعضهم من أجل القيام بالتحقيقات أو المتابعات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة الإلكترونية من خلال المواد 32 و 33، كما شجَعتهم على إرسال المعلومات التي يتم الحصول عليها من أي دولة طرف إلى دولة أخرى حتى ولو لم تطلبها، متى تبين لها أن حصول هذه الأخيرة على المعلومات المقدمة سيساعدها على فتح تحقيقات في جرائم معلوماتية، أو يدفع بها إلى تقديم طلب للتعاون الدولي، بشرط المحافظة على سرية تلك المعلومات.

وعلى المستوى الوطني، أجاز المشرع الاستجابة لطلبات المساعدة القضائية الدولية الرامية إلى تبادل المعلومات، بما في ذلك الطلبات المقدمة عن طريق وسائل الاتصال السريعة، مثل أجهزة الفاكس أو البريد الإلكتروني، وأناط للهيئة مهمَة تنفيذ طلبات المساعدة الواردة من الجهات الأجنبية في إطار الاتفاقيات الدولية ذات الصلة والاتفاقيات الدولية الثنائية ومبدأ المعاملة بالمثل.[3]

02- اتخاذ إجراءات تحفظية: أتاحت المواد 37 و38 من (ا ع م ج ت م) لأعضائها تقديم طلب لأي دولة طرف بغرض الحفظ العاجل للمعلومات المخزنة ضمن إقليمها، أو الكشف العاجل عن معلومات تتبع المستخدمين المحفوظة، متى اكتشفت خلال تنفيذ طب المساعدة بأن مزود خدمة في دولة أخرى اشترك في بث الاتصال، وذلك لتمكينها من تحديد مزود الخدمة ومسار اتصالاته.

---

[1]- وهو ما كرسته المادة 18 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.

[2]- عادل عبد العال ابراهيم الخراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسلب التغلب عليها، دار الجامعة الجديدة، الإسكندرية، ص: 32

[3]- راجع المادة 04 الفقرة الأخيرة من المرسوم الرئاسي رقم: 21-439.

وقد كرَس المشرع الجزائري بدوره هذه الإجراءات من خلال القانون رقم 09-04،[1] وأتاح بالمقابل رفضها تفاديا لما يمكن أن تحمله البيانات الإلكترونية من معلومات تمس بالنظام العام للدولة أو بسيادتها الوطنية، كما أتاح تقديم المساعدة القضائية مع اشتراط المحافظة على سرَية المعلومات المقدمة، وذلك بعدم استعمالها خارج الغرض الذي سلمت لأجله.[2]

03- الإنابة القضائية الدولية: وهي طلب تقدمه الدولة المحقَقة في الجريمة إلى دولة أخرى بغرض اتخاذ إجراء معين من إجراءات التحقيق، تعذر القيام به من طرف الدولة الطالبة"،[3] كتقديم طلب لإجراء تفتيش أو لسماع ضحية أو شاهد في غير البلد الذي تتم فيه إجراءات التحقيق.

وتهدف الإنابة القضائية الدولية إلى تسهيل الحصول على أدلة الجريمة الإلكترونية بتذليل العقبات الناتجة عن مبدأ احترام سيادة الدول،[4] نظَمها المشرع الجزائري بموجب أحكام الباب الثاني من الكتاب السابع ق إ ج (في المواد 721 و 722)، ونميز فيها بين حالتين:

أ- الإنابات القضائية الواردة من الخارج: في حالة المتابعات الجزائية في بلد أجنبي فإن الإنابات القضائية الصادرة من السلطة الأجنبية ترد إلى السلطات الجزائرية عبر الطريق الدبلوماسي، ولدى وصولها لوزارة الخارجية تقوم بتحويلها إلى وزارة العدل، التي ترسلها بدورها إلى قضاة التحقيق المختصين لتنفيذها عن طريق النيابة العامة.[5]

ب- الإنابة القضائية الصادرة إلى الخارج: وترسل بدورها من طرف قاضي التحقيق الجزائري عن طريق السلم الإداري إلى وزير العدل، الذي يرسلها بدوره إلى وزارة الخارجية الجزائرية، لتقوم بتبليغها إلى السلطات القضائية الأجنبية من أجل تنفيذها.[6]

---

[1]- راجع المادة 17 من القانون رقم 09-04.

[2]- راجع المادة 18 من القانون رقم 09-04.

[3]- جميل عبد الباقي الصغير، الأحكام الموضوعية للجرائم المتعلقة بالإنترنت، مرجع سابق، ص: 88.

[4]- ليلى عصماني، صهيب سهيل غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، مجلة القانون المجتمع والسلطة، المجلد 09، العدد 02، 2020، ص 23

[5]- راجع المادة 721 ق إ ج.

[6]- محمد حزيط، المرجع السابق، ص: 130.

وباعتبار أن عامل السرعة مسألة مهمة خلال رحلة التحري عن الجريمة، فقد أبرمت العديد من الاتفاقيات الدولية التي ساهمت في اختصار الوقت عن طريق الاتصال المباشر بين سلطات التحقيق، مثال ذلك ما كرسته المادة 15 من اتفاقية الرياض العربية للتعاون القضائي لسنة 1983، والمادة 46 من اتفاقية الأمم المتحدة لمكافحة الفساد،[1] كما سعت الجزائر بدورها إلى إبرام العديد من الاتفاقيات الثنائية في مجال التعاون الجزائي، على غرار الاتفاقية المبرمة مع إيطاليا سنة 2005،[2] والاتفاقية المبرمة مع جمهورية الصين الشعبية سنة 2007.[3]

04- نقل الإجراءات: وهو أن تقوم دولة معينة استنادا إلى اتفاقية أو معاهدة بمباشرة إجراءات الدعوى الجزائية (المتابعة، التحقيق، المحاكمة) على مستوى إقليمها، بخصوص جريمة ارتكبت في إقليم دولة أخرى، ولمصلحة هذه الأخيرة، متى توافر شرطين رئيسيين:

أ- التجريم المزدوج: ويقتضي به أن يكون الفعل المنسوب إلى الشخص يشكل جريمة في الدولة الطالبة، والدولة المطلوب نقل الإجراءات إليها.[4]

وللتخفيف من شروط استيفاء التجريم المزدوج، وتعزيزا للتعاون الدولي عمدت غالبية الدول إلى تذليل عقبة التجريم، فلم تعد تعتد بما يوجد في تشريعاتها الداخلية من اختلاف في التكييف القانوني، وبالمقابل قد يتخلف تحقق هذا الشرط حال تخلف دولة عن تحديث تشريعاتها العقابية بما يتناول الأشكال الجديدة من الجريمة مثل الجرائم الإلكترونية.[5]

---

[1]- يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، ص: 315

[2]- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجزائر وإيطاليا، المؤرخة في 13-02-2005، المصادق عليها بالمرسوم الرئاسي رقم 05-73، الصادر في الجريدة الرسمية لسنة 2005، العدد 13.

[3]- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجزائر وجمهورية الصين االشعبية، المؤرخة في 06-06-2007، المصادق عليها بالمرسوم الرئاسي رقم 07-175، الصادر في الجريدة الرسمية لسنة 2007، العدد 38.

[4]- سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، أطروحة دكتوراه، حقوق، جامعة عين شمس، 1997، ص: 427-428.

[5]- كمال بوبعاية، عبد اللطيف والي، الإشكالات التي تعترض تنسيق التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، مجلة الدراسات والبحوث القانونية، المجلد 06، العدد 01، 2021، ص: 95.

ب- شرعية الإجراءات المطلوب اتخاذها: أي أن تكون الإجراءات المطلوبة مقررة في قانون الدولة المطلوب منها، وأن تؤدي هذه الإجراءات دورا مهما في الوصول إلى الحقيقة. [1]

تم التنصيص على هذا الإجراء بموجب المادة 03 من الاتفاقية الأوروبية للمساعدة المتبادلة في القضايا الجنائية لعام 1959،[2] كما أقرته العديد من الاتفاقيات الدولية والإقليمية على غرار اتفاقية الأمم المتحدة النموذجية بخصوص نقل الإجراءات في المسائل الجنائية،[3] واتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية.[4]

وفي الجزائر، تقدمت وزارة العدل الأمريكية سنة 2009 بطلب إلى نظيرتها الجزائرية قصد مباشرة الإجراءات القانونية اللازمة، وذلك إثر تعرض المنظومة المعلوماتية لإحدى مؤسساتها الواقعة بولاية فلوريدا (SAGO NET WORKS) للاختراق، أين قام شخص بإرسال رسائل مجهولة عبر عناوين إلكترونية موزعة بالجزائر، مستعملا في ذلك شبكة انترنت تابعة لاتصالات الجزائر، استطاع من خلالها اختراق المنظومة المعلوماتية لهذه المؤسسة التي تعتبر كبنك معلوماتية، ثم قام بتحويل المعلومات التي تحصل عليها إلى شركات أخرى منافسة لها، مقابل حصوله على مبالغ مالية، تم تحويلها إلى حسابه البنكي، وبعد قيام مصالح الضبطية القضائية في الجزائر بالبحث والتحري عن الجريمة توصلت إلى تحديد عنوان (IP) الذي استعمله المشتبه فيه، ومن خلاله تم تحديد رقم هاتف المشترك، ليتم التعرف على هوية المشتبه فيه، وبعد توقيفه وتفتيش منزله بموجب

---

[1]- سالم محمد سليمان الأوجلي، المرجع نفسه، ص: 427-428.

[2]- تنص المادة: 03 من الاتفاقية الأوروبية للمساعدة المتبادلة في القضايا الجنائية على أنه: "يجب على الدولة المطلوب منها أن تنفذ وفقا للنمط المنصوص عليه في قانونها الداخلي أية رسائل تتعلق بالقضايا الجنائية، والموجهة إليها من السلطات القضائية للدولة الطالبة من أجل الحصول على شهادة أو إرسال أشياء أو مواد لتقديمها كدليل، أو محاضر رسمية أو أية وثائق قضائية".

[3]- المعاهدة النموذجية لنقل الإجراءات في المسائل الجنائية، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم 14-252 المؤرخ في: 14-12-1990.

[4]- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من قبل الجمعية العامة للأمم المتحدة 217 (أ-د) بتاريخ: 15-11-2000، المصادق عليها بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05-02-2002، الجريدة الرسمية لسنة 2002، العدد 09.

الإذن بالتفتيش المؤرخ في: 26-12-2009 تم العثور على أجهزة إعلام آلي وملحقاته، ومبالغ مالية بالعملة الوطنية ووصولات لحوالات مالية واردة إليه عبر بنك وسترن يونيون.

وعند سماع المشتبه فيه اعترف بقرصنته لعدة مواقع إلكترونية لشركات أجنبية، وأكد بأن الحوالات المحجوزة بمنزله ناتجة عن ترويج المعلومات التي كان يتحصل عليها إلى مؤسسات أخرى، لتتم متابعته في أمام محكمة باتنة بجنح الدخول عن طريق الغش لمنظومة معالجة آلية للمعطيات، والبحث والتجميع والاتجار في معطيات مخزنة معالجة ومرسلة عن طريق منظومة معلوماتية، الأفعال المنصوص والمعاقب عليها بالمواد: 394 مكرر و 394 مكرر 2 و394 مكرر 6 من قانون العقوبات، وانتهت الدعوى إلى صدور حكم مؤرخ في:01-06-2010 قضى بإدانته بالجرائم المنسوبة إليه، ومعاقبته بسنة حبس نافذ و50.000 دج غرامة نافذة، وبعد استئناف هذا الحكم أصدر مجلس قضاء باتنة قرارا بتاريخ: 04-07-2010 قضى بتأييد الحكم المستأنف مبدئيا وتعديله بجعل نصف عقوبة الحبس المحكوم بها موقوفة التنفيذ.[1]

ثانيا: إجراءات المساعدة القضائية الدولية

تتم المساعدة القضائية الدولية وفق الإجراءات التالية:

01- تقديم الطلب: وهو طلب تقدمه الدولة الراغبة في المساعدة (وتسمى الدولة الطالبة) وفقا لقانونها الداخلي، إلى الدولة المراد منها تقديم المساعدة (وتسمى الدولة المطلوب منها)، لغرض مساعدتها في نطاق الاتفاقية المبرمة بين الدولتين، يتم إرسال الطلب عادة بالطرق الدبلوماسية، أو عن الاتصال المباشر بين الجهات القضائية المعنية به في كلتا الدولتين ربحا للوقت، وغالبا ما تتكفل الاتفاقيات الثنائية بتحديد القنوات التي يتم من خلالها إرسال طلبات المساعدة القضائية. [2]

وبالرجوع إلى المادة 18 ف 14 من اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية فإن الطلب يكون مكتوبا، ويمكن أن يكون شفاهة في الحالات المستعجلة، بشرط تأكيده

[1]- قرار، مجلس قضاء باتنة، الغرفة الجزائية، بتاريخ: 04-07-2010، فهرس رقم: 05812/10، انظر ملحق رقم 06.

[2]- سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013، ص: 421.

كتابة على الفور بالتوافق بين الدولتين، كما يجب أن يكون باللغة المقبولة في الدولة المطلوب منها، ويتضمن: (هوية السلطة مقدمة الطلب، موضوع وطبيعة المتابعة الجزائية أو الإجراء القضائي الذي يتعلق به الطلب، ملخص عن وقائع القضية، تحديد المساعدة المطلوبة، والغرض من جمع هذه الأدلة أو المعلومات أو التدابير).

وفي هذا الصدد، أجاز المشرع الجزائري قبول طلبات المساعدة القضائية الواردة عن طريق وسائل الاتصال السريعة بما فيها أجهزة الفاكس أو البريد الإلكتروني، وذلك بقدر ما توفره هذه الوسائل من شروط كافية للتأكد من صحتها،[1] كما يمكن توجيه الطلب شفاهة في حالة الاستعجال القصوى، مع ضرورة تأكيده بوثيقة مكتوبة أو إلكترونيا في أقرب الآجال.[2]

02- فحص الطلب: تقوم الدولة المطلوب منها بمعالجة الطلب المقدم إليها، وذلك بالتحقق من أن الواقعة موضوع التحقيق تشكل جريمة وفقا لقانون الدولة الطالبة، كما يتم التأكد من مدى اختصاصها بتنفيذ الطلب وفقا لقانونها الداخلي، وفي نطاق الاتفاقية المبرمة مع الدولة الطالبة.[3]

03- تنفيذ الطلب: ينفذ طلب المساعدة وفقا لقانون الدولة المطلوب منها،[4] لذلك تقوم هذه الأخيرة بالإجابة على الطلب وتزويد الدولة الطالبة بالمعلومات الممكنة، أو رفض الطلب إذا رأت فيه مساسا بسيادتها الوطنية، أو كان يتعارض مع نظامها العام.

إن المجتمع الدولي ورغم نجاحه في إرساء قواعد للتعاون الدولي من خلال الاتفاقيات الدولية، إلا أن الواقع العملي يبقى بعيدا عن الغاية المنشودة، إذ نلاحظ أن الإجرام الإلكتروني في تزايد مستمر، سواء من حيث القائمين به، أو من حيث الآليات المستخدمة في ارتكاب الجريمة، ويرجع ذلك أساسا إلى تغليب بعض الدول لمصالحها الخاصة على حساب المصلحة العامة

[1]- راجع المادة 02/16 من القانون رقم 09-04.

[2]- راجع المادة 36 ف 03 من قانون مكافحة التهريب المعدل والمتمم.

[3]- رامي وسام أبو ملحم، المرجع السابق، ص: 165.

[4]- تنص المادة 721 ق إ ج :"وتنفذ الإنابات القضائية إذا كان لها محل وفقا للقانون الجزائري".

للمجتمع في مكافحة هذه الظاهرة، والأخطر من ذلك أن بعض الدول تتورط في الجريمة، وهو ما يؤثر سلبا على مسار التحقيق الجنائي.

المطلب الثاني

عقبات التحقيق وسبل تجاوزها

يواجه التحقيق في الجريمة الإلكترونية العديد من العقبات التي تنعكس آثارها على المجتمع بفقدان ثقته في العدالة، وتزيد المجرمين ثقة بأنفسهم، مما يدفعهم إلى ارتكاب المزيد من الجرائم التي قد تكون أكثر خطورة وأشد ضررا، لذلك ينبغي تشخيص هذه العقبات، حتى يمكن وصف الحلول المناسبة لها، وهو ما سنعالجه من خلال هذا المطلب.

الفرع الأول: عقبات التحقيق في الجريمة الإلكترونية

نتج عن الطبيعة الخاصة للجريمة الإلكترونية العديد من العقبات التي واجهت جهاز التحقيق الجنائي خلال تحريه عن الجريمة، ويمكن تقسيمها إلى قسمين أساسيين:

أولا: عقبات قانونية: يعتري جهاز التحقيق خلال التحري عن الجريمة الإلكترونية العديد من العقبات القانونية، أهمها:

01- قصور القوانين: من بين عقبات التحقيق في الجريمة الإلكترونية غياب أو نقص القوانين الوطنية المجرمة لهذا النوع من الأفعال، كونها لا تزال من الجرائم المستحدثة، ويرجع ذلك أساسا إلى عدم تطور القانون الجنائي بنفس السرعة التي تتطور بها التكنولوجيا،[1] مما يجعل القضاء يستبعد الأخذ بالأدلة التي تضبطها هيئات التحقيق عند غياب نصوص التجريم تطبيقا لمبدأ الشرعية الجنائية.[2]

[1]- علي خيرت محرز، المرجع السابق، ص: 87.

[2]- خالد عياد الحلبي، المرجع السابق، ص: 221.

كما يمتد قصور القوانين كذلك إلى النصوص الإجرائية التي تكفل إجراءات البحث عن الأدلة الإلكترونية وسط بيئة افتراضية، إذ أن أغلب التشريعات مازالت لم تضبط القواعد القانونية التي يتم على أساسها تفتيش الحاسبات الآلية، أو الكيفية التي يتم من خلالها حجز المعلومات أو الأدلة الموجودة داخلها، ومراقبة المعلومات عند انتقالها، ولم تحدَد الإجراءات اللازمة عند رفض مستخدم الحاسوب الدخول إلى ملفاته أو نظام حاسوبه، أو رفض إعطاء الرقم السري، أو وضعه لفيروس من أجل تعطيل عمل جهاز التحقيق، أو محوه لأدلة الجريمة،[1] وهو الأمر الذي يعيق المحقق الجنائي عند البحث عن الأدلة الرقمية، احتراما لمبدأ الشرعية الإجرائية.[2]

إن تنوع النظم القانونية بين الدول أدى بدوره إلى اختلاف إجراءات التحقيق، فإذا كان أحد إجراءات التحقيق مشروعا في دولة معينة، فقد يكون غير مشروع في دولة أخرى امتدت لها آثار الجريمة، وهو ما يحول دون إتمام إجراءات التحقيق بالنسبة للجرائم العابرة للحدود.

02- عدم التبليغ عن الجريمة: تظل الجريمة الإلكترونية مستترة ما لم يتم الإبلاغ عنها، ومن بين الصعوبات التي تعترض جهاز التحقيق أن هذه الجرائم لا تصل إلى علم السلطات المعنية بنفس الصورة التي تصل بها الجريمة التقليدية، إذ تفضل الكثير من المؤسسات المتضررة عدم الإبلاغ عمَا تعرضت له حفاظا على سمعتها،[3] بل وتلجأ بعض المؤسسات إلى تعويض عملائها المتضررين خوفا من فقدان ثقتهم، لأن فقدان الثقة يفوق بكثير مقدار تعويضهم، ويكثر ذلك خصوصا في المؤسسات المالية والبنوك،[4] في حين ترى بعض المؤسسات الأخرى أن الإبلاغ عن

---

[1]- لينا محمد الأسدي، المرجع السابق، ص: 241.

[2]- تكفل الشرعية الإجرائية احترام الحرية الشخصية للمتهم عن طريق أن يكون القانون هو المصدر للتنظيم الإجرائي، وأن يفترض هذا التنظيم براءة المتهم في كل إجراء من الإجراءات التي تتخذ قبله، وأن تخضع الإجراءات لضمان القضاء، راجع محمد أحمد أبو زيد أحمد، إرشادات وتطبيقات عملية في التحقيق الجنائي، ط2، دار الإيمان للكمبيوتر، مصر، 2002، ص: 9.

[3]- خيرت علي محرز، المرجع السابق، ص: 68.

[4]- عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011، ص: 271.

الجريمة يؤدي إلى إحاطة المجرمين علما بنقاط ضعف أنظمتها المعلوماتية، فتكتفي باتخاذ إجراءات إدارية داخلية.[1]

وفي هذا الصدد، كشفت إحدى الدراسات التي أجراها المعهد الوطني للقضاء التابع لوزارة العدل الأمريكية بأن 70% من الجرائم الإلكترونية المكتشفة لا يتم التبليغ عنها إلى السلطات الأمنية، ونفس النتيجة أكدتها دراسة منجزة من طرف معهد أمن الحاسوب بمشاركة مكتب التحقيق الفيدرالي الأمريكي.[2]

03- تنازع الاختصاص القضائي الدولي: تتسم الجرائم الإلكترونية بالبعد الدولي، وغالبا ما يتجزأ فيها الركن المادي، ويتوزع على أكثر من دولة، ويتحقق ذلك عندما يرتكب السلوك الإجرامي في دولة معينة، وتتحقق النتيجة في دولة أو دول أخرى، مما يعطي الاختصاص لجميع هذه الدول للنظر في الجريمة، ويؤدي ذلك إلى تنازع الاختصاص فيما بينهم.

مثال ذلك أن يرسل المتهم برنامج فيروسات من جهاز كمبيوتر متواجد في دولة معينة إلى جهاز يقع في دولة ثانية، مرورا بجهاز ثالث ورابع يقعان في دول أخرى، ففي هذه الحالة تثار مشكلة الاختصاص بحدَة، لأن تحديد الجهة القضائية المختصة بالتحقيق في هذه الجريمة، ومعرفة القانون واجب التطبيق يتوقفان مبدئيا على مكان وقوع الجريمة، فترى كل دولة أنها وقعت على إقليمها وتتمسك باختصاصها.

أجرى الباحث SMITH دراسة سنة 2001 بهدف التعرف على المشكلات التي تواجه المحققين في جرائم الحاسوب، باعتبار أن الملاحقة القضائية قد تتطلب توجيه اتهام أو رفع دعوى على أشخاص يتواجدون في دول أخرى، وهذا الأمر يؤخَر التحقيق، ويزيد من أعبائه، وتوصل إلى أن جرائم الحاسوب خلَفت صعوبات تتمثل بشكل رئيسي في أن الكثير منها غير قارة، مما يخلَف عقبات حق إقامة الدعوى والاختصاص القضائي، ويزيد من صعوبات التصدي لها.[3]

[1] -NIGEL WALKER, Crime and Criminology, Oxford University PRESS, 1987, P: 17.

[2]- حسين بن سعيد الغافري، المرجع السابق، ص: 19-20.

[3]- عبد الله بن سعود محمد السراني، المرجع السابق، ص: 153.

كما أشار تقرير منظمة الأمم المتحدة حول الإجرام المعلوماتي إلى أن أي اختراق مباشر لقاعدة بيانات حاسوب متواجد على إقليم دولة أجنبية قصد استرجاع بيانات تم تخزينها فيه دون علم هذه الدولة أو رضاها المسبق يعد خرقا لسيادتها.[1]

04- قصور التعاون الدولي وتعقيد إجراءاته: إن طبيعة الجريمة الإلكترونية العابرة للحدود تحتم على المجتمع الدولي التعاون لمواجهتها، ويترتب على قصوره ضعف القدرة على إثباتها أمام اختلاف الأنظمة القانونية والسياسية والدينية للدول، وعدم وجود نص قانوني يلزمها بالتعاون.

وإذا كانت المساعدة القضائية الدولية مطلبا أساسيا تسعى إليه أغلب الدول في إطار تعزيز جهودها الرامية إلى مكافحة الجريمة الإلكترونية، إلا أنها تبقى في الوقت نفسه أحد أصعب المواضيع المطروحة بسبب العوائق التي تعترضها، فرغم أن جل الاتفاقيات الدولية تشجع على تبسيط الإجراءات وتبادل المعلومات، إلا أن العديد من الدول مازالت تقدم طلبات المساعدة القضائية وفقا للطرق الدبلوماسية، التي تتسم عادة بالبطء والتعقيد، وهو ما يتعارض مع طبيعة عمل الإنترنت وما تتميز به من سرعة،[2] فضلا عن التباطؤ في الرد من طرف الدولة المطلوب منها، والذي يرجع أساسا إلى نقص الموظفين ذوي الكفاءة الفنية، أو نتيجة الصعوبات اللغوية، أو بسبب اختلاف الإجراءات، وغيرها من الأسباب.[3]

إن غياب قنوات اتصال مرنة تسمح لجهاز التحقيق الجنائي بالتعجيل في جمع الأدلة الرقمية سيؤثر بدوره سلبا على مسار التحقيق الجنائي، ويساعد الجناة على إخفاء أدلة إدانتهم.

---

[1]- أكد القضاء الألماني هذا الموقف في عدة قضايا، أشهرها "قضية الغش المعلوماتي" التي طرحت أمامه ورفضت محكمة التحقيق الألمانية منح الإذن للولوج عن بعد إلى بيانات مخزنة في حاسوب موجود في سويسرا بقصد تفتيشها قبل موافقة أو مساعدة السلطات القضائية السويسرية، معتبرة ذلك مظهر من مظاهر احترام السيادة. هلالي عبد اللاه أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم لمعلوماتي، دار النهضة العربية، القاهرة، 2006، ص: 70.

[2]- محمد أحمد سليمان عيسى، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016، ص: 63.

[3]- عادل عبد العال ابراهيم الخراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون، دقهلية، المجلد، 01 العدد 16، 2014، ص: 244.

وتبقى قاعدة التجريم المزدوج إحدى العقبات التي تمنع الدولة من طلب المساعدة القضائية ويرجع ذلك إلى الاختلاف حول مسألة تجريم الاعتداءات المعلوماتية، أين استطاعت بعض الدول مواكبة هذا التطور وتحديث قوانينها الداخلية بتجريم هذه الأفعال، فيما عجزت دول أخرى عن مواكبة ذلك.

ثانيا: عقبات تقنية: خلفت الطبيعة الخاصة للجريمة الإلكترونية العديد من العقبات، أهمها:

01: صعوبة اكتشاف وإثبات الجريمة الإلكترونية: تتميز الجرائم الإلكترونية بارتكابها وسط بيئة رقمية معقدة ومتشابكة، مما يجعلها صعبة الاكتشاف وصعبة الإثبات كما سبق توضيحه.

وفي هذا الصدد، أجرى الباحث (Wahbler) دراسة عن الجرائم الإلكترونية سنة 1998 استهدفت المحققين العاملين في قطاع الشرطة في ملبورن بأستراليا، وكان من أهم نتائجها أن عددا كبيرا منهم قليل الخبرة يواجه صعوبات فنية وعملية للحصول على أدلة رقمية في هذه الجرائم، وأن أغلب المدانين في جرائم الحاسوب من أصحاب المهارات، وأوصت الدراسة بضرورة عقد ندوات تدريبية متقدمة للمحققين في مجال الجريمة المعلوماتية.[1]

كما ناقش مؤتمر الانتربول السادس لجرائم تقنية المعلومات، المنعقد بالقاهرة خلال الفترة الممتدة من 13 إلى 15 -04-2005 مجموعة من التحديات التي تعرقل عمليات التحري عن الجريمة الإلكترونية، ومن بينها تحدي انتشار مقاهي الإنترنت، التي يستغلها المجرم المعلوماتي لتنفيذ جرائمه، وهو ما يؤدي إلى صعوبة اكتشافه، نظرا لقدرته على التنقل بين أكثر من مقهى خلال اليوم الواحد، ولم تسلم تكنولوجيا الإنترنت فائق السرعة (ADSL) هي الأخرى من يد المجرمين، الذين يستغلونها لتنفيذ جرائمهم عن طريق اشتراكهم مع أشخاص آخرين في جهاز واحد عبر موزع خطوط، مما يؤدي إلى صعوبة اكتشافهم.[2]

02- غياب التخصص التقني للمحقّقين: إن التحري عن الجرائم الإلكترونية لا يكفيه الإلمام بأصول البحث الجنائي وقواعد البحث الكلاسيكية، وإنما يتطلب أيضا إلمام المحقق بأصول

[1]- عبد الله بن سعود محمد السراني، المرجع السابق، ص: 152.

[2]- يحيى عطوة الزنط، المرجع السابق، ص: 357.

التحقيق التقني المعلوماتي، فضلا عن المهارات الخاصة، التي تسمح له باستيعاب تقنيات الحاسوب الآلي من حيث برامجه وأنظمة تشغيله، وأساليب التعامل معها.

لذلك تعتبر شخصية المحقق الجنائي من أهم عقبات التحقيق، ويظهر ذلك من خلال قلة معرفته باستخدام الحاسوب، وضعف استخدامه لشبكة الإنترنت، وعدم قدرته على استنباط الأدلة الرقمية،[1] وعدم متابعته للمستجدات في مجال جرائم الحاسوب والإنترنت، وجهله بالأساليب المتبعة في ارتكاب هذه الجرائم،[2] إذ يحتاج اكتشاف جريمة التزوير الإلكتروني مثلا لاستعمال تقنيات تتبع واسترجاع المعلومات، وغيرها من التقنيات التي تهدف إلى تتبع مصدر الاختراق، ويتطلب استخدام هذه التقنيات خبرة فنية متقدمة.[3]

أجرى الباحث KELLY سنة 1995 دراسة عن جرائم الكمبيوتر بهدف التعرف على أسباب عدم اهتمام رجال العدالة بها رغم تزايد آثارها السلبية، وتوصل إلى أن ذلك راجع إلى قلة إلمامهم بأساليب التحقيق في هذا النوع من الجرائم، فضلا عن اعتبارها عبئا إضافيا عليهم بجانب الجرائم التقليدية، مما يجعلهم مطالبين بالتدريب على هذه الجرائم التقنية، التي تتطلب تخصَصا دقيقا لاستخدام الحاسب الآلي من أجل استخلاص الأدلة الرقمية، ومعرفة أفضل الطرق والأساليب للتعامل معها، كون التعامل الخاطئ يؤدي إلى فقدانها، وأوصت الدراسة بضرورة تنمية ثقافة الحاسوب لدى المحققين، وتزويدهم بتدريب متخصص للإلمام بتفاصيل الحاسب الآلي، ومعرفة أساليب استغلاله في ارتكاب الجرائم الإلكترونية، وقدرتهم على استخدام تقنيات التتبع واسترجاع المعلومات لالتقاط الدليل الرقمي.[4]

03- نقص الأجهزة المساعدة للمحقق الجنائي: من بين الصعوبات التي تعيق عمليات التحقيق في الجرائم الإلكترونية نقص الخبراء المختصين في الحاسوب والإنترنت على مستوى جهات

[1]- سليمان العنزي، المرجع السابق، ص: 119.

[2]- عبد الرحمان بحر، معوقات التحقيق في جرائم الإنترنت، (رسالة ماجستير)، أكاديمية نايف العربية للعلوم الأمنية، الرياض 1999، ص: 54.

[3]- عبد الله بن سعود محمد السراني، المرجع السابق، ص: 270

[4]- المرجع نفسه، ص: 156-157.

التحقيق، وعدم التنسيق بين المحققين والعاملين في مجال المعلوماتية، إضافة إلى نقص الأجهزة والبرامج التقنية التي يستعان بها لكشف هذه الجرائم وتعقب مرتكبيها.[1]

كما أن ارتفاع تكاليف الأجهزة والتقنيات المستخدمة في عمليات فحص وتحليل مسرح الجريمة الافتراضي، التي تستورد غالبا من الخارج، وما يتبعه من سفر للتدريب عليها، واكتساب خبرات جديدة دائمة التطور، يتطلب بدوره تكاليف باهظة، وهو ما يشكل أحد عقبات التحقيق.

أجرى الباحث (Hollis et) دراسة خلال سنة 2001 شملت العاملين في المعهد الوطني للعدالة الأمريكية قصد التعرف على متطلباتهم من أجل التصدي للجرائم الإلكترونية، توصل من خلالها إلى حاجتهم إلى الدعم المادي من أجل إنشاء وتطوير جهاز متخصص في مكافحة هذا النوع من الجرائم، فضلا عن إنشاء وحدات للفحص والتحليل في مجال الأدلَة الرقمية الجنائية.[2]

كما أشار المؤتمر الدولي لجرائم الحاسوب المنعقد في أوسلو في الفترة ما بين 29 و 30 ماي 2000 إلى أن ضعف البنية التحتية للإنترنت يعيق عمليات التحقيق، فهي وإن ساعدت في التعرف على عنوان ورقم الحاسوب المستعمل في ارتكاب الجريمة عن طريق (IP)، إلا أنها تعجز عن الوصول إلى شخصية مرتكبها أو معرفة مصدره الحقيقي.[3]

04- نقص تأمين الأنظمة المعلوماتية: من بين عقبات التحقيق الجنائي في الجريمة الإلكترونية كذلك أن الكثير من ضحايا هذه الجرائم لا يتخذون الحيطة والحذر اللازمين لمنعها، فأغلب مستخدمي الإنترنت لا يضعون برامج وتقنيات الحماية ضد الاختراق والتجسس والوقاية من الفيروسات، مما يحول دون اكتشافهم للجريمة لحظة ارتكابها، وقد لا يكتشفونها أبدا، ويمتد هذا النقص حتى إلى المؤسسات العمومية والشركات المالية والتجارية.

[1]-علي خيرت محرز، المرجع السابق، ص :87.

[2]- عبد الله بن سعود محمد السراني، المرجع السابق، ص: 160-161.

[3]- يحيى عطوة الزنط، المرجع السابق، ص: 362.

إن إغفال المؤسسات للجانب الأمني للأجهزة، وتسابق الشركات نحو تبسيط الإجراءات وزيادة المنتجات وقصر اهتماماتها على تقديم الخدمة، دون إدراك لخطورة هذه الجرائم، ساهم بدوره في زيادة انتشارها.[1]

أجرى الباحث العنزي دراسة سنة 2002 حول وسائل التحقيق في جرائم نظم المعلومات شملت المحقّقين بأقسام الشرطة في مدينة الرياض، والعاملين بمجال نظم المعلومات بالقطاع العام، توصل من خلالها إلى وجود تقصير في إجراءات أمن المعلومات، وعدم وجود سياسة أمنية واضحة، وأوصت الدراسة بضرورة إلزام الموظفين باتباع إجراءات السياسة الأمنية، وإعلانها للموظفين، وتقيد الرؤساء بها عند إسداء التعليمات، وسن عقوبات للمخالفين لها.[2]

الفرع الثاني: سبل تجاوز عقبات التحقيق

تعرفنا على العقبات التي واجهت جهاز التحقيق خلال تحريه عن الجريمة الإلكترونية وجعلته يقف عاجزا عن تتبعها، ولتدارك ذلك وجب تكثيف الجهود على المستويين الوطني والدولي.

أولا: على المستوى الوطني: إن أكثر ما يعيق الدول عن مواجهة الإجرام السيبراني راجع لقصور قوانينها الوطنية، وعجز محققيها عن مواكبة التطور التكنولوجي، فضلا عن غياب سياسة أمنية واضحة لحماية الأنظمة المعلوماتية، لذلك وجب تدارك هذه النقائص من خلال:

01- مسايرة القوانين الوطنية للتطور التكنولوجي: إن قصور القوانين بشكل عام يؤثر سلبا على الجانب الإجرائي للتحقيق في الجريمة الإلكترونية، لذا يجب على كل دولة مسايرة تطورات الجريمة بتحديث قوانينها الداخلية، سواء الموضوعية من خلال تجريم الأفعال الإجرامية المستحدثة، أو الإجرائية من خلال استحداث آليات مرنة قادرة على مواكبة هذه التطورات، بشكل يحقق التكامل مع القواعد الدولية، ويضمن لها سيادتها الوطنية.

[1]- سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، أكاديمية نايف للعلوم الأمنية، الرياض، 2003، ص: 98.

[2]- عبد الله بن سعود محمد السراني، مرجع سابق، ص: 148.

02- التوعية بضرورة التبليغ عن الجريمة: من أجل تفعيل عملية الإبلاغ عن الجريمة طالب البعض في الولايات المتحدة الأمريكية بتضمين قوانينها نصوصا تلزم موظفي المؤسسات بضرورة الإبلاغ عما يصل إلى علمهم من جرائم معلوماتية، وبعد عرض هذا المقترح على "لجنة خبراء مجلس أوروبا" قوبل بالرفض، خوفا من أن تصبح الشركة التي ارتكبت في حقها الجريمة متهمة بعد أن كانت ضحية، وقدمت اللجنة اقتراحات بديلة، مثل الالتزام بإبلاغ جهة خاصة أو إبلاغ السلطات الوصية.[1]

لذلك ندعو المؤسسات الإعلامية والقانونية وفاعلي المجتمع المدني إلى توعية المجتمع بضرورة الإبلاغ المبكر عن هذا النوع الخطير من الجرائم، كما ندعو المشرع إلى توفير الحماية القانونية للمبلَغين، حتى يمكنهم اللجوء إلى القضاء دون خوف أو تردد، مع ضرورة إنشاء هيئة خاصة بتلقي البلاغات والشكاوى تعمل على مدار الساعة، وبكافة الوسائل بما فيها الإلكترونية.

03- التكوين المستمر لجهاز التحقيق: إن مواجهة هذه العقبات تفرض على جهاز التحقيق مواكبة التطورات التكنولوجية في مجال الحاسوب والمعلوماتية، وذلك بإعداد برامج طموحة للتدريب المستمر أثناء الخدمة، وتنظيم دورات وطنية ودولية لتجديد المعلومات وتبادل الخبرات، وقد دعت مختلف الاتفاقيات الدولية إلى تعزيز التعاون الدولي في مجال التدريب ونقل الخبرات، ومن بينها اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية لسنة 2000 في مادتها 29، كما دعا المجلس الأوروبي إلى ذلك في توصياته المنبثقة سنة 1999، واهتمت منظمة الأنتربول هي الأخرى بالتدريب من خلال تنظيمها لعدة دورات تدريبية للمحققين في الجرائم الإلكترونية.[2]

وفي هذا الصدد، قامت وزارة العدل الجزائرية في إطار التعاون مع البرنامج الأوروبي لمكافحة الجريمة الإلكترونية بتكوين معمق لفائدة 25 قاض حول "الجريمة الإلكترونية والأدلة الإلكترونية"، بالمدرسة العليا للقضاء خلال الفترة الممتدة من 29 جانفي إلى 02 فيفري 2023 على أن يكون القضاة المشاركون في هذه الدورة بمثابة قضاة مرجعيين على مستوى جهاتهم

[1]- خيرت علي محرز، المرجع السابق، ص: 75.

[2]- ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، أطروحة مقدمة لنيل شهادة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2019، ص: 226.

القضائية في المسائل المرتبطة بالجريمة الإلكترونية،[1] كما شارك 08 قضاة وإطارين 02 من الديوان المركزي لقمع الفساد في تكوين حول "مكافحة الجريمة الاقتصادية والمعلوماتية"، تم تنظيمه من طرف معهد مكافحة الجريمة الاقتصادية بسويسرا، خلال الفترة الممتدة من 24 أفريل إلى 05 ماي 2023.[2]

ولم يقتصر التكوين على القضاة وإطارات الوزارة، بل شمل 100 موظف (مهندسين وتقنيين في الإعلام الآلي) من مختلف المجالس القضائية والمحاكم الإدارية في دورة تكوينية –عن بعد– تم تنظيمها بتاريخ: 26–04–2023 من طرف المدرسة الوطنية لمستخدمي أمانات الضبط، تناولت موضوع "تأمين الأنظمة المعلوماتية لقطاع العدالة"، وذلك بغرض تحسيس الموظفين المكلفين بتسيير مصالح الإعلام الآلي بخطورة الجرائم السيبرانية وسبل الوقاية منها، إذ تم من خلالها التطرق إلى مختلف المحاور ذات الصلة، لاسيما حماية أنظمة المعلومات من الاعتداءات الإلكترونية، الضوابط الأساسية للأمن السيبراني، التدابير الواجب اتخاذها لمواجهة الاعتداءات الإلكترونية، التنسيق مع مصالح المديرية العامة للعصرنة للتحكم في التطبيقات المختلفة المعمول بها، الاطلاع على أساليب اختراق المنظومات الخاصة بقاعدة المعطيات، ومعرفة سبل تأمين الأجهزة والمنظومات.[3]

لذلك نرى أنه من الضروري تكوين المحققين في الجرائم الإلكترونية تكوينا تقنيا متخصصا عن طريق تنظيم دورات مستمرة، تمكنهم من التعرف على طبيعة الجريمة الإلكترونية وأساليب ارتكابها، وكيفية استخلاص الأدلة الرقمية والاحتفاظ بها دون إتلافها، ويمكن اقتصاد نفقات التكوين من خلال استعمال تقنيات التخاطب المرئي عن بعد، أو حصر التكوين على عدد معين من المحققين ذوي الكفاءة ليكونوا بدورهم مكوَنين مرجعيين لزملائهم.

[1]– بيان لوزارة العدل، الرابط: https://2cm.es/Rhec، تاريخ الاطلاع: 30–01–2023، الساعة: 10:16.

[2]– بيان لوزارة العدل، الرابط: https://n9.cl/asghh7، تاريخ الاطلاع: 24–04–2023، الساعة: 09:40.

[3]– بيان لوزارة العدل، الرابط: https://n9.cl/asghh7، تاريخ الاطلاع: 24–04–2023، الساعة: 09:40.

كما ينبغي على المحقق الجنائي المبادرة باتخاذ أي إجراء مشروع يمكّنه من الوصول إلى الحقيقة، كاللجوء إلى الخبرة الفنية، أو ندب مستشارين تقنيين لمساعدته، أو إلزام مقدمي الخدمات بالتعجيل بحفظ المعطيات المخزنة، وعدم اكتفائه ببعض الإجراءات التقليدية.

04- التوجه نحو التخصص: اتجهت الكثير من دول العالم نحو التخصص من أجل مواجهة نقص الخبرة لدى جهاز التحقيق الجنائي، أين قامت الولايات المتحدة الأمريكية بإنشاء وحدة متخصصة بالتحقيق في الجرائم الإلكترونية ومكافحتها ضمن مكتب التحقيق الفيدرالي، مع ضمان تدريب مستمر لعناصر الوحدة حتى يواكب تطور جرائم الإنترنت.[1]

وفي هذا الصدد استحدثت مصالح الأمن والدفاع الوطني وحدات متخصصة في مكافحة الجريمة الإلكترونية موزعة عبر وحداتها المختلفة، وهي خطوة حميدة ينبغي تثمينها مع الدعوة إلى توسيعها أكثر، وتزويدها بأحدث الأجهزة المادية والتقنية، فضلا عن الكفاءات البشرية المؤهلة في مجال المعلوماتية.

كما استحدث المشرع قطبا وطنيا متخصصا في معالجة الجرائم الإلكترونية الخطيرة والمعقدة، وهي خطوة تستحق التشجيع، غير أننا نرى أن تخصيص قطب وطني سيؤدي إلى تراكم القضايا المعروضة أمامه، وهو ما ينعكس سلبا على نوعية الأحكام القضائية، ويؤدي إلى إطالة أمد النزاع، كما أنه يبعد العدالة عن المتقاضي، ويثقل كاهله بأعباء إضافية جرَاء التنقل، وبالمقابل فإن الأقطاب الجهوية لم تعد قادرة على مواجهة هذه النمط الإجرامي بسبب تنوع الجرائم المعروضة أمامها، لذلك ندعو إلى إنشاء عدة أقطاب جهوية متخصصة في مكافحة الجريمة الإلكترونية، مع تدعيمها بأحدث الأجهزة التكنولوجية، وتزويدها بالكفاءات البشرية المؤهلة في مجال المعلوماتية.

05- توفير الوسائل المادية والبشرية المساعدة لجهاز التحقيق: من أجل مساعدة جهاز التحقيق الجنائي في التحري عن الجريمة الإلكترونية والحفاظ على أدلتها الرقمية قامت بعض الدول باستقطاب المختصين وذوي الكفاءات العالية في مجال المعلوماتية ضمن أجهزتها الأمنية

[1]- حسين بن سعيد الغافري، المرجع السابق، ص: 22.

والقضائية،[1] في حين بادرت دول أخرى إلى إنشاء وحدات متخصصة في مكافحة الجريمة الإلكترونية، وتعتبر الولايات المتحدة الأمريكية من الدول الرائدة في هذا المجال، بسبب معاناتها الدائمة من الجرائم الإلكترونية.[2]

لذلك ينبغي تزويد جميع الجهات المكلفة بالتحقيق في الجريمة الإلكترونية بالإمكانات المادية الكافية لاقتناء المعدات التكنولوجية المتطورة، وتدعيمها بالكفاءات البشرية المؤهلة من الخبراء والمختصين في مجال المعلوماتية البشرية لمساعدتهم على سرعة الكشف عن الأدلة الإلكترونية والحفاظ عليها، ثم تقديمها أمام القضاء كأدلة إثبات يقينية يمكن الاستناد إليها في إصدار الحكم.

كما ندعو إلى تعزيز نشاط المخابر الوطنية والجهوية المتخصصة في التحقيق في الجريمة الإلكترونية، وتزويدها بكفاءات بشرية مؤهلة، ومعدات تكنولوجية متطورة، وتكليفها بمهام التكوين التقني المستمر لجهاز التحقيق الجنائي والخبراء المعتمدين في هذا المجال، والعمل على تبادل الخبرات المعلوماتية مع مختلف الجهات الوطنية والدولية، وتقديم المساعدة لجهاز القضاء متى طلب منهم ذلك.

06- تحصين أمن الأنظمة المعلوماتية: تعد سهولة اختراق الأنظمة المعلوماتية من بين الأمور التي تساعد على انتشار الجريمة الإلكترونية، لذلك نرى أنه من الضروري تحصينها بكلمات مرور يصعب اختراقها، وتوعية الموظفين بخطورة تداول رقمهم السري، إلى جنب نشر الثقافة المعلوماتية بين أفراد المجتمع، وتوعيتهم بخطورة الإدلاء ببياناتهم عبر الإنترنت، ومخاطر التصفح العشوائي للمواقع الإلكترونية والانبهار بالعروض الوهمية.

ويبدو أن معالجة هذه العقبة تتوقف عموما على قيام الدولة ممثلة بمؤسساتها التعليمية والقانونية والإعلامية بنشر الثقافة القانونية بين مواطنيها ومؤسسات المجتمع المختلفة، وتحذيرهم

[1]- جمال براهيمي، المرجع السابق، ص: 211.

[2]- عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير، دراسة معمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، 2004، ص: 81.

من خطورة الجرائم الإلكترونية، وإرشادهم إلى ضرورة اتخاذ الاحتياطات الكفيلة بحمايتهم، مع ضرورة إعداد استراتيجية وطنية متكاملة لحماية نظم المعلومات وتأمينها، كما يجب على مستخدمي الإنترنت لاسيما المؤسسات والشركات الكبرى وضع أنظمة وقاية يصعب اختراقها.

ثانيا: على المستوى الدولي: يعتبر التعاون الدولي بمختلف صوره من أنجع الحلول الكفيلة بتجاوز عقبات التحقيق في الجريمة الإلكترونية العابرة للحدود الوطنية، لذلك ينبغي تكاتف جهود المجتمع الدولي من خلال:

01- تقارب التشريعات الدولية: تقتضي مواجهة هذه الظاهرة الإجرامية تنسيق التشريعات الدولية من خلال خلق منظومة قانونية مشتركة تتقارب فيها الأفكار وتتوحد فيها الرؤى لمواجهة هذه الظاهرة، وذلك بمحاولة وضع تعريف موحد للجريمة الإلكترونية، وضبط السلوكات المادية المجرمة، وتعميم إجراءات التحري عن هذه الجرائم.

كما ينبغي الاهتمام بدراسة ظاهرة الإجرام الإلكتروني بشكل علمي يأخذ بعين الاعتبار المعلومات الإحصائية والبيانات اللازمة، سواء فيما تعلق بالجريمة الإلكترونية أو بمرتكبيها، وبذلك يمكن وضع آليات قادرة على مواجهتها.

02- تعزيز التعاون الدولي: إن ما تبذله الدولة من جهود بمعزل عن باقي الدول المعنية بالجريمة الإلكترونية غير كاف لمواجهتها، لذلك ينبغي تعزيز التعاون بين مختلف المؤسسات الأمنية والإدارية والقضائية المتخصصة في هذا المجال، وذلك بتكثيف برامج التدريب والندوات العلمية والمحاضرات ذات الصلة بالموضوع، وتبادل الخبرات والمهارات الفنية من أجل مواكبة التطور التكنولوجي، وإبرام الاتفاقيات الدولية التي تقرب وجهات النظر بين الدول، وبذلك يمكن التصدي لمشكلة تنازع الاختصاص القضائي الدولي التي أرَقت الدول والحكومات.

كما ندعو المجتمع الدولي إلى تبني نظام قانوني يأخذ على عاتقه مهمة إنشاء كيان متخصص في مكافحة الجريمة الإلكترونية، يعمل على تنسيق الجهود بين الدول المعنية بالجريمة الإلكترونية.

03- تبسيط إجراءات المساعدة القضائية: من أجل التوفيق بين ضرورة السرعة التي تقتضيها بعض إجراءات التحقيق العابرة للحدود تفاديا لفقد الدليل، ومبدأ احترام سيادة الدول، نرى أنه لابد من توافر إرادة حقيقية لتبني نظام قانوني موحد للمساعدة القضائية، يعمل على تبسيط إجراءات التحقيق وسرعة تنفيذها، قصد الحصول على المعلومات والأدلة الرقمية في حينها، مع سعي الدول إلى وضع هيئات وطنية مختصة تعمل على استقبال وتنفيذ طلبات المساعدة القضائية على مدار الساعة، وبجميع الوسائل بما فيها الوسائل الإلكترونية.

كما أن التخلي عن شرط التجريم المزدوج يعد خطوة لازمة من أجل تفعيل دور المساعدة القضائية بشكل أكبر، ويمكن تكريس ذلك من خلال الاتفاقيات الثنائية بين الدول، وهو الأمر الذي سيساهم لا محالة في ضبط أدلة الجريمة الإلكترونية وردع الجناة.

ولعلَ عدم التزام بعض الدول بمحتوى الاتفاقيات الدولية، وتمسكها بمبدأ سيادة قوانينها الوطنية من أكثر ما يعيق المساعدة القضائية الدولية، لذلك يجب التوعية بخطورة هذه الجرائم التي لا تستثني أحدا، والدعوة إلى تغليب المصلحة العامة للمجتمع الدولي على المصالح الضيقة لبعض الدول.

خلاصة الفصل

حوصلة للفصل الأخير من هذه الدراسة؛ يتضح أن الجانب التقني للجريمة الإلكترونية شكل تحدَيا في مكافحتها من الناحية القانونية، مما فرض على مختلف التشريعات العمل على تحيين منظوماتها القانونية من أجل ضمان النجاعة والفعالية اللازمين للتصدي لها وطنيا ودوليا.

والجزائر ليست في منأى عن هذا التحدي، لذلك ركن المشرع إلى تعديل ق إ ج سنة 2006، من خلال استحداث أساليب تحري جديدة، تتمثل في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور، فضلا عن التسرب الإلكتروني، وحصر نطاقها في بداية الأمر على بعض الجرائم الخطيرة، بما فيها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، غير أن تزايد خطورة الإجرام الإلكتروني وانتشاره دفعه إلى توسيع نطاق هذه الآليات لتشمل جرائم أخرى أشد خطورة وأكثر تعقيدا، مع إحاطتها بضوابط قانونية كفيلة بحماية الحياة الخاصة للأفراد.

وواصل المشرع سيره على نهج الاتفاقيات الدولية، التي دعت الدول إلى اتخاذ التدابير اللازمة لحفظ الأدلة الرقمية وسلامتها إلى غاية تقديمها لسلطات التحري للاستعانة بها في كشف ملابسات الجريمة، فضلا عن تعزيز المساعدة القضائية الدولية وتبسيط إجراءاتها، وهو ما تم تجسيده من خلال القانون رقم 09-04 وبعض القوانين الأخرى.

ومع ذلك تبقى الضرورة قائمة للعمل على مواكبة تطور هذه الظاهرة الإجرامية، وتكثيف الجهود دوليا ومحليا لتذليل ما قد يعترض التحقيق بشأنها قانونيا وتقنيا.

خاتمة

خاتمة

ختاما لهذه الدراسة الموسومة بـ: "**التحقيق الجنائي في الجريمة الإلكترونية**"، يتضح جليا أن خصوصية هذه الجرائم، وتوظيفها لأحدث التقنيات التكنولوجية، جعلها تختلف عن نظيرتها التقليدية، وتثير تحديا قويا حول كيفية مكافحتها سواء على مستوى المنظومة التشريعية، أو المنظومة القضائية.

وتزداد خطورة هذه الجريمة حين تتجاوز حدود الدولة، متأثرة بالبعد العالمي لشبكات الإعلام والاتصال، وهو ما عجّل بدعوة المجتمع الدولي إلى تعزيز التعاون لمكافحة هذه الظاهرة من خلال عديد الاتفاقيات الدولية والإقليمية؛ أهمها الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، والاتفاقية العربية لمكافحة جرائم تقنية المعلومات، إذ صادقت الجزائر على هذه الأخيرة، وأخذت من الأولى مرجعا لإعداد القواعد الإجرائية الخاصة بمكافحة هذا النمط الإجرامي.

ورغم ما بذله المشرع من جهود لتطوير أساليب التحقيق في الجريمة الإلكترونية، إلا أن التطور التكنولوجي المستمر، وأثره المباشر على تطورها، حال دون فعالية الأساليب التقليدية وفرض ضرورة البحث عن أساليب أخرى قادرة على مواجهة هذه التحديات.

ونظرا لخطورة إجراءات التحقيق على الحقوق والحريات، التي تكفلها مختلف الصكوك الدولية والدساتير، أناطه المشرع إلى سلطة قضائية محايدة، يمكنها أن تستعين بجهاز الشرطة القضائية لمساعدتها على جمع أدلة الجريمة، أو بالهيئة باعتبارها جهة تقنية متخصصة من أجل تزويدها بالمعلومات، وإنجاز الخبرات، وتبادل المساعدة القضائية الدولية.

وقد توصلنا من خلال البحث في هذا الموضوع إلى عدة نتائج، أبرزها:

01- عدم اتفاق المجتمع الدولي على تعريف موحد للجريمة الإلكترونية، نتيجة ما أفرزه تطورها وخصوصيتها، إذ تعددت المعايير في ذلك بين وسيلة ارتكابها، والمحل الذي تستهدفه إضافة إلى إلمام مرتكبيها بحد أدنى من التقنية المعلوماتية.

02- وظَف المشرع الجزائري مصطلح "الجرائم المتصلة بتكنولوجيات الإعلام والاتصال" للدلالة على الجرائم الإلكترونية، وتبنى تعريفا موسعا لها ضمن صلب المادة 02/أ من القانون رقم 09-04، وقد وفق في ذلك، باعتبار أن تعريف الجريمة في صلب النص يعد نقطة مهمة في التشريع، لما تحمله من تكريس لمبدأ الشرعية، وتعزيز للتعاون الدولي.

03- تلعب المعاينة المادية دورا هاما في الكشف عن أدلة الجريمة المنطقية وسط بيئة افتراضية، نظرا لما تحتويه من معلومات ضخمة، غير أن ذلك لا يرقى إلى نفس الدور الذي تلعبه في استبيان الأدلة المادية، ويرجع ذلك أساسا إلى تردَد العديد من الأشخاص على مسرح الجريمة الرقمي، فضلا عن إمكانية التلاعب بأدلتها عن بعد.

04- خصوصية الأدلة الرقمية أوجبت وضع نصوص قانونية تسهل إجراء الخبرة وسط مسرح افتراضي، تفاديا لنقص المعرفة بالتقنية المعلوماتية، وتذليلا لما قد يعترض جهاز التحقيق من صعوبات في جمع أدلتها، وحفاظا عليها من الضياع والتلف جرَاء أي خطأ أو جهل في التعامل معها.

05- إمكانية الولوج إلى مستودع الأسرار عن طريق إجراء التفتيش الإلكتروني وحجز الأدلة المعنوية المتعلقة بالجريمة الإلكترونية، جعل التشريعات الإجرائية تحيطها بضوابط قانونية، بحثا عن الموازنة بين حقوق الأفراد في صون حرياتهم الخاصة، وتحقيق النجاعة المطلوبة لكشف غموض الجريمة، بما في ذلك الدستور الجزائري.

06- عجز أساليب التحقيق التقليدية عن مواكبة تطورات الجريمة الإلكترونية، دفع بالمشرع إلى استحداث أساليب حديثة، تعتمد على نفس التقنية المستخدمة في الجريمة، والتي اعترتها بدورها صعوبات قانونية وتقنية وجب علاجها.

07- تفاديا لما قد ترتّبه أساليب التحري الخاصة بهذا النوع من الجرائم من مساس بحقوق الأفراد وحرياتهم، أحاطها المشرع بجملة من الضمانات القانونية للحيلولة دون التعسف في استعمالها.

08- الإلمام بالجانب التقني للجريمة الإلكترونية، فرض ضرورة تأهيل المحققين وتدريبهم المستمر على التقنية المعلوماتية، من خلال إعداد برامج طموحة للتدريب أثناء الخدمة، وتنظيم دورات وطنية ودولية لتجديد المعارف وتبادل الخبرات.

09- توجه الدولة الجزائرية تدريجيا نحو التخصَص في مكافحة الجريمة الإلكترونية على مستوى مختلف الأجهزة؛ قضائيا من خلال استحداث قطب وطني متخصص في معالجة الجرائم الإلكترونية الخطيرة والمعقدة، وأمنيا من خلال تكوين فرق بحث وتحري متخصصة في مكافحة هذا الصنف، وإداريا من خلال تنصيب الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، كجهة تقنية متخصصة في هذا المجال.

10- مساعدة للسلطات المكلفة بالتحريات القضائية لجمع أدلة الجريمة الإلكترونية وتحديد هوية مرتكبيها، ألزم القانون مقدمي خدمة الإنترنت سواء أكانوا أشخاصا طبيعيين أم معنويين بالتعجيل في حفظ وإفشاء معطيات حركة السير، تحت طائلة العقوبات المقررة قانونا.

11- تعزيز المشرع الجزائري لقدرات جهاز التحقيق الجنائي في مكافحة الجريمة الإلكترونية العابرة للحدود، من خلال اعتماد المساعدة القضائية الدولية الهادفة إلى جمع الأدلة الخاصة بهذه الجريمة وتبسيط إجراءاتها، وهو ما جسَده القانون رقم 09-04، رغم ما يعيقها من مصالح ضيقة لبعض الدول، وبطء في تنفيذها من طرف البعض الآخر.

وعلى ضوء النتائج التي أظهرتها الدراسة، توصلت إلى بعض التوصيات التي أتمنى أن تجد لها صدى يسهم في إثراء الفكر القانوني وحقول البحث العلمي، تتمثل في:

01- تنمية الوعي لدى المجتمع بمخاطر الاستخدام غير الآمن للانترنت وشبكاتها وتأثيرها السلبي على مختلف المستويات، اجتماعيا، سياسيا، اقتصاديا، وثقافيا، بما يكفل تكريس منظومة متكاملة قادرة على مجابهة الجريمة الإلكترونية، والحد من خطورتها.

02- الاستعانة بذوي الكفاءة والخبرة في مجال المعلوماتية لتعزيز الأمن الإلكتروني، وذلك بإعداد استراتيجية وطنية متكاملة لحماية الأنظمة المعلوماتية، وتأمينها من الاختراق والاعتداء.

03- التوعية بضرورة الإبلاغ المبكر عن هذا النوع من الجرائم، مع إنشاء هيئة خاصة بتلقي البلاغات والشكاوى، تعمل بصفة دائمة، وبكافة الوسائل بما فيها الإلكترونية.

04- الحرص على التكوين التقني المتخصص والمستمر للمحققين في الجريمة الإلكترونية للإحاطة بكل ما يتعلق بها، لاسيما من حيث أساليب ارتكابها، وطرق استخلاص أدلتها الرقمية دون إتلافها، مع إمكانية الاستعانة في ذلك بتقنيات التخاطب المرئي عن بعد اقتصادا للنفقات، أو حصر التكوين على ذوي الكفاءة من المحققين ليكونوا بدورهم مكوَنين مرجعيين لزملائهم.

05- تكريس التخصص في مكافحة الجريمة الإلكترونية، على مستوى مختلف الأجهزة ذات الصلة، شرطية، قضائية، إدارية، مع الاستفادة من خبرات الدول الرائدة في هذا المجال.

06- دعوة المشرع إلى استبدال مصطلح "التفتيش الإلكتروني" بمصطلح "الولوج" أو "النفاذ"، باعتبار أن التفتيش مصطلح تقليدي ينصب على المكونات المادية.

07- استبدال مصطلح جرائم المساس بأنظمة المعالجة الآلية للمعطيات في قانون الإجراءات الجزائية بمصطلح الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وتعميم استخدامه في النصوص المنظمة للضوابط القانونية لأساليب التحري عن هذه الجرائم، بما يكفل مبدأ الشرعية الإجرائية.

08- دعوة المشرع إلى رفع التجريم عن تسجيل المجني عليه لاتصاله مع شخص آخر متى اقترنت تصريحات هذا الأخير بوصف مجرم، يتجاوز حدود خصوصيته، لما يشكله ذلك من توفير للدليل وضبطه.

09- دعوة المشرع إلى استحداث أقطاب جهوية متخصصَة في مكافحة الجرائم الإلكترونية الخطيرة والمعقدة والجرائم المرتبطة بها، من أجل بلوغ الفعالية اللازمة لجهاز التحقيق، وتذليل العقبات التي تعترضه.

10- تفعيل آلية المساعدة القضائية الدولية، وتعزيزها بوضع نظام قانوني موحد لها، يعمل على تبسيط إجراءات التحقيق وسرعة إنجازها، قصد الحصول على المعلومات والأدلة الرقمية في

حينها، مع سعي الدول إلى وضع هيئات مختصة تعمل باستمرار على استقبال وتنفيذ طلبات المساعدة القضائية، وبجميع الوسائل بما فيها الإلكترونية.

11- دعوة المجتمع الدولي إلى تبني اتفاقية موحدة، تعمل على توحيد المفاهيم المتعلقة بالجريمة الإلكترونية، وتبسيط أساليب التحقيق الخاصة بها، حتى يمكن لجهاز التحقيق بلوغ الفعالية اللازمة لمواجهتها.

كانت هذه جملة النتائج التي توصلنا إليها، والتوصيات التي ندعو إلى تبنيها من أجل الوصول إلى تحقيق فعالية قصوى في عمل جهاز التحقيق الجنائي، وبذلك تتجسد السياسة الجنائية الهادفة إلى مكافحة الجريمة الإلكترونية.

الملاحـــق

ملحق رقم: 01

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

مجلس قضاء: باتنة
الغرفة الجزائية

قرار جزائي

رقم الملف: 23/06957
رقم الفهرس: 23/07759
تاريخ القرار: 23/07/02

بالجلسة العلنية المنعقدة بمقر مجلس قضاء باتنة
بتاريخ الثاني من شهر جويلية سنة الفين و ثلاثة و عشرون
للنظر في قضايا الجنح و المخالفات

برئاسة السيد (ة): رئيسا
وبعضوية السيد (ة): مستشارا
وبعضوية السيد (ة): مستشارا مقررا
وبمحضر السيد (ة): نائب عام
وبمساعدة السيد (ة): أمين الضبط

صدر القرار الجزائي الآتي بيانه

النيابة ضد /

السيد النائب العام - مدعيا باسم الحق العام

من جهة

ضد /

1): /

طبيعة الجرم /

جنحة القيام اثناء نشر مواضيع الامتحانات المهنية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد

متهم مستأنف — موقوف — حاضر

من مواليد: ب:
ابن: و
الساكن: حي 50 مسكن طريق سطيف بلدية نقاوس
بواسطة الأستاذ (ة):

من جهة أخرى

** بيان وقائع الدعوى **

- حيث أن المتهمة متابعة من طرف نيابة الجمهورية لارتكابها منذ زمن لم يمض عليه أمد التقادم بعد بدائرة اختصاص محكمة نقاوس مجلس قضاء باتنة جنحة القيام أثناء الإمتحانات مواضيع الامتحانات المهنية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد الفعل المنصوص والمعاقب عليه بنص المادة 253 مكرر 06 و253 مكرر 7 من قانون العقوبات
- حيث أن المتهمةأحيلت على المحكمة بناء على إجراءات المثول الفوري عملا بأحكام المادة 339 مكرر من الأمر رقم 15-02 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية حسب ما هو ثابت من الاخطار بإجراءات المثول الفوري الصادر عن السيد وكيل الجمهورية بتاريخ 12-06-2023 طي الملف ضد المتهمة لتمثل أمام المحكمة بنفس التاريخ
- حيث يستخلص من الملف أنه بتاريخ 11-06-2023 وفي اطار تأمين امتحانات البكالوريا جوان 2023 ومكافحة كل أشكال الغش خاصة منها عم طريق التواصل الاجتماعي قامت المصلحة المركزية لمكافحة الجرائم السيبرانية برصد مجموعة الكترونية مفتوحة عبر موقع فايسبوك (بلاك اداب وفلسفة) حامل للاسم المستعار على الساعة 10:18 صباحا بنشر موضوع مادة اللغة العربية بعد مدة زمنية قدرها ساعة و48 دقيقة وتم التوصل لرقم الهاتف الخاص بصاحب الحساب وتبين انه بحمل رقم المسجل باسم
وعند التنقل الى عنوان الإقامة اين تم الترصد لصاحب الرقم والحساب وتم توقيف المدعو الذي تم تلمسه والعثور بحوزته على الهاتف النقال الذي يحمل الرقم التسلسلي والرقم مزود بشريحة تحمل الرقم مسجل باسم والدته وكلمة السر

ولدى سماع المدعو أمد انه صاحب الهاتف النقال ورقم الهاتف المسجل باسم والدته ويحوز حساب فايسبوك يحمل الاسم المستعار يستعمله في اتصالاته مع اصدقائه وبتاريخ الوقائع 11-06-2023 على الساعة 9:00 صباحا اثناء مغادرته للسكن طلبت منه اخته ان يترك لها هاتفه فأخبرها أنه بالشاحن ولم تخبره انها ستستعمله في نشر مواضيع البكالوريا دورة 2023 نافيا اي علاقة له بنشر موضوع اللغة العربية لدورة جوان 2023 شعبة أداب وفلسفة ولا يعلم ان كانت اخته من نشرته مضيفا ان شقيقته تجتاز امتحان البكالوريا شعبة آداب وفلسفة ببريكة وان هاتفه كان عند اخته طيلة اليوم

ولدى سماع المدعوة صرحت انها بتاريخ الوقائع كانت متواجدة بالمسكن العائلي بحي 50 مسكن طريق سطيف وفي حدود التاسعة صباحا اثناء مغادرة شقيقها طلبت منه ان يترك هاتفه بالمنزل وتستعمله دون اذنه مفيدة انها ولجت الى حساب الفيسبوك الخاص بشقيقها الذي تركه مفتوحا وبدأت بالتصفح كونها تشعر بالملل واثناء تصفحها وجدت مجموعة خاصة ببكالوريا 2023 شعبة آداب وفلسفة اين انتابها الفضول فقدمت طلبا للانضمام للمجموعة وبعدها دخلت فوجدت العديد من الأشخاص ينشرون موضوعا خاصا باللغة العربية فقامت بإعادة نشره في مجموعة بها اكثر من الف شخص وانها قامت باستعمال تطبيق الايمو الخاص بشقيقها دون علمه وأكدت ان عبارة (سوجي آداب لي باغي نكملوا اسئلة بريفي) فهي من قامت بتدوينها واكدت انها لم ترسل اي اجابات لشقيقتها الممتحنة وانها تحوز تطبيق ايمو وقامت باستعماله في مجموعات تقوم لتبادل اسئلة ومواضيع شهادة البكالوريا 2023

ولدى سماع المدعوة صرحت انها تجتاز امتحان شهادة البكالوريا دورة جوان 2023 كمترشحة حرة شعبة اداب وفلسفة ببريكة وامها تجتاز بتاريخ الوقائع مادة اللغة العربية والفلسفة وأثناء الامتحان لم تجتاز اي اجابة

ولدى سماع المدعوة صرحت ان الرقم الهاتفي مسجل باسمها وان ابنها هو من يستعمله ولا علم لها ان استعمله لفتح حساب فيسبوك ام لا .

وتم الإشارة الى التوصل الى المعلومات بناء على اذن بالولوج الى منظومة المعلوماتية الخاصة بالهاتفين المستعملين من طرف المشتبه فيها وشقيقها بمساعدة خلية مكافحة الجريمة السيبرانية وكان الرد ايجابيا ثبت منه ضلوع المشتبه فيها في تسريب مواضيع البكالوريا

- على إثرها تم اتخاذ الإجراءات القانونية وتقديم المتابعة أعلاه للسيد وكيل الجمهورية الذي أحالها على المحكمة بناء على إجراءات المثول الفوري بعد تمسكها بنفس التصريحات التي أدلت بها لدى سماعها من طرف الضبطية القضائية

- حيث أن المتهمة مثلت بالجلسة فور تقديمها وبعد التأكد من هويتها وتنبيهها إلى حقها في طلب مهلة لتحضير دفاعها طبقا للمادة 339 مكرر 05 من قانون الإجراءات الجزائية تمسكت بالمحاكمة الفورية وبعد مواجهتها بالتهمة المنسوبة اليها صرحت أنها من قامت بنشر الموضوع الخاص بامتحان اللغة العربية بعدان اخذته من مجموعة كانت قد قبلت الانضمام اليها وانها لم تكن تقصد اي نية فقط عن حسن نية قامت بنشره بعد ان أخذت هاتف شقيقها واستعملت حساب الفيسبوك الخاص به وعن سؤال المحكمة عن العبارة المدونة بالمحادثة ((سوجي آداب لي باغي نكملوا اسئلة بريفي) أجابت انها كانت تقصد الاسئلة نفسها فقط مؤكدة سابق تصريحاتها

حيث أنه صدر حكم بتاريخ: 12-06-2023 فهرس رقم: 23/01098 حضوري وجاهي قضى بإدانة المتهمة بما نسب إليها، ومعاقبتها بعام حبس نافذ و100.000 دج مع الأمر بإيداعها الحبس في الجلسة.

حيث أن المتهمة استأنفت هذا الحكم بتاريخ:13-06-2023 كما هو ثابت من خلال شهادة الاستئناف المرفقة بملف الدعوى .

حيث أن وكيل الجمهورية استأنف هذا الحكم بتاريخ:19-06-2023 كما هو ثابت من خلال شهادة الاستئناف المرفقة بملف الدعوى .

حيث أن المتهمة حضرت جلسة المحاكمة، وبعد التأكد من هويتها وإحاطتها علما بالوقائع اعترفت بنشر موضوع البكالوريا.

حيث أن ممثل الحق العام التمس تشديد العقوبة.

حيث أن الأستاذ رافع في حق المتهمة، والتمست لها البراءة كون الموضوع كان منشورا قبل قيام المتهمة بنشره، واحتياطيا إفادتها بظروف التخفيف.
حيث أن الكلمة الأخيرة منحت للمتهمة ومحاميها .
حيث أن القضية وضعت في المداولة لجلسة: 02-07-2023 للفصل فيها طبقا للقانون

** وعـليه فإن المجـلس **

- بعد الاستماع إلى المستشار المقرر
- بعد الإطلاع على قانون الإجراءات الجزائية لاسيما المواد من : 416 إلى 439 .
- بعد الإطلاع على المواد: 253 مكرر 6 ، 253 مكرر 7 من قانون العقوبات المعدل والمتمم
- بعد المداولة في القضية وفقا للقانون .
- في الشكل :
- حيث أن استئنافي المتهمة ووكيل الجمهورية وردا في الآجال وطبقا للأوضاع المقررة قانونا يتعين قبولهما شكلا .
- في الموضوع:
حيث ثبت للمجلس من خلال الإطلاع على الملف وما دار في جلسة المحاكمة أن المتهمة قامت بتاريخ: 11-06-2023 على الساعة: 10:18 صباحا بنشر موضوع البكالوريا مادة اللغة العربية لشعبة الآداب والفلسفة دورة جوان 2023 داخل مجموعة إلكترونية مفتوحة تحمل الاسم المستعار "باك 2023 آداب وفلسفة"، باستعمال تطبيقتي الإيمو والفايسبوك، وهو ما يستشف من خلال محضري المعاينة والتفتيش الإلكترونيين المنجزين من طرف مصالح الضبطية القضائية لمكافحة الجرائم السيبرانية بباتنة، واعتراف المتهمة بذلك أمام قاضي الدرجة الأولى وخلال جلسة المحاكمة.
حيث أن المتهمة قامت عن وعي منها وإدراك بنشر موضوع امتحان البكالوريا خلال فترة اجتياز الامتحان باستعمال التطبيقين الإلكترونين الإيمو والفايسبوك، وهو ما يشكل النموذج القانوني لجنحة نشر مواضيع الامتحانات النهائية للتعليم الثانوي باستعمال وسائل الاتصال عن بعد، الفعل المنصوص والمعاقب عليه بالمواد: 253 مكرر 6 و 253 مكرر 7 من قانون العقوبات.
حيث أصاب قاضي الدرجة الأولى حين قضى بإدانة المتهمة بالجرم المنسوب إليها، مما يتعين معه تأييد الحكم المستأنف مبدئيا فيما قضى به من إدانة.
حيث ثبت للمجلس من خلال الإطلاع على صحيفة السوابق القضائية للمتهمة أنها غير مسبوقة قضائيا، مما يجيز إفادتها بظروف التخفيف مع وقف تنفيذ عقوبة الحبس طبقا للمادة:53 مكرر 4 من قانون العقوبات والمواد: 592 ، 593 من قانون الإجراءات الجزائية المعدل والمتمم، مما يتعين معه تعديل الحكم المستأنف بتخفيف عقوبة الحبس المحكوم بها مع شملها بوقف التنفيذ
حيث أنه وطبقا للمادة: 594 من قانون الإجراءات الجزائية فإنه يتعين على المحكمة تنبيه المحكوم عليه بأنه في حالة صدور حكم جديد عليه بالإدانة فإن العقوبة الأولى ستنفذ عليه دون أن تلتبس بالعقوبة الثانية، كما يستحق عقوبات العود بنصوص المواد:57 ،58 من قانون العقوبات
حيث أن المصاريف القضائية تتحملها المحكوم عليها طبقا للمادة: 432 من قانون الإجراءات الجزائية.
حيث أن مدة الإكراه البدني تحددها المحكمة بحدها الأقصى طبقا للمواد: 599، 600، 602 من قانون الإجراءات الجزائية.

** لهـذه الأسـباب **

قرر المجلس علنيا نهائيا حضوريا وجاهيا للمتهمة:
- في الشكل:- قبول الاستئنافين.
- في الموضوع:- تأييد الحكم المستأنف مبدئيا، وتعديله بخفض عقوبة الحبس المحكوم بها إلى ستة (06) أشهر حبس مع جعلها موقوفة التنفيذ.

رقم الجدول: 23/06957
رقم الفهرس: 23/07759

- مع تحميل المحكوم عليها المصاريف القضائية المقدرة ب: 1800 دج
وتحديد مدة الإكراه البدني بحدها الأقصى .
- بذا صدر هذا القرار ونطق به في الجلسة العلنية المنعقدة بالتاريخ المذكور أعلاه ،ولصحته أمضي أصله من طرف الرئيس وأمين الضبط.

الرئـــيس (ة) أميـن الضبـط

رقم الجدول: 23/06957
رقم الفهرس: 23/07759

ملحق رقم : 02

رقم: 2024 /4/م ت م/م م م إ س/د.و

بطاقة معلومات

حول حصيلة المصلحة المركزية لمكافحة الإجرام السيبراني

سنة 2019 قامت المصلحة بإنجاز 1245 تحري سيبراني.

سنة 2020 قامت بإنجاز 1620 تحري سيبراني.

سنة 2021 قامت بإنجاز 2.828 تحري سيبراني.

سنة 2022 قامت بإنجاز 2.316 تحري سيبراني.

سنة 2023 قامت بإنجاز 2.473 تحري سيبراني.

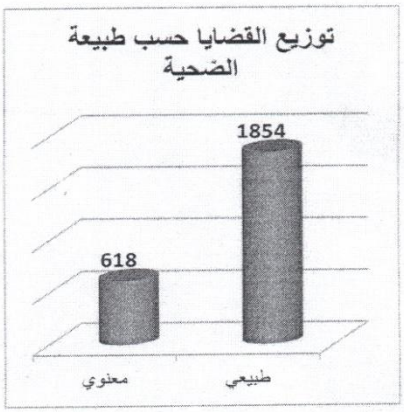
إحصائيات المصلحة المركزية لمكافحة الإجرام السيبراني للدرك الوطني حسب طبيعة الضحية، الجنس وأصناف الجريمة في الفترة ما بين 2023/01/01 الى غاية 2023/12/31

1- عدد القضايا : 2472.

2- عدد الضحايا الأطفال : 230.

3- توزيع القضايا حسب طبيعة الضحية:

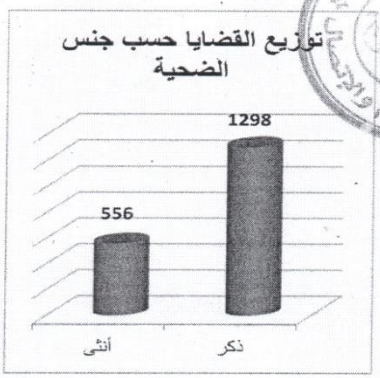
طبيعة الضحية	العدد
معنوي	618
طبيعي	1854



3/1

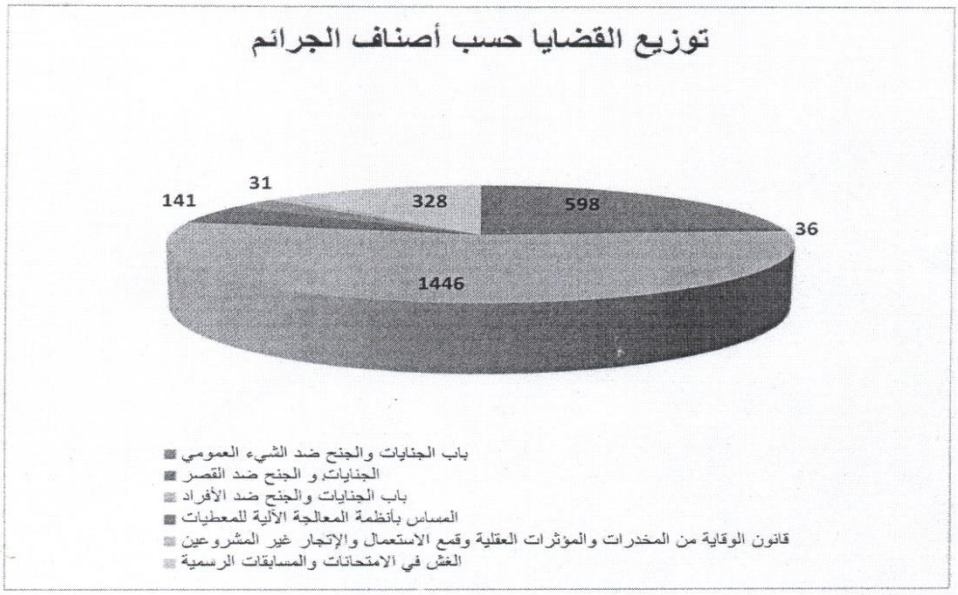
4- توزيع القضايا حسب جنس الضحية:

جنس الضحية	العدد
أنثى	556
ذكر	1298



5- توزيع القضايا حسب أصناف الجرائم:

التصنيف	العدد
باب الجنايات والجنح ضد الشيء العمومي	598
الجنايات و الجنح ضد القصر	36
باب الجنايات والجنح ضد الأفراد	1446
المساس بأنظمة المعالجة الآلية للمعطيات	141
قانون الوقاية من المخدرات والمؤثرات العقلية وقمع الاستعمال والإتجار غير المشروعين	31
الغش في الامتحانات والمسابقات الرسمية	328



3/2

6- توزيع القضايا حسب الجريمة:

التصنيف	العدد
الإعتداء، الضرب و الجرح العمدي	1
المساس بأنظمة المعالجة الآلية للمعطيات	141
تكوين جمعيات الأشرار	3
المساس بالحياة الخاصة للأشخاص	999
التجمهر غير مرخص و الحركات الاحتجاجية	44
تصنيف آخر	38
الفعل المخل بالحياء و المساس بالآداب العامة	9
الجرائم ضد القصر	36
المخدرات و الحبوب المهلوسة و المؤثرات العقلية	31
النصب، الاحتيال و السرقة	371
النقود المزورة	7
الخيانة الزوجية	7
التزوير و استعمال المزور	7
الهجرة غير الشرعية و تهريب المهاجرين	11
القتل	10
انتحال الشخصية	107
أوامر القيادة	75
الإساءة إلى إطارات و مؤسسات الدولة	67
الإساءة إلى الرسول محمد صلى الله عليه و سلم أو بقية الأنبياء أو المعلوم من الدين أو شعائر الإسلام	14
الغش في شهادة البكالوريا	327
الغش في شهادة التعليم المتوسط	1

ملحق رقم: 03

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

قرار جزائي

مجلس قضاء: باتنة
الغرفة الجزائية

رقم الملف: 23/10980
رقم الفهرس: 24/00648
تاريخ القرار: 24/01/14

بالجلسة العلانية المنعقدة بمقر مجلس قضاء باتنة
بتاريخ الرابع عشر من شهر جانفي سنة ألفين و أربعة و عشرون
للنظر في قضايا الجنح و المخالفات

برئاسة السيد (ة): رئيسا
وبعضوية السيد (ة): مستشارا مقررا
وبعضوية السيد(ة): مستشارا
وبحضور السيد (ة): نائب عام
وبمساعدة السيد (ة): أمين الضبط

صدر القرار الجزائي الآتي بيانه
السيد النائب العام - مدعيا باسم الحق العام

النيابة ضد /

من جهة

و /

1): ضحية غير مستأنف
من مواليد:
ابن: و
الساكن : باتنة

طبيعة الجرم /
جنحة التهديد و الاحتفاظ بصور لشخص دون رضاه

من جهة ثانية

ضد /

1): متهم غير مستأنف غائب
من مواليد: بـ:
ابن: و
الساكن : المقيم هي سطيف

من جهة أخرى

** بيان وقائع الدعوى **

حيث أن المتهم ق سبق متابعته من طرف نيابة الجمهورية لدى محكمة باتنة، لارتكابه منذ زمن لم يحض اعليه أمد التقادم القانوني بعد، بدائرة اختصاص محكمة باتنة و مجلسها القضائي جنحة التهديد و جنحة الاحتفاظ بصور لشخص دون رضاه الفعل المنصوص والمعاقب عليه بالمواد: 287 - 284 -303 مكرر ، من قانون العقوبات
حيث أن المتهم أحيل على محكمة الجنح وفقا لإجراءات الاستدعاء المباشر طبقا للمادتين 333 و 335 من قانون الإجراءات الجزائية، اين صدر حكم غيابي بتاريخ 14-11-2021 قضى بادانة المتهم بما هو منسوب إليه و معاقبته عنه، و قد تم تبليغه بهذا الحكم شخصيا بتاريخ 20-03-2023 أين سجل معارضته فيه بتاريخ 21-03-2023 و حددت له جلسة 28-05-2023 للنظر في معارضته.
- حيث يستخلص من ملف التحري أن المسماة تقدمت بشكوى أمام وكيل الجمهورية بمحكمة باتنة مفادها أنها تتعرض للتهديد من طرف احد الاشخاص على موقع الفايسبوك و ذلك بنشر صورها في جميع مواقع التواصل الاجتماعي، كما قام بسبها ، و ذلك بعد ان تعرفت عليه لمدة قصيرة.

- بسماع الشاكية المسماة / ، صرحت أنها تملك حساب على موقع التواصل الإجتماعي بالفايسوك ، يحمل الاسم المستعار " " أنشأته بواسطة هاتفها النقال رقمه .0554 رقمه السري " " وقائع القضية تعود إلى تاريخ 30-07-2018 أين تعرفت على شخص تجهل هويته ، عبر الفايسبوك ، مضيفة أن السالف الذكر قام بتهديدها بنشر صورها عبر موقع التواصل الإجتماعي ، كما قام بسبها و شتمها بشتى عبارات السب عبر تطبيق الماسنجر و المتمثلة " " أين هددها برسائل أخرى بقوله لها " ذرك نخرجها للناس غدوة ننشرهم مليح راني لقيت لي قروب تاع باتنة ، صورلي كلش بلا وجهك و لا ننشرهم ، ذرك تشوفي لامادرتكش عريانة " و غيرها من عبارات الشتم و التهديد، كما أضافت أن السالف الذكر بعد التهديدات المتواصلة بنشر صورها من أجل تشويه سمعتها عبر موقع التواصل الإجتماعي فايسبوك ، الشيئ الذي أثر عليها شخصيا و الحق لها أضرار معنوية و نفسية في نفس الوقت ، مؤكدة أنها لم تلتق به إطلاقا ، كما أنها تتواصل معه عبر الفايسبوك فقط ، و كل ما في الأمر صرح لها أنه من بلدية رأس العيون ولاية باتنة ، في الأخير أصرت على المتابعة القضائية ضد صاحب الحساب السالف الذكر إن توصل التحقيق الى كشف هويته .

- تمكنت التحريات التقنية التي قامت بها مصالح فرقة محاربة الجرائم الالكترونية من استرجاع عنوان بروتوكول الانترنات المدون على الشكل التالي ( ) الموافق لحساب الفايسبوك المشكو منه و الحامل للاسم المستعار ( )، و بتكليف لوكالة اتصالات الجزائر تبين ان عنوان بروتوكول الأنترنات السالف الذكر موافق للرقم الهاتفي ( ) و المسجل باسم المقيم برقم 12 حي 32 مسكن الشيخ العيفة دائرة عين ارنات.

- تعذر سماع المشتكى منه.

حيث أنه صدر حكم بتاريخ: 09-07-2023 فهرس رقم: 23/6488 حضوريا غير وجاهي، قضى ببراءة المتهم.

حيث أن المتهم استأنف هذا الحكم بتاريخ:10-07-2023 كما هو ثابت من خلال شهادة الاستئناف المرفقة بملف الدعوى .

حيث أن المتهم تغيب عن حضور جلسة المحاكمة.

حيث أن الضحية تغيبت عن حضور جلسة المحاكمة.

حيث التمس ممثل الحق العام إلغاء الحكم المستأنف، والقضاء من جديد بإدانة المتهم بالجرم المنسوب إليه ومعاقبته طبقا للقانون.

حيث أن القضية وضعت في المداولة لجلسة: 14-01-2024 للفصل فيها طبقا للقانون

** وعـليه فإن المجـلس **

- بعد الاستماع إلى المستشار

- بعد الإطلاع على قانون الإجراءات الجزائية لاسيما المواد من : 416 إلى 439

- بعد الإطلاع على المواد:287، 303 مكرر، 303 مكرر 1 من قانون العقوبات

- بعد المداولة في القضية وفقا للقانون .

- في الشكل:

- حيث أن استئناف وكيل الجمهورية ورد في الآجال وطبقا للأوضاع المقررة قانونا، يتعين قبوله شكلا .

- في الموضوع :

حيث ثبت للمجلس من خلال الاطلاع على ملف الدعوى وما دار خلال جلسة المحاكمة أن المتهم قد احتفظ بصور الضحية دون رضاها، كما هددها بنشر صورها على موقع التواصل الاجتماعي فيسبوك في حالة عدم إرسال صور أخرى، وهو ما يستشف من خلال تصريحات الضحية المعززة بصورها المرفقة والرسائل المرسلة إليها عبر حساب الفيسبوك الحامل للاسم المستعار

حيث أن التحريات التقنية التي قامت بها عناصر فرقة الجرائم المعلوماتية بالمصلحة الولائية للشرطة القضائية مكنت من استرجاع عنوان بروتوكول الإنترنت (IP) الخاص بالحساب الحامل للاسم المستعار ، وهو: ، بتاريخ 16-08-2018 على الساعة 23:28 و 40 ثا، وبعد مراسلة مصالح مديرية اتصالات الجزائر لتحديد هوية المرسل صاحب البروتوكول المذكور، أجابت الأخيرة بأنه يتعلق بالمتهم، صاحب الرقم الهاتفي:

حيث أن المتهم قام بهذه الأفعال عن وعي وإدراك منه مع علمه بأنها مجرمة قانونا، وهو ما يشكل النموذج القانوني لجنحة جنحة الاحتفاظ بصورة لشخص دون رضاه،وجنحة التهديد، الأفعال المنصوص والمعاقب عليها بالمواد:287، 303 مكرر 1 من قانون العقوبات.
حيث جانب قاضي الدرجة الأولى حين قضى ببراءة المتهم، مما يتعين معه إلغاء الحكم المستأنف والقضاء من جديد بإدانته بما نسب إليه، ومعاقبته طبقا للقانون.
حيث أن المتهم تغيب عن حضور جلسة المحاكمة ولا يوجد بالملف ما يفيد توصله شخصيا بمحضر التكليف بالحضور، مما يتعين القضاء في مواجهته غيابيا طبقا للمادة: 346 من قانون الإجراءات الجزائية.
حيث ان المصاريف القضائية يتحملها المحكوم عليه طبقا للمادة: 432 من قانون الإجراءات الجزائية.
حيث أن مدة الإكراه البدني تحدد بحدها الأقصى المقرر قانونا طبقا للمادتين 600 و 602 من قانون الإجراءات الجزائية.

** لهـذه الأسـباب **

قرر المجلس علنيا نهائيا غيابيا للمتهم:
- في الشكل:- قبول الاستئناف.
- في الموضوع:- إلغاء الحكم المستأنف، والقضاء من جديد بإدانة المتهم بما نسب إليه، ومعاقبته بستة (06) أشهر حبس نافذ وخمسين ألف دينار جزائري (50.000 دج) غرامة نافذة.
- مع تحميل المحكوم عليه المصاريف القضائية المقدرة ب: 1800 دج
وتحديد مدة الإكراه البدني بحدها الأقصى .
- بذا صدر هذا القرار ونطق به في الجلسة العلنية المنعقدة بالتاريخ المذكور أعلاه ، ولصحته أمضي أصله من طرف الرئيس وأمين الضبط.

الرئـــيس (ة) أميـن الضبـط

ملحق رقم: 04 نموذج إنابة قضائية

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء: المسيلة **إنابة قضائية**

محكمة: المسيلة

الغرفة: الأولى

رقم الترتيب: /2024

رقم النيابة: /2024

رقم التحقيق: /2024

نحن: ..... **قاضي التحقيق** بمحكمة المسيلة، الغرفة: الأولى.

- بعد الاطلاع على المواد 138 وما بعدها من قانون الإجراءات الجزائية.
- وبعد الاطلاع على القضية المتبعة ضد:
- (أ، ي)، **موقوف،** المولود في: ، ابن: وابن: الساكن بـ:
- التهمة: جنحة الترويج العمدي للمخدرات
- المواد: 16 مكرر 1 من قانون الوقاية من المخدرات والمؤثرات العقلية.
- نندب السيد: **قائد فرقة الدرك الوطني بالمسيلة**
- لمباشرة الإجراءات الآتية:
- الاتصال بوكالة أوريدو من أجل تحديد هوية صاحب الرقم الهاتفي ** ** ** 0550.

وأن يفيدنا علما بما طلبناه باسم الشعب الجزائري

حرر بمكتبنا بـ: المسيلة، في: 07-01-2024.

قاضي التحقيق

ملحق رقم: 05 نموذج لإذن بالتفتيش الإلكتروني

الجمهورية الجزائرية الديمقراطية الشعبية

مجلس قضاء: المسيلة وزارة العدل

محكمة: المسيلة

نيابة الجمهورية

رقم /ب ع/ 23

إذن بالتفتيش الإلكتروني

نحن وكيل الجمهورية لدى محكمة المسيلة.

– بعد الاطلاع على الطلب المقدم من طرف رئيس فرقة الشرطة القضائية لأمن دائرة المسيلة، المؤرخ في: 13-06-2023 تحت رقم /2023، الرامي إلى منح الإذن بالتفتيش الإلكتروني لمنظومة معلوماتية.

– وبنـاء على التحقيق الجـاري حاليـا في قضية: نشر وتسريب مواضيـع البكالوريـا، دورة جـوان 2023 ضد المشتبه فيه (ب، س) المولود في: بـ: ابن: وابن: ، الساكن بـ:

– بعد الاطلاع على المواد: 01، 03، 05، 06 من القانون 09-04 المتضمن القواعد لخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته.

– نأذن لـ: **رئيس فرقة الشرطة القضائية لأمن دائرة المسيلة** بمباشرة إجراءات التفتيش داخل المنظومة المعلوماتية، وذلك بالولوج إلى:

–الهاتف من نوع A5S يحمل رقم الإيماي الأول: والثاني: ،ملك للمدعو (ب، س) لغرض استخراج كل ما يفيد التحقيق.

– مع ضرورة استعمال المعلومات المتحصل عليها إلا في الحدود الضرورية للتحريات والتحقيقات القضائي، والاستعانة في ذلك و تسخير أي شخص له دراية بعمل المنظومة المعلوماتية محل البحث عملا بأحكام المادة 05 من القانون 09-04.

حرر بـ: المسيلة، في: 12-06-2023.

وكيل الجمهورية.

ملحق رقم: 06

نسخة عادية

الجمهورية الجزائرية الديمقراطية الشعبية

باسم الشعب الجزائري

قرار جزائي

مجلس قضاء: باتنة
الغرفة الجزائية

رقم الملف: 10/05805
رقم الفهرس: 10/05812
تاريخ القرار: 10/07/04

بالجلسة العلانية المنعقدة بمقر مجلس قضاء باتنة
بتاريخ الرابع من شهر جويلية سنة ألفين و عشرة
للنظر في قضية الجنح و المخالفات

برئاسة السيد (ة): رئيسا مقررا
وبعضوية السيد (ة): مستشارا
وبعضوية السيد (ة): مستشارا
وبحضور السيد (ة): نائب عام
وبمساعدة السيد (ة): أمين الضبط

صدر القرار الجزائي الآتي بيانه
السيد النائب العام - مدعيا باسم الحق العام

النيابة ضد /

من جهة

و /

1): المؤسسة الأمريكية ساتوفات واركس طرف مدني غير مستأنف

الساكن : المؤسسة الامريكية ساتوفات واركس

طبيعة الجرم /
الدخول عن طريق الغش في منظومة لمعالجة الآلية للمعطيات + البحث والتجميع والنشر والاتجار في معطيات مخزنة معالجة ومرسلة عن طريق منظومة معلوماتية

من جهة ثانية

ضد /

1): متهم مستأنف موقوف حاضر

من مواليد: 1986/ بـ: باتنة
ابن:
الساكن : رقم عازب -ة ، مهنة حرة
بواسطة الأستاذ (ة): بباتنة//موقوف

من جهة اخرى

** بيان وقائع الدعوى **

حيث أن المتهم تمت متابعته من طرف نيابة محكمة باتنة بجرائم الدخول عن طريق الغش في منظومة المعالجة الآلية للمعطيات والبحث والتجمع والنشر والاتجاز في المعطيات المخزنة معالجة ومرسلة عن طريق منظومة معلوماتية طبقا للمواد 394 مكرر و394 مكرر02 و394 مكرر 06 من ق.ع والذي هو متهم القيام بهم على الطرف المدني المؤسسة الامريكية ساتوفات واركس وذلك بتاريخ 2009/04/08 وعلى كل حال منذ زمن لم يمض عليه التقادم بعد بدائرة اختصاص مجلس قضاء باتنة وقد أحيل على محكمة الجنح ببتنة بموجب أمر بالاحالة المحرر من طرف قاضي التحقيق بتاريخ 2010/04/20 وأن المحكمة أصدرت حكما بتاريخ 2010/06/01 قضى حضوري وجاهي بادانة المتهم بجريمتي الدخول عن طريق الغش في منظومة للمعالجة الالية للمعطيات والبحث والتجمع والنشر والاتجاز في معطيات مخزنة معالجة ومرسلة عن طريق منظومة معلوماتية طبقا للمواد 394 مكرر و394 مكرر 02 و394 مكرر 06 من ق.ع والحكم عليه بعام حبس نافذ و 50.000 دج غرامة نافذة مع مصادرة المحجوزات وهو الحكم المستانف من طرف المتهم بواسطة دفاعه بتاريخ 2010/06/02 ومن طرف النيابة بتاريخ 2010/06/03 .

** وعـليه فإن المجـلس **

-بعد الإستماع الى الرئيس المقرر في تلاوة تقريره المكتوب.
- بعد الاطلاع على ملف القضية والاوراق المرفقة به
-بعد الإطلاع على المادة 416 ومابعدها من ق إ ج .
-بعد الإستماع الى المتهم
-بعد الإستماع الى طلبات السيد النائب العام.
- بعد الاستماع الى دفاع المتهم واعطاء الكلمة الاخيرة لهذا الاخير
-بعد المداولة طبقا للقانون.
-من حيث الشكل:إن الإستئنافين المرفوعين قد وردا داخل الأجال القانونية مما يتعين قبولهما.
-من حيث الموضوع:أنه يستخلص من خلال الملف انه بناء على ارسالية واردة من وزارة العدل الامريكية (المكتب الفيدرال للتحقيقات) تفيد تعرض المنظومة المعلوماتية لمؤسسة أمريكية SAGO NET WORKS التي تعتبر بنك معلوماتية جهوية كبيرة بولاية فلوريدا الامريكية المنطقة (TAMPA) وتعود الوقائع الى تاريخ 2009/04/08 أين استلمت مؤسسة سافونات ووركس في بريدها الالكتروني من طرف شخص مجهول صاحب علبة البريد الالكتروني وأكد من خلاله انه اكتشف طريقة للدخول عن طريق الغش الى المعطيات الالكترونية لهذه المؤسسة عبر نظام المشتغل logiciel والمسمى ubersmith المرتبط بشبكة الانترنات وبتاريخ 2009/04/10 تلقت نفس المؤسسة بريدين إلكترونيين من نفس العنوان: @gmail.com . الاول يحمل تصريح صاحبه بان جميع المعطيات والمعلومات الخاصة بمؤسسة SAGO تم استنافها وهي بحوزته وتضمن البريد صورة شلشة لقائمة المواقع الالكترونية التابعة للمؤسسة اما البريد الثاني فجاء فيه عبارة tentative bonne كرد للمؤسسة بعد اكتشافها للاختراق الواقع على نظامها المعلوماتي وقد استعمل الشخص المجهول عناوين الالكترونية موزعة بالجزائر والتابعة لاتصالات الجزائر فوري وبعدها بتاريخ 2009/04/10 تلقت مؤسسةSAGO رسالة مجهولة يطلب من خلالها مبلغ مالي مستعملا العنوان الالكتروني : التابع لاتصالات الجزائر فوري وبتاريخ 2009/04/16 تلقت المؤسسة بريدا الكترونيا من طرف صندوق بريد يحمل عنوان يخطرهم بأن نظامهم قد اختراقه وأن المعلومات الخاصة بالصرف التي تسمح باختراقه معروضة للبيع على موقع unknown.wn وأن الضبطية القضائية بالجزائر قد استطاعت تحديد هوية الشخص الذي اخترق موقع ومعطيات الالكترونية لشركات أجنبية لما فيها شركة سافونات ووركس والذي كان يستعمل الخط الهاتفي يحمل لصحابه المدعو يقم بمدينة باتنة وقد تعرفوا بان المشتبه فيه هو الذي كان يستعمل شبكة الانترنات ADSL FAWRI وتم استعمال عنوان بروتوكول الانترنيت(IP) وهو تابع لمؤسسة اتصالات الجزائر فوري وتم الدخول من قبل المشترك على الخط وهو ان المشتبه فيه وبعد توقيفه من طرف الضبطية القضائية وبموجب الاذن بالتفتيش رقم 3135/ن ع /2009 المحرر بتاريخ 2009/12/26 وقد تم العثور على أجهزة اعلام آلي وملحقاته ومبالغ مالية بالعملة الوطنية تقدر (219000 دج) وكذلك وأحد وثلاثون وصل للحوالات المالية عن طريق وسترن يونيون بنك باسم المشتبه فيه .
- حيث ان المتهم قد اعترف في محضر التحقيق الابتدائي بالوقائع المنسوبة اليه وأكد انه فعلا قام باختراق عدة مواقع ومعطيات معلوماتية لعدة شركات أجنبية وذلك عن طريق القرصنة وأنه كان يستعمل خلال هذه العمليات عدة عناوين الكترونية واستحدث من خلالها أسماء خاصة بها أرقام سرية وقد قام باختراق مؤسسة (صاكوناتواركس) الامريكية كما أقر بأنه يقوم بعمليات الاختراق والقرصنة منذ سنة 2006 وقد اعترف بأنه تحصل على مبالغ مالية وأكد ايضا بان الحوالات البريدية التي حجزت بمنزله كان مصدرها نشاطه بهذا الغش وحصوله على المعلومات التي يروجها باختراق الانظمة المعلوماتية .
حيث ان المتهم قد اعترف أثناء مرحلة التحقيق القضائي باختراقه عدة برامج معلوماتية لعدة

رقم الجدول: 10/05805
رقم الفهرس: 10/05812

مؤسسات وشركات اجنبية منها صاكوناتوركس.
- حيث انه اكد في جلسة المحاكمة بالمجلس بأنه فعلا دخل عن طريق الخطأ وليس عن طريق القصد.
- حيث انه بناء على ذلك فقد ثبت للمجلس بأن المتهم تاجر في المعطيات الذي تحصل عليها بواسطة القرصنة والاختراق الغير المشروع وهذا ما تؤكده الحوالات المالية الذي تحصل عليها المتهم عن طريق وسترن يونيون بنك.
حيث أن دفع المتهم بأنه دخل عن طريق الخطأ غير مؤسس وتعين رفضه لأنه دخل متعمدا او باع المعلومات المتحصل عليها وتحصل مقابل ذلك على مبالغ مالية وأن سوء النية ثابت بالدخول والاختراق للمنظومة المعلوماتية للغير.
- حيث ان دخول المتهم الى مواقع تتضمن منظومة للمعالجة الالية للمعطيات الخاصة بالشركة الامريكية صافونا ووركس والتي تعتبر بنك معلوماتية جهوية عن طريق الغش ثابت في حق المتهم باستعمال لبرامج القرصنة ومنها برنامج إيبار سميث في حقه أيضا تجميعه وتخزينه للمعطيات الآتية ثابت في حقه ايضا حسبما وجد بالقرص المضغوط المحجوز وكذلك القرص الصلب الخاص بجهاز الكمبيوتر الذي كان يستعمل من طرف المتهم.
- حيث أنه تثبت هذه المعطيات المتحصل عليها الخاصة ببعض الشركات وقيامه بارسال هذه المعطيات الى قراصنة آخرين .
- حيث انه تبعا لكل ما تقدم فقد ثبت للمجلس بان أركان جنحتي الدخول وعن طريق الغش في منظومة للمعالجة الالية للمعطيات والبحث والتجميع والنشر والاتجار في معطيات مخزنة معالجة ومرسلة عن طريق منظومية معلوماتية ثابتة في حقه مما يتعين ادانته والحكم عليه طبقا للمواد 394 مكرر و394 مكرر02 و394 مكرر 06 من ق.ع.
حيث انه تبعا ذلك فقد ثبت للمجلس بان الحكم المستانف قد اصاب وطبق صحيح القانون مما يتعين تاييده مبدئيا وتعديله بعد اسعاف المتهم بظروف التخفيف طبقا للمادة 592 من ق.إ.ج لأنه لم يسبق الحكم عليه من قبل بأية عقوبة سالبة للحرية بجعل ستة أشهر حبس نافذة في حقه وستة أشهر حبس موقوفة التنفيذ .
- حيث ان المتهم قد حضر جلسة المحاكمة امام المجلس وكذلك عند النطق بالقرار وعليه فهو حضوري وجاهي في حقه .
- حيث أن الطرف المدني لم يحضر ولا يوجد بالملف ما يثبت صحة تبليغه لذلك فالقرار يكون غيابيا في حقها.
حيث أن المصاريف القضائية يتحملها المتهم
حيث أن المجلس قرر تحديد مدة الاكراه البدني بحدها الاقصى .

** لهـــذه الأســـباب **

قرر المجلس علنيا حضوريا وجاهي للمتهم وغيابيا للطرف المدني نهائيا :
في الشكل : قبول الاستئنافين
في الموضوع :تاييد الحكم المستانف مبدئيا وتعديله بجعل ستة اشهر حبس نافذة في حق المتهم وستة اشهر حبس موقوفة التنفيذ.
-وتحميله بالمصاريف القضائية .
-وتحديد مدة الاكراه البدني بحدها الاقصى قانونا

المصاريف الابتدائية : 800دج
المصاريف الاستئناف 1000دج
المجموع : 1800دج.

الرئـــيس (ة) المقرر — أميـن الضبـط

رقم الجدول: 10/05805
رقم الفهرس: 10/05812

قائمة المصادر والمراجع

قائمة المصادر والمراجع

- **باللغة العربية**

أولا: القرآن الكريم، برواية ورش عن الإمام نافع.

ثانيا: النصوص القانونية

I. النصوص التشريعية

1. التعديل الدستوري لسنة 2020، المصادق عليه في استفتاء 01-11-2020 المؤرخ في 30-12-2020، الصادر بالمرسوم الرئاسي رقم 20-442، الصادر بتاريخ: 30-12-2020، الجريدة الرسمية لسنة 2020، العدد 82.

2. الاتفاقيات الدولية

أ- الإعلان العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة للأمم المتحدة 217 ألف (د-3)، المؤرخ في 10-12-1948.

ب- المعاهدة النموذجية لنقل الإجراءات في المسائل الجنائية، اعتمدت بموجب قرار الجمعية العامة للأمم المتحدة رقم 14-252 المؤرخ في: 14-12-1990.

ت- اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية، المعتمدة من قبل الجمعية العامة للأمم المتحدة 217 (أ-د)، بتاريخ: 15-11-2000، المصادق عليها بتحفظ بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في: 05-02-2002، الجريدة الرسمية لسنة 2002، العدد 09.

ث- القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات، تم اعتماده إثر اجتماع مجلس الوزراء العرب في دورته 19 بالقرار رقم 490-د 19، بتاريخ: 08-10-2003.

ج- الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، المعتمدة من طرف مجلس أوروبا بتاريخ: 08-01-2001، تم فتح باب التوقيع في بودابيست بتاريخ: 23-11-2001، دخلت حيز التنفيذ عام 2004.

ح- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجزائر وإيطاليا، المؤرخة في 13-02-2005، المصادق عليها بالمرسوم الرئاسي رقم 05-73، الصادر في الجريدة الرسمية لسنة 2005، العدد 13.

خ- الاتفاقية المتعلقة بالتعاون القضائي في المجال الجزائي بين الجزائر وجمهورية الصين الشعبية، المؤرخة في 06-06-2007، المصادق عليها بالمرسوم الرئاسي رقم 07-175، الصادر في الجريدة الرسمية لسنة 2007، العدد 38.

د- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، المحررة بالقاهرة بتاريخ: 21-12-2010، المصادق عليها بموجب المرسوم الرئاسي رقم 14-252، المؤرخ في 08-09-2014، الجريدة الرسمية رقم لسنة 2014، العدد 57

3. القوانين

03-01- القوانين الوطنية

أ- قانون رقم 90-07 المؤرخ في: 03-04-1990، المتعلق بالإعلام، الجريدة الرسمية لسنة 1990، العدد 14، الملغى بموجب القانون العضوي رقم 12-05 المؤرخ في: 12-01-2005.

ب- القانون العضوي رقم 04-11 المؤرخ في 06-09-2004 المتضمن القانون الأساسي للقضاء، الجريدة الرسمية لسنة 2004، العدد 57.

ت- قانون رقم 90-03 مؤرخ في 06 فبراير سنة 1990، المتعلق بمفتشية العمل، الجريدة الرسمية لسنة 1990، العدد 06.

ث- القانون رقم 2000-03 المؤرخ في 05-08-2000 المحدد للقواعد العامة المتعلقة بالبريد والمواصلات السلكية واللاسلكية، الجريدة الرسمية لسنة 2000، العدد 48.

ج- القانون رقم 04-15 المؤرخ في 10-11-2004 المعدل والمتمم لقانون العقوبات، الجريدة الرسمية لسنة 2004، العدد 71.

ح- القانون رقم 07-05 المؤرخ في 13-05-2007 المعدل والمتمم للأمر رقم 75-58 المؤرخ في 26-09-1975 المتضمن القانون المدني.

خ- القانون رقم 09-03 المؤرخ في 25 فبراير 2009، المتعلق بحماية المستهلك وقمع الغش الجريدة الرسمية لسنة 2009، العدد 15.

د- القانون رقم 09-04 المؤرخ في 05-08-2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية لسنة 2009، العدد 47.

ذ- القانون رقم 15-12 المؤرخ في 15-07-2015 المتعلق بحماية الطفل، الجريدة الرسمية لسنة 2015، العدد 39.

ر- القانون رقم 20-05 المؤرخ في 28-04-2020 المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية الجزائرية لسنة 2020، العدد 25.

ز- القانون رقم 20-15 المؤرخ في 30-12-2020 المتعلق بالوقاية من جرائم اختطاف الأشخاص ومكافحتها، الجريدة الرسمية لسنة 2020، العدد 81.

س- القانون رقم: 21-15 المؤرخ في 28-12-2021 المتعلق بمكافحة المضاربة غير المشروعة، الجريدة الرسمية لسنة 2021، العدد 99.

ش- القانون 23-01 المؤرخ في 07-02-2023 المتعلق بالوقاية من تبييض الأموال وتمويل الإرهاب ومكافحتهما، المعدل والمتمم للقانون رقم 05-01 المؤرخ في 06-02-2005، الجريدة الرسمية لسنة 2023، العدد 08.

ص- القانون رقم 23-04 المؤرخ في 07-05-2023 المتعلق بالوقاية من الاتجار بالبشر ومكافحته، الجريدة الرسمية لسنة 2023، العدد 32.

ض- القانون رقم 24-02 المؤرخ في 26-02-2024 المتعلق بمكافحة التزوير واستعمال المزور، الجريدة الرسمية لسنة 2024، العدد15.

03-02- القوانين الأجنبية

أ- قانون الإجراءات الجزائية الفرنسي رقم 1426/57 المؤرخ في: 31-12-1957، الجريدة الرسمية، عدد 20، الصادرة بتاريخ 08-01-1958، المعدل والمتمم بالقانون رقم 1109/2021 المؤرخ في 24-08-2021.

ب- قانون الإجراءات الجنائية المصري الصادر بالقانون رقم 150 لسنة 1950، المعدل بالقانون رقم 01 لسنة 2024، الجريدة الرسمية الصادرة بتاريخ 16-01-2024، عدد 02 مكرر.

ت- قانون العقوبات السوري، الصادر بالمرسوم التشريعي رقم 148 بتاريخ: 1949، المعدل بموجب المرسوم التشريعي رقم 04 لعام 2020، المؤرخ في: 18-01-2020.

ث- قانون رقم: 63 لسنة 2015 في شأن مكافحة جرائم تقنية المعلومات، الصادر بتاريخ: 07 يوليو 2015، الجريدة الرسمية للكويت، العدد: 1244، الصادرة بتاريخ: 12-07-2015.

ج-نظام مكافحة الجرائم المعلوماتية السعودي، الصادر بموجب المرسوم الملكي رقم: م/17 بتاريخ: 08-03-1428 الموافق لـ: 27-03-2007.

4. الأوامر

أ- الأمر رقم 20-01 المؤرخ في: 30-07- 2020 المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية لسنة 2020، العدد 44.

ب- الأمر رقم 20-03 المؤرخ في: 20-08-2020، المتعلق بالوقاية من عصابات الأحياء ومكافحتها، الجريدة الرسمية لسنة 2020، العدد 51.

ت- الأمر رقم 20-04 المؤرخ في 30-08-2020 ، المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية لسنة 2020 ، العدد 51.

ث- الأمر رقم 21-09 المؤرخ في 08-06-2021 المتعلق بحماية المعلومات والوثائق الإدارية، الجريدة الرسمية لسنة 2021، العدد 45.

ج- الأمر رقم 21-11 المؤرخ في 25-08-2021 المتمم للأمر رقم 66-155 المتمم لقانون الإجراءات الجزائية، الجريدة الرسمية لسنة 2021، العدد 65.

II. النصوص التنظيمية

1. المراسيم الرئاسية

أ- مرسوم رقم 66-167 المؤرخ في 08-06-1966، يحدد لتأليف وتسيير اللجنة المكلفة بامتحان المترشحين لمهام ضباط شرطة قضائية، الجريدة الرسمية لسنة 1966، العدد 50.

ب- مرسوم رئاسي رقم 04-183، مؤرخ في 26-06-2004 يتضمن إحداث المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، الجريدة الرسمية لسنة 2004، العدد 41.

ت- مرسوم رئاسي رقم: 09-143 المؤرخ في: 27-04-2009، يتضمن لمهام الدرك الوطني وتنظيمه، الجريدة الرسمية لسنة 2009، العدد 26.

ث- مرسوم رئاسي رقم 15-261 مؤرخ في: 08-10-2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية لسنة 2015، العدد 53.

ج- مرسوم رئاسي رقم 19-172 مؤرخ في: 06-06-2019 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية لسنة 2019، العدد 37.

ح- مرسوم رئاسي رقم 20-183 مؤرخ في: 13-07-2020 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية لسنة 2020، العدد 40.

خ- مرسوم رئاسي رقم 21-439 مؤرخ في: 07-11-2021 يتضمن إعادة تنظيم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، الجريدة الرسمية لسنة 2021، العدد 86.

2. المراسيم التنفيذية

أ- مرسوم تنفيذي رقم: 06-348 المؤرخ في: 05-10-2006 يتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية لسنة 2006، العدد 63.

ب- مرسوم تنفيذي رقم: 16-267 مؤرخ في: 17-10-2016 يعدل المرسوم التنفيذي رقم: 06-348 المتضمن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق، الجريدة الرسمية لسنة 2016، العدد 62.

3. القرارات الوزارية المشتركة

- القرار الوزاري المشترك المؤرخ في 14-04-2007 المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، الجريدة الرسمية لسنة 2007، العدد 15.

ثالثا: المعاجم والقواميس

1. أبو الفضل جمال الدين ابن منظور، لسان العرب، دار صادر للطباعة والنشر، بيروت، بدون سنة نشر.

2. علي بن هادية وآخرون، القاموس الجديد للطلاب، ط15، المؤسسة الوطنية للكتاب، الجزائر، 1984.

3. مجمع اللغة العربية، المعجم الوسيط، الإدارة العامة للمجمعات وإحياء التراث، ط 4، مكتبة الشروق الدولية، مصر، 2004.

رابعا: المؤلفات

1. ابراهيم صادق الجندي، حسين حسن الحسيني، تطبيقات البصمة الوراثية في التحقيق والطب الشرعي، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2002.
2. أبو زيد أحمد محمد، إرشادات وتطبيقات عملية في التحقيق الجنائي، ط2، دار الإيمان للكمبيوتر، مصر 2002.
3. أبي زكرياء محي الدين يحيى بن شرف النووي، رياض الصالحين من كلام سيد المرسلين، ط2، دار ابن الجوزي للنشر والتوزيع، مصر، 2014.
4. أحسن بوسقيعة، التحقيق القضائي، ط13، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021.
5. أحسن بوسقيعة، الوجيز في القانون الجزائي العام، ط 11، دار هومة للطباعة والنشر والتوزيع، 2012.
6. أحمد بسيوني أبو الروس، التحقيق الجنائي والتصرف فيه والأدلة الجنائية، ط 2، المكتب الجامعي الحديث، الإسكندرية، 2008.
7. أحمد داودي، تأثير تكنولوجيا المعلومات في تحسين صورة المؤسسة (دراسة ميدانية)، المركز الأكاديمي للنشر، الإسكندرية، 2022.
8. أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، ط 3، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2017.
9. أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، 1993.
10. أحمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، ط1، دار النهضة العربية، القاهرة، 2003.
11. أحمد هلالي عبد اللاه، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابيست، دار النهضة العربية، القاهرة، مصر، 2006.
12. أحمد هلالي عبد اللاه، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دار النهضة العربية، القاهرة، 2006.

13. أحمد يوسف الطحطاوي، الأدلة الإلكترونية ودورها في الإثبات الجنائي (دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2015.

14. أسامة عبد الله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، ط3، دار النهضة العربية، القاهرة، 1994.

15. انتصار نوري الغريب، أمن الكمبيوتر والقانون، ط1، دار الراتب الجامعية، بيروت، 1994.

16. إيهاب عبد المطلب، تفتيش الأشخاص والأماكن، ط1، المركز القومي للإصدارات القانونية، مصر، 2009.

17. برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية، دار النهضة العربية، القاهرة، 2006.

18. برهامي أبو بكر عزمي، الشرعية الإجرائية للأدلة العلمية، دار النهضة العربية، القاهرة، 2006.

19. بهاء المرَي، جرائم المحمول ووسائل التواصل الاجتماعي وحجية الدليل الإلكتروني في الإثبات، ط1، دار الأهرام للنشر والتوزيع والإصدارات القانونية، مصر، 2022.

20. توفيق الشاوي، فقه الإجراءات الجنائية، الجزء الأول، ط 2، دار الكتاب العربي، مصر، 1994.

21. توم فوريستر، مجتمع التقنية العالية، قصة ثورة تقنية المعلومات، ترجمة ونشر مركز الكتاب الأردني، عمان، الأردن، 1989.

22. ثريا تيجاني، القيم الاجتماعية والتلفزيون في المجتمع الجزائري، دار الهدى للطباعة والنشر، عين مليلة، الجزائر، 2011.

23. جمال نجيمي، دليل القضاة للحكم في الجنح والمخالفات، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2014.

24. جمال نجيمي، قانون الإجراءات الجزائية على ضوء الاجتهاد القضائي، الجزء الأول، ط1، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015.

25. جميل عبد الباقي الصغير، الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002.

26. جميل عبد الباقي الصغير، الجرائم الناشئة عن استخدام الحاسب الآلي، ط1، دار النهضة العربية، القاهرة، 1992.

27. جيلالي بغدادي، التحقيق، الديوان الوطني للأشغال التربوية، ط 1 ، الجزائر، 1999.

28. حازم محمد خلفي، الدليل الإلكتروني ودوره في المجال الجنائي، ط1، دار النهضة العربية، القاهرة، 2017.

29. حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دار النهضة العربية، القاهرة، 2009.

30. حسين طاهري، إجراءات جمع الأدلة والتحقيقات الأولية في الجرائم المعلوماتية، درا العلا للطباعة والنشر، أم البواقي، الجزائر، 2023.

31. خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنيت، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

32. خير الدين علي عويس، عطا حسن عبد الرحيم، الإعلام الرياضي، ج 1، ط1، مركز الكتاب للنشر، القاهرة، 1998.

33. خيرت علي محرز، التحقيق في جرائم الحاسب الآلي، دار الكتاب الحديث، القاهرة، 2012.

34. رامي وسام أبو ملحم، المجرم والضحية المعلوماتيين على ضوء علم الإجرام، المؤسسة الحديثة للكتاب، لبنان، 2022.

35. رحيمة الطيب عيساني، الوسائط التقنية الحديثة وأثرها على الإعلام المرئي والمسموع، الرياض، 2010.

36. رشا مصطفى أبو الغيط، الحماية القانونية للكيانات المنطقية، ملتقى الفكر، الإسكندرية، 2000.

37. رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري والمقارن، ط1، منشورات الحلبي الحقوقية، بيروت، 2012.

38. رفعت رشوان، مبدأ إقليمية قانون العقوبات في ضوء القانون الجنائي الداخلي والدولي، ط1، دار الجامعة الجديدة، مصر، 2007.

39. رمضان مدحت، جرائم الاعتداء على الأشخاص والإنترنت، ط1، دار النهضة العربية، القاهرة، 2000.

40. رؤوف عبيد، مبادئ الإجراءات الجنائية في القانون المصري، دار الجبل للطباعة، مصر، 1995.

41. زهير احدادن، مدخل إلى علم الإعلام والاتصال، ديوان المطبوعات الجامعية، الجزائر، 1993.

42. زياد القاضي، أساسيات علم الحاسوب، ط1، دار صفاء للنشر والتوزيع، عمان، الأردن، 1997.

43. زيدان زيبحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر، 2011.

44. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي، دار الكتب القانونية، مصر، 2011.

45. سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، ط1، دار النهضة العربية، مصر، 1972.

46. سليم علي عبده، التفتيش في ضوء أصول المحاكمات الجزائية الجديد، ط 01، منشورات زين الحقوقية، بيروت، 2006.

47. سليمان أحمد فضل، المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، 2013.

48. سليمان بن عبد الله بن سليمان العجلان، حق الإنسان في حرمة مراسلاته واتصالاته الهاتفية الخاصة في النظام الجنائي السعودي، دراسة تطبيقية مقارنة، الرياض، 2005.

49. الشهاوي قدري عبد الفتاح، ضوابط التفتيش في التشريع المصري والمقارن، منشاة المعارف، الإسكندرية، 2005.

50. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، دار الجامعة الجديدة، الإسكندرية، مصر 2009.

51. طارق الشدي، آلية البناء الأمني لنظم المعلومات، دار الوطن للطباعة والنشر والإعلام، الرياض، 1999.

52. عادل عزام سقف الحيط، جرائم الذم والقدح والتحقير المرتكبة عبر الوسائط الإلكترونية، ط1، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2011.

53. عامر ابراهيم قنديلجي، علاء الدين عبد القادر الجنابي، نظم المعلومات الإدارية، ط1، دار الميسرة، الأردن، 2005.

54. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي، درا الجامعة الجديدة، الإسكندرية، 2015.

55. عبد الرحمان خلفي، الإجراءات الجزائية في التشريع الجزائري والمقارن، ط 4، دار بلقيس، الجزائر، 2018-2019.

56. عبد الفتاح بيومي حجازي، الأحداث والإنترنت، ط1، دار الفكر لجامعي، الإسكندرية، 2002.

57. عبد الفتاح بيومي حجازي، الجرائم المستحدثة في نطاق تكنولوجيا الاتصالات الحديثة، ط1، المركز القومي للإصدارات القانونية، القاهرة، 2001.

58. عبد الفتاح بيومي حجازي، الدليل الجنائي في جرائم الكمبيوتر والتزوير، دراسة معمقة في جرائم الحاسب الآلي والإنترنت، دار الكتب القانونية، مصر، 2004.

59. عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار المطبوعات الجامعية، الإسكندرية، مصر، 2003.

60. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2015.

61. عبد الله أوهايبية، شرح قانون العقوبات الجزائري، المؤسسة الوطنية للفنون المطبعية، الرغاية، الجزائر، 2011.

62. عبد الله بن سعود محمد السراني، فاعلية الأساليب المستخدمة في إثبات جريمة التزوير الإلكتروني، ط1، جامعة نايف العربية للعلوم الأمنية، الرياض، 2011.

63. عبد الله سليمان، شرح قانون العقوبات الجزائري (القسم العام)،ج 1، ط 6، ديوان المطبوعات الجامعية، الجزائر، 2005.

64. عبد الله سليمان، نظام الإثبات في المواد الجنائية في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، بن عكنون الجزائر، 1999.

65. عبد الله عبد الكريم عبد الله، جرائم المعلوماتية والإنترنت، ط1، منشورات الحلبي الحقوقية، لبنان، 2007.

66. عبد المطلب حمزة، الإعلام والدعاية، دار الفكر العربي، القاهرة، 1984.

67. عبد المهيمن بكر، إجراءات الأدلة الجنائية، الجزء الأول، ط1، دار الفكر العربي، القاهرة، 1997.

68. عبد الواحد إمام مرسى، التحقيق الجنائي علم وفن(بين النظرية والتطبيق)، دار الفكر الجامعي، القاهرة، 1998.

69. عصام أبو العز، دور التقنيات العلمية الحديثة في الإثبات الجنائي، دار النهضة العربية، القاهرة، 2020.

70. عصام سليمان الموسى، مدخل إلى الاتصال الجماهيري،ط 6، إثراء للنشر، عمان، الأردن، 2008.

71. علي حسن الطوالبة، الجرائم الإلكترونية، ط1، مؤسسة فخراوي للدراسات والنشر، البحرين، 2008.

72. علي عبود جعفر، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، ط1، منشورات زين الحقوقية والأدبية، لبنان، 2013.

73. علي فلاح الضلاعين وآخرون، مقدمة في الإعلام، دار الإعصار للنشر والتوزيع، الأردن، 2015.

74. عمر زودة، الإثبات في المواد الجزائية، ط2، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2021.

75. عمر محمد بن يونس، أشهر المبادئ المتعلقة بالإنترنت في القضاء الأمريكي، دار النهضة العربية، القاهرة، 2004.

76. العياشي زرزار، كريمة غياد، استخدامات تكنولوجيا المعلومات والاتصال في المؤسسة الاقتصادية ودورها في دعم الميزة التنافسية، دار صفاء للنشر والتوزيع، عمان، الأردن، 2015.

77. عيسى طوني، التنظيم القانوني لشبكة الإنترنت، ط1، المنشورات الحقوقية، 2001.

78. غسان قاسم اللامي، إدارة التكنولوجيا، ط1، دار المناهج، عمان، الأردن، 2006.

79. غنية باطلي، الجريمة الإلكترونية (دراسة مقارنة)، الدار الجزائرية للنشر والتوزيع، الجزائر، 2016.

80. فادي حجار، بنية الحاسب، ط 1، دار شعاع للنشر والعلوم، حلب، سوريا، 1999.

81. فاروق الحفناوي، موسوعة قانون الكمبيوتر ونظم المعلومات، ط1، دار الكتاب الحديثة، القاهرة، 2001.

82. قوي بوحنية، الاتصالات الإدارية داخل المنظمات المعاصرة، ديوان المطبوعات الجامعية، الجزائر، 2010.

83. كامل عفيفي عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية ودور الشرطة والقانون، منشورات الحلبي الحقوقية، لبنان، 2007.

84. لحسن ناني، التحقيق في الجرائم المتصلة بتكنولوجيا المعلوماتية بين النصوص التشريعية والخصوصية التقنية، النشر الجامعي الجديد، تلمسان، الجزائر، 2018.

85. لينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، ط1، دار الحامد للنشر والتوزيع، الأردن، 2015.

86. محمد الدريني، مقدمة في أساسيات الحاسب، ط1، معهد الإدارة العامة، المملكة العربية السعودية، 1987.

87. محمد الصيرفي، إدارة تكنولوجيات المعلومات، ط1، دار الفكر الجامعي، الإسكندرية، 2009.

88. محمد الطراونة، ضمانات حقوق الإنسان في الدعوى الجزائية (دراسة مقارنة)، ط 1، دار وائل للنشر والتوزيع، عمان، الأردن، 2003.

89. محمد المنشاوي، جرائم الإنترنت في المجتمع السعودي، أكاديمية نايف العربية للعلوم الأمنية، 2003.

90. محمد الهوش أبو بكر، تقنية المعلومات ومكتبة المستقبل، مكتبة الإشباع، الجماهيرية العظمى، 1996.

91. محمد أمين الخرشة، مشروعية الصوت والصورة في الإثبات الجنائي، ط1، دار الثقافة للتوزيع والنشر، عمان، الأردن، 2011.

92. محمد أمين الرومي، جرائم الكمبيوتر والإنترنت، ط1، دار النهضة العربية، القاهرة، 2003.

93. محمد حزيط، قاضي التحقيق في النظام القضائي الجزائري، ط 4، دار هومه للطباعة والنشر والتوزيع، الجزائر، 2014.

94. محمد حماد مرهج الهيتي، جرائم الحاسوب، ط1، دار المناهج للنشر والتوزيع، عمان، الأردن، 2006.

95. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن، دار الجامعة الجديدة، الإسكندرية، 2007.

96. محمد زكي أبو عامر، الإجراءات الجنائية، منشورات الحلبي الحقوقية، لبنان، 2010.

97. محمد سيد علي السيد، الجرائم الإلكترونية، دار التعليم الجامعي، الإسكندرية، 2020.

98. محمد عبد الرحمن عنانزه، القصد الجرمي في الجرائم الإلكترونية، ط1، دار الأيام للنشر والتوزيع، عمان، الأردن، 2017.

99. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة، الإسكندرية، 2004.

100. محمد علي عياد، شرح قانون العقوبات، دار الثقافة للنشر والتوزيع، عمان، الأردن، 1997.

101. محمد محمد الألفي، ندوة مكافحة الجريمة عبر الإنترنت على المستوى العربي، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، شرم الشيخ، مصر، 2008.

102. محمود ابراهيم غازي، الحماية الجنائية للخصوصية والتجارة الإلكترونية، ط1، مكتبة الوفاء القانونية، الإسكندرية، 2014.

103. محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، ط1 دار الثقافة للنشر والتوزيع، عمان، 2009.

104. محمود جمال الدين زكي، الخبرة في المواد المدنية والتجارية، مطبعة جامعة القاهرة، مصر، 1990.

105. محمود عبد الله حسين، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002.

106. محمود محمد محمود جابر، الأحكام الإجرائية للعلوم الناشئة عن استخدام الهواتف النقالة، المكتب الجامعي الحديث، مصر، 2018.

107. محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ط3، دار النهضة العربية، القاهرة، 1995.

108. محمود نجيب حسني، شرح قانون العقوبات اللبناني، المجلد الأول، ط3، منشورات الحلبي الحقوقية، بيروت، 1988.

109. مزهر شعبان العاني، شوقي ناجي جواد، العملية الإدارية وتكنولوجيا المعلومات، ط1، إثراء للنشر والتوزيع، الأردن، 2008.

110. مصطفى عليان ربحي، إيمان فاضل السامرائي، تسويق المعلومات، دار الصفاء للطباعة والنشر، عمان، الأردن، 2004.

111. منصور رحماني، الوجيز في القانون الجنائي العام، دار العلوم للنشر، الجزائر، 2006.

112. موسى مصطفى محمد، التحقيق الجنائي في الجرائم الإلكترونية، ط1، مطابع الشرطة، القاهرة، 2009.

113. مي العبد الله، نظريات الاتصال، ط2، دار النهضة العربية، بيروت، 2010.

114. نائلة عادل محمد قورة، جرائم الحاسب الآلي الاقتصادية (دراسة نظرية وتطبيقية)، منشورات الحلبي الحقوقية، بيروت، 2005.

115. نبيلة هبة هروال، الجوانب الإجرائية لجرائم الإنترنت في مرحلة جمع الاستدلالات (دراسة مقارنة)، دار الفكر الجامعي، الإسكندرية، 2013.

116. نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الأردن، 2010.

117. هدى حامد قشقوش، جرائم الحاسب الإلكتروني في التشريع المقارن، دار النهضة العربية، القاهرة، 1992.

118. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، أسيوط، مصر، 1994.

119. هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، مصر، 1992.

120. ياسر الأمير فاروق، مراقبة الأحاديث الخاصة في الإجراءات الجنائية، دار المطبوعات الجامعية، الإسكندرية، 2009.

121. يحيى عطوة الزنط، الممارسات العملية لأمن نظم المعلومات الحكومية ومنهجية مكافحة الجرائم السيبرانية، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، 2022.

122. يحيى مصطفى حلمي، الحاسبات الإلكترونية، مكتبة عين شمس، القاهرة، 1996.

123. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، الإسكندرية، 2019.

124. يوسف مناصرة، الدليل الإلكتروني في القانون الجزائي، دار الخلدونية، الجزائر، 2021.

125. يوسف مناصرة، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، دار الخلدونية، الجزائر، 2018.

خامسا: الأطروحات و الرسائل الجامعية

I. أطروحات الدكتوراه

1. جمال براهيمي، التحقيق الجنائي في الجرائم الإلكترونية، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2018.

2. حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، 2015-2016.

3. خضرة شنتير، الآليات القانونية لمكافحة الجريمة الإلكترونية، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية، أدرار، الجزائر، 2020-2021.

4. رابح لهوى، الشرعية الإجرائية للأدلة المستمدة من التفتيش، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة باتنة 1، الجزائر، 2020-2021.

5. سالم محمد سليمان الأوجلي، أحكام المسؤولية الجنائية عن الجرائم الدولية في التشريعات الوضعية، (أطروحة دكتوراه)، جامعة عين شمس، 1997.

6. عادل بوزيدة، المسؤولية الجزائية لمتعهدي مواقع الإنترنت، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة تبسة، الجزائر، 2017.

7. علي سالم النعيمي، المواجهة الجنائية للجريمة المنظمة، (دكتوراه في الحقوق)، كلية الحقوق، جامعة عين شمس، 2011.

8. فضيلة عاقلي، الحماية القانونية للحق في حرمة الحياة الخاصة (دراسة مقارنة)، (أطروحة دكتوراه)، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2011-2012.

9. فوزي عمارة، قاضي التحقيق، (أطروحة دكتوراه)، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2009-2010.

10. كاظم عبد الله نزال المياحي، حجية المراقبة الإلكترونية للصوت والصورة في الإثبات الجنائي (دراسة في القانون العراقي والمقارن)، (دكتوراه في الحقوق)، قسم القانون الجنائي، كلية الحقوق، جامعة عين شمس، مصر، 2016.

11. كمال بلارو، الشرطة القضائية في التشريع الجزائري، (أطروحة دكتوراه)، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، 2020-2021.

12. كمال عايد، تكنولوجيا الإعلام والاتصال وتأثيراتها على قيم المجتمع الجزائري، (أطروحة دكتوراه)، كلية العلوم الإنسانية والاجتماعية، جامعة أبي بكر بلقايد، تلمسان، الجزائر، 2016-2017.

13. ليندا بن طالب، الدليل الإلكتروني ودوره في الإثبات الجنائي، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، الجزائر، 2019.
14. نصيرة بوحزمة، التحقيق الجنائي في الجرائم الإلكترونية (دراسة مقارنة)، (أطروحة دكتوراه)، كلية الحقوق والعلوم السياسية، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، 2021-2022.
15. نورة هارون، جريمة الرشوة في التشريع الجزائري، (أطروحة دكتوراه)، جامعة مولود معمري، تيزي وزو، الجزائر، 2017.

II. رسائل الماجستير

1. أحمد كيلان عبد الله، الجرائم الناشئة عند إساءة استخدام الحاسوب، (رسالة ماجستير)، جامعة بغداد، 2002.
2. سليمان العنزي، وسائل التحقيق في جرائم نظم المعلومات، (رسالة ماجستير)، أكاديمية نايف للعلوم الأمنية، الرياض، 2003.
3. عبد الرحمن بحر، معوقات التحقيق في جرائم الإنترنت، (رسالة ماجستير)، أكاديمية نايف العربية للعلوم الأمنية، الرياض 1999.
4. علاء مغايرة، الأوجه الحديثة للجرائم المعلوماتية، (رسالة ماجستير)، جامعة الحكمة، بيروت، 2000.
5. نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتي في القانون الجزائري، (رسالة ماجستير)، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2012-2013.
6. نورة طرشي، مكافحة الجريمة المعلوماتية، (رسالة ماجستير)، كلية الحقوق، جامعة الجزائر 1، 2011-2012.

سادسا: المقالات العلمية المنشورة

1. أسامة بن غانم العبيدي، التفتيش عن الدليل في الجرائم المعلوماتية، المجلة العربية للدراسات الأمنية والتدريب، جامعة نايف العربية للعلوم الأمنية، المجلد 29، العدد 58، السعودية، 2013.

2. جمال الدين عنان، عولمة القانون الجنائي (الآليات والمظاهر)، مجلة الدراسات والبحوث القانونية، المجلد 3، العدد 4، 2018.

3. حسام الدين كامل الأهواني، الحماية القانونية للحياة الخاصة في مواجهة الحاسب الإلكتروني، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، العدد 1، 1990.

4. حمزة عبدلي، خصوصية إجراءات المتابعة وتوقيع الجزاء في جرائم الفساد، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 06، العدد 02، 2021.

5. ربيحة نبار، تكنولوجيا المعلومات والاتصالات (الخصائص والتأثيرات)، مجلة الباحث في العلوم الإنسانية والاجتماعية مجلد 9، عدد 2، 2018.

6. رحيمة لدغش، ضوابط تفتيش الحاسب الآلي، مجلة الحقوق والعلوم الإنسانية، المجلد 1، العدد 25، 2015.

7. رضا مهدي، الجرائم السيبرانية وآليات مكافحتها في التشريع الجزائري، مجلة إيليزا للبحوث والدراسات، المجلد 06، العدد 02، 2021.

8. رضا هميسي، تفتيش المنظومات المعلوماتية في القانون الجزائري، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد محمد لخضر، الوادي، العدد 5، جوان 2012.

9. زين العابدين سليم، محمد ابراهيم زيد، الأساليب الحديثة في مكافحة الجريمة، المجلة العربية للدفاع الاجتماعي، العدد 15، 1983.

10. سعاد رابح، ضوابط مكافحة الجريمة المعلوماتية، مجلة القانون العام الجزائري والمقارن، المجلد السابع، عدد 01 ، جامعة جيلالي اليابس، سيدي بلعباس، الجزائر، جوان،2021.

11. السعيد برابح، كمال بوبعاية، الأساليب المستحدثة ضمن استراتيجية الكشف عن الجرائم المستحدثة في التشريع الجزائري (التسرب نموذجا)، دفاتر البحوث العلمية، المجلد 09، العدد 01، 2021.

12. سليمان عيسى محمد أحمد، التعاون الدولي لمواجهة الجرائم الإلكترونية، المجلة الأكاديمية للبحث القانوني، المجلد 14، العدد 02، 2016.

13. الطيب بلواضح، الخدمات الإلكترونية المتاحة في مجال عصرنة الإدارة الجزائرية، مجلة الدراسات القانونية والسياسية، المجلد 06، العدد 01، 2020.

14. عادل عبد العال ابراهيم الخراشي، إشكالات التعاون الدولي في مكافحة الجرائم المعلوماتية وسبل التغلب عليها، مجلة كلية الشريعة والقانون، دقهلية، المجلد،01 العدد 16، 2014.

15. عبد القادر مصطفاوي، أساليب البحث والتحري الخاصة وإجراءاتها، مجلة المحكمة العليا، العدد الثاني، الجزائر، 2009.

16. فواز لجلط، خصائص الدعوى الإدارية ضمانة لمبدأ الشرعية، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد 01، 2016.

17. كمال بوبعاية، والي عبد اللطيف، الإشكالات التي تعترض تنسيق التعاون الدولي لمكافحة الجريمة المنظمة عبر الوطنية، مجلة الدراسات والبحوث القانونية، المجلد 06، العدد 01، 2021.

18. ليلى عصماني، صهيب سهيل غازي زامل، المساعدة القضائية الدولية آلية للحصول على الدليل الإلكتروني، مجلة القانون، المجتمع والسلطة، المجلد 09، العدد 02، 2020.

19. ليندا بن طالب، التفتيش في الجريمة المعلوماتية، مجلة العلوم القانونية والسياسية، كلية الحقوق والعلوم السياسية، جامعة الشهيد حمه لخضر الوادي، العدد 16، جوان 2017.

20. محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والإنترنت، المجلة العربية للدراسات الأمنية والتدريب، أكاديمية نايف للعلوم الأمنية، العدد 30، 2000.

21. محمد بعجي، التزامات مقدمي الخدمة عبر الانترنت، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 01، العدد 01، 2019.

22. محمد دفون، تكنولوجيا الإعلام والاتصال واستخداماتها، مجلة التراث، جامعة الجلفة، العدد 16، الجزائر، 2014.

23. المديرية العامة للأمن الوطني، "الجزائر تدعم المسعى الدولي لمكافحة الجريمة المنظمة العابرة للحدود"، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، رويبة، الجزائر، العدد 150، 2022.

24. المديرية العامة للأمن الوطني، "مديرية الشرطة القضائية: الحصن المنيع لصد الجريمة الإلكترونية"، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، رويبة، الجزائر، العدد 151، 2022.

25. المديرية العامة للأمن الوطني، "مصلحة التعاون الدولي: الإشعاع الدولي للشرطة الجزائرية"، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، رويبة، الجزائر، العدد 151، 2022.

26. المديرية العامة للأمن الوطني، أشغال الجمعية العامة الأولى لآلية أفريبول تتوج بقرارات هامة ستشكل خارطة طريق بالنسبة لقادة الشرطة الفارقة، "مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، رويبة، الجزائر، العدد 136، 2017، ص: 35.

27. المديرية العامة للأمن الوطني، المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: تشكيل عملياتي لمحاربة الجريمة عبر الشبكة العنكبوتية، مجلة الشرطة، المؤسسة الوطنية للاتصال والإشهار والنشر، رويبة، الجزائر، العدد 144، 2019.

28. نزيم محمد الترزي، سلطات النيابة العامة في الجرائم المعلوماتية، مجلس أندلس للعلوم الاجتماعية والإنسانية، مجلد 15، العدد 19، 2017.

29. نوال مغيزلي، تكنولوجيا الإعلام والاتصال في الجزائر (دراسة للمؤشرات وتشخيص للعقبات)، المجلة الجزائرية للأمن والتنمية، العدد 12، 2018.

30. هبة شعوة، تطبيق الشرطة الجزائرية، مجلة المعيار، م 02، عدد 22، جامعة الأمير عبد القادر للعلوم الإسلامية، قسنطينة، الجزائر، 2018.

31. هدى زوزو، التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة والقانون، جامعة قاصدي مرباح، ورقلة، العدد 11، 2014.

32. هشام محمد فريد رستم، جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة، مجلة الدراسات القانونية، جامعة أسيوط، العدد 17، 1990.

33. وسيمة مصطفى هنشور، النظام القانوني لمقدمي خدمات الإنترنت في التشريع الجزائري، مجلة البحوث القانونية والسياسية، العدد 05، 2015.

34. يزيد بوحليط، تفتيش المنظومة المعلوماتية في القانون الجزائري، مجلة التواصل في الاقتصاد والإدارة والقانون، العدد 48، 2016.

سابعا: المداخلات المنشورة في المؤتمرات

1. عبد الله حسين محمود، إجراءات جمع الأدلة في مجال الجريمة المعلوماتية، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي، 2003.

2. علي محمود علي حمودة، الأدلة المتحصلة من الوسائل الإلكترونية في إطار نظرية الإثبات الجنائي، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، أكاديمية شرطة دبي، مركز البحوث والدراسات، عدد رقم: 01 ، الإمارات العربية المتحدة، 2003.

3. محمد أبو العلا أبو عقيدة، التحقيق وجمع الأدلة في الجرائم الإلكترونية، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للمعاملات الإلكترونية، دبي، 2004.

4. هلال البياتي، استخدام الحاسبات الفنية وحمايتها، بحث مقدم إلى ندوة القانون والحاسوب، بغداد، 1998.

5. وليد عاكوم، التحقيق في جرائم الحاسوب، مؤتمر الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي 2003.

ثامنا: القرارات والاجتهادات القضائية

1. قرار صادر عن الغرفة الجنائية، المحكمة العليا، بتاريخ: 29-12-2004، ملف رقم: 355105، مجلة المحكمة العليا، عدد خاص، الجزائر، 2019.

2. قرار صادر عن الغرفة المدنية، المحكمة العليا، ملف رقم: 806311، بتاريخ: 21-06-2012، مجلة المحكمة العليا، العدد 01، الجزائر، 2013.

تاسعا: المحاضرات والدروس

1. حسين العيساوي، محاضرات في مقياس النيابة العامة لطلبة السنة أولى ماستر جنائي، كلية الحقوق والعلوم السياسية، جامعة المسيلة، السنة الدراسية: 2020-2021، ص: 23.
2. نادية ضريفي، محاضرات حول السلطات الإدارية المستقلة (لطلبة السنة الأولى ماستر)، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2019-2020.

عاشرا: المواقع الالكترونية

1. الاتفاقية الأوروبية المتعلقة بالجريمة الإلكترونية، الرابط الإلكتروني: https://rm.coe.int/budapest-convention-in-arabic/1680739173، تاريخ الاطلاع: 05-02-2022
2. بيان لوزارة العدل الجزائرية، الرابط الإلكتروني: https://2cm.es/Rhec، تاريخ الاطلاع: 30-01-2023.
3. بيان لوزارة العدل الجزائرية، الرابط الإلكتروني: https://n9.cl/asghh7، تاريخ الاطلاع: 30-01-2023.
4. بيان لوزارة العدل الجزائرية، الرابط الإلكتروني: https://n9.cl/fvp98، تاريخ الاطلاع: 16-07-2023.
5. بيان لوزارة العدل الجزائرية، الموقع الإلكتروني: https://n9.cl/hzc33r، تاريخ الاطلاع: 11-03-2022.
6. جريدة البلاد، الرابط الإلكتروني: https://.elbilad.net/s@gz4ovcar109356، تاريخ الاطلاع: 15-03-2022.
7. فريد درامشية، (رائد بقيادة الدرك الوطني، مختص في الإجرام السيبراني)، مداخلة عبر الموقع الإذاعة الجزائرية، الرابط الإلكتروني: https://my.radioalgerie.dz/ar/node/11978، تاريخ الاطلاع: 12-03-2024.

- **باللغة الأجنبية**

I. Dictionnaires

1. Serge Guinchard, Thierry Debard, L'exique des termes juridiques, terme "perquisition", 2017-2018, 25e ed, Dalloz, France, 2018.

II. Ouvrages

1. Benson Carl، Andrew Jablon، Paul kaplan، Mara Rosenthal، Computer crimes، Americain law review ، 1997.

2. Bettai M, Oliver Duhamel Laurent Geilsamer, la déclaration universelle des droits de l'homme, gallimard, 1999.

3. Bossan Jérome "le droit pénal confronté a la diversité des intermédiaires de l'internet", édition Dalloz, 2013.

4. Charon Jean-Luk, Sépari Sabine, Organisation et gestion de l' entreprise, éprouve n° 3, 2éme édition, Paris, 2001.

5. Chawki Mohamed, Combattre La Cybercriminalité, Edition de saint Amans, Paris, France, 2009.

6. David Johnson, Electronic privacy, stodder,Canada, 1997.

7. Donn B Parker, Combatre la criminalité informatique, ed oras, 1985.

8. Donn B Parker, Nycm (S), Aura (S), Computer abuse, Stanford Research Institute, 1989.

9. Fawn T. Ngo, Raymond Paternoster, Cybercrime Victimization- An examination of Individual and Situational level factors, International Journal of Cyber criminology, Vol 5, 2011.

10. Malcom Anderson, Policing the world – Interpol the politics of International Police Cooperation, Carendon press, Oxford, 1989.

11. Merwe (Van Der), Computer crimes and other crimes against information technology in south Afrca, R.I.D.P, 1993.

12. Michel Mass. la droit pénal spécial ne de l'informatique, in informatique et droit pénal travaux de l'institute de sciences criminelles de poitiers, 1981.

13. Myriam Quéméner, Jean Paul Pinte, Cybersécurité, Edition Hermès science, Paris, 2013.

14. Myriam Quéméner, Joel Ferry , Cybercriminalité Défi mondial, Edition Economica, Paris, 2009.

15. Robert Reix, Système d'information et management des organisations, Vuibert , France, 4éme édition, 2002.

16. WALKER NIGEL, Crime and Criminology, Oxford University PRESS, 1987.

III. conférences international

1. Ancel, les problèmes poses par l'application des techniques scientifiques nouvelles au droit pénal et a la procédures pénal, rapport au journée franco-polonaises, 1960.

2. Levasseur, les méthodes scientifiques de recherche de la vérité collogue d'abidijan 10-16, paris 1972

الفهرس

ملخص

تعد الجريمة الإلكترونية من الجرائم المستحدثة التي أوجدتها تكنولوجيات الإعلام والاتصال، والتي تختلف عن الجرائم التقليدية كونها تقع وسط بيئة افتراضية، لتشكل بذلك تحديا قويا أمام جهاز التحقيق الجنائي لكشف ملابساتها وضبط أدلتها الرقمية قبل العبث بها.

ومن أبرز خصائص هذه الجريمة تخطيها للحدود الجغرافية للدول، أين تجد الدولة نفسها عاجزة لوحدها عن تتبعها، وهو ما جعل المجتمع الدولي يدق ناقوس الخطر، ويدعو إلى تعزيز التعاون لمواجهتها.

وتسعى الجزائر بدورها إلى مكافحة هذه الظاهرة الإجرامية، من خلال تشريع القوانين المتعلقة بمكافحتها، واستحداث أساليب جديدة تتماشى مع طبيعتها الخاصة، تضاف للأساليب التقليدية التي لم تعد قادرة لوحدها.

الكلمات المفتاحية: الجريمة الإلكترونية، التحقيق الجنائي، تكنولوجيات الإعلام والاتصال، التعاون الدولي.

Abstract

Cybercrime is considered as an emerging crime created by information and communication technologies, it differs from traditional crimes, being committed in a virtual environment, which presents a strong challenge to the criminal investigation service in order to detect its circumstances and adjust its digital evidence before tampering with it.

One of the most prominent features of this crime is that it crosses the geographical borders of countries, thus a country finds itself incapable of tracking it alone.

This situation has caused the international community to sound the alarm and call for cooperation to confront it.

Algeria, in turn, seeks to combat this criminal phenomenon by legislating laws and implementing new procedures that align with the characteristics of this crime.

Keywords : Cybercrime, Criminel investigation, Information and communication technologies, International coopération.