



جامعة مولود معمري- تيزي وزو
كلية الحقوق والعلوم السياسية
قسم الحقوق



أساليب البحث والتحري عن الجريمة الإلكترونية

مذكرة لنيل شهادة الماستر في القانون
تخصص: القانون الجنائي والعلوم الإجرامية

إشراف الأستاذ:
— د. خلوي خالد

من إعداد الطالبين:
— حداد سيلىة
— زروقي أحمد

لجنة المناقشة:

د. لعمامري عصاد، أستاذ التعليم العالي، جامعة مولود معمري تيزي وزو رئيسا
د. خلوي خالد، أستاذ محاضر (أ)، جامعة مولود معمري تيزي وزو مشرفا ومقررا
د. عباشي كريمة، أستاذة محاضرة (ب)، جامعة مولود معمري تيزي وزو ممتحنا

السنة الجامعية: 2024-2025

قائمة المختصرات

أولاً: باللغة العربية

ج. ر. ج. ج	الجريدة الرسمية للجمهورية الجزائرية
ص	الصفحة
ص - ص	من الصفحة إلى الصفحة
ط	الطبعة
ق. إ. ج. ج	قانون الإجراءات الجزائية الجزائري
ق. ع. ج	قانون العقوبات الجزائري
د. س. ن	دون سنة نشر
د. د. ن	دون دار النشر

ثانياً: باللغة الأجنبية

Page	P
Electric Fond Transfer System	EFTS
Internet protocol	IP
Media access control	MAC

الإهداء

بسم الله الرحمن الرحيم: "يرفع الله الذين آمنوا منكم و الذين أوتوا العلم درجات و الله بما تعملون خبير" (11) سورة المجادلة.

الحمد لله حبا و امتنانا على البدء و الختام

لم تكن سهلة و لكن فعلتها، ها أنا اليوم أكتب إهداء تخرجي، أهدي ثمرة هذا العمل و إنجاز وراءه سنوات من الاجتهاد لكل من دعمني و كان مصدر تشجيع لي:

إلى أمي

أمي التي ضلت و مازالت بجانبني في كل خطاي تدعمني، دعاءها يبقيني شامخة، أمي مصدر قوتي و ملهمتي، أهدي لكي هذا النجاح يا نور دربي و أدعو الله أن يبقيك بجانبني بصحة و عافية.

إلى أبي

كرس حياته ليوفر لي كل محال على البال، أبي الذي قدم لي كل الحب و الاهتمام، إنه لفخر لي أن أرفع رأسك اليوم بهذا الإنجاز و أجعل منك أسعد الآباء.

أخواتي-أخي

أكبر مسندين في حياتي، لي حظ لا يحصى لكونكم أخواتي، جعل الله يومي هذا أجمل بوجودكم بجانبني.

أصدقائي

الفرحة لا تكتمل إلا بكم أجمع، أعطى لي الله إخوة من أنعم الناس، أهدي فرحتي بهذا الإنجاز لكم

زميلي في هذا العمل

درسنا، عملنا، تعبنا معا، لكي نصل إلى هذا اليوم نختمها بهذا الإنجاز الذي شاركنا في إنجازه، لي السرور و الامتنان بمشاركتي لثمرة هذا العمل معك.

الطالبة/ حداد سيلية

الإهداء

الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله

أهدي هذا العمل إلى:

من أوصاني بهما ربي بالإحسان، إلى من كانت دعواتهما سر توفيقِي، وإلى من كان

رضاهما غاية أمنيّاتي أطال الله في عمرهما والدي العزيزين

إلى من أعز لعزتهم وأفرح لفرحتهم إخوتي وأخواتي الأعزاء

إلى زوجاتهم وأزواجهم وأولادهم كل باسمه

إلى من جمعتني بهم الأقدار أصدقائي وزملاء العمل والدراسة

إلى زميلتي في هذا العمل لكي مني كل الشكر والتقدير على تعاونك وجهودك المبذولة في

إنجازه، أتمنى لكي التوفيق في جميع مساعيك المستقبلية

إلى كل هؤلاء وغيرهم ممن تجاوزهم قلبي ولن يتجاوزهم قلبي

أهدى ثمرة جهدي المتواضع

الطالب: زروقي أحمد

شكر و عرفان

بعد بسم الله الرحمن الرحيم

قال الله تعالى " ولئن شكرتم لأزيدنكم "

أول الشكر وآخره إلى الله العلي القدير سبحانه وتعالى فله سبحانه وتعالى الحمد والمنة

وسلاما على سيد الخلق القائل

" لا يشكر الله من لا يشكر الناس "

و انطلاقا من هذا التوجيه النبوي نتقدم بأسمى آيات الشكر والتقدير والعرفان للأستاذ "خلوي خالد" الذي تشرف بقبوله الإشراف على إنجاز هذا البحث العلمي لنيل شهادة الماستر كما يسعدنا أنا نتقدم بالشكر إلى لجنة المناقشة كل باسمه لتفضل سيادتهم بقبول مناقشة هذه المذكرة وتقديرها زادنا فخرا وإشرافا.

الطالب: زروقي أحمد/ الطالبة حداد سيلية

مقدمة

عرفت الجريمة منذ بدء البشرية فهي قديمة قدم الوجود الإنساني، فقديمًا كانت تقع جرائم تقليدية مألوفة، كجرائم السرقة والقتل والتهريب على سبيل المثال، وكحد لها وضعت قوانين وقواعد تحكمها، كما سلط عليها المشرع عقوبات تتناسب وطبيعة جسامتها، ولكن بعد نهاية الثورة الصناعية ومع بداية القرن الواحد والعشرين دخلت البشرية مرحلة جديدة، حيث شهد العالم ثورة علمية تكنولوجية هائلة قد انعكست بصورة إيجابية على الكثير من نواحي الحياة الحديثة، بسبب ما توفره من مزايا وخصائص من ربح للوقت وتخفيف للجهد، فهذه الثورة تلاشت مقابلها الحواجز السياسية بين الكيانات والأمم وضاعت معها الأماكن وتقلصت فيها المسافات وأختزلت الأبعاد وهذا نتيجة ما تتميز به من عنصري السرعة والدقة، حتى أضحت الكرة الأرضية قرية صغيرة بفضلها والعالم يعيش في بوتقة واحدة، غير أنه بالرغم من المزايا والفوائد الجمة التي حققتها ولا زالت تتحقق يوما بعد يوم إلا أنه إنطوى في الوقت نفسه على بعض الجوانب السلبية التي هي وليدة الاستخدام المتنامي للتقنيات والوسائل التكنولوجية التي أتاحها هذه الثورة التكنولوجية، وهذه الأخيرة باتت تشكل تهديدا خطيرا على حياة الفرد والمجتمع، نتيجة سوء استخدام هذه التقنية وإستغلالها على نحو غير قانوني، الشيء الذي أعقبه ظهور نمط جديد من الجرائم حديثة العهد لم تكن من قبل سميت بالجرائم الإلكترونية أو بجرائم تقنية المعلومات.

في الحقيقة إن الجرائم الإلكترونية هي ثمرة من ثمار التقدم المعلوماتي الذي فرضته الثورة التكنولوجية في شتى مجالات الحياة، فهي تنشأ في الخفاء وتسعى للوصول إلى المعلومات المتواجدة عبر نظم وشبكات المعلومات وفي مقدمتها الأنترنت، وتقع الجرائم الإلكترونية كأصل عام إما على الحاسب الآلي أو بواسطته وصار لها طابع دولي ينمو يوما بعد يوم فكان من اللازم مكافحتها وملاحقة المجرم فيها، فهي ترتكب من قبل مجرم غير المجرم الذي يرتكب الجرائم التقليدية المعهودة، والذي تغير إسمه من المجرم العادي إلى المجرم المعلوماتي، فهو يتميز بالذكاء والخبرة في مجال تقنية المعلومات والتي تؤهله بأن يتعامل مع طبيعة المعلومات، وكذلك الإحتراافية والسرية والتخطيط في تنفيذ مخططاته الإجرامية من أجل تحقيق هدفه المنشود، ولإخفاء هويته وعدم تتبع أثره.

ولا خلاف في أن الجرائم الإلكترونية من أخطر الجرائم على الإطلاق وهي في طليعة الأشكال المستحدثة للجريمة المنظمة، وخطورة هذه الجرائم نابعة من طبيعتها المميزة وخصوصية مرتكبيها ووسائل كشفها، وتتبلور المشكلات الإجرائية في هذه الجرائم في العراقيل العملية والقانونية التي تثيرها عملية البحث والتحري أمام الضبطية القضائية،

وبالضبط فيما يتعلق بإستخلاص الأدلة وإثباتها لأنها مغايرة عن الأدلة التقليدية في الجرائم العادية التي إعتادت جهات البحث والتحري التحقيق فيها، والتي تقع في عالم مادي محسوس يمكن إدراكه بالحواس، لأنه يخلف أثار في مسرح الجريمة مما من شأنه الوصول إلى المجرم كالبصمات أو قطرات الدم أو محررات مزورة....، على خلاف الجريمة الإلكترونية التي يكون فيها مسرح الجريمة مغاير تماما عن من سبقه من مسرح الجريمة العادية، فهو يكون في البيئة الافتراضية ولا تخلف أثارا مادية بسبب إمكانية التخلص منها وحذفها بسرعة وفي برهة من الزمن.

وأمام كل هذه الخصائص والميزات أثار البحث والتحري عن هذه الجرائم عراقيل للضبطية القضائية ذلك بسبب صعوبة إستخلاص الأدلة التي تثبت وقوعها وتدين مرتكبها، وكذلك عراقيل فيما يخص الآليات المناسبة لمباشرة إجراءات جمع الإستدلالات عبر الفضاء الرقمي .

أبانت الأساليب التقليدية المتعارف عنها للبحث والتحري عن عجزها في التصدي ومواجهة الجرائم الإلكترونية، وذلك يرجع لعدم مواكبة التشريعات التقليدية للسرعة التي تتطور بها التكنولوجيات الحديثة وعصر المعلوماتية وعدم قدرتها على التكيف مع الوضع الحالي، أين تطورت طرق تنفيذها متحدية في ذلك الأنظمة القانونية والأعراف الإجتماعية التي تعارفت عليها المجتمعات، وهذا ما أدى إلى إنتقال الجريمة بمفهومها التقليدي إلى مفهومها الإحتراقي والمنظم، وفي ظل هذه المعضلة التي ولدتها التكنولوجيا الحديثة سعت مختلف الدول إلى سن حزمة من النصوص والإجراءات القانونية في سبيل السعي لإيجاد آليات ووسائل جديدة كفيلة لمجابهة هذا النوع المستحدث من الجرائم، والتي من شأنها أن تمنح لرجال الضبطية القضائية كونهم الجهة الأولى المعنية بمتابعة المجرم المعلوماتي صلاحيات أوسع في مجال البحث والتحري من أجل إستخدام أساليب وأدوات فنية وحيل مشروعة متاحة بغية جمع الاستدلالات لإقامة دليل يثبت الفعل الإجرامي ومعه قيام الجريمة.

أصبحت الجرائم الإلكترونية إحدى أهم الأخطار التي تواجهها الدول النامية والمتقدمة على حدا سواء، فهي لم تعد مجرد حوادث فردية بل تهديدا عابرا للحدود، فرض على الحكومات والمنظمات التصدي لها عن طريق وضع إستراتيجيات متكاملة وتحديث تشريعاتها بما يتناسب مع طبيعة هذا النمط من الجرائم.

والجزائر كغيرها من الدول لم تسلم من تداعيات هذه الظاهرة، لذا حاولت التصدي لها من خلال إحداث تعديلات على ترسانتها القانونية، وذلك بسن جملة من القوانين التي سمحت بإيجاد طرق إجرائية ذات طبيعة تقنية تتلاءم معها وتمكن رجال الضبطية القضائية من

البحث والتحري و استنباط الدليل الذي يتوافق مع الطبيعة التقنية لهذه الجرائم، ومن ثم تحقيق التوازن بين الضرورة الملحة في عصرنا إلى الاستفادة من إمكانيات الحسابات وتقنيات التكنولوجيا الحديثة وبين الحاجة الفردية والإجتماعية إلى الحماية الجزائية من انعكاسات هذه التقنيات.

وتتبع أهمية دراسة هذا الموضوع نظرا لخطورة الجريمة الإلكترونية وتحولها إلى أحد أكثر المعضلات استفحالا في المجتمع الدولي وعلى المجتمع الجزائري خاصة، لأنها تؤرق الدول وبصفة خاصة الدول التي تشهد تقدما على الصعيد العلمي والتكنولوجي.

تسعى هذه الدراسة لتحقيق هدف أساسي هو تسليط الضوء على الآليات التي أقرها المشرع الجزائري لتسهيل البحث والتحري عن الجريمة الإلكترونية وإبراز أهم ما جاء به في سبيل ذلك، دون تخطي باقي الجوانب التي تمس الجرائم المعلوماتية.

بناء على ما سبق تطرح هذه الدراسة إشكالية أساسية تتجلى في :

ماهي الوسائل الإجرائية التي تبناها المشرع الجزائري لتمكين الضبطية القضائية من مباشرة البحث التمهيدي عن الجرائم المرتكبة في الفضاء الرقمي؟

سنحاول الإجابة عن هذه الإشكالية معتمدين على المنهج الوصفي والمنهج التحليلي باعتبارهما من المناهج البحثية والتي لا تقتصر على الوصف والتحليل أو التشخيص فقط، بل تتعداه إلى تحليل النصوص القانونية المتعلقة بآليات البحث والتحري المتبعة من قبل الضبطية القضائية التي أقرها المشرع الجزائري ومحاولة تبسيط وشرح هذه الآليات من جميع الجوانب المختلفة لموضع الدراسة.

بهدف الإحاطة بالإشكالية المطروحة ولإجابة عليها إرتأينا تقسيم الخطة إلى التقسيم الثنائي بحيث تناولنا في الفصل الأول الإطار المفاهيمي للبحث و التحري عن الجريمة الإلكترونية، فيما خصصنا الفصل الثاني لإجراءات البحث والتحري عن الجريمة الإلكترونية.

الفصل الأول

الإطار المفاهيمي للبحث والتحري عن الجريمة الإلكترونية

لقد شهدت الألفية الأخيرة تطورا مذهلا في المجال التكنولوجي ومن ابرز مخرجات هذا التطور حدوث ما يسمى بالثورة التكنولوجية، والتي هي من أهم التطورات التي يعيشها العالم اليوم لاسيما ثورة الاتصالات، حيث ساعدت هذه التكنولوجيا على تطور العديد من الميادين إلا أنها في المقابل عرفت العديد من الانعكاسات السلبية مما أدى إلى انتشار ظاهرة خطيرة على المجتمعات وعلى أمنها واستقرارها تعرف بالجريمة الإلكترونية، حيث صنفَت هذه الأخيرة على أنها من أخطر الجرائم المعاصرة، وذلك من منطلق الخصائص التي تمتاز بها عن الجرائم التقليدية من حيث الدقة والتقنية العالية والسرعة في ارتكابها وكذا صعوبة اكتشافها وبالتالي التحقيق فيها، وعلى ضوء ذلك ومن أجل الإلمام أكثر وتوضيح الأمر بخصوص الجريمة الإلكترونية والتحقيق فيها قسمنا هذا الفصل إلى شطرين، أولهما ماهية الجريمة الإلكترونية في (المبحث الأول) و ثانيهما ماهية البحث والتحري عن الجريمة الإلكترونية في (المبحث الثاني).

المبحث الأول

ماهية الجريمة الإلكترونية

الجريمة الإلكترونية هي من الآثار السلبية التي خلفتها تقنية المعلومات حيث أخذت هذه الظاهرة الإجرامية حيزاً من الدراسات من أجل تحديد مفهومها مما أدى إلى وضع عدة مصطلحات للدلالة عليها، منها الجرائم المعلوماتية، جرائم تقنية المعلومات، جرائم الحاسوب، والجرائم الإلكترونية وصولاً إلى جرائم الانترنت، ويعتبر عدم الاستقرار على مصطلح واحد للدلالة عليها من الصعوبات الوردية على وجود تعريف جامع ومانع محدد لها، والجرائم الإلكترونية تستهدف الاعتداء على المعطيات بدلالاتها التقنية الواسعة وهي جريمة ناعمة ترتكب دون عنف و في الخفاء ولا أثر خارجي لها، حيث يقترفها مجرمون أذكيا يمتلكون أدوات المعرفة والمهارة التقنية، ومن ماسبق سوف يتم تقسيم هذا المبحث إلى مطلبين يتم فيهما عرض أساسيات حول الجريمة الإلكترونية (مطلب أول) ومن ثم الأحكام الخاصة بالجرائم الإلكترونية (مطلب ثاني).

المطلب الأول

أساسيات حول الجريمة الإلكترونية

نظراً للطبيعة الخاصة للجريمة الإلكترونية باعتبارها تقع في العالم الرقمي، سنقوم من خلال هذا المطلب باستعراض مختلف التعريفات التي قدمها الفقهاء لهذا النوع من الجرائم في (الفرع الأول)، وسنتولى كذلك تبيان الخصائص التي تجعلها فريدة عن غيرها من الجرائم في (الفرع الثاني)، من ثم عرض الدوافع التي تحفز المجرم على إتيانها (الفرع الثالث).

الفرع الأول

تعريف الجريمة الإلكترونية

باعتبار أن الجريمة الإلكترونية حديثة ومعاصرة فهي لا زالت محل بحث ودراسة من طرف القانونيين والعديد من الفقهاء وهذا ما يجعل استحالة وجود تعريف موحد لهذا النوع من الجرائم، ومن أجل ضبط تعريف الجريمة الإلكترونية سنطرق في هذا الفرع إلى التعريف الذي جاء به الفقه (أولاً)، ثم التعريف القانوني (ثانياً).

أولاً: تعريف الفقه للجريمة الإلكترونية

اختلف الفقهاء وتباين رأيهم في تعريف الجريمة الإلكترونية فاعتمدوا على أساسيات هذه الجريمة المتمثلة في ثلاث أساسيات وهي كالتالي:

1 - تعريف الجريمة الإلكترونية على أساس وسيلة ارتكابها:

يرى هذا الاتجاه أن الحاسوب الآلي هو أساس هذه الجريمة ويكون دور الحاسب الآلي له جزء كبير في ارتكاب الجريمة.

- ويعرفها الأستاذ الألماني تيدمان (Tidman): بأنها كافة أشكال الفعل الغير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الآلي، كما قد تكون مسهل لها بالنظر للعلاقة بين الجناة كتسهيل تبادل المعلومات فيما بينهم.¹

- كما عرفها الفقيه بال ليدسلي (Ball D Leslie): بأنها فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية.²

- يرى كذلك الفقيه ميرو (Merwe): بأنها الفعل الغير مشروع الذي يستخدم في ارتكابه الحاسب الآلي.

- عرفها أيضا الفقيهان هارد كاستل و توتي (Hardcastle et totty): بأنها تلك الجرائم التي يكون قد وقع في مراحل ارتكابها بعض العمليات الفعلية داخل نظام الحاسوب وبعبارة أخرى هي تلك الجرائم التي يكون الحاسب فيها إيجابيا أكثر منه سلبي.³

2- تعريف الجريمة الإلكترونية على أساس الإلمام بالمعرفة التقنية:

يعتمد أنصار هذا الاتجاه في تعريفهم للجريمة الإلكترونية على معيار إلمام مرتكب الجريمة بتقنية المعلومات وهو معيار شخصي ومن بين أصحاب هذا الاتجاه الفقيه ديفيد طمسون (David thompson) الذي عرف الجريمة الإلكترونية بأنها أية جريمة يكون متطلب للإقترافها أن تتوفر لدى فاعلها معرفة بتقنية الحاسب.⁴

- كما عرفها جانب من الفقه أيضا بأنها: ذلك النوع من الجرائم التي تتطلب إلماما خاصا بتقنيات الحاسب الآلي ونظم المعلومات للإرتكابها أو التحقيق فيها ومقاضاة فاعلها.

- كما عرفت وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للأبحاث بأن: الجريمة الإلكترونية هي أي جريمة يكون لفاعلها معرفة فنية بالحسابات تمكنه من ارتكابها.

3- تعريف الجريمة الإلكترونية على أساس موضوعها:

يري أنصار هذا التوجه أن تعريف الجريمة الإلكترونية لا يكون على أساس الوسيلة المستعملة ولا الفاعل وإنما الأمر متعلق بموضوع الجريمة فعرفها على هذا الأساس الفقيه روزبلت (Rosbelet) على أنها نشاط غير مشروع موجه لنسخ وتغيير أو وصول إلى معلومات مخزنة داخل الحاسب الآلي، أو تلك التي يتم تحويلها عن طريقه.⁵

¹ يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة للنشر، مصر، 2019، ص48

² عبد الفتاح بيومي الحجازي، مكافحة جرائم الكمبيوتر والانترنت في القانون العربي النموذجي، دار الفكر الجامعي، الإسكندرية، 2006، ص2.

³ محمد سامي شيو، ثورة المعلومات وانعكاساتها على قانون العقوبات، ط الرابعة، دار النهضة، مصر، 1998، ص7.

⁴ بوبقرة خيرة، أليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماستير، تخصص في القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية، قسم عام، جامعة عبد الحميد بن باديس، مستغانم، 2019-2020، ص9.

⁵ مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة مقدمة لنيل شهادة الماجستير، في القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية، قسم العلوم القانونية، جامعة الجزائر، 2008-2009، ص10.

كما عرفها الخبير الأمريكي باركر (Parker) بأنها كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية ترتبت عنه خسارة تلحق المجني عليه أو مكسب يحققه الجاني¹.

ومن أنصار هذا المعيار الفقيه العربية الدكتورة هدى قشوش التي عرفت الجرائم الإلكترونية بأنها مجموعة من الجرائم التي تتصل بالمعلوماتية، فهذه الجرائم وفقا رأيها هي جرائم الاعتداء على الأصول المعلوماتية أو هي نمط من أنماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات².

يرى أيضا الأستاذ ماس (Mass) أن المقصود بالجريمة الإلكترونية هي اعتداءات ترتكب بواسطة المعلومات بغرض تحقيق ربح³.

على هذا الأساس الجريمة الإلكترونية هي كل فعل أو امتناع عمدي ينشأ عند الاستخدام الغير مشروع لتقنية إلكترونية هدفه الاعتداء على الأموال المادية أو المعنوية.

ثانيا: التعريف القانوني

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد عمل المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال، وعرفها بموجب المادة 02 من القانون رقم 04-09 على أنها "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"⁴.

الملاحظ من خلال قراءة المادة سالفة الذكر أن المشرع الجزائري أعتمد في تعريف الجريمة الإلكترونية على معيار موضوع الجريمة ومعيار وسيلة ارتكابها، وحسب المشرع الجزائري فإنه تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل ارتكابها عن طريق منظومة معلوماتية، أو نظام الاتصالات الإلكترونية مما يجعل التعريف يشمل عدد كبير من الجرائم ومن أمثلة الجريمة الإلكترونية المرتكبة في الجزائر تسريب أسئلة البكالوريا سنة 2016⁵، كما نشير إلى أنه اعتمد في هذا التعريف على القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

¹ أبوقرة خيرة، مرجع السابق، ص 8.

² هدى حامد قشوش، جرائم الحاسب الإلكتروني، د. ط، دار النهضة العربية، مصر، د. س. ن، ص 5-ص 6.

³ جلال محمد الزعبي، أسامة محمد المناعة، جرائم تقنية المعلومات الإلكترونية، دار الثقافة للنشر والتوزيع، عمان، ص 65.

⁴ قانون رقم 04-09، 5 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، الجريدة الرسمية، العدد 47، تاريخ الصدور 16 أوت 2009.

⁵ بوضياف إسمهان، "الجريمة الإلكترونية و الإجراءات التشريعية لمواجهتها في الجزائر"، "مجلة الأستاذ الباحث للدراسات القانونية و السياسية"، كلية الحقوق

والعلوم السياسية، جامعة محمد بوضياف المسيلة، العدد 11، 09 ماي 2018، ص 352-ص 353.

الفرع الثاني

خصائص الجريمة الإلكترونية

نظرا للطبيعة المميزة للجريمة الإلكترونية باعتبارها تمس المعلومات هذا جعلها تتميز عن الجرائم التقليدية بمجموعة من الخصائص أو السمات، إذ أن التعرف أكثر على خصائص هذه الجريمة يساعد في إيجاد الحلول لمكافحتها، وتتلخص هذه السمات فيما يلي:

أولا- الجريمة الإلكترونية مرتبطة بالحاسب الآلي وشبكته:

يلعب الحاسب الآلي دورا مهما ومحوريا في الجريمة الإلكترونية، فقد يكون هدفا للجريمة (مثلا في قرصنة البرامج أو وضع الفيروسات... الخ)، وقد يكون أداة لارتكاب الجريمة أو البيئة التي ترتكب فيها، فقد تكون المعلوماتية هي وسيلة للغش والتحايل أو تكون محل للاعتداء.

ومن ثم نشير إلى تعريف الجهاز الذي يلعب دورا مهما في هذا النوع من الجرائم ألا وهو جهاز الحاسوب أو الحاسب الآلي أو الحاسب الإلكتروني وهي مسميات عديدة أطلقت عليه، فالكمبيوتر "هو جهاز إلكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية طبقا للتعليمات المعطاة له بسرعة كبيرة تحل عشرات الملايين من العمليات الحسابية"¹

أما شبكات الحاسب الآلي وهي الفضاء أو مسرح الجريمة الإلكترونية، فيقصد بها "اتصال جهازين أو أكثر من أجهزة الحاسب الآلي اتصالا سلكيا أو لا سلكيا، أو هي حزمة من أجهزة الحاسب المتصلة معا، وقد تكون الأجهزة موجودة في نفس الموقع، فتسمى شبكة محلية أو تكون موزعة في أماكن متفرقة ويتم ربطها عن طريق خطوط الهاتف وتسمى في هذه الحالة بالشبكة واسعة النطاق أو الممتدة، ومنها شبكة الانترنت التي تلزم للدخول إليها جهاز حاسوب ومودع بالإضافة إلى خط هاتف، ويجب أن يقع الاعتداء على الحاسب الآلي وشبكات أو بواسطتها، أما بخصوص الشبكة فأكثرها استعمالا هي الانترنت وهي كلمة إنجليزية مكونة من كلمتين: International أي دولي و Net Works أي شبكة.²

ثانيا- صعوبة اكتشاف الجريمة الإلكترونية:

تنتم الجرائم الناشئة عن استخدام الانترنت بأنها خفية ومستتر في أغلبها، لأن الضحية لا يلاحظها رغم أنها قد تقع أثناء وجوده على الشبكة العنكبوتية، لأن الجاني يتمتع بقدرات فنية تمكنه من ارتكاب جريمته مثلا عند إرسال الفيروسات وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وغيرها من الجرائم، فالجرائم المعلوماتية في أكثر صورها خفية لا يلاحظها المجني عليه أو لا يدري حتى بوقوعها، والإمعان في حجب السلوك المكون لها وإخفائه عن طريق التلاعب غير المرئي في النبضات أو الذبذبات الإلكترونية التي تسجل البيانات عن طريقها أمرا ليس عسيرا في الكثير من الأحوال بحكم توافر المعرفة والخبرة في مجال الحسابات غالبا لدى مرتكبها، كما أن المجني عليه يلعب دورا رئيسا في صعوبة اكتشاف وقوع الجريمة المعلوماتية حيث تحرص أكثر الجهات التي تتعرض

¹ بن عنتر سيهام، "التحقيق الجنائي في الجرائم الإلكترونية"، مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر، السنة الجامعية 2023، ص16.

² مرجع نفسه، ص17.

أنظمتها المعلوماتية لانتهاك أو تمنى بخسائر فادحة من جراء ذلك إلى عدم الكشف حتى لا يتبين لموظفيها عما تعرضت له وتكتفي عادة باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة تجنباً للإضرار بسمعتها ومكانتها وهز الثقة في كفاءتها.¹

ويرى البعض أن للمجني عليه دوراً مثيراً للريبة في بعض الأحيان، فهو قد يشارك بطريقة غير مباشر في ارتكاب الفعل، وذلك بسبب وجوده في ظروف تجعل تعرضه للجريمة المعلوماتية أمراً مرتفعاً بشكل كبير، ويرجع ذلك بشكل أساسي إلى القصور الأمني الذي يعتري الأنظمة المعلوماتية الذي قد يساعد على ارتكاب الفعل الإجرامي، وفي الواقع فإن إحجام المجني عليه عن الإبلاغ عن وقوع الجرائم المعلوماتية يبدو أكثر وضوحاً في المؤسسات المالية مثل البنوك والمؤسسات الادخارية و مؤسسات الإقراض والسمسرة حيث تخشى مجالس إدارتها من أن تؤدي الدعاية السلبية التي قد تنجم عن كشف هذه الجرائم أو اتخاذ الإجراءات القضائية حيالها إلى تضائل الثقة من جانب المتعاملين معها.² حيث أن الجانب الأكبر من الجرائم المعلوماتية لا يتم الكشف أو التبليغ عنه فإن ذلك يؤثر سلباً في السياسة التي يمكن أن توضع لمكافحةها.

وبما أن مستعملي التكنولوجيا الإعلام والاتصال غير مجبرين على الكشف عن هويتهم عند استعمالهم لهذه التكنولوجيات يكون من الصعب التوصل إليهم فالكثير من الجرائم المرتكبة من قبل هذا الأخير لا ينالون جزائهم لعدم إمكانية إكتشافهم والوصول إليهم، وخاصة في الدول التي لا تملك التقنية والمهارات اللازمة في مؤسستها الأمنية أو خلال التحقيق في تلك الجرائم من طرف سلطاتها القضائية، كما أن في الغالب هذه الجرائم لا تترك أثر مادي لها بعد ارتكابها، وهذا كله من شأنه أن يجعل من العسير على المحققين العاديين التعامل معها.³

ثالثاً- صعوبة إثبات الجريمة الإلكترونية:

الجريمة الإلكترونية تتم في بيئة غير تقليدية بحيث تقع خارج إطار الواقع المادي الملموس، لتقوم أركانها في بيئة الحاسوب والانترنت مما يجعل الأمور تزداد تعقيداً لدى سلطات الأمن وأجهزة التحقيق والملاحقة، وما يميز هذا النوع من الجرائم هو صعوبة إيجاد الدليل المادي لإدانة مرتكبها بسهولة ويسر، ولأن محو الدليل إجراء بسيط، خاصة مع ما يوفره العالم من مجرمين معلوماتيين محترفين برعوا في هذا المجال وتفننوا في علم القرصنة والمعلومات، لذا يصعب معهم إثبات الفعل الجنائي المرتكب على عكس الجرائم العادية المرتكبة، كما ساهم في صعوبة اكتشاف هذه الجرائم وإثبات مرتكبها هو عدم توفر مختصين لدى رجال الأمن والمحققين، وهذا يستلزم أن تقوم سلطات التحقيق بالتدريب والتأهيل اللازمين والاستعانة بذوي الخبرة حتى تكون أعمالهم في التحري والتحقيق على قدر من المهنية التي يمكن بها تقديم دليل إلكتروني موثوق إلى القضاء.⁴

4- جريمة سهلة وناعمة:

لا تحتاج الجريمة الإلكترونية إلى جهد عضلي في ارتكابها بل تعتمد على القدرات الذهنية للجاني، كما أنه لا يحتاج الجاني في ارتكابها إلى التنقل والاستعانة بأدوات أو مركبات لنقل المسروقات، كما لا يحتاج في غالب الأحيان لمساعدة شخص آخر لارتكاب جريمته بل يمكن للجاني ارتكابها وهو مستلقي في منزله وهو يرتشف فنجان قهوة دون أن يشعر به أحد، لأنها لا تتطلب سوى عدد من اللمسات

¹ - حسنين المحمدي بوادي، إرهاب الانترنت (الخطر القادم)، دار الفكر الجامعي، مصر، 2006، ص76.

² - محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، د.ط، دار النهضة العربية، مصر، 2009، ص31.

³ - محمد عبيد الكعبي، مرجع نفسه، ص31

⁴ - محمد عبيد الكعبي، مرجع نفسه، ص32..

الخاطفة على لوحة المفاتيح حتى تؤدي لاختراق نظم المعالجة الآلية وهتك خصوصيتها أو حذف ما تحتويه من معلومات.¹

توصف الجريمة الإلكترونية بأنها جريمة ناعمة لأنها لا تترك أثارا مادية كالتي تتركها الجرائم التقليدية فلا وجود للكسر ولا بقع الدم، وكل ما تخلفه هي أثار رقمية ليس لها وجود مادي ملموس، كما أن الوسائل التي ترتكب بها لا تحدث جروحا ولا تسيل دماء، فإنها جريمة لا يستعمل فيها العنف الجسدي على الإطلاق، بل كل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال غير المشروعة فتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو تغريب بالقاصرين كل ذلك دون حاجة لسفك الدماء.²

خامسا-الامتداد الجغرافي و الزمني(جريمة متعددة للحدود):

فما يعرف بالمجتمع المعلوماتي هو مجتمع منفتح لا يعترف بالحدود الجغرافية فهو عالم شاسع عبر الفضاء الرقمي الإلكتروني يخترق الزمان والمكان دون الخضوع لحرس الحدود، إن عملية التشبيك المعلوماتي كسرت الحدود والحواجز التقليدية بين الدول والقارات، فلا وجود لنقاط تفتيش ولا مراكز عبور في هذه البيئة الرقمية، هذه الميزة أتاحت الفرصة لمرتكبي الجرائم الإلكترونية لتوسيع نطاق ارتكاب جرائمهم من حيث الزمان والمكان، فالجرائم الإلكترونية قد ترتكب عن طريق الحاسب الآلي في دولة ما في حين يتحقق الفعل الإجرامي في دولة أخرى، فبعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة، فالمقدار التي تتمتع بها الحواسيب وشبكتها في نقل كميات كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها آلاف الكيلومترات قد أدت إلى نتيجة مؤداها أن أماكن متعددة في دول مختلفة قد تتأثر بالجريمة الإلكترونية الواحدة في آن واحد، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل الإمكان ارتكاب جريمة عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى، والحقيقة أن الطبيعة المميزة للجريمة الإلكترونية كونها جريمة عابرة للحدود ومسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير إشكالات في مجال الجرائم المعلوماتية وبشكل خاص الإجراءات الجزائية والاختصاص القضائي وكذا القانون الواجب التطبيق والإشكاليات التي تتعلق بإجراءات الملاحقة القضائية، وغير ذلك من النقاط التي تثيرها الجرائم العابرة للحدود بشكل عام، وهذا بدوره عامل رئيسي في تضافر الجهود الدولية لمكافحة هذه الجرائم، ويجعلها من المواضيع الرئيسية على أجندة اهتمام المجتمع الدولي.³

¹ -بن مكي نجا، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية، الجزائر، 2017، ص21

² -بن مكي نجا، مرجع نفسه، ص22.

³ -عبد الله علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، دار النهضة العربية، القاهرة، 2002، ص351.

سادسا- صعوبة التحقيق الجنائي في الجرائم الالكترونية :

إن اختلاف الجريمة الالكترونية عن الجريمة العادية جعلها تتفرد حتى في شكل دليها فالدليل فيها غير مرئي، وصعب الوصول إليه بسبب الحماية التقنية (التشفير)، كلمة السر...، وكذا سهولة حذفه أو تخزينه مع ضخامة حجم المعلومات والبيانات الواجب فحصها مع إمكانية خروجها عن النطاق الإقليمي للدولة بسبب البعد الجغرافي بين الجاني والمجني عليه.¹

الفرع الثالث

دوافع ارتكاب جرائم الالكترونية

مما لا شك فيه أن السلوك الإنساني أين كان شرا أم خيرا له ما يفسره، وما الذي بعث على ارتكابه وهو الذي يطلق عليه الدافع، وفي مجال الجرائم المعلوماتية ثمة دوافع عديدة تحرك مجرمي المعلوماتية لارتكاب أفعال الاعتداء المختلفة المنطوية تحت مفهوم الإجرام المعلوماتي، ويمكن تخلص هذه الدوافع في ما يلي:

أولا- الرغبة الأكيدة في الانتقام :

الانتقام موجود داخل النفس البشرية، فكثير من الأفراد يفصلون تعسفا أو بغير وجه حق من شركة أو منظمة حكومية أو حتى مصرف، وهم يملكون المعلومات اللازمة والمعرفة الكافية بخفايا هذه الجهة، لذلك يرتكب الجاني الجريمة رغبة منه في الانتقام لجعل الشركة أو المؤسسة تتكبد خسائر مالية كبيرة من جراء ما يسببه لها من ضرر يحتاج إصلاحه إلى وقت لا بأس به.²

ثانيا- الرغبة في تحدي وقهر النظام التقني و المعلوماتي:

فالدافع في هذا الغرض، لا ينبئ عن خطورة إجرامية كامنة في نفس مقترف هذه الأفعال، إذ أنهم عادة لا يكونون من معتادي الإجرام، بل يتمثل في رغبة هؤلاء بتحدي النظام التكنولوجي المعقد للحاسب الآلي بكل مكوناته ومعطياته ومحاولة اختراقه عن طريق الوصول إلى المعلومات، ففي الوقت الذي يزداد فيه الاهتمام بأمن الحاسب الآلي عن طريق تطوير طرق جديدة وصعبة لاختراقه كبرمجيات التشفير التي تمكن مستقبلها وحده من فهمها، ومن الأمثلة على ذلك وزارة الدفاع الأمريكية التي تقوم بتغيير أنظمة الترميز للبيانات المستخدمة يوميا، فإن الجانب الآخر الذي يقف على الضفة الأخرى أصحاب الشغف الإلكتروني يتسابقون لخرق هذه الأنظمة وإظهار تفوقهم عليها، والدليل على ذلك قيام أحد الهواة في أوروبا بحل شفرة أحد مراكز المعلومات في البنتاغون وتمكنه من العبث في بيانات هذا المركز.³

¹ د- بومحراث ليندة، "إجراءات التحقيق الخاصة بالجرائم السيبرانية، يوم دراسي حول الجريمة السيبرانية"، المنعقد، جامعة الأمير عبد القادر قسنطينة بتاريخ يوم 20 أبريل 2022، ص10.

² محمد أمين الرومي، جرائم الكمبيوتر و الإنترنت، دار المطبوعات الجامعية، مصر، 2004، ص25.

³ زين مكي نجا، مرجع السابق، ص44.

ثالثا- الولوج في جمع المعلومات وتعلمها:

يرى قراصنة الكمبيوتر أن الحصول على المعلومة يجب ألا يكون عليه أي قيد، فالقرصان يكرس جهده في تعلم كيفية اختراق المواقع الممنوعة، وغالبا ما يكون القراصنة مجموعات يكون الهدف منها التعاون وتبادل المعلومات وتقاسم البرامج والأخبار، كما يفضل القراصنة أن يكونوا مجهولين حتى يكون الهدف منها التعاون وتبادل المعلومات داخل الأنظمة لأطول فترة ممكنة.¹

رابعا- السعي إلى تحقيق الربح:

يعتبر السعي إلى تحقيق الربح في المرتبة الأولى من دوافع ارتكاب جرائم الحاسب الآلي، وفي دراسة أشار إليها الأستاذ باركر (PARKER) فإن 43% من حالات الغش المعلن عنها قد بوشرت من أجل الحصول على المال، و وفقا للدراسات فإن القطاع المالي يعد أكثر القطاعات استهدافا من قبل جرائم الحاسب الآلي، ويرجع ذلك إلى أن هذه البنوك تعتمد و بشكل أساسي على أنظمة التمويل إلكترونيا (EFTS) Electric Fond Transfer System الأمر الذي زاد فرص النصب وبشكل هائل، فمجرد سقوط رموز التحويل الإلكتروني المستخدمة في (EFTS) في الأيدي الخاطئة فإن ملايين الدولارات يمكن أن تنقل وبثواني معدودة، دون أن يترك دليلا ضده، وتعتبر الدوافع المادية من البواعث على ارتكاب الجرائم المعلوماتية لما تحققه من ثراء فاحش سريع وبدون تعب، ولقد أشارت مجلة sécurité informatique إلى الرغبة في تحقيق الثراء من بين العوامل الأساسية لارتكاب الجريمة المعلوماتية حيث أشارت إلى أن:

43 % من حالات الغش المعلن عنها من أجل اختلاس الأموال.

23 % من أجل سرقة المعلومات.

19 % أعمال إتلاف.

10 % سرقة وقت الآلة أي استعمال غير المشروع للآلة لتحقيق أغراض شخصية.²

خامسا- ارتكاب الجرائم كوسيلة للتسلية والدعابة:

يعتبر دافع المزاح والدعابة من الدوافع التي تجعل الشخص يقوم بتصرفات، وإن كان لا يقصد من ورائها إحداث جرائم وإنما بغرض المزاح فقط، ولكن هذه التصرفات قد تنتج عنها نتائج ترقى إلى درجة الجريمة لأنه من الطبيعي أن الشخص الذي يقوم بمسح مجموعة من الملفات من جهاز شخص آخر، وكانت هذه الملفات تحتوي على معلومات مهمة فلا يمكن القول بأن هذا التصرف مجرد دعابة،

¹ - محمد الأمين الرومي، مرجع السابق، ص25.

² - سعدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، 2017، ص38، 37.

بل إن هذا التصرف في حقيقته جريمة إتلاف وتخريب متعمد في حالة ما إذا كان هناك قانون يجرم هذا الفعل.¹

سادسا- الدافع الديني:

يسعى الجناة أحيانا إلى بث معتقدات وأفكار دينية أو سياسية أو اجتماعية متطرفة، ولفت النظر إلى هذه المعتقدات والأفكار وفرضها بالقوة باستخدام الأشخاص والممتلكات، والبعض الآخر يكون دافعه التجسس على دولة ما أو شركة منافسة.²

سابعا-الدافع السياسي والعسكري:

التطور العملي والتقني أديا إلى الاعتماد بشكل شبه كامل على أنظمة الحاسوب، وبذلك أصبح الاختراق من أجل الحصول على معلومات سياسية وعسكرية واقتصادية مسألة أكثر أهمية.³

ثامنا- دافع الإرهاب:

يمكن أن يتحول الدافع الإيديولوجي والسياسي على التوجه آخر وهو الإرهاب بشكله الإلكتروني، من خلال شبكة الانترنت التي يمكن أن تأوي مواقع خاصة بجماعات إرهابية، تمارس نشاطها من خلال التحريض على القتل والتمرد والعصيان المدني، وتهدف إلى ترويع المواطنين والأفراد من خلال نشرها لصور وفيديوهات على كيفية صنع المتفجرات والقنابل والإشادة بأعمالها الإجرامية، زيادة على ذلك فإنها عادة ما تستهدف النظم المعلوماتية الحكومية بغرض تعطيلها وتدميرها.⁴

المطلب الثاني

الأحكام الخاصة بالجرائم الالكترونية

لا شك أن في الفقه الجنائي لا يوجد جريمة وإلا ولها أركان محددة سنبحث من خلال هذا المطلب بيان الملامح التي توضح لنا الإطار القانوني للجريمة الإلكترونية، وهذا يتطلب بيان أركانها (الفرع الأول) ثم أطرافها (الفرع الثاني) وأشكالها (الفرع الثالث) وأخيرا تقسيمها في التشريع الجزائري (الفرع الرابع).

¹ - بن مكي نجا، مرجع سابق، ص43-ص44.

² - محمد عبد الرحمن عنانزه، القصد الجرمي في الجرائم الإلكترونية، دار الأيام للنشر و التوزيع، عمان، 2017، ص77.

³ - نفس المرجع، ص77.

⁴ - نفس المرجع، ص78.

الفرع الأول

أركان الجريمة الإلكترونية

تتخذ الجريمة المرتكبة عبر الانترنت من الفضاء الافتراضي مسرحا لها مما يجعلها تتميز بخصوصيات تنفرد بها، إلا أن ذلك لا يعني عدم وجود تشابه لها مع الجريمة المرتكبة في العالم التقليدي أو المادي فهي تشترك في وجود الفعل الغير المشروع، وتقوم الجريمة على أركان رئيسية هي الركن الشرعي (أولا) والركن المادي (ثانيا) وكذا الركن المعنوي (ثالثا). ولهذا ستتطرق إلى تبيان هذه الأركان التي تقوم عليها الجريمة الإلكترونية تباعا .

أولا-الركن الشرعي:

طبقا للمادة الأولى من قانون العقوبات الجزائري فإنه " لا جريمة ولا عقوبة و لا تدابير امن بغير قانون " هذه المادة هي اللبنة الأساسية لمبدأ الشرعية القانونية بشكل عام لجميع الجرائم، وهذا ما يقصد بالركن الشرعي للجريمة أي وجود نص يجرم الفعل ويوضع العقاب المترتب عليه وقت وقوع الفعل فيبينى على ذلك عدم جواز ملاحقة الشخص عن فعل ارتكبه قبل صدور نص التجريم وهذا ما أوضحته المادة الثانية من قانون العقوبات "لا يسري قانون العقوبات على الماضي إلا ما كان منه اقل شدة"، أما بخصوص الجريمة الإلكترونية فالمشرع الجزائري قد تناولها في قانون العقوبات في القسم السابع المكرر من الفصل الثالث الخاص بجرائم الجنايات والجرح ضد الأموال تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وكذلك القانون المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وبعض النصوص الأخرى سنتناولها لاحقا.¹

ثانيا- الركن المادي:

لابد من فعل أو امتناع يمكن إثباته إذ لا عبرة بما في خلد الإنسان من أفكار لأنها لا تدخل دائرة التجريم، والركن المادي هنا يختلف من حال لأخر حسب التصنيف الذي يقع على الفعل وعليه لا يمكن حصر الجريمة المعلوماتية تحت تكييف واحد، فقد تشكل الواقعة المرتكبة والتي تحمل وصف الجريمة المعلوماتية واقعة قذف أو تهديد أو تحريض وبشكل مطابق تماما لما يجري عليه قانون العقوبات من خلال بعض القواعد التي ينطبق حكمها حتى على الجرائم الواقعة عن طريق الحاسوب، وهذا لا يسبب إشكالا، إذ يمكن تطبيق نصوص قانون العقوبات على هذه السلوكيات التقليدية، إلا أن هناك أنواعا من السلوك يتطلب التمييز بينها وبين سابقها، وهذا ما يدعو للتدخل الشرعي²، ويقصد بالركن المادي للجريمة كل فعل أو سلوك إجرامي صادر من إنسان عاقل سواء كان إيجابيا أو سلبيا، يؤدي إلى نتيجة تمس حقا من الحقوق التي يكفلها الدستور والقانون، وليكتمل الركن المادي للجريمة الإلكترونية يجب أن تتوفر فيه العناصر التالية:

¹ أسامة أحمد المناعة، جلال محمد الزغبى، جرائم تقنية نظم المعلومات الإلكترونية، ط 3، دار النشر و التوزيع، عمان، 2014، ص45.

² بوضياف إسمهان، "الجريمة الإلكترونية و الإجراءات التشريعية لمواجهةها في الجزائر"، مجلة الاستاذ الباحث للدراسات القانونية و السياسية، العدد الحادي عشر، جامعة محمد بوضياف-المسيلة، 9 ماي 2018، ص353.

1- السلوك الإجرامي: يعد السلوك الإجرامي الأمر الذي يصدر من الفاعل ويخشى المشرع منه ضررا على الأشخاص فما لم يصدر من الفاعل نشاط في صورة من صورته لا يتدخل المشرع بالعقاب وهي أعمال خارجية تختلف باختلاف الجرائم كما نجدها عمل إيجابي أو سلبي.¹

2- النتيجة الإجرامية:

يقصد بها الأثر المادي الذي يحدث، فالسلوك قد أحدث تغييرا ملموسا ومفهوم النتيجة يقوم على أساس ما يعتد به المشرع وما يترتب عليه من نتائج بغض النظر عما يحدثه السلوك الإجرامي من نتائج أخرى.²

3- العلاقة السببية :

وهي الصلة بين السلوك الإجرامي والنتيجة الإجرامية، بحيث تثبت بان السلوك الإجرامي الواقع هو الذي أدى إلى حدوث تلك النتيجة الضارة، على انه يمكن لبعض صور هذه الجرائم أن يتحقق الركن المادي دون النتيجة وهو ما يطلق عليه بالجرائم الشكلية تكتفي بعنصر واحد لقيام ركنها المادي.³

ويتخذ الركن المادي في الجريمة الإلكترونية عدة صور بحسب كل فعل إيجابي مرتكب، فمثل جريمة الغش المعلوماتي الركن المادي فيها هو تغيير الحقيقة في التسجيلات الإلكترونية أو المحررات الإلكترونية.⁴

ثالثا – الركن المعنوي:

تعد الجريمة المعلوماتية كغيرها من الجرائم والتي تفترض بالأساس وجود القصد العام (العلم، والإدارة) لتحديد المسؤولية الجنائية، ولا يمكن تصور وجود قصد خاص بالجريمة دون أن يسبقه القصد العام، أما عن وجود القصد الخاص في الجرائم المعلوماتية، فهذا يرجع بالدرجة الأولى إلى طبيعة الجريمة المرتكبة والنية الخاصة لدى الجاني من وراء القيام بالفعل غير المشروع أو ارتكاب الجريمة.⁵

ويقوم الركن المعنوي للجريمة المرتكبة عبر الانترنت على أساس مجسد في توفر الإرادة الجرمية لدى الفاعل، وتوجيه هذه الإرادة إلى القيام بعمل غير مشروع جرّمه القانون كانتحال شخصية مزود عبر الانترنت، وسرقة أرقام البطاقات الائتمانية، كما يجب أن تتوفر نتيجة الجريمة المترتبة عن الأعمال السابقة، فتكتسب إرادة الجاني الصفة المجرمة من العمل غير المشروع الذي يبين الشبه في ارتكابه وعالم بالآثار الضارة الناشئة عنه.⁶

يختلف الركن المعنوي في الجرائم الإلكترونية من جريمة إلى أخرى، فجريمة الدخول الغير المصرح به إلى نظام الحاسب الآلي يتطلب قصدا جنائيا عاما يتمثل في علم الجاني بعناصر الركن المادي للجريمة، أي العلم بأن الولوج إلى داخل النظام المعلوماتي بشكل غير مصرح به يعد جريمة

¹ بوضياف إسمهان، مرجع سابق، ص 354.

² بالعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، دار الخلدونية، الجزائر، 2007، ص 18.

³ - أسامة أحمد المناعة، جلال محمد الزغي، المرجع السابق، ص 58، 59.

⁴ - بوضياف إسمهان، مرجع سابق، ص 354.

⁵ - مرجع نفسه، ص 354.

⁶ - مرجع نفسه، ص 355.

باعتبار المشرع حماية الحق وهو جهاز الحاسب الآلي لما يتضمنه من معلومات وبرامج الحاسوب، وعلى هذا النحو فدخوله إلى نظام الحاسب الآلي خطأ أو سهواً ينفي عنه شرط القصد الجنائي بشرط المغادرة فور علمه بدخوله غير الشرعي،² وفي جريمة الاحتيال الإلكتروني التي بدورها جريمة عمدية، يتطلب المشرع قصداً جنائياً لقيام مسؤولية الجاني، والقصد الجنائي المشروط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم أنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع.¹

الفرع الثاني

أطراف الجريمة

إن الجانب المشرق من التحول التكنولوجي في حياة المجتمع ولد وكغيره من الظواهر المستحدثة جانباً مظلماً، يتمثل في صورة الجريمة الإلكترونية، وهذه الأخيرة كغيرها من الجرائم المعتادة لها أطراف ومراكز قانونية هم الجاني (أولاً) والمجني عليه (ثانياً) وهذا ما سنتناوله كآتي:

أولاً- الجاني أو المجرم المعلوماتي :

لطالما ارتبطت شخصية المجرم المعلوماتي بصورة الطالب في مجال علوم المعلوماتية ، أو في صورة ذلك الشخص الموهوس بالتقنية المعلوماتية، والذي لا يستهدف من خلال فعله سوى اختبار قدراته في مواجهة النظام المعلوماتي، غير أن التحول الجذري من حيث مدى خطورة هذه الأفعال دفع وبصفة تدريجية إلى تصنيفها ضمن مجال الاعتداءات التي تتدرج في صنف الجريمة الخطيرة، فقد تحول المجرم المعلوماتي من مجرد اللهو والعبث بالأنظمة المعلوماتية إلى أهداف أكبر من ذلك يتصدرها تحقيق الربح المادي، الانتقام أو الإضرار بالغير وصولاً إلى الإرهاب المعلوماتي²، ومنه فالمجرم المعلوماتي هو المجرم الذي يرتكب الجريمة الإلكترونية يطلق عليه تسمية المجرم الإلكتروني أو المعلوماتي، ليس هناك اتفاق على صفات مرتكبي الجرائم الإلكترونية ، ولا يوجد قالب يتضمن الفئات والسمات التي يتسم بها مرتكب الجريمة الإلكترونية إلا أن هناك صفات ذات دلالة مشتركة يجمع المختصون بأنها توجد في كل الأشخاص الذين تم التحقيق والقبض عليهم في جرائم من هذا النوع، ولهذا فالصفات التي يتسم بها هذا المجرم تتمثل في:

- المجرم الإلكتروني غالباً ما يكون متوسط العمر بحيث يتراوح عمره بين 14 إلى 38 سنة، وهذا يدل بأن أغلب مرتكبي هذا النوع من الجرائم من فئة الشباب.

-المجرم المعلوماتي يتمتع بالمهارة والمعرفة والذكاء، حيث يمكنه التغلب على الكثير من العقبات التي تواجهه أثناء ارتكاب الجريمة .

¹ - زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، د.ط، دار الهدى للطباعة و النشر و التوزيع، الجزائر، 2011، ص65-ص66.
² - مرجع نفسه، ص67.

- المجرم المعلوماتي يتمتع بالسلطة اتجاه النظام المعلوماتي، حيث أن المزايا التي يتمتع بها المجرم المعلوماتي تمكنه من ارتكاب جريمته، وقد تتمثل هذه السلطة مثلاً في الشفرة الخاصة بالدخول إلى النظام الذي يحتوي على معلومات ، التي تعطي المجرم إمكانية فتح الملفات وقراءتها وكتبتها و محو المعلومات.
- المجرم المعلوماتي شخص ذو مهارات فنية عالية متخصص في الإجرام المعلوماتي، قادر على استخدام خبراته فالاختراقات وتغيير المعلومات.
- المجرم المعلوماتي قادر على تقليد البرامج و تحويل الأموال، محترف في التعامل مع شبكات الحاسبات، وهو شخص غير عنيف لأن تلك الجريمة لا تلجأ إلى العنف لارتكابها.
- وكذا امتلاكه الوسيلة أو الموارد وهي الإمكانيات التي يتزود بها الفاعل لارتكاب جريمته سواء من حواسيب أو الهواتف أو أجهزة أخرى.
- كما أنه يملك الباعث وهو الدافع الذي يجعل المجرم المعلوماتي يرتكب هذا النوع من الجرائم ، كما ينقسم المجرم المعلوماتي إلى فئات وهي كالتالي:

1- صغار مجرمي المعلوماتية:

هناك من يسميهم بصغار نوابغ المعلوماتية، وهم فئة المهووسون بالمعلوماتية ويرتكب هؤلاء المجرمين الجرائم بنية المزاح مع الآخرين دون أن تكون نيتهم إحداث ضرر بالمجني عليه، ولكن يجب عدم التقليل من خطورة هؤلاء الأشخاص، فهذه الفئة قد تتخطى مرحلة الهواية والعبث لتدخل مرحلة متقدمة أكثر في ارتكاب الجرائم المعلوماتية، وهي مرحلة الاحتراف لهذه الجرائم، كما أنه هناك مخاوف تتمثل في احتضان منظمات الجريمة المنظمة لهذه الفئة للاستفادة مهارتهم وتطوريتها، حيث أن هذه الفئة هي الأكثر سهولة للتأثر عليها.¹

2- محترفون في الجريمة الالكترونية:

يتمتع أصحابها بالخبرة والدراية أكثر من الفئة الأولى وينقسمون حسب خطورتهم إلى:

-الهواة الهاكر (HACKERS): يعرف الهاكرز بأنهم الأشخاص الذين يعملون على إنشاء و تعديل البرمجيات و العتاد الحاسوبي² ، هم عادة شباب فضوليين يسعون للتسلية ولا يشكلون خطورة ولكن يهتمون بسرقة جرائمهم لكي لا يشعر بهم احد.

ب-المحترفون الكراكر (CRACKERS): وهم الصنف الأكثر خطورة الذين يحدثون أضرار كبيرة وهدفهم كسب المال و إلحاق الضرر بالمجني عليه، ومعنى الكراكرز هو المقتحمون ويدعون

¹ محمد بوعمر و سيد علي ببنال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في العلوم القانونية ، تخصص قانون الأعمال، كلية الحقوق و العلوم السياسية ، جامعة أكلي محند أو لحاج البويرة، 2019-2020، ص14

² رشيدة بوكري، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية ، لبنان ، 2012، ص95-ص96.

بالمجرمين البالغين أو المخربين، وهم أكبر سن من الفئة التي سبقتهم، أعمارهم تتراوح ما بين 25-45 سنة، ومن أبرز صفاتهم أنهم من المتخصصين في مجال التقنية الإلكترونية، ومعارف فنية في مجال الأنظمة الإلكترونية والتحكم في البيئة الرقمية.¹

ج-المخادعون: وهؤلاء يتمتعون بقدرات فنية عالية باعتبارهم من الأخصائيين في المعلوماتية، يسعون لإلحاق الضرر بالمؤسسة التي يعملون بها مستعملون الوسائل الموضوعية التي تحت تصرفهم.²

3- فئة مجرمو المعلوماتية في إطار الجريمة المنظمة:

الجريمة المنظمة هي عبارة عن مجتمع إجرامي يعمل خارج الشعب و الحكومة ويضم في طياته عدد كبير من المجرمين الذين يعملون وفقا لنظام بالغ الدقة و التعقيد يفوق النظم التي تتبعها أكثر المنظمات تطورا و تقدما، كما يخضع أفرادها إلى أحكام قانونية سنوها بأنفسهم، و تفرض عليهم أحكام بالغة القساوة على من يخرج عن الجماعة، و يلتزمون في أداء أنشطتهم الإجرامية التخطيط الدقيق و المدروس، حيث يجنون من ورائه أموال طائلة، و من أمثلة عن هذه الجرائم عصابات سرقة السيارات الذين يحددون بواسطة شبكة الانترنت الأماكن التي ترتفع فيها أسعار بيع قطع غيار السيارات و من ثم يبيعون تلك القطع المسروقة بأكثر ربح ممكن.³

ثانيا- المجني عليه في الجريمة الإلكترونية:

النظم المعلوماتية باعتبارها من أهم مجالات الحياة أصبحت تتحكم في مختلف قطاعات الدولة سواء العامة أو الخاصة وأصبح العمل لا مفر منه، ولكن أصبح المجرم المعلوماتي يستعمل طرق احتيالية لاخترق النظام المعلوماتي حيث يستهدف كل المكونات المادية والمنطقية للحاسوب، وقد يكون المجني عليه إما شخص طبيعي أو معنوي وليتحقق عليه مصطلح المجني عليه إلكترونيا يجب أن يمس مكونات الحاسب و مكوناته، و ما يميز الضحية في الجريمة الإلكترونية عن الضحية الجريمة العادية أن أغلب الضحايا لا يريدون التبليغ عن الجرائم التي حدثت لهم ولا يعترفون أنهم وقعوا ضحية اعتداء إلكتروني وخصوصا المؤسسات المالية والبنوك فيكون الجاني في موقف قوة حيث إن تم التبليغ عنه فإن المؤسسة ستخسر أضعاف المبالغ التي تحصل عليها الجاني وذلك بسبب سمعتهم، ذلك أن المتعاملين عند ورود إلا مسامعهم أن مدخراتهم في تلك المؤسسات التي أودعوا أموالهم بها قد تعرضت لاعتداء سيهبون بسرعة من أجل سحب أموالهم من تلك المؤسسات المالية ، و هذا ما ينجم عنه خسائر مالية كبيرة لها، وفي هاتيه الحالة يمكن للمعتدي التصرف في هذه المعلومات و البيانات سواء عن طريق بيعها أو إتلافها أو مقايضتها.⁴

¹ مرجع نفسه، ص 96-97.

² غريبي بشر، "خصوصية المجرم المعلوماتي ودوافعه"، مجلة نومي روس الأكاديمية"، العدد الثاني، جامعة أبو بكر بلقايد تلمسان، 01 جوان 2021، ص 108.

³ مرجع نفسه، ص 109.

⁴ عبد الفتاح البيومي حجازي، مكافحة جرائم الأنترنت، دار الفكر الجامعي، مصر، 2006، ص 96، 97.

الفرع الثالث

أشكال الجريمة الإلكترونية

انتشرت الجريمة الإلكترونية بشكل كبير وبعده أشكال هذا ما استدعى منا التطرق لهذه الأشكال على النحو التالي:

أولاً: الجريمة المادية

هي التي تسبب أضرار مادية على الضحية أو المستهدف من عملية النصب و تأخذ واحدة من الأشكال الثلاثة التالية:

- عملية السرقة الإلكترونية كالاستيلاء على ماكنات الصرف الآلي والبنوك كذلك المنتشرة فالكثير من الدول و بها يتم نسخ البيانات الإلكترونية لبطاقة الصراف الآلي ثم استخدامها لصرف أموال حساب الضحية.

- إنشاء صفة انترنت مماثلة جدا لموقع أحد البنوك الكبرى أو المؤسسات المالية الضخمة.

- الرسائل البريدية الواردة من مصادر مجهولة بخصوص المساهمة في تحرير الأموال من الخارج و الوعد بنسبة من الأرباح، أو تلك توهم صاحب البريدي الإلكتروني بفوزه بأحد الجوائز أو اليانصيب.¹

ثانياً: الجرائم الثقافية :

هي إستلاء المجرم على الحقوق الفكرية ونسبتها لهم دون موافقة الضحية وتكون على إحدى الصور الآتية:

- قرصنة البرمجيات وهي عملية نسخ أو تقليد لبرامج إحدى الشركات العالمية وبيعها للناس بسعر أقل.

- التعدي على القنوات الفضائية المشفرة وإتاحتها عن طريق الانترنت من خلال تقنية .SOFT COPY

- جريمة لنسخ المؤلفات العلمية والأدبية بالطرق الإلكترونية المستحدثة.²

ثالثاً: الجرائم السياسية والاقتصادية:

تستخدم المجموعات الإرهابية حالياً تقنية المعلومات لتسهيل الأشكال النمطية من الأعمال الإجرامية وهم لا يتوانون عن استخدام الوسائل المتقدمة مثل: الاتصالات التنسيق وبث الأخبار المغلوطة وتوظيف بعض صغار السن وتمويلهم في سبيل تحقيق أهدافهم.

¹ محمد بوعمره ، سيد علي ببنال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر في العلوم القانونية، تخصص قانون الأعمال، كلية الحقوق والعلوم الإنسانية ، جامعة أكلي محند أو لحاج، البويرة، 2020/2019، ص11.

² مرجع سابق ، ص11.

- الاستيلاء على المواقع الحساسة وسرقة المعلومات بامتلاك القدرة على نشر الفيروسات.
- نشر الأفكار الخاطئة بين الشباب كالإرهاب والإدمان والزنة لفساد الدولة لأسباب سياسية واقتصادية بالدرجة الأولى.¹

رابعاً: الجرائم الجنسية

توجد مواقع على شبكة الانترنت تعرض على ممارسة الجنس، سواء على الكبار أو الأطفال، وتقوم هذه المواقع بنشر صور جنسية أكثر تخصصية، فمنها ماهو متخصص في أفلام الفيديو، ومنها ماهو متخصص في الصور، وعن طريق هذه المواقع الجنسية تبدأ المراسلات الإلكترونية والعروض للإيقاع بأكبر عدد من الضحايا من صغار السن²، ويمكن لهذا النوع من الجرائم أن يأخذ إحدى الصور الآتية:

- **الابتزاز:** من أشهر حوادث الابتزاز عند يقوم أحد الشباب باختراق جهاز إحدى الفتيات، أو الاستيلاء عليه وفيه مجموعة من صورها وإجبارها على الخروج معه أو فضحها بما يملكه من صورها، كما يمكن أن تكون عن معلومات عادة محرّجة أو ذات طبيعة مدمرة اجتماعيا وهو بمعنى الحصول على أهداف غير مشروعة بإتباع وسائل غير مشروعة، وقد يستخدم الابتزاز في أي وظيفة مهما كان نوعها للتأثير على الشخص الذي يكون عرضه لهذا الفعل لتحقيق مكاسب نوعية وغير مشروعة.³

- **التغريب والاستدراج:** في العادة هذا الاستدراج يمس الفئة الهشة من المجتمع وهم الأطفال صغار السن، فهم معرضون لخطر الوقوع ضحايا لمحرشي الأطفال، وهذا النوع لا يتضمن تلامسا جسديا، وإنما من خلال إجبار أو تشجيع الطفل على مشاهدة الطفل على محتوى جنسي مثل الصور، الفيديوهات والمحادثات وغيرها، أو سماع أو قول كلما ذات محتوى جنسي.⁴

خامساً: جرائم حسب الأفراد:

هي الجرائم التي يتم الوصول فيها إلى الهوية الإلكترونية للأفراد بطرق غير شرعية كحسابات البريد الإلكتروني وكلمات السر التي تخصهم وقد تصل إلى انتحال شخصيتهم وأخذ صور وملفاتهم المهمة من أجهزتهم بهدف تهديدهم وينطوي تحت هذا القسم من الجرائم كل من:

- جرائم التهديد والتخريب.

- جرائم التشهير بهدف تشويه سمعة الأفراد.

- جرائم السب والشتم والقذف.

¹ نواوي سليمة، "دور الدرك الوطني في محاربة الجريمة الإلكترونية"، مذكرة لنيل شهادة الماستر في علوم الإعلام و الإتصال، تخصص اتصال وعلاقات عامة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف، المسيلة، 2018-2019، ص26.

² مرجع نفسه، ص26-ص27.

³ سعيد زيوش، "ظواهر الابتزاز الإلكتروني وأساليب الوقاية - قراءة سوسيولوجية وأراء نظرية"، مجلة العلوم الاجتماعية"، العدد 22، جانفي 2017، ص 71.

⁴ صورية عثمانى، رابط، سعاد بن جديدي، "التحرش الجنسي بالأطفال المظاهر و المخاطر بين "متحرش و متحرش به"، دراسة حالة"، مجلة دراسات في سيكولوجيات الانحراف"، العدد 30:01 - 2016-12، ص82:83.

- جرائم المطاردة الإلكترونية.¹

الفرع الرابع

تقسيم الجرائم الإلكترونية في التشريع الجزائري

كما هو معلوم قسم المشرع الجزائري الجرائم حسب خطورتها إلى جنايات وهي أخطر الجرائم، تليها الجناح وهي متوسطة الخطورة، ثم المخالفات وهي جرائم بسيطة وقل خطورة من سابقتها، وصنفها بحسب طبيعتها إلى جريمة عادية وجريمة سياسية، جريمة عسكرية وأخرى إرهابية²، والجريمة الإلكترونية قسمها المشرع الجزائري إلى جرائم مرتكبة بواسطة النظام المعلوماتي والتي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والاتصال وهذا هو النوع الأول، والنوع الثاني من الجرائم المعلوماتية التي عرج عليها المشرع الجزائري يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات، وهذا ما سيتم بيانه في هذا الفرع أين سنوضح الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي (أولاً)، والجريمة الإلكترونية الواقعة على النظام المعلوماتي (ثانياً).

أولاً: الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي.

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها، وهي أنواع منها الجريمة الواقعة على الأشخاص (1)، والجريمة الواقعة على النظم المعلوماتية الأخرى (2)، وأخيراً الجريمة الواقعة على الأسرار (3).

1- الجريمة الإلكترونية الواقعة على الأشخاص الطبيعية:

تنقسم هذه الجرائم بدورها إلى جرائم واقعة حرمة الحياة الخاصة (أ)، وجرائم واقعة على حقوق الملكية الفكرية (ب).

أ- الجريمة الإلكترونية الواقعة على حرمة الحياة الخاصة:

هي تلك الجرائم التي تهدد وتشكل خطر على الحقوق ذات الطابع الشخصي أي اللصيقة بشخص المجني عليه ومنها جرائم القذف والسب والذم وجرائم حث قاصرين على أنشطة جنسية تتم عبر الوسائط الإلكترونية، والتهديد والتحرش والمضايقة عبر الوسائل التقنية، وجرائم التصنت وإلتقاط الرسائل الإلكترونية.³

كل هذه الجرائم الماسة بالأشخاص تدخل ضمن الحياة الخاصة للأفراد التي كفلها القانون وفي مقدمتها الدستور الجزائري من خلال المادتين:

¹ بن سولة نور الدين، "الجرائم الإلكترونية في ضوء التشريع الجزائري"، "مجلة الحوار المتوسطي"، المجلد التاسع، العدد 1، مارس 2018، ص 272.

² أحسن بوسقيعة، الوجيز في القانون الجزائري العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002، ص 24.

³ إلينا محمد الأسدي، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية (دراسة مقارنة)، دار حامد للنشر والتوزيع، عمان، 2015، ص 43، 35.

المادة 39: "تضمن الدولة عدم انتهاك حرمة الإنسان".

المادة 47: "لكل شخص الحق في حماية حياته الخاصة وشرفه، لكل شخص الحق في سرية مراسلاته واتصالاته الخاصة في أي شكل كانت، لا مساس بالحقوق المذكورة في الفقرتين الأولى والثانية إلا بأمر من السلطة القضائية، حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي، يعاقب على كل انتهاك لهذه الحقوق".¹

لقد كرس الدستور الجزائري حرصه على حماية الحياة الخاصة للمواطنين و عدم الاعتداء على هذه الحرمة، و لأن الحاسب الآلي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين أكبر قدر ممكن من المعلومات، هذا ما جعل للحاسب الآلي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، و مثاله أن يقوم شخص يعمل بالنظام المعلوماتي بإعداد ملف يحتوي على معلومات تخص شخص آخر بدون علمه، أو أن يجمع المعلومات بعلم الشخص المعني و لكن يقوم المكلف بحفظها وإطلاع الغير عليها دون إذن صاحبها، أو أن يقوم شخص باختراق معلومات هي بمثابة أسرار مكتوبة وسير ذاتية و مذكرات شخصية لشخص آخر، وكذا إساءة جمع البيانات عن الأشخاص و استخدامها في غير الغرض المخصص لها.²

ب- الجريمة الإلكترونية الواقعة على حقوق الملكية الفكرية:

يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفكرية، و مثاله السطو على بنك المعلومات و تخزين و استخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون إذن صاحبها يعتبر اعتداء على حق معنوي، إضافة إلى كونه اعتداء على قيمتها المالية كون أن للمعلومة قيمة أدبية بجانب قيمتها المادية، و يندرج ضمن الحقوق الفكرية كذلك براءات الاختراع، إذ تمثل فكرة للمخترع تحتوي على حق معنوي وآخر مالي للمخترع و قد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية و هي الأمر رقم 03-05 الصادر في 2003، المتعلق بحقوق المؤلف و الحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق براءات الاختراع.³

2- الجرائم الواقعة على الأموال:

لقد صاحب ظهور شبكة الأنترنت تطورات كثيرة في شتى المجالات، حيث أصبحت معظم المعاملات التجارية تتم من خلال هذه الشبكة، مثل البيع والشراء مما أنجر عنه تطور وسائل الدفع والوفاء وأضحت جزء لا يتجزأ من هذه المعاملات، وفي خضم هذا التداول المالي عبر الأنترنت انتهاز

¹ الدستور الجزائري لسنة 2020، ج.ج.ج، العدد 82، صادر في 30 ديسمبر 2020..

² ابتسام مناع، "جريمة الاعتداء الإلكتروني على الحياة الخاصة في التشريع الجزائري"، "مجلة الشريعة و الاقتصاد"، المجلد الثامن، العدد 15، جامعة منتوري، قسنطينة، 2019، ص319-ص324.

³ نفس المرجع، ص325.

بعض المجرمين الفرصة من أجل السطو والسرقة والتحويل الإلكتروني غير المشروع للأموال وقرصنة أرقام البطاقات الممغنطة.¹

في ظل هذا التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الرقمية وما أنجر عنه من تطور وسائل الدفع والوفاء ، وفي خضم التداول المالي عبر الأنترنت أصبحت هذه المعاملات عرضة لشتى أنواع الجرائم ومنها:

السطو على أرقام بطاقات الائتمان والتحويل الإلكتروني الغير مشروع.

القمار وغسيل الأموال عبر الأنترنت.

جريمة السرقة والسطو على أموال البنوك.

تجارة المخدرات عبر الأنترنت.²

3- الجريمة الإلكترونية الواقعة على الأسرار:

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأسرار سواء كانت أسرار عامة أو أسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة ، ويتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعة على أسرار الدولة²، حيث أتاح الأنترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الأسرار العسكرية والاقتصادية لهذه الأخيرة خاصة في الدول التي يكون فيها نزاعات ، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهيمه الأمر أو يستخدمها للضغط على أصحابها من أجل القيام بعمل أو الامتناع عن القيام بعمل³. وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 إلى المادة 96 مكرر من قانون العقوبات بالإضافة إلى المادة 394 مكرر 03 التي تنص على أنه: "تضاعف العقوبات المنصوص عليها في هذا القسم إذا استهدفت الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام دون الإخلال بتطبيق عقوبات أشد".⁴

¹ - صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري ، تيزي وزو، 2013، ص44.

² بوضياف أسمهان، "الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر"، "مجلة الأستاذ الباحث للدراسات القانونية والسياسية"، العدد 11، جامعة محمد بوضياف المسيلة، 2018، ص358.

³ نفس المرجع، ص26.

⁴ - قانون رقم 15-04، مؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-156، الصادر في 08 جوان 1966، متضمن قانون العقوبات، ج. ر ، العدد

ثانيا: الجريمة الإلكترونية الواقعة على النظام المعلوماتي.

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04-15 الصادر في 10 نوفمبر 2004، المعدل والمتمم لقانون العقوبات ليجرم كل أنواع الاعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المواد 394 مكرر إلى 394 مكرر 07، وتأخذ صور الاعتداء صورتين وهما: الدخول والبقاء في منظومة معلوماتية(1)، المساس بمنظومة معلوماتية(2)، كما تضمن صور أخرى للغش وهي ما سنتناوله في البنود الموالية(3)

1- جرمي الدخول والبقاء غير المشروعان في منظومة معلوماتية.

تنص المادة 394 مكرر من قانون العقوبات على معاقبة كل شخص يدخل أو يبقى بواسطة استعمال الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك، و إذا نتج عن هذا الدخول أو البقاء غير المشروع إما دمج أو محو أو تغيير في المعطيات الموجودة في النظام.¹

أ- فعل الدخول غير المشروع :

لا يقصد هنا الدخول بالمعنى المادي، أي الدخول إلى مكان معين كمنزل أو غيره، بل هو التوصل أوولوج دون إذن ودون تصريح إلى نظام إلكتروني أو مجموعة نظم عن طريق انتهاك إجراءات الأمن، وعرف الدخول غير المشروع للنظام الإلكتروني بأنه "هو الدخول عن طريق انتهاك الإجراءات الأمنية"، كما عرف بأنه: التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام²، وكما ينظر إليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو إلى ملكية التفكير لدى الإنسان، أي الدخول إلى العمليات الذهنية التي يقوم بها نظام المعالجة الآلية للمعطيات، وتقع هذه الجريمة من كل إنسان أيا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، و سواء كان يستطيع أن يستفيد من الدخول أم لا، فيكفي أن يكون الجاني ممن ليس له الحق في الدخول بالطريقة التي دخلوا بها، كما تقع الجريمة سواء تم الدخول إلى النظام كله أو إلى جزء منه فقط، أي أن الجريمة تقوم بفعل الدخول إلى النظام مجردا عن أي نتيجة أخرى، ولا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام، ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت أو غير محمية، كما تشمل استعمال من لاحق له في ذلك المفتاح للدخول إلى المنظومة.³

ويتحقق الدخول بأي وسيلة تقنية، وذلك عن طريق كلمة السر الحقيقية متى كان الجاني غير مخول في استخدامها، أو باستخدام برنامج أو شفرة خاصة، أو عن طريق الرقم السري لشخص آخر أو الدخول من

¹ - حمزة بن عقون، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012، صص 182-183.

² - عبد الفتاح بيومي حجازي، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجين دراسة معمقة في القانون المعلوماتي، دار الفكر الجامعي، مصر، 2006، ص 357، 360.

³ - حمزة بن عقون، مرجع سابق، ص 183.

خلال شخص مسموح له بالدخول وسواء كان عن طريق شبكة الاتصال التلفونية أو الشبكات المحلية أو العالمية، و كذلك يتحقق فعل الدخول غير المصرح به وغير المشروع متى كان مسموحا للجاني بالدخول إلى جزء معين من البرنامج حيث تجاوزه إلى جزء آخر غير مسموح له بالدخول فيه.¹

ب- فعل البقاء غير المشروع:

يقصد بفعل البقاء غير المشروع هنا، الدخول إلى النظام والاستمرار في التواجد داخله وذلك دون إذن صاحبه، رغم علمه بأن بقاءه فيه غير مرخص²، و يعتبر فعل البقاء مثله مثل فعل الدخول، بمثابة الركن المادي للجريمة، ونضيف هنا و نؤكد أن البقاء قد يحتمل صورتين، أولهما فعل البقاء غير المشروع داخل النظام تبدأ من اللحظة التي يتم فيها الدخول الفعلي للمجرم إلى النظام، وذلك بتجوله وتنقله داخل هذا الأخير، و هنا تكون جريمة الدخول مكتملة، و هناك من يرى بأن جريمة البقاء تكون في الوقت الذي يعلم في المتدخل بان بقاءه في النظام غير المشروع، و لم ينسحب من النظام.³ ومهما يكن من أمر فإن المشرع الجزائري ومن خلال المادة 394 مكرر قد تطرق إلى الدخول ثم إلى البقاء، و كأن المشرع يصنف الأولى بجريمة وقتية كون فترة استمرارها قصيرا جدا والأخرى بجريمة مستمرة مقارنة بالأولى.⁴

2- جريمة المساس بمنظومة معلوماتية:

عرفها البعض بأنها الجرائم التي تقع على جهاز الحاسب الآلي ومن شأنها المساس بالبيانات أو المعطيات، و حقوق الأفراد وحررياتهم، كما عرفها البعض الآخر على أنها كل نشاط غير مشروع يستهدف جهاز الكمبيوتر، فيمكن تعريف هذه الجرائم بأنها هي كل فعل غير مشروع مرتكب بواسطة جهاز الحاسوب أو الهاتف الذكي أو أي وسيلة إلكترونية أخرى.

وحيث نصت المادة 394 مكرر 01 من قانون العقوبات على معاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش، هذا السلوك الإجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما أن المشرع لم يشترط اجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداها فقط لكي يتوافر الركن المادي، و أفعال الإدخال و الإزالة و التعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الآلية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة، أو محو أو تعديل معطيات موجودة من قبل، كما أن هذا السلوك يجسد فعل التخريب و إفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثال ذلك إدخال فيروس المعلوماتية في البرامج من أجل إتلافها.⁵

¹ - حمزة بن عقون، مرجع سابق، ص 183-184.

² - أمال قارة ، الحماية الجزائية للمعلوماتية في التشريع الجزائري ، دار هومة للطباعة و النشر والتوزيع، الجزائر، 2007، ص 102.

³ - نفس المرجع، ص 103.

⁴ - نفس المرجع، ص 103-104.

⁵ - نفس المرجع، ص 104.

المبحث الثاني

ماهية البحث و التحري عن الجريمة الإلكترونية

إن التطورات التي شهدتها العالم في مجال الإلكترونيات و تكنولوجيا المعلومات أثرت على جهات التحقيق و مكافحة الجريمة ، فأصبحت ملزمة بالأخذ بكل ما هو جديد في العلوم و التكنولوجيا لرصد حركة الجريمة و التحري عنها فبالتالي أسلوب البحث و التحري عن الجريمة الإلكترونية يجب أن يتغير و يتطور لمواجهة فكر و أسلوب المجرم الإلكتروني و المحاولة بكل جهد الوصول إلى كشف و جمع الأدلة، فالتحري في هذا النوع من الجرائم فن بحاجة إلى موهبة وإتقان، ونعني بالتحري مجموعة من الإجراءات الأولية التي تباشرها سلطة التحقيق عند وقوع الجريمة بهدف البحث والتنقيب عن الأدلة التي تفيد الكشف عن غموض الجريمة، فتعطي هذه المرحلة صورة واضحة عن وقوع الجريمة وكيفية حدوثها والظروف التي رافقتها، على ذلك فإننا سنبين مفهوم البحث والتحري في الجريمة الإلكترونية (المطلب الأول)، وأجهزة البحث والتحري في الجريمة الإلكترونية (المطلب الثاني).

المطلب الأول

مفهوم البحث و التحري عن الجريمة الإلكترونية

إذا وقعت جريمة ما ونما إلى علم السلطات العامة نبئ ارتكابها فإن تلك السلطات تبدأ في التحرك وتتخذ مجموعة من الإجراءات التمهيدية بهدف تجميع أكبر قدر ممكن من المعلومات حول الجريمة وظروف ارتكابها وهذا ما يدعى بالبحث والتحري عن الجريمة والذي يتم بطرق قانونية، فإذا كانت الجهات المكلفة بالبحث والتحري عن الجريمة والمجرمين متعودة على التعامل مع الجريمة بصورها التقليدية، والتي يمكن إدراكها بالحواس لما يمكن أن يخلفه مرتكبوها من آثار مادية فإنها ستواجه مشكلات إجرائية عند التعامل مع الجريمة الإلكترونية وذلك نظرا للطبيعة الافتراضية والتقنية التي ترتكب فيها والتي لا يخلف فيها مرتكبها أي أثر مادي محسوس كما يسهل عليه تدمير الدليل و محوه من مسرح الجريمة مما يعقد أمر كشفها وتحديد مرتكبها، هذا ما يدفعنا إلى التطرق إلى تعريف البحث والتحري الخاص بالجرائم الإلكترونية (الفرع الأول)، وبيان خصائص البحث والتحري عن هذا النوع من الجرائم والشروط الملزم إتباعها لإجراء البحث والتحري (فرع الثاني)، كما سنتعرض إلى الوسائل المستعملة في البحث والتحري عن الجرائم الإلكترونية (الفرع الثالث).

الفرع الأول

تعريف البحث والتحري في الجريمة الإلكترونية

يمكن تعريف البحث والتحري في الجرائم الإلكترونية بأنه عمل قانوني يقوم به رجال الضبط القضائي المختصين في ضبط الجرائم الإلكترونية الرقمية من فاعل ودليل إلكتروني رقمي لتقديمه إلى

سلطات التحقيق القضائي التي يجب أن تكون متخصصة في هذه النوعية من الجرائم للإقامة العدل¹، وهو إجراء من أهم إجراءات التي تتخذ بعد وقوع الجريمة لما لها من أهمية في إثبات حقيقة وقوعها وإقامة الإسناد المادي على مرتكبها بأدلة الإثبات على اختلاف أنواعها، وهو كما يدل اسمه عليه استجلاء الحقيقة لغرض الوصول إلى إدانة المتهم من عدمه بعد جمع الأدلة القائمة على الجريمة والتحري يمر بمرحلتين، مرحلة التحري الأولى وهي مرحلة جمع استدلالات التي يباشرها أعضاء الضبط القضائي حيث تنص المادة 12 فقرة 03 من قانون الإجراءات الجزائية الجزائي "يناط بالشرطة القضائية مهمة البحث والتحري عن الجرائم المقررة في قانون العقوبات..."²

أثار البحث عن هذه الجرائم مشاكل وصعوبات في استخلاص الأدلة التي تثبت وقوعها وتدين مرتكبها كونها تختلف عن الأدلة التقليدية في الجرائم العادية من حيث خصائصها وأنواعها وسبل جمعها ووسط ارتكابها وحتى صفات مرتكبها، كما يؤثر الدليل الإلكتروني صعوبات تتعلق بعدم ظهوره بشكل مرئي وفقدنا الآثار التقليدية للجريمة الإلكترونية بالإضافة إلى صعوبات المتعلقة بسلطات البحث والتحري لصعوبة اكتشافها ونقص خبرة السلطات، فالمشكلات الإجرائية التي ستواجه هذه الجهات عند تعاملها مع الجريمة الإلكترونية تبدأ من طبيعة البيئة الافتراضية التقنية التي ترتكب فيها مما يعقد أمر كشفها والتحري عنها.³

الفرع الثاني

خصائص البحث والتحري في الجريمة الإلكترونية و شروطه

سننتظر في هذا الفرع إلى الخصائص التي تميز البحث و التحري في الجرائم الإلكترونية عن باقي الجرائم المألوفة (أولا) وأهم الشروط التي يجب التقيد بها لإجراء عملية البحث والتحري (ثانيا)

أولا: خصائص البحث و التحري عن الجريمة الإلكترونية

تتشترك الجرائم التقليدية مع الجرائم العادية في التحري لكونها تكون الإجراءات المتبعة نفسها المتمثلة في المعاينة، التفتيش والمراقبة والتحريات والاستجواب بالإضافة إلى جمع وتحليل الأدلة إلا أن الجرائم الإلكترونية لها خصائص أو ما يميزها عن غيرها من الجرائم فيما يلي :

1- الجرائم الإلكترونية لا تترك آثار في مسرح الجريمة كما يمكن للجاني إتلاف الدليل بسهولة وهذا ما يجعل البحث والتحري فيها فيه نوع من الصعوبة و يحتاج إلى بذل جهد اكبر و إعطاء طاقة مضاعفة في جمع الاستدلالات الخاصة بالجريمة الإلكترونية.

¹ مصطفى محمد موسى، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، مصر، 2008، ص166.

² قانون 22/06 مؤرخ في 29 ذي القعدة 1427، الموافق ل20 ديسمبر 2006 و المعدل و المتمم لمر 66-155، 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج. ر.ج، العدد 48، الصادر في 24 ديسمبر 2006.

³ مرجع نفسه، ص167.

2- يعتمد البحث و التحري الالكتروني على وسائل تقنية وبرامج كفيلة بكشف هذا النوع من الجرائم و تكون إمكانية الحصول على الدليل و عمل نسخ في ظرف قياسي وبطريقة سريعة و سلسلة، و كما تساهم هذه الوسائل في جعل الدليل أكثر مصداقية و يؤخذ به.

3- التحري في الجرائم الالكترونية يكون مرهون بالمعرفة القانونية و الفنية للمحقق الالكتروني، كما يشكل فريق مختص و ذو خبرة فنية في هذا المجال من اجل ضمان اكتشاف الجرم بطريقة مضمونة و صحيحة.¹

4- خلو مرحلة التحري الالكتروني من أي عنف أو كره أو قهر أو إجبار لان الهدف هنا هو السرعة في جمع المعلومات بشأن الجريمة المفتعلة ، كما لا يكون في غالب الأحيان أي تواصل أو اتصال مباشر بين المحقق الإلكتروني و الجاني لكون الجرائم الالكترونية تتم كلها عن بعد و في الفضاء الرقمي لذا على ضابط الشرطة القضائية أخذ الحيطة و الحذر بشكل مضاعف عند قيامه بالتحري كما يضمن عدم المساس بحقوق الأفراد و حرياتهم².

5- وضع خطة عمل قبل الشروع في التحري الإلكتروني و تحديد الفريق الفني اللازم للقيام بالتحري و لا يبدأ في التحري إلا بعد معاينة مسرح الجريمة المتمثل في جهاز الحاسوب و التعرف على الأنظمة و تحديد مصدر الخطر ووضع البديهيات الكفيلة للتصدي لأي تغير في الجريمة³.

ثانيا: شروط البحث و التحري عن الجرائم الالكترونية:

البحث والتحري عموما هو مجموع الإجراءات التي يقوم بها المحقق تؤدي إلى اكتشاف الجريمة ومعرفة مرتكبها ولكي تتم يجب مراعاة مجموعة من الشروط الأساسية المتمثلة في :

1- أولا يجب التأكد من وقوع جريمة يعاقب عليها القانون كأي واقعة إجرامية ثم معرفة نوع هذه الجريمة و درجة خطورتها و اكتشاف مرتكبها والتطبيقات المستعملة ونوع الحاسوب المستعمل .

2- وضع خطة عمل مناسبة على ضوء المعلومات المتوفرة لدى المحقق وتحديد الفريق الفني اللازم لمساعدته في أعمال التحري و تحديد مصدر الخطر و وضع تطورات الكفيلة للتصدي للجريمة.

3- يجب أن يشكل فريق التحقيق من فنيين و أخصائيين ذوي خبرة في مجال الحاسوب و الانترنت و يمتازون بمهارات في التحري الجنائي بشكل عام و التحري الجنائي الالكتروني بشكل خاص و هذا يسهل فك التعقيدات التي يواجهونها.⁴

¹ بدرة وعلي، المواجهة الإجرائية للجرائم المعلوماتية، مذكرة الماستر تخصص القانون الجنائي، كلية الحقوق و العلوم القانونية، جامعة محمد بوضياف المسيلة، 2018-2019، ص ص 24-25.

² مرجع نفسه، ص ص 25-26.

³ سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، جامعة الحاج لخضر ، باتنة، 2012-2013، ص ص 60-61.

⁴ نفس المرجع، ص 61.

4- تحديد نوع نظام المعالجة الآلية للمعطيات، هل هو كومبيوتر معزول أم متصل بشبكة معلومات و إذا وقعت الجريمة في شبكة فإنه يجب حصر طرق الاتصال منها أو بها لمعرفة الطريقة التي تمت بها عملية الاختراق من عدمه.

5- يجب فصل التيار الكهربائي عن موقع المعاينة أو الذي يجمع فيه الاستدلالات، لشل فعالية الجاني في أن يقوم بطريقة ما بمحو آثار الجريمة كما قد يتدخل من خلال الشبكة من إتلاف كل المعلومات المخزنة.

الفرع الثالث

وسائل البحث و التحري عن الجرائم الالكترونية

عند البدء في إجراء البحث و التحري على المحقق الالتزام بالقوانين والتشريعات لتحقيق الشرعية وسهولة الوصول للجاني وبمأن الجرائم الالكترونية تتميز بطابع خاص ومميز عن غيرها من الجرائم فإن التحري فيها يحتاج إضافة إلى الالتزام السابق ذكره، يحتاج أيضا إلى معرفة وإدراك لوسائل وقوع الجريمة، فحل لغز الجريمة والوصول إلى الجاني يعتمد المحقق المعلوماتي على مجموعة من الوسائل نذكر منها :

أولا: الوسائل المادية

هي الأدوات الفنية التي غالب ما تستخدم في بنية النظام المعلوماتي والتي تستخدم في تنفيذ أساليب وإجراءات التحري المختلفة والتي تثبت وقوع الجريمة وتساعد على تحديد شخصية مرتكبها وتتمثل أهمها في :

1- عناوين الـ IP، MCA و البريد الالكتروني و برامج المحادثة:

وهي المسؤلة عن تراسل حزم البيانات عبر شبكة الانترنت و توجهها إلى أهدافها وهو يشبه عنوان البريد العادي، في حالة حدوث أي خلل أو إشكال أو أي أعمال تخريبية فإن أول ما يقوم به المحقق المعلوماتي هو البحث عن رقم الجهاز وتحديد موقعه لمعرفة الجاني الذي قام بتلك الأعمال التخريبية الغير قانونية.¹

2- البروكسي PROXY:

مزودات البروكسي تستخدم عالميا، وهو عبارة عن تطبيق يتم تركيبه على أجهزة الحاسوب ويعمل كجسم أو وسيط بين نقطتي اتصال الانترنت كما يؤمن الاتصال بواسطة بروتوكول الانترنت بين الشبكة الداخلية المحمية والعالم الخارجي أي شبكة الانترنت.²

¹ - سليمان بن مهجع الغنزي، و وسائل التحقق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا بجامعة نيف التدريبية للعلوم الأمنية، السعودية، ص98.

² - نفس المرجع، ص99.

3- الجدار الناري FIRE WALL:

هي أجهزة أمان الشبكة وتعتمد طريقة عملها على الفصل بين الشبكة الداخلية موثوقة وأخرى خارجية غير موثوقة ، وهي مسؤولة عن تنظيم حركة المرور الواردة والصادرة إلى ومن الشبكة تبعاً لقواعد الأمان ، و للجدار الناري أهمية فائقة في حماية الشبكة من الأنشطة الضارة على الانترنت والتهديدات المحتملة والدخول غير المصرح بيه، فلها سلطة فعالة لمنع المستخدمين من الأنشطة الغير مصرح لهم بها، أو منع البيانات المحظورة أو المشبوهة من المرور إلى الشبكة الداخلية، كما تقوم بحفظ السجلات على شكل ملفات حاسوبية يمكن الرجوع لها وقراءتها في أي وقت ¹.

4- برامج التتبع:

تقوم هذه البرامج بتتبع أنشطة الشخص مثل المواقع التي يزورها والبرامج التي يستخدمها وحتى مدة استخدامها، يعمل التطبيق بهدوء مسجلاً هذه التفاصيل ، وهو عبارة عن أداة أمان تساعد في الكشف عن أي محاولة غير مصرح بها للوصول لجهاز الكمبيوتر الخاص بالشخص وحمايته من أي تهديدات محتملة مما يحافظ على أنظمتها ومعلوماتها، كما يقوم بتقديم بيان شامل إلى المستخدم الذي تم اختراق جهازه محتوي اسم الحدث ، تاريخ حدوثه وعنوان الـ IP التي تم من خلاله الاختراق ².

5- برمجيات استعراض الصور:

هذا النوع من البرمجيات لا يختص بالتحري في جرائم الحاسوب فقط بل يمكن أن يستعمله المستخدم العادي أيضاً ، تؤدي هذه البرمجيات خدمة كبيرة للمحقق من خلال تمكنهم في مشاهدة و استعراض الصور الرقمية المخزنة داخل الحواسيب ³.

6- أدوات الضبط:

هي أدوات تعتبر من الوسائل المادية التي تساعد في ضبط الجريمة المعلوماتية نجد منها برامج الحماية، أدوات المراجعة و كذا برامج التصنت على الشبكة و برامج النسخ.

7- أدوات الفحص و مراقبة الشبكات :

تستخدم في فحص بروتوكول النقل الـ TP(transmission protocol) و بروتوكول طبقة النقل TLP(transport layer protocol) و ذلك لمعرفة ما قد يصيب الشبكة من مشاكل ومعرفة العمليات التي تتعرض لها ومن هذه الأدوات بروتوكول تحليل العنوان ARP(address resolution protocol) ⁴.

¹ - مرجع سابق، ص 99.

² محمد بن ناصر السرحاني، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الأنترنت، بحث مقدم لاستكمال متطلبات الحصول على درجة الماجستير، في قسم العلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نيف العربية للعلوم الأمنية ، السعودية، 2004، ص86،87.

³ نفس المرجع، ص ص 87-88.

⁴ سليمان بن مهجع الغنزي، مرجع سابق، ص30.

ثانياً: الوسائل الإجرائية:

تتمثل الوسائل الإجرائية في الإجراءات التي تستخدم لتنفيذ أو التي يعتمد عليها المحقق لتنفيذ التحري المحددة و الغير محددة التي تثبت وقوع الجريمة و تحدد شخصية الجاني و نذكر منها:

1- **اقتفاء الأثر:** من الأشياء التي تثير إشكال لدى المجرم المعلوماتي من ارتكابه أو بداية ارتكابه للجريمة الإلكترونية هو تقفي أثره و ذلك يتم بطرق عدة سواء عن طريق بريده الإلكتروني تم استقباله، أو عن طريق تتبع أثر الجهاز الذي تم استخدامه للقيام بالجرم اختراق كان أو نصب... الخ، كما يمكن من قيامه بعملية الاختراق على المواقع الخاصة بالمخترقين لو أثره وهذا يؤدي إلى القبض عليه حتى و إن كانت عملية الاختراق تمت بشكل سليم .

2- **الاطلاع على عمليات النظام المعلوماتي و أسلوب حمايته:** أصبحت النظم المعلوماتية و قواعد البيانات و شبكات الاتصال عصب العالم المعرفي و الصناعي و غيرها من القطاعات، حيث أصبح من المهم الحفاظ على امن المعلومات بعناصره الرئيسية الثلاث السرية ، الصوابية، الاستمرارية ،و يعتبر من كل الأنظمة الأمنية نظام الإيزو ISO للاعتماد و التقييس لضمان امن المعلومات ¹.

3- **الاستعانة بالذكاء الاصطناعي:** أثبتت تقنيات الحاسب الآلي نجاحها في جمع الأدلة الجنائية و تحليلها و استنتاج الحقائق منها، كما يمكن بالذكاء الاصطناعي من خلال استنتاج النتائج على ضوء معاملات حسابية يتم تحليلها بالحاسبة الإلكترونية وفق برامج.

4- **مراقبة الاتصالات الإلكترونية:** وهي من بين إجراءات التحقيق الحديثة و التي تلجئ إليها جهات التحقيق في سعيها لجمع الأدلة الإلكترونية و ذلك من خلال تقنيات حديثة تتمشى و طبيعة الجريمة الإلكترونية².

المطلب الثاني

أجهزة البحث و التحري عن الجريمة الإلكترونية

إن حداثة الجريمة المعلوماتية جعلها تتميز بخصوصية فريدة عن غيرها من الجرائم العادية، وهذا الاختلاف استوجب إيجاد مختصين بالتحقيق في هذه الجرائم يمتلكون ويتمتعون بقدر عالي من التحكم في التكنولوجيا ومهارة فنية لكي يتولون مهمة البحث والتحري عن هذا النوع من الجرائم وكشف النقاب عنها، ومن أجل احتواء هذه الجرائم وفك شفراتها استوجب كذلك إيجاد هيئات أو أجهزة مختصة في ذلك، ولهذا سوف نتطرق إلى المحقق في الجرائم الإلكترونية (الفرع الأول)، والهيئات المختصة بإجراء البحث والتحري عن الجرائم الإلكترونية (الفرع الثاني).

¹ على عدنان الفيل، إجراءات التحري و جمع الأدلة و التحقيق الابتدائي في الجريمة المعلوماتية(دراسة مقارنة)، المكتب الجامعي ، الإسكندرية، 2012، ص67.

² نفس المرجع، ص ص 67-69.

الفرع الأول

المحقق في الجرائم الإلكترونية

المحقق هو حجر الأساس في أي تحقيق وفي الجرائم الإلكترونية هو صمام الأمان الذي يتصدى لهذا النوع من الجرائم، ولأن الجرائم الإلكترونية ذات طابع خاص كما سبق وأن ذكرنا ذلك يلزم محققين ذوو مهارات خاصة كذلك، ولذلك سوف نوضح من هو المحقق الجنائي في الجرائم الإلكترونية (أولا) والخصائص التي يجب أن يتمتع بها (ثانيا).

أولا: تعريف المحقق الجنائي في الجرائم الإلكترونية

عرف المحقق أنه ذلك الشخص الذي عهد إليه قانونا باتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيها يصل إلى علمه من جرائم بهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة هذا هو التعريف الأصلي للمحقق ككل، أما المحقق الجنائي في الجرائم الإلكترونية هو حلقة وصل حيوية بين عالم القانون وعالم التكنولوجيا حيث يستخدم مهاراته ومعرفته وإلمامه بعالم التكنولوجيا لمكافحة الجريمة في الفضاء الرقمي وحماية المجتمع من أضرارها، فهو شخص متخصص في تحديد هوية مرتكبي الجرائم الإلكترونية وجمع الأدلة الرقمية وتحليلها وتقديمها إلى العدالة، ومن بين أهم مهارات المحقق الجنائي في الجرائم الإلكترونية أنه محقق غير المحقق في الجرائم العادية حيث يتمتع بمهارات عالية وتدريب خاص، كما يمتلك خبرة في مجال القانون الجنائي وعلم الحاسوب والأمن السيبراني من أجل جمع الأدلة الرقمية والحفاظ على سلامتها وكذلك تحليل تلك الأدلة الرقمية وتحديد هوية الجناة، وهؤلاء المحققين يحظون باهتمام كبير في القطاعين الخاص والعام.¹

ثانيا: خصائص المحقق في الجرائم الإلكترونية

مع الثورة التقنية والتطور التكنولوجي الذي شهده العالم مؤخرا صاحبه تطور الجريمة، فأصبحنا نعرف نوع جديد من الجرائم المستحدثة هي الجرائم الإلكترونية، و للتعامل مع هذا النوع من الجرائم استدعى إيجاب مختصين بالتحقيق في هذا النوع من الجرائم يختلفون عن الأشخاص المختصين بالتحقيق في الجرائم العادية والمألوفة من حيث الخصائص وطريقة التكوين، وبما أننا تحدثنا سابقا عن المحقق في الجرائم الإلكترونية ينبغي علينا ذكر الخصائص التي يجب أن تتوفر عليها من أجل أن يتصدى لمهمة البحث والتحري في هذا النوع من الجرائم والمجرمين، ونذكر منها :

1-المهارة التقنية والتحكم في جهاز الحاسوب TECHNICAL SKILLS:

وذلك من أجل إدارة كل ما يتعلق بالجرائم المرتكبة، لان افتقار ضباط الشرطة القضائية للتأهيل و التدريب الكافيين في الميدان التقني قد يؤدي إلى الوقوع في المحذور أي إتلاف و تدمير دليل إدانة

¹ على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية، دراسة مقارنة، المكتب الجامعي الحديث، الإسكندرية، 2012، ص17.

المجرم دون دراية، على اعتبار أن عدم إحاطته بأساليب ارتكاب الجريمة المعلوماتية يجعله يقع في أغلب الأحيان في أخطاء قد تؤدي من شأنها إلى محو الأدلة الرقمية، وعلى سبيل المثال لا الحصر إتلاف محتويات الأقراص الممغنطة¹، وعليه فإن الكشف عن هذا النوع من الجرائم يقتضي بالضرورة أن يكون الأشخاص المعنيين بالتحري على دراية كافية بأساسيات التعامل مع هذه الجرائم، كما يتوجب على المحقق معرفة آلية عمل تشكيلات الحاسوب والانترنت، وتبرز أهمية فهم المحقق لهذه المبادئ في كونها ضرورية لتصوير كيفية ارتكاب الفعل الإجرامي في العالم الافتراضي، من اختراق للشبكات واعتراض حزم البيانات أثناء انتقالها عبر الشبكة والتجسس وتحويلها عن مسارها، كما أنها تعطي للمحقق تصورا جيدا عن مدى إمكانية متابعة مصدر الاعتداء الشبكة والمعوقات التي تحول دون ذلك.

2- أن يكون ملما بتقنيات الأمن المعلوماتي و الحاسوبية:

من الأمور المهمة التي لا بد للمحقق المعلوماتي أن يكون عالما بها و مستوعبا لها هو إلمامه بالأمن المعلوماتي و الحاسوبية، لأنها تساعد في معرفة مجريات التحقيق، فالمحقق في مجال الجرائم الإلكترونية عندما يباشر اتصاله بجريمة ما و يبدأ التحقيق فيها يسأل القائمين على الشبكة عن نوع برامج الحماية المستخدمة وكيفية إعدادها، لان فهمه للبرامج الحماية وظيفتها و أسلوب عملها يساعده على فك اللباس و اكتشاف الفاعل، ومن الأمور التي يجب أن تتوفر في المحقق الإلكتروني أيضا معرفته واطلاعه على الأساليب المستخدمة في ارتكاب الجرائم المعلوماتية، ذلك أن معرفة المحقق لهذه الأساليب يعد من الأمور المهمة التي تساعد في معرفة الجناة و مواقع ارتكاب الجريمة و كذلك مناقشة الشهود وسماع المشتبه فيهم واكتشاف الحقيقة ومعرفة الفاعلين، وهذا لكونها لها أهمية بالغة وضرورية

لجعله يتصور كيفية وقوع الأفعال الإجرامية في الفضاء الرقمي وكذا كيفية اختراق الشبكات والولوج إليها والتصدي واعتراض البيانات عند إرسالها أو استقبالها عبر شبكات الحاسب والتجسس عليها وتحويلها عن وجهتها².

3- مؤهل ومدرّب:

من الضروري إعداد و تأهيل المحققين في الجرائم المعلوماتية باعتبارهم يواجهون أنشطة إجرامية معقدة و تنفذ بطرق دقيقة وذكية، و يتأتى ذلك من خلال الإسراع أن يطور رجال البحث الجنائي و سائلهم البحثية و قدراتهم العلمية و ليس بالضرورة أن يكون المحقق في الجريمة المعلوماتية خبيراً في الحاسوب و النظم المعلوماتية، و لكن لا بد من الإلمام ببعض المسائل الأولية التي تمكنه من التفاهم مع خبراء الحاسوب وحسن استغلالهم في كشف الجرائم وجمع الأدلة ، كما أنه من الضروري أن

¹ جميل عبد الباقي صغير، أدلة الإثبات الجنائي و التكنولوجيا الحديثة، دار النهضة العربية، القاهرة، 2002، ص115.

² نفس المرجع، ص116.

يكون المحقق ملما بالإجراءات الاحتياطية التي ينبغي اتخاذها على مسرح الجريمة والتدابير اللازمة لتأمين الأدلة و معلوماتها الممغنطة بصورة عملية وسليمة.¹

كما أن الوعي الجيد من قبل المحقق بالجرائم الإلكترونية و أنواعها المختلفة يعتبر بمثابة الحجر الأساس في مواجهتها و بدونه لن تنجح السبل و الوسائل الأخرى فلا يعقل أن تتم مواجهة جريمة ما إذا كان الشخص المسؤول عن البحث والتحقيق فيها غير ملم و يجهل ماهيتها.²

الفرع الثاني

الأجهزة المختصة بإجراء البحث والتحري في الجريمة الإلكترونية.

تفاقت الجرائم الإلكترونية وتزايدت بشكل طردي وملفت بحجم تطور التكنولوجيا والتقنية، ومع حداثة هذه الأخيرة جعل أجهزة التحقيق في الجرائم العادية غير قادرة على التصدي لها، وعلى هذا الأساس أنشأت هيئات وأجهزة خاصة من أجل تقصي أثر الجريمة الإلكترونية وكبحها، وتتمثل هذه الأجهزة في الهيئات الفنية المختصة في البحث والتحري عن الجرائم الإلكترونية.

أولاً: الهيئات الفنية المختصة في البحث والتحري عن الجرائم الإلكترونية

هذه الهيئات هي عبارة عن أجهزة غير قضائية والتي تتمثل في كل من الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال (1) وجهاز الشرطة والدرك الوطنيين (2).

1_ الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال

وقد استحدثتها المشرع الجزائري بموجب القانون رقم 04-09 السالف الذكر، ومن مهامها تفعيل التعاون القضائي والأمني الدولي وإدارة وتنسيق العمليات الوقائية والمساعدة التقنية للجهات القضائية والأمنية مع إمكانية تكليفها بالقيام بخبرات قضائية في حال الاعتداءات على منظومة معلوماتية على نحو يهدد مؤسسات الدولة أو الدفاع الوطني.³

الهيئة الوطنية تعد سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل، وتضم أساساً أعضاء من الحكومة معنيين بالموضوع، مسؤولي مصالح الأمن، وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء، تضم الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك والأمن الوطنيين، وفقاً لأحكام قانون الإجراءات الجزائية تكلف بتجميع وتسجيل وحفظ المعلومات الرقمية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية وضمان المراقبة والوقائية للاتصالات الإلكترونية، وذلك

¹ - هشام محمد فريد رستم، الجرائم المعلوماتية، بحث مقدم إلى مؤتمر القانون و الكمبيوتر و الانترنت، مجلد 02، كلية الشريعة والقانون جامعة الإمارات العربية المتحدة، الفترة من 01 إلى 03 مايو 2000، ص 495.

² - نفس المرجع، ص 497.

³ - أمال بن صوليج، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني في الجزائر"، مداخلة الملتقى الدولي حول "الإجرام السيبراني المفاهيم والتحديات"، 11-12 أبريل 2017، ص 29.

قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والماسة بأمن الدولة أو الجرائم الأخرى وذلك تحت سلطة القاضي المختص، وأيضا تبادل المعلومات مع نظيرتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم.

للإشارة هنا تمكنت الجزائر ممثلة أساسا في أجهزتها الأمنية التابعة للدرك الوطني و الأمن الوطني و بالتعاون مع الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال من معالجة أكثر من 100 جريمة الكترونية منها 30 من مواقع التواصل الاجتماعي، هذا وقد سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني خلال السداسي الأول من عام 2016 وجود 11 قضية متعلقة بالإرهاب الإلكتروني أغلبها خاصة بالتهديدات الإرهابية باسم تنظيم داعش الإرهابي لتسفر جهود البحث و التحري و التنسيق بين مختلف القطاعات المختصة توقيف 58 شخصا متورطا في قضايا إرهاب إلكتروني تمت إحالتهم على القضاء، هذا وقد استطاعت الشرطة الجزائرية المتخصصة من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق، سوريا وليبيا كما تمكنت من فك شفرات الرسائل المتبادلة وما يزيد من 30 خلية تسعى لاستقطاب الشباب لتجنيدهم عبر مرقع الانترنت ومنصات التواصل الاجتماعي وفي مقدمتها فيسبوك لصالح التنظيمات الإرهابية نتيجة استعمالها لأنظمة تكنولوجية حديثة وتلقيها معلومات تفيد بوجود منشورات إرهابية داعمة وتدعو للمشاركة في منديات إرهابية على جانب اتصالات محلية ودولية¹.

ثانيا- جهازي الأمن الوطني والدرك الوطني

إضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها هناك أجهزة أمنية مكلفة بالتدخل للمواجهة العملية على المستوى التطبيقي للجرائم الإلكترونية، أين سعت المديرية العامة للأمن الوطني وكذا جهاز الدرك الوطني في إنشاء فرق خاصة لمكافحة الجرائم المعلوماتية، وكذا تكوين عناصر متخصصة في هذا المجال سواء على المستوى الداخلي أو المستوى الخارجي، بالإضافة إلى توافر هاذين الجهازين على مخابر علمية مزودة بأحدث الأجهزة ذات التكنولوجيا المتطورة لكشف هذا النوع من الجرائم²، وتصنف هذه الهيئات الأمنية المكلفة بمكافحة الجرائم ذات الصلة إلى نوعين:

أ-الوحدات التابعة لسلك الأمن الوطني:

تضع مديرية الأمن الوطني في إطار تحديد سياسة أمنية فعالة، كافة الإمكانيات البشرية والتقنية المتاحة لديهم لأجل التصدي لكل أنواع الجرائم بالخصوص تلك المستحدثة منها كالجرائم الإلكترونية، والتي تعتبر نتاج القصور الحاصل على المستوى الدولي والوطني في مجال تكنولوجيات الإعلام والاتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا

¹ - نفس المرجع، ص30.

² - محمد السعيد زناتي، "الجريمة المعلوماتية في ظل التشريع الجزائري و الاتفاقيات الدولية"، "مجلة اليزي للبحوث و الدراسات"، العدد الثاني، المركز الجامعي اليزي، الجزائر، ديسمبر 2017، صص34-35.

النوع من التكنولوجيات، حيث يوجد على مستوى جهاز الأمن الوطني ثلاث وحدات مكلفة بالبحث والتحقيق في الجرائم المعلوماتية وهي كآلاتي:

- المخبر المركزي للشرطة العلمية بالجزائر العاصمة.

- المخبر الجهوي للشرطة العلمية بقسنطينة.

- المخبر الجهوي للشرطة العلمية بوهران.

في سبيل تدعيم المصالح الولائية للشرطة القضائية قامت المديرية العامة للأمن الوطني سنة 2010 بخلق ما يقارب 23 خلية لمكافحة الجريمة المعلوماتية على مستوى ولايات الوسط، الشرق، الغرب، الجنوب، لتقوم فيما بعد بتعميم الخلايا على جميع مصالح الأمن ولايات الوطن¹.

ب-الوحدات التابعة للقيادة العامة للدرك الوطني:

يضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني و النظام العام و محاربة الجريمة بكافة أنواعها، وحدات متنوعة وعديدة على مستوى القيادة العامة، أو على مستوى القيادات الجهوية والمحلية ونذكر منها:

- المصالح و المراكز العلمية و التقنية.

- هياكل التكوين.

- المصلحة المركزية للتحريات الجنائية.

- المعهد الوطني للأدلة الجنائية وعلم الإجرام.

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع لقيادة العلمية للدرك الوطني قسم الإعلام والإلكتروني الذي يختص بالتحقيق في الجرائم الإلكترونية، حيث يقوم بتحليل الأدلة الخاصة بالجرائم الإلكترونية، وذلك بتحليل الدعامات الإلكترونية، و انجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية و الفيديو و الصورة وذلك لتسهيل استغلالها بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مراد راييس والتابع لمديرية الأمن العمومي للدرك الوطني².

الوظيفة الأساسية للمعهد الوطني للأدلة الجنائية وعلم الإجرام هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيه الجريمة

¹ - نفس المرجع، ص36.

² - نفس المرجع، ص ص36-37.

المعلوماتية حيث يوجد بهذا المركز قسم الإعلام الآلي ولإلكترونيك الذي يختص بالتحقيق في الجرائم المعلوماتية.¹

¹ - مرجع سابق، ص37.

الفصل الثاني

إجراءات البحث والتحري عن الجريمة الإلكترونية

إن تتبع الجرائم بصفة عامة والجريمة الإلكترونية بصفة خاصة من أهم التحديات التي تقف أمام رجال الضبطية القضائية، حيث تتميز هذه الجرائم بصعوبة مراقبتها ومنع حدوثها، وكذلك البحث والتحري عن مرتكبيها نظرا لخطورتها، لهذا حرص المشرع الجزائري على التصدي ومكافحتها من أجل الحفاظ على أمن و سلامة المجتمع، ولأن التشريع هو اللبنة الأولى والأساسية التي يمكن للمشرع من خلالها مجابهة ومكافحة الجريمة مهما كانت فلا جريمة ولا عقوبة إلا بنص، تدخل المشرع وأصدر جملة من القوانين التي تساعد الجهات التي تباشر البحث والتحري وكذا التحقيق عن الجرائم الإلكترونية قصد التفصي و الكشف اللبس عنها، و نظرا لعجز وسائل التحري و التحقيق الكلاسيكية عن مواجهة الجرائم الحديثة إستحدث وأرسى قواعد إجرائية جديدة إضافة إلي التي قبلها تساو و تتمشى مع التطور الذي شهدته الجرائم الإلكترونية، و من أهمها التفتيش و ضبط الدليل الإلكتروني، مراقبة الإتصالات الإلكترونية والتسرب وكذا اعتراض المراسلات وتسجيل الأصوات ..، فاستحدث المشرع الجزائري هذه الإجراءات في قانون الإجراءات الجزائية بعد تعديله سنة 2006 وذلك في الفصل الأول من المادة 45 إلى الفصل الرابع من المادة 65 مكرر 05 عندما تقتضي ضرورات التحري و التحقيق في إحدى الجرائم المذكورة في المادتين، ومنه وبناء على ما سبق سوف ندرس في هذا الفصل إجراءات البحث و التحري المقررة في القانون رقم 09-04 (المبحث الأول)، تليها إجراءات البحث والتحري المقررة في قانون الإجراءات الجزائية الجزائري(المبحث الثاني).

المبحث الأول

إجراءات البحث و التحري المقررة في القانون رقم 09- 04

سبق و تحدثنا عن مدى التطور الذي لحق بثورة المعلومات والاتصالات و مآثرته من وسائل إلكترونية متقدمة و متعددة، الذي انعكس سلبا على حياة البشرية وذلك جراء الجرائم وليدة التطور التكنولوجي العالي والتي يصعب مواجهتها جنائيا، إذ أن ظاهرة الإجرام الإلكتروني قد أثارت بعض المشكلات فيما يتعلق بالقانون الجنائي الموضوعي، بحثا عن كيفية تطبيق نصوصه التقليدية على هذا النوع من الجرائم مع احترام مبدأ الشرعية والتفسير الضيق للنصوص الجزائية، إذ أن طبيعة هذه الجرائم يتطلب إعادة تقييم منهج الإجراءات التقليدية، خاصة أن الوسائل المستخدمة في ارتكاب الجرائم الإلكترونية تختلف عن الوسائل التقليدية مما يتطلب مواكبة الإجراءات للتطورات الحاصلة في المجال المعلوماتي، فمن أجل تسهيل التعامل مع الكمبيوتر وكافة الأجهزة الحديثة الأخرى مع مراعاة عدم المساس بحريات وحقوق الأفراد نظم المشرع كيفية استنباط الدليل عن طريق إجراءات ثابتة وصولا إلى الغاية المرجوة و المتمثلة في فك خيوط الجرائم، و لهذا سنعالج إجراء التفتيش و ضبط الدليل الإلكتروني (المطلب الأول)، ثم إجراء مراقبة الاتصالات الإلكترونية و حفظ المعطيات المتعلقة بحركة السير (المطلب الثاني).

المطلب الأول

إجرائي التفتيش الإلكتروني والمعاينة

تتمثل إجراءات التحري الكلاسيكية للكشف عن الجريمة الإلكترونية في جميع الإجراءات التي يمكن إيجادها في الجرائم التقليدية، التي نقصد بها إجراء التفتيش وضبط الأدلة، و هذه الإجراءات بحاجة إلى تطوير لكي تناسب مع طبيعة الجريمة الإلكترونية الخاصة و طبيعة الدليل الذي يصلح إثباته، لذا سوف نقوم بدراسة هذه الإجراءات التقليدية فتطرقنا أولا إلى بيان المقصود بالتفتيش في البيئة الإلكترونية (الفرع الأول)، ثم كيفية التفتيش الإلكتروني و السلطة المختصة بإجرائه (الفرع الثاني)، و منها سنتعرف على إجراء المعاينة في الجريمة الإلكترونية (الفرع الثالث).

الفرع الأول

مفهوم التفتيش في الجرائم الإلكترونية

أولاً: تعريف التفتيش الإلكتروني

لم يورد المشرع الجزائري تعريفاً خاصاً ودقيقاً للتفتيش بقدر ما اعتبره إجراء من إجراءات التحقيق وأحاطه بضوابط صارمة نظراً لأهميته في كشف الأدلة من جهة، وخطورته إذ يترتب عنه مساس بحرية حياة الأشخاص وكرامتهم من جهة أخرى، ومما يؤكد ذلك اهتمام الدستور الجزائري بهذه النقطة إذ نصت المادة 48 من دستور 2020 على أنه "تضمن الدولة عدم انتهاك حرمة المسكن .

لا تفتيش إلا بمقتضى قانون و في إطار احترامه.

لا تفتيش إلا بأمر مكتوب صادر من السلطة القضائية المختصة".

يمكن القول عن التفتيش على أنه إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة محل التحقيق و كل ما يفيد في كشف الحقيقة إذ يمس حق المتهم في سرية حياته الخاصة و يتمثل مجال هذه السرية إما في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه، وفقاً لقانون الإجراءات الجزائية الجزائري¹، ويعرف تفتيش نظام الحاسوب بأنه "البحث في مستودع سر المتهم على أشياء مادية أو معنوية تفيد في كشف الحقيقة ونسبها إليه"².

كما يعرف كونه إجراء من إجراءات التحقيق يهدف إلى الوصول إلى أدلة منبثقة من جنائية أو جنحة لإثبات ارتكابها ونسبتها إلى المتهم، بشرط أن يتحقق وقوعها فعلاً داخل نظم المعالجة الآلية للمعطيات فقد نصت المادة 05 الفقرة الأولى من القانون رقم 04/09 على أنه "يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات و في الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين المعلوماتية."

¹ - أمدر رجاء، خصوصية التحقيق في مواجهة الجرائم المعلوماتية، أطروحة مقدمة لنيل شهادة دكتوراه العلوم الثالث ل. م د ، تخصص القانون الخاص، قسم الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة محمد البشير الإبراهيمي، برج بوعريش، السنة الجامعية 2021/2020، ص 137.

² - نفس المرجع، ص 138.

فمن خلال التعريف يتبين لنا أن التفتيش ماهو إلا وسيلة للإثبات المادي لأنه إجراء يستهدف الوصول إلى أدلة مادية، كما أن عملية التفتيش تنصب على المكونات المادية والمعنوية لنظام الحاسوب بأوعيتها المختلفة، للبحث في أي شي يتصل بجريمة إلكترونية ما للكشف عنها، يدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها إلا أن هناك حالات خاصة للتفتيش في هذه المكونات سنتطرق إليها لاحقا.

ثانيا: الشروط المتبعة لإجراء التفتيش الإلكتروني

تتمثل هذه الشروط كالتالي:

أ- الشروط الموضوعية:

يقصد بالشروط الموضوعية للتفتيش بصفة عامة في الجرائم التقليدية و بصفة خاصة في الجرائم الماسة بالمعطيات الرقمية، الشروط اللازمة لإجراء التفتيش الصحيح ويمكن حصره في الشروط الأساسية التالية:

1- سبب التفتيش:

وقوع جريمة إلكترونية و المتمثلة في كونها سلوك غير مشروع الذي يكون للحاسب الآلي دور في فيه إما كوسيلة أو محل بهدف الاعتداء على النظم المعلوماتية وتخريبها كما يجب أن ترتكب من شخص أو أشخاص معينين لإحدى هذه الجرائم المعلوماتية أو الاشتراك فيها كما يجب أن يتوفر الشخص المطلوب دلائل كافية تؤدي إلى الاعتقاد بأنه قد ساهم في ارتكاب الجريمة المعلوماتية إما بصفته شريك أو فاعلا، ومن الأسباب الأساسية و المبررة للتفتيش هو الحصول على الدليل المادي يفيد جهات التحقيق من أجل الحصول على الحقيقة، ويتحقق بوقوع جريمة ما أو جنائية أو جنحة يتم بموجبها توجيه اتهام شخص المراد تفتيشه بناء على

أدلة أو براهين أو توفر قرائن قوية تفيد في كشف الحقيقة لدى المتهم أو في مسكنه وهو ماينطبق على الجريمة الإلكترونية الذي تطرقنا له و المتمثلين في النقاط التالية:

-وقوع جريمة إلكترونية تحمل وصف جنائية أو جنحة.

- توفر قرائن قوية على وجود بيانات أو معدات معلوماتية لدى المتهم بالجريمة الإلكترونية أو غيره.¹

¹-أمدور رجاء، مرجع سابق، ص139.

فيما يخص القرائن لم يشترط المشرع وجود قرائن قوية لذا بمجرد وجود اتهام موجه إلى المتهم يعد في ذاته قرينة أو أمارات على وجود أشياء في منزله تتعلق بالجريمة التي يجري التفتيش فيها، وهذا إذا كانت طبيعة الجريمة تسمح بذلك ولكن شرط أن يكون هذا الاتهام جديا حتى لا يكون تفتيش المسكن ذريعة لإلصاق التهمة بالمتهم.

لابد وأن يكون التفتيش بقصد ضبط تتعلق بالجريمة أو تفيد في كشف الحقيقة و هذه الغاية الأساسية منه، فالتفتيش باعتباره إجراء من إجراءات التحقيق يلزم أن يكون قد بوشر لغاية معينة وهي الكشف عن أشياء تتعلق بالجريمة و تفيد في إظهار الحقيقة.

فالهذا سبب التفتيش يمكن تلخيصه في ثلاث نقاط مهمة: وقوع الجريمة الإلكترونية، وجود قرينة تؤكد إلزامية التفتيش مع غاية لإجرائه.

2- محل التفتيش: يقصد به بشكل عام مستودع سر الإنسان، وهذا المستودع إما أن يكون في محل له حرمة خاصة كالمسكن أو قد يكون شخص أو رسائله وهذا بالنسبة للجرائم التقليدية، أما بالنسبة للجرائم الماسة بجرائم الماسة بأنظمة الاتصال و المعلوماتية فمحل التفتيش هو الحاسب الآلي الذي يعتبر النافذة التي تطل بها الانترنت على العالم.

يكون محل للتفتيش الأجهزة و الوسائل الإلكترونية التي تكون في مسكن له حرمة، وتتكون من الحواسيب والأجهزة، ونقصد هنا جهاز الحاسب الآلي بكل مكوناته أي المادية والمعنوية، فالحاسوب الآلي يتكون من مكونات مادية وهي مجموع الوحدات لكل منها وظيفة معينة وهي متصلة ببعضها في شكل نظام متكامل منها وحدات الإدخال ومهمتها استقبال البيانات المعلوماتية، ووحدة الذاكرة التي تقوم بتخزين البرامج و المعلومات وذاكرة القراءة و وحدة الحساب وهذا فيما يخص المكونات المادية، أما بالنسبة للمكونات المعنوية لجهاز الكمبيوتر والتي تسمى أيضا بالكيانات المنطقية و هي مجموعة البرامج و الوثائق المتعلقة بتشغيل وحدة معالجة البيانات، و مما سبق يمكن القول أن محل التفتيش عندما يكون على المكونات المادية للحاسوب لايشكل أي عائق بعكس مكوناته المادية وهذا الذي سوف نفصل فيه في الفرع الثاني لاحقا.¹

ب- الشروط الشكلية:

يجب احترام هذه الشروط من أجل ضمان صحة إجراءات التفتيش و هي ثلاث شروط ندرسها كتالي:

¹ - قادري عبد الفتاح الشبهاوي ، ضوابط التفتيش في التشريع المصري و المقارن، ط 2، منشأة المعارف، مصر ، ص111

1-إجراء التفتيش يكون بحضور أشخاص :

الحضور ضروري لبعض الأشخاص أثناء إجراء تفتيش نظم الحاسب الآلي، فتفتيش السكنات و المحلات التي يقوم بها رجال الضبطية القضائية أثناء مباشرة مهامهم و بإذن مسبق من السلطة القضائية يعتبر إجراء هام في عمليات التحري خاصة فيما يتعلق بمكافحة الجرائم الإلكترونية.

فالتفتيش إذا لا يقوم إلا بحضور المتهم أو ما يقوم مقامه أو ما ينوب عنه كونه شرط ضروري يفرضه القانون لصحة إجراء التفتيش أو شاهدين من غير المعنيين بالتحقيق²، على هذا الأساس حدد المشرع الجزائري نظاما خاص لعملية التفتيش في المادة 45 من ق.إ.ج.ج و لكن هذا عامة إذ ورد تعديل على أحكام المادة 45 بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 من قانون الإجراءات الجزائية الجزائري²، حيث أضيفت فقرة تتضمن استثناء الجرائم الماسة بأنظمة الآلية للمعطيات من الأحكام المنصوص عليها في المادة سابقة الذكر ما عدا ما تعلق منها بالسر المهني، بمعنى أن ضباط الشرطة القضائية بموجب هذا التعديل غير ملزمين بحضور المشتبه فيه و لا رضاه أثناء التفتيش، أو حضور من يمثله عند مباشرة التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، فاما نصت المادة 47 مكرر إذا كان الشخص الذي يتم تفتيش مسكنه موقوفا للنظر أو محبوسا في مكان آخر يمكن إجراء التفتيش بعد موافقة مسبقة من وكيل الجمهورية أو قاضي التحقيق و بحضور شاهدين مسخرين أو بحضور ممثل يعينه صاحب المسكن محل التفتيش.

وإذا خالف شروط المادتان 45 و 47 من قانون الإجراءات الجزائية يترتب عنه بطلان إجراء التفتيش.¹

2-وقت إجراء التفتيش:

يجب تحديد الميعاد الزمني أو الفترة الزمنية التي يتم فيها التفتيش و ذلك حماية لحرية الأفراد و حرمة مسكنهم، فنجد المشرع الجزائري حدد وقت التفتيش بين الخامسة صباحا و الثامنة ليلا و هذا حسب المادة 47 من قانون الإجراءات الجزائية الجزائري²، و لكن جاءت الفقرة الثالثة من نفس المادة للإجازة إجراء التفتيش و المعاينة و الحجز في كل محل سكني أو غير سكني و بأي ساعة من ساعات النهار أو الليل و هذا فيما يخص جرائم الاعتداء على نظم المعالجة للمعطيات بشرط أخذ إذن مسبق من وكيل الجمهورية المختص و يعتبر هذا خروجا عن القاعدة المنصوص عليها في الفقرة الأولى من المادة سالف الذكر و هذا راجع

¹- يحي بن إسماعيل، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراة العلوم في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة [أوبكر بلقايد تلمسان، الجزائر، 2022، ص209.

²- مرجع نفسه.

لطبيعة هذه الجرائم كون أدلة الإثبات فيها غير مرئية و سهلة الإتلاف¹، فنلاحظ هنا أن المشرع غلب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حريتهم الخاصة، خاصة في هذا الدليل الوحيد في الدعوى الجزائية، أما بالنسبة للأماكن العامة فإذا وجد الشخص في هذه الأماكن و هو يحمل معه ما هو تابع لمكونات الحاسوب أو الحاسوب أجمع أو كان مسيطر عليها أو حائز لها فإن التفتيش هنا يتم حسب القاعدة دون الاستثناء أي في الحالات التي يجوز فيها تفتيش الأشخاص و بنفس الضمانات والقيود².

3- تحرير محضر التفتيش:

باعتبار التفتيش من أعمال التحقيق لا بد من تحرير محضر يثبت فيه ما أسفر التفتيش عنه من أدلة، إذ أن القانون لم يتطلب شكلا خاصا في محضر التفتيش وبالتالي فإن لا يشترط لصحته سوى ما تستوجبه القواعد العامة في المحاضر عموما التي تقضي بأن يكون المحضر مكتوبا باللغة رسمية، فيشترط أن يكون في المحضر يحمل البيانات التالية:

أ- الكتابة: يشترط أن يكون المحضر مكتوبا .

ب- التاريخ: يجب أن يحمل المحضر تاريخ تحريره من طرف الشخص الذي حرره، فالتاريخ يفيد تحديد اليوم الذي أُنْخِذ فيه إجراء التفتيش و يفيد ذلك لحساب مدة التقادم بالنسبة للدعوى العمومية.

د- التوقيع: التوقيع على المحضر من طرف الشخص الذي حرره و يصبح بذلك ذو قيمة قانونية و إلا لا يكون مشروعا، كما يفيد التوقيع معرفة من قام بإجراء التفتيش و يهم هذا في تحديد الاختصاص و السلطة المخولة للقائم بالتفتيش و يتبع التفتيش بيان اسم و صفة القائم بتحرير المحضر.

ج- بيانات التفتيش: ينبغي أن يحتوي المحضر على كافة الإجراءات التي اتخذها القائم بالتفتيش، ومن ثم فكل إجراء لم يذكر في المحضر يفترض أنه لم يتم، و عليه يجب على القائم بالتفتيش وصف المكان وصفا دقيقا وكذا الأشياء التي عثر عليها في المكان المفتش أو الجهاز المفتش³.

¹ - براهيم جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه، تخصص قانون، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2018، ص 41-42.

² - ليندة بن طالب، " التفتيش في الجرائم المعلوماتية"، مجلة العلوم القانونية و السياسية، الجزائر، العدد 22، جوان 2017، ص 494.

³ - يحيى بن إسماعيل، مرجع سابق، ص 207.

الفرع الثاني

كيفية إجراء التفتيش الإلكتروني و السلطة المختصة به

سنطرق في هذا الفرع إلى الإجراءات المتبعة للإتمام التفتيش في الجريمة الإلكترونية (أولاً) وكذا السلطة المختصة بأداء التفتيش (ثانياً).

أولاً: كيفية إجراء التفتيش في الجريمة الإلكترونية

بحسب نص المادة 5 التي أحالتنا بخصوص الحالات التي نلجأ إلى التفتيش إلى المادة 04 من القانون 04-09 وهي التي تحدد حالات اللجوء إلى مراقبة الاتصالات الإلكترونية، فإن حالات اللجوء إلى تفتيش النظم المعلوماتية هي نفسها الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية للاتصالات، وهما حالتين المتعلقتين بالوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، وكذلك في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام والدفاع الوطني أو مؤسسات الدولة والاقتصاد الوطني، و بما أن نظم الحاسوب تتكون من مكونات مادية و أخرى معنوية كما أنه تربطه بغيره من الحواسيب شبكات اتصال بعدية فعلى التطرق إلى كيفية إجراء التفتيش الإلكترونية المتمثلة في:

أ- تفتيش المكونات المادية للحاسوب الآلي:

إن الولوج إلى المكونات المادية للحاسوب الآلي من أجل البحث عن أدلة مادية التي تكشف عن حقيقة الجريمة الإلكترونية و مرتكبها، تخضع الإجراءات التفتيش المألوفة لأن حكم التفتيش في هذه الكيانات المادية يتوقف أساساً على طبيعة المكان الموجود فيه، إذ أن لصفة المكان أهمية خاصة في مجال التفتيش، فإذا كانت خاصة كمسكن المتهم، و أحد ملحقاته كانت لها حكمة فلا يجوز تفتيشه إلا في الحالات التي يجوز فيها تفتيش مسكنه، مع الأخذ باعتبار إذا كانت مكونات الكمبيوتر المراد تفتيشه منعزلة عن جهاز الكمبيوتر آخر في مكان آخر كمسكن الغير، و إذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة كالحدائق العامة و الطرقات و أماكن عامة بالتخصيص مقاهي الانترنت فإجراء تفتيشها يكون وفقاً للأصول الخاصة لتلك الأماكن¹.

فحسب المادة 45 من قانون الإجراءات الجزائية الجزائري التي تنص على مايلي: "تتم عمليات التفتيش التي تجرى طبقاً المادة 44 من نفس القانون على الوجه الآتي :

¹ - براهيمى جمال، مرجع سابق، ص 16.

1- إذا وقع التفتيش في مسكن شخص يشتبه فيه أنه ساهم في ارتكاب جناية فإنه يجب أن يحصل التفتيش بحضوره، فإذا تعذر عليه الحضور وقت إجراء التفتيش فإن ضابط الشرطة القضائية ملزم بأن يكلفه بتعيين ممثل له و إذا أمتنع عن ذلك، و كان هاربا استدعى ضابط الشرطة القضائية لحضور تلك العملية شاهدين من غير الموظفين الخاضعين للسلطة.

2- إذا جرى التفتيش في مسكن شخص آخر يشبه بأنه يحوز أوراقا أو أشياء لها علاقة بالأفعال الإجرامية فإنه يتعين حضوره وقت إجراء التفتيش و إن تعذر ذلك اتبعا الإجراءات المنصوص عليها في لفقرة سابقا.

ولضابط الشرطة القضائية وحده مع الأشخاص السابق ذكرهم في الفقرة الأولى الحق في الإطلاع على الأوراق و المستندات قبل حجزها، غير أنه يجب التوضيح أن عند التفتيش أماكن يشغلها شخص ملزم قانونا بكتمان السر المهني يجب أن تتخذ مقدما جميع التدابير اللازمة لضمان احترام ذلك السر، فتغلق الأشياء و المستندات المحجوزة و يختم عليها، إذا أمكن ذلك، فإذا تعذر الكتابة عليها فإنها توضع في وعاء أو كيس يضع عليه ضابط الشرطة القضائية شريطا من الورق و يختم عليه بختمه¹.

استثناء على الأحكام المذكورة لا تطبق الأخيرة إذا تعلق الأمر بجرائم المخدرات و الجريمة المنظمة للحدود الوطنية و الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات و جرائم تبيض الأموال و الإرهاب و الجرائم المتعلقة بالتشريع الخاص بالصرف، باستثناء الأحكام المتعلقة بالحفاظ على السر المهني و كذا جرد الأشياء و حجز المستندات المذكورة أعلاه².

فبناء على ماسبق التطرق له يتضح لنا أن تفتيش المكونات المادية للحاسوب و ملحقاته من لوحة المفاتيح و الشاشة، و غيرها من الأشياء المادية المحسوسة لا يثير مشاكل إجرائية أمام سلطات الاستدلال لكون المادتين 44-45 السابقة الذكر جاءت واضحة و مبينة لكيفية تفتيش المكونات المادية للحاسوب.

ب- مدى صلاحية المكونات المعنوية للحاسوب لألي للتفتيش:

تعتبر المكونات المعنوية للحاسب مجموعة من البرامج و الأساليب و القواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات، و التي تعد من الوسائل الرئيسية في الكشف عن أكثر جرائم الاعتداء على النظم المعالجة الآلية للمعطيات لوجود برمجيات المسح للكشف عن الأبواب المفتوحة التي تشكل منطقة استفهام و دلالة كافية أيضا على ارتكاب

¹ - مرجع سابق، ص 18.

² - القانون 03/82، المؤرخ في 13 فبراير 1982، المتضمن لقانون الإجراءات الجزائية الجزائري، المعدل و المتمم، للأمر رقم 66-155 ج.ر.ج، العدد 07، الصادر بتاريخ 16 فبراير 1982.

الشخص لجريمة الدخول الغير المشروع لنظام المعالجة الآلية للمعطيات¹، و في هذه الحالة قد ثار الجدل حول مدى صلاحية المكونات المعنوية للأن تكون محلا للتفتيش باعتبار البيانات الإلكترونية تفتقر إلى مظهر ملموس و حول مدى صلاحيتها أن تكون محل للبحث عن الأدلة المعنوية لتقديمها للمحكمة المختصة كدليل إدانة لذا يثور الشك في ما إذا كان البحث عن الأدلة في الحاسوب نوعا من التفتيش باعتبارها ليس لها مظهر مادي، ولكن هذا لم يطول إذ المشرع الجزائري لم يبقى مكتوف الأيدي اتجاه المتغيرات التي تحدث في العالم التكنولوجيا الحديثة، بل قام بدوره باستخدام النصوص القانونية جديدة أجاز من خلالها تفتيش المكونات المنطقية والمعطيات المعلوماتية للحاسب فقد بين من خلال المادة 5 من القانون 04-09 السالف الذكر التي تنص على: "يجوز للسلطات القضائية وكذا ضباط الشرطة القضائية، في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش و لو عن بعد إلى:

أ- منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية المخزنة فيها.

ب- منظومة تخزين معلوماتية"².

ثانيا: السلطة المختصة بإشراف على عمليات التفتيش:

لكي يكون التفتيش في الجرائم الإلكترونية صحيحا و منتجا لأثاره، لابد أن يتم من طرف سلطات التحقيق الأصلية، باختلاف تشريعات الدول، و مع مراعاة الاختصاص المحلي الذي يتحدد إما بمكان وقوع الجريمة أو بمكان إقامة المتهم، أو مكان القبض عليه و هذا طبقا للمادة 16 من القانون الإجراءات الجزائية الجزائري³.

لصحة إجراء التفتيش الذي يقوم به رجال الضبطية يجب أن يكون بناء على إذن صريح صادر من هيئة مختصة، إذ أن التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمس حقوق و حريات الأفراد، هذا ما جعل المشرع يحرص على إسناد هذه المهمة لجهة قضائية تكفل تلك الحقوق، و تتمثل هذه الجهة في قاضي التحقيق أو النيابة العامة و بدورها تتناط مهمة الإشراف على هذه العملية للشرطة القضائية، و هذا بناء على إذن من وكيل الجمهورية أو قاضي التحقيق و مع مراعاة الضوابط القانونية التي تتمثل في الحصول على إذن مكتوب

¹ - عفيفي كمال، جرائم الكمبيوتر و حقوق المؤلف والمصنفات الفنية ودور الشرطة القضائية، دراسة مقارنة، ط 2، منشورات الحلبي القانونية، دمشق، 2007، ص 61.

² - مرجع نفسه، ص 62.

³ - الأمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق لـ 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، المعدل المتمم بالقانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، ج.ر.ج.ج، العدد 71، الصادر في 24 ديسمبر 2006.

بالتفتيش، و حضور صاحب الشيء المراد تفتيشه ، و التأكد من لتفتيش في لوقت المحدد قانوناً¹.

لقد جاءت المادة 05 من القانون 04-09 السالف الذكر صريحة موضحة لهذه النقطة بحيث أجازت للضبطية القضائية بإجراء تفتيش في إطار قانون الإجراءات الجزائية ، و ذلك في الحالات المنصوص عليها في المادة 04 من نفس القانون ، كما يمكن للسلطات المكلفة بالتفتيش بتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة و هذا لحماية المعطيات المعلوماتية التي تتضمنها و تزويدها بكل المعلومات الضرورية لإنجاز مهمتها.

الفرع الثالث

إجراء المعاينة

حتى تتمكن سلطات التحقيق من استخلاص الدليل الإلكتروني عن طريق الآثار التي أحدثها المجرم بمسرح الجريمة، على هذه الأخيرة التنقل إلى مسرح الجريمة من أجل معاينته و جمع الاستدلالات و الآثار، و تعتبر المعاينة من المراحل الأولى للاستدلال على ملابسات الجريمة، و من أهم إجراءات التحقيق، نظراً لما يمكن توفره من أدلة إثبات، و تزداد أهميتها أكثر إذ تعلق الأمر بالجرائم الإلكترونية، و ، سنتطرق لتعريف إجراء المعاينة و الضوابط التي تتم فيه (أولاً) وكيفية معاينة الجرائم الواقعة على المكونات المادية للحاسوب (ثانياً) والغير مادية (ثالثاً).

أولاً: تعريف المعاينة والضوابط التي تتم فيها إجراء المعاينة

أ-تعريف المعاينة: يقصد بالمعاينة رؤية العين لمكان أو شخص أو شيء للإثبات حالته وضبط كل ما يلزم لكشف الحقيقة ، أو هي إثبات لحالة الأماكن و الأشخاص وكل ما يفيد في كشف الحقيقة وهي تتطلب أن ينتقل ضابط الشرطة القضائية إلى عين المكان لمباشرتها للإثبات حالته و حالة ما قد يوجد فيه من أشخاص أو أشياء تفيد في إظهار الحقيقة للكشف عن الجريمة محل الإجراء.²

كما تعرف أيضا بأنها إجراء بمقتضاه ينتقل المحقق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلقة بالجريمة وكيفية وقوعها كذلك جمع الأشياء الأخرى التي تفيد في الكشف عن الحقيقة، واتخاذ ما يلزم من إجراءات كضبط بعض الأشياء فالهدف من المعاينة

¹ - عبد الصديق شيخ، "الوقاية من الجرائم في ظل القانون 09-04 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها"، مجلة المعالم للدراسات القانونية و السياسية، المدية، العدد 01/15/2020، ص ص 189-204.

² - مرجع نفسه، ص 193.

هو لجمع الأدلة الناتجة من الجريمة وكذا إتاحة الفرصة للمحقق لكي يشاهد بنفسه مكان وقوع الجريمة لكي تكون لديه فكرة واضحة وكشف الغموض عن كيفية وقوع الجريمة، وهي إجراء جائز في كافة الجرائم إلا أن أغلبية التشريعات بما فيها التشريع الجزائي في المادة 42 الفقرة الأولى من قانون الإجراءات الجزائية الجزائي، وضعها للجنايات والجناح الهامة، وإذا كانت في مكان عام ضابط الشرطة القضائية لا يحتاج إلى إذن من النيابة العامة لإجرائها، أما إذا كانت بمكان خاص فلا بد لصحتها رضا صاحب المكان، ووجود إذن مسبق من سلطة التحقيق بإجرائها.

وبما أن الجريمة الإلكترونية تعتمد على التقنية الحديثة فيجب إعداد فريق من الخبراء مختصين في مجال التقنية الحديثة وإخطاره مسبقاً حتى يستعيد من ناحية فنية والعملية ويعد خطة مناسبة للمعاينة مع مراعاة ما جاء في القوانين الجنائية حول المعاينة تحقيقاً لمبدأ الشرعية.¹

إن معاينة مسرح الجريمة الإلكترونية هو معاينة الآثار التي يتركها مستخدم الشبكة الإلكترونية أو الانترنت، وتشمل الوسائل المرسلة منه أو التي يستقبلها و كل الاتصالات التي تمت من خلال الحاسوب الآلي و الشبكة الإلكترونية، كما تثبت حالة المكان الذي وقعت فيه الجريمة بضبط لأشياء وحالة الأشخاص بالمشاهدة والوصف، سواء بالكتابة، والرسم التخطيطي أو بتصوير ومشاهدة آثار الجريمة على فاعلها، إن هذا الإجراء يهدف أيضاً ضمان عدم الشك في الدليل المستفيد منها، وذلك لأن انقضاء فترة ملا بين وقوع الجريمة وإجراء المعاينة يمكن أن يسمح بان يتمكن الجاني من إزالة العناصر المادية التي تفيد كشف الحقيقة، لكي تتم المعاينة بطريقة صحيحة يجب إتباع خطوات وبناء على ضوابط أساسية سنتعرف عليها تالياً.²

ب-ضوابط إتمام إجراء المعاينة:

تبدأ هذه العملية الإجرائية بنزول فريق متخصص مزود بكامل الإمكانيات اللازمة للسيطرة على جميع الأجهزة و الأشخاص العاملين عليها وحجزهم بعيداً عنها، مع ضبط الفلاشات و الأقراص الصلبة و الموبيليات الخاصة بهم...، و من ثم الاتصال بالمبلغين لكي يزود الفريق بكل المعلومات التي قد حصلوا عليها و يتم العمل وفقاً للإجراءات المبينة حتى تكون جاهزة لتقديمها للقضاء كأدلة إثبات دون أن يشوبها أي قصور بتنسيق مع النيابة والخبراء المتخصصين في هذا المجال،¹ وتتم هذه العملية بناء على النحو الآتي:

¹ طارق عبد الرحيم الردايدة، التفتيش الإلكتروني في الجرائم الرقمية، دراسة وصفية مقارنة، مذكرة ماجستير، ضمن تخصص امن نظم المعلومات والجرائم الرقمية، جامعة الأميرة سمية للتكنولوجيا، الأردن، 2017، ص 27.

² - مرجع نفسه، ص 28.

1- مسرح الجريمة التقليدي: ويقع خارج بيئة الحاسوب، ويتكون بشكل رئيسي من المكونات المادية المحسوسة للمكان الذي وقعت فيه الجريمة، وأقرب ما يكون إلى مسرح جريمة تقليدية، وقد يترك فيها الجاني آثار عدة كال بصمات و غيرها، وربما ترك متعلقات شخصية أو وسائل تخزين رقمية، ويتعامل أعضاء فريق التحقيق مع الأدلة الموجودة فيه كل بحسب اختصاصه وفي هذه الحالة ليست هناك صعوبة مادية لتقدير صلاحية مسرح الجريمة الذي يضم هذه المكونات للمعاينة من قبل عناصر الضبط القضائي، والتحفظ على الأشياء التي تعد أدلة مادية على ارتكاب الجريمة ونسبتها إلى شخص معين، وكذلك وضع الأختام في الأماكن التي تمت المعاينة فيها، وضبط كل ما استعمل في ارتكاب الجريمة والتحفظ عليها، مع إخطار النيابة العامة بذلك، والسبب في سهولة المعاينة في هذه الحالة أنها تتم على عناصر مادية ملموسة كانت محلا للجريمة، أو تخلفت عنها عكس المعاينة التي تتم عقب وقوع الجريمة بوسيلة مكونات غير مادية.¹

2- مسرح الجريمة الافتراضي: يقع داخل البيئة الإلكترونية، ويتكون من البيانات الرقمية التي تتواجد وتنتقل داخل بيئة الحاسوب وشبكة الانترنت، وفي ذكرته وفي الأقراص الصلبة الموجودة بداخله، والتعامل مع الأدلة الموجودة في هذا المسرح يجب ألا يتم إلا على يد خبير متخصص في التعامل مع الأدلة الرقمية من هذا النوع.

وفي هذه الجرائم تظهر صعوبات تحول دون فاعلية المعاينة أو فائدتها، ويمكن تلخيصها كالآتي:

-الصعوبة الأولى تتمثل في ندرة الآثار المادية التي تتخلف عن الجرائم التي تقع على الأدوات المعلوماتية بصفة عامة، وبرامج الحاسوب الآلي وبياناته بصفة خاصة .

-الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة خلال المدة الزمنية التي غالبا ما تكون طويلة نسبيا، ما بين وقوع الجريمة و الكشف عنها، الأمر الذي منح فرصة لحدوث تغير أو تلفيق أو عبث بالآثار المادية أو زوال بعضها، وهو ما يلقي ظلا من الشك على الدليل المستمد من المعاينة.

و بخلاف ذلك فمن الممكن أن تكون الآثار المعلوماتية أو الرقمية المستخلصة من أجهزة الحاسوب الآلي ثرية جدا فيما تحتويه من معلومات مثل صفحات المواقع المختلفة و البريد الإلكتروني و الفيديو الرقمي و الصوت الرقمي و غرف الدردشة المحادثة، و الملفات

¹ - نبيلة هبة هروال، الجوانب الإجرائية للجريمة المعلوماتية، د.ط ، دار الفكر الجامعي، الإسكندرية، د.س.ن، ص219، 220.

المخزنة في الحاسوب الآلي الشخصي، و الصورة المرئية، و الدخول للخدمة و الاتصال بالانترنت و الشبكة عن طريق مزود الخدمات.¹

و لذلك، فإنه يجب عند معاينة مسرح الجرائم التقنية للمعلومات مراعاة القواعد و الإرشادات الفنية الآتية:

- القيام بتصوير الحاسوب الآلي، و ما قد يتصل به من أجهزة طرفية و محتوياته و أوضاع المكان الذي يوجد به بصفة عامة، مع العناية بتصوير أجزائه الخلفية، و ملحقاته الأخرى على أن يراعي تسجيل تاريخ المكان الذي تم التقاط الصورة فيه و زمانه.

- ملاحظة طريقة إعداد نظام الحاسوب بعناية بالغة.

- إثبات الحالة التي تكون عليها كابلات الحاسوب و توصيلاته مكونات النظام، حتى يسهل عليه القيام بعملية المقارنة و التحليل لها عند عرض الموضوع على المحكمة المختصة.

- عدم التسرع في نقل أي مادة معلوماتية من مكان وقوع الجريمة قبل إجراء الاختبارات اللازمة، للتيقن من عدم وجود أية مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث أي إتلاف للبيانات المخزنة بسبب تدخل المجالات مغناطيسية مع بعضها البعض.

- حفظ ما تحويه سلة المهملات من الأوراق الملقاة أو الممزقة، وأوراق الكربون المستعملة والشرائط و الأقراص الممغنطة غير السليمة أو المحطمة و فحصها، و رفع البصمات التي قد تكون لها علاقة بالجريمة المرتكبة، لأن دليل الجريمة قد يكمن ضمن هذه القصاصات.

- حفظ المستندات الخاصة بالإدخال، و كذلك مخرجات الحاسوب الورقية التي قد تكون ذات صلة بالجريمة، و ذلك من أجل رفع البصمات التي قد تكون موجودة عليها و مضاهاتها، و يجب قصر عملية المعاينة على عناصر الضبط القضائي سواء أكانوا من الباحثين أم المحققين الذين تلقوا التدريب الكافي و الذين تتوفر فيهم الكفاءة العلمية و الخبرة الفنية في مجال الحسييات و استرجاع المعلومات، و مواجهة هذه النوعية من الجرائم، و التعامل مع أدلتها التي قد تتخلف عنها على مسرح الجريمة التقليدي².

ثانياً: معاينة الجرائم الواقعة على المكونات المادية للحاسوب

إن معاينة الجرائم الواقعة على المكونات المادية للحاسوب لا يثير أي صعوبة أو إشكال في إتمام هذا الإجراء بحيث تتم المعاينة بما يسمى بالمسرح التقليدي أي الشيء الملموس وهو ما يقع خارج بيئة الحاسوب و الانترنت، و يتكون من المكونات المادية المحسوسة

¹-نبيلة هبة هروال، مرجع سابق، ص 219.

²-مرجع نفسه، ص 220.

للمكان الذي وقعت فيه الجريمة و هو أقرب ما يكون إلى مسرح جريمة تقليدية يترك فيها الجاني آثار كالبصمات أو وسائل تخزين رقمية¹، فتتم المعاينة في جهاز الإعلام الآلي كشاشة العرض و مفتاح التشغيل و الأقراص و غيرها من مكونات الجهاز ذات الطابع المادي المحسوس، فهي كما قلنا لا تثير أي إشكال حيث يمكن لضباط الشرطة القضائية معيبتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة.

ثالثا: معاينة الجرائم الواقعة على المكونات الغير مادية للحاسوب

تعتبر الحواسيب مصدر غني بالأدلة الرقمية خاصة الحواسيب الشخصية التي يمكن اعتبارها أرشيف لسلوك الفرد ونشاطهم لذلك عملية فحص مضمون هذه الحواسيب تمثل نقطة البداية للكشف عن خفايا الجريمة الإلكترونية²، فنسعى في هذا البحث بالحاسوب بالمرحح الافتراضي، إذ يقع داخل البيئة الإلكترونية ويتكون من البيانات الرقمية التي تتواجد داخل الحاسوب في ذاكرة الأقراص الصلبة الموجودة بداخله³، والتعامل مع الأدلة الرقمية الموجودة في هذا المسرح يجب أن لا يتم إلا على يد خبير متخصص كون التعامل مع هذا النوع من الأدلة يثير صعوبات لهذا من الضروري إتمام هذا الإجراء من طرف محققين ذوي كفاءة علمية وخبرة فنية في مجال المعلوماتية وأن تتم وفقا مبدأ المشروعية⁴، ونجد المادة 49 من قانون الإجراءات الجزائية الجزائري تؤكد ذلك حيث تنص على: "إذا اقتضى الأمر إجراء معاينات لا يمكن تأخيرها فالضباط الشرطة القضائية أن يستعين بأشخاص مؤهلين لذلك وعلى هؤلاء أن يحلفوا اليمين كتابة على إبداء رأيهم بما يمليه الشرف والضمير".

المطلب الثاني

ضبط الدليل الإلكتروني و مراقبة الإتصالات الإلكترونية

يعتبر الضبط من إجراءات جمع الأدلة و هو النتيجة الطبيعية التي ينتهي إليها التفتيش و هو الهدف الرئيسي من التفتيش لذلك نجد أن التشريعات الإجرائية تجمع عادة بين أحكام الضبط و التفتيش في موضع واحد لكن ليس معنى ذلك أن الضبط هو التفتيش إذ قد يكون نتيجة معاينة و غيرها، و من بين الإجراءات الضرورية للكشف عن الجرائم المعلوماتية نجد مراقبة الإتصالات الإلكترونية، لذا تطرقنا في هذا المطلب لدراسة الأحكام

¹ - عمر محمد أبوبكر بن يونس، الجرائم الناشئة عن إستخدام الانترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين تمس، مصر، ص830.

² - مرجع نفسه، ص831.

³ - عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد السماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية، مداخلة تطبيقية، المؤتمر العربي الأول لعلوم الأدلة الجنائية و الطب الشرعي، جامعة نيف للعلوم الأمنية، الرياض، 2017، ص17.

⁴ - مرجع نفسه، ص18.

إجراء الضبط الإلكتروني (الفرع الأول)، ثم إجراء مراقبة الاتصالات الإلكترونية (الفرع الثاني):

الفرع الأول

إجراء ضبط الدليل الإلكتروني

ضبط الأشياء من إجراءات جمع الأدلة، بحيث أعطى المشرع أهمية لهذا الإجراء خاصة في هذا النوع من الجرائم، إذ اعتبره جائز سواء كان الشيء مملوك للمتهم أو لغيره من الأشخاص، لذا سنبين تعريف ضبط الدليل الإلكتروني (أولاً)، بعدها إجراءات ضبط الدليل الإلكتروني (ثانياً)، ثم أنواع الدليل الإلكتروني و الصعوبة التي تواجه المحقق في ضبطها (ثالثاً).

أولاً: تعريف ضبط الدليل الإلكتروني

يقصد بالضبط وضع اليد على شيء يتصل بجريمة وقعت، و يفيد في كشف الحقيقة عنها و عن مرتكبها، و هو من حيث الطبيعة القانونية قد يكون من إجراءات الاستدلال أو من إجراءات التحقيق¹، و تتحدد طبيعته بحسب الطريقة التي يتم بها وضع اليد على الشيء المضبوط، فإذا كان الشيء وقت ضبطه في حيازة شخص و اقتضى الأمر تجريده من حيازته كان الضبط بمثابة إجراء تحقيق أما إذا كان الاستيلاء عليه دون الاعتداء على حيازة قائمة فإنه يكون بمثابة إجراء استدلال².

وكما يمكن أيضاً تعريف الضبط بأنه العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والتحفظ على هذه الأدلة، والضبط هو الخاصية من التفتيش كما أشرنا سابقاً ونتيجة المباشرة المستهدفة، ولذلك يتعين عند إجراءه أن تتوفر فيه نفس القواعد التي تطبق بشأن التفتيش ويؤدي بطلان التفتيش إلى بطلان الضبط³.

كما يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز، السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، فقد جعلها قابلة للاستغلال للأغراض التحقيق شرط أن لا يؤدي ذلك إلى المساس بمحتوى المعطيات⁴، كما نجد أن

¹ - عبد الفتاح بيومي حجازي، المرجع السابق، ص 669.

² - عبد الله حسين علي محمود، سرقة معلومات المخزنة في الحاسب الآلي، دار النهضة العربية، مصر، 2001، ص 396.

³ - مرجع نفسه، ص 396-397.

مصطلح الضبط استبدل بمصطلح الحجز أي حجز الأدلة الرقمية في القانون رقم 04-09 السابق ذكر.

إن تحصيل الأدلة في الجرائم الإلكترونية قد يرتبط بعناصر مادية كالحاسوب و ملحقاته فكما قلنا سابقا في التفتيش عندما يكون التفتيش للمكونات المادية للحاسوب في هذه الحالة لا يطرح أية إشكال، فاف نفس الشيء بالنسبة لضبط هذه المكونات المادية لا يطرح أي إشكال قانوني أو عملي للإمكانية إخضاعها للإجراءات الضبط و التحرير التقليدية، الإشكال يطرح عندما يرتبط الدليل الإلكتروني بالمكونات المعنوية للحاسب ،كمختلف البرامج والبيانات المعالجة الآلية والمرسلات والاتصالات الإلكترونية التي يجري تبديلها عبر شبكة الإنترنت والبريد الإلكتروني ،فالطبيعة المجردة لهذه المكونات تخلق جدل حول مدى إمكانية ضبطها وفقا لقواعد الضبط المألوفة هذا ما دفع المشرع إلى وضع نص بهذا الخصوص لنزع الغموض.

ثانيا: إجراءات ضبط الدليل الإلكتروني

نص المشرع الجزائري على حجز المعطيات في المواد 6 إلى 9 من القانون 04-09 فوفقا للمادة 6 نجدها تنص على ما يلي: "عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبها و أنه ليس من الضروري حجز كل المنظومة ،يتم نسخ المعطيات محل البحث و كذا المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز و الوضع في أحرار و وفقا للقواعد المقررة في القانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش و الحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية .

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".

بعد استقراء المادة نجد أنا جاءت واضحة بالنسبة للإجراءات التي يجب أن تتبعها السلطة الخاصة للحصول على الدليل الإلكتروني، كما وضع المشرع طريقة أخرى للضبط الدليل وهي الحجز عن طريق منع الوصول إلى المعطيات ،فحسب المادة 07 من نفس القانون تنص على أنه: "إذا استحال إجراء الحجز وفقا لما هو منصوص عليه في المادة 06 أعلاه، للأسباب تقنية ،يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى

المعطيات التي تحتويها المنظومة المعلوماتية، أو إلى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة".

كما يمكن لضباط الشرطة القضائية حجز كل الأشياء و الوثائق التي استعملت في الجريمة و شكلت نتيجة لها ، عندما تكون هذه المضبوطات ضرورية لكشف الحقيقة، فالدعائم الرقمية (الإلكترونية) مثل الأقراص المضغوطة ، المفاتيح USB (flash disk)، الهواتف النقالة يمكن وضعها في أحزنا حسب قانون الإجراءات الجزائية الجزائي، كما يجب تنسيق إجراءات حجز و استغلال المعطيات المعلوماتية قصد جعلها مفهومة و قابلة للإدراك من طرف الأشخاص الذين ستطرح عليهم كدليل، كما أنه من الضروري توضيح أساليب جمع الأدلة الرقمية و الحفاظ على سلامتها كل ذلك مع وجوب حماية هذا الإجراء (ضبط الدليل) على الشبكة المعلوماتية كمثال: بروتوكولات نموذجية لجمع الأدلة الرقمية لتسمح بحماية الإجراءات و ذلك لتقليص خطر إبطالها إجرائيا.¹

ثالثا: أنواع الدليل الإلكتروني و الصعوبة التي تواجه المحقق في ضبطه

أ- أنواع الدليل الإلكتروني:

من بين الأشياء أو الأدلة التي تضبط و تحتفظ بها في الجرائم المتعلقة بالجريمة الإلكترونية و التي لها قيمة في إثبات تلك الجريمة و تنسبها إلى المتهم:

- **الورق:** على الرغم من أن الحاسوب قلل من استخدام أو حجم الأوراق والملفات التقليدية، حيث يتم حفظ المعلومات و الأغراض المراجعة أو التأكد من الشكل العام، للمستند أو الرسالة فهي تعتبر من الأدلة التي ينبغي الاهتمام بها.

- **ضبط جهاز الكمبيوتر و ملحقاته:** أي أن وجوده و ضبطه أمر مهم جدا للقول بان الجريمة الواقعة هي جريمة معلوماتية أو أنها مرتبطة بالمكان أو الشخص الحائز على الجهاز أو أجهزة الكمبيوتر أشكال و أنواع مختلفة الأمر الذي يتطلب على ضباط الشرطة القضائية المعرفة الكافية التي تأهله لتعامل معه و مواصفات بسرعة فائقة إما بنفسه أو بواسطة خبير.

- **البرمجيات (software):** إذا كان الدليل الرقمي ينشأ باستخدام برنامج خاص فإن ضبط الأقراص الخاصة بالتنصيب وتنصيب هذا البرنامج أمر في غاية الأهمية عند فحص الدليل.²

¹ - صالح تشنين، "إجراءات التحري و التحقيق في الجرائم الإعلام و الإتصال في التشريع الجزائري"، مجلة الدراسات القانونية"، العدد 01، جامعة عبد الرحمان ميرة، بجاية، 2014، ص 283.

² - عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكر مقدمة لنيل شهادة الماستر في الحقوق و العلوم السياسية، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق و العلوم السياسية قسم الحقوق، جامعة مولاي طاهر، سعيدة، الجزائر، سنة 2021-2022، ص 90.

- وسائل التخزين المتحركة: كالأقراص المدمجة "أقراص الليزر والأقراص المرئية والأشرطة المغناطيسية وغيرها...

-المودم(modem):وهي الوسيلة التي تمكن أجهزة الكمبيوتر من الاتصال ببعضها البعض عبر خطوط الانترنت.¹

- ضبط البريد الإلكتروني: عن طريق تحديد صندوق البريد الخاص بالمتهم محل التفتيش بعد معرفة اسم المستخدم و الرقم السري للدخول و فتح البريد الإلكتروني، إما عن طريق الورد أو الصادر أو الحافظ أو المهملات أو ضبط الرسائل الإلكترونية عن طريق تشغيل برامج البريد الإلكتروني في جهاز المتهم ومراجعة قائمة الرسائل الجديدة لينتقل الرسالة المطلوبة².

ب-الصعوبات التي تواجه المحقق في ضبط الدليل الإلكتروني:

إن عملية ضبط البيانات الإلكترونية تواجه عدة صعوبات للمحقق أهمها:

- ضخامة البيانات التي من الواجب فحصها والحرص على عدم المساس بالبيانات الشخصية.

- الضبط في المجال لمعلوماتية قد يمثل أحيانا اعتداء على حقوق الغير أو على حرمة حياتهم الخاصة مما يستوجب اتخاذ ضمانات لازمة لحماية هذه الحقوق .

-قد توجد هذه البيانات و المعطيات في شبكات وأجهزة تابعة لدولة أجنبية مما يستدعي تعاونها مع جهاز التحقيق الوطني.³

الفرع الثاني

مراقبة الاتصالات الإلكترونية

لقد أدرك المشرع الجزائري جيدا بأن المواجهة الفعالة للجرائم الإلكترونية لا تكون فقط بإرساء قواعد قانونية موضوعية ذات طبيعة ردعية،إنما لابد من مصاحبة هذه القواعد بقواعد أخرى إجرائية،حرصا منه على مواكبة التشريعات المقارنة فيما يتعلق بالإجراءات الجنائية في مجال المعلوماتية، ودعما لجهات التحقيق في مواجهة الجريمة الإلكترونية عمد المشرع الجزائري إلى مواصلة سن تلك النصوص القانونية التي تسهل إلى حد ما تقصي أثر المجرم الإلكتروني و جمع أكبر قد من الأدلة التي تقضي إلى كشف الحقيقة، و ممارسة

¹ - la preuve électronique , :www.internt juridique.net. consulté le 09. 052025

²-سعید سالم المزروعی و عزماني عبد الرحمان،"إجراءات التحقيق الجنائي في جرائم تقنيات المعلومات وفقا لتشريع الإماراتي"، "مجلة العلوم الاقتصادية و الإدارية القانونية،المجلة العربية للعلوم و نشر الأبحاث"،العدد13،المجلد الثاني،أكتوبر 2018،ص111-124.

³-مرجع نفسه، ص ص 113-117.

المشرع الجزائري من تدابير إجرائية مستحدثة ما تضمنه القانون 06-22 المعدل لقانون الإجراءات الجزائية الذي تناول إدراج أسلوب جديد للتحقيق هو المراقبة الإلكترونية وعليه سنتناول في هذا الفرع بيان تعريف مراقبة الاتصالات الإلكترونية (أولا)، ثم أحكام مراقبة الاتصالات الإلكترونية (ثانيا)، بعدها تطرقنا إلى توضيح إجراء حفظ المعطيات المتعلقة بحركة السير (ثالثا).

أولا: تعريف مراقبة الاتصالات الإلكترونية:

تعد مراقبة الاتصالات الإلكترونية إجراء أورده المشرع الجزائري بموجب المادة 56 من القانون رقم 01/06 المتعلق بالوقاية من الفساد ومكافحته المعدل و المتمم كأحد أساليب التحري الخاصة غير انه لم ينص على تعريفه وكذا تنظيمه، غير أن المشرع تدارك الوضع بموجب القانون رقم: 22/06 المعدل و المتمم لقانون الإجراءات الجزائية يستحدث الفصل الرابع كاملا بخصوص هذا الإجراء، فخصص له المواد من 65 مكرر 5 إلى 65 مكرر 10¹.

وكما جرت عليه العادة عرف الفقه إجراء المراقبة الاتصالات الإلكترونية على انه مراقبة شبكة الاتصالات، أو هو العمل الذي يقوم به المراقب باستخدام التقنية الإلكترونية لجمع معطيات و معلومات على المشتبه فيه سواء كان شخصا أو مكانا أو شيئا حسب طبيعته مرتبط بالزمن لتحقيق غرض امني أو لأي غرض آخر، في حين لم يتطرق المشرع الجزائري إلى تحديد المقصود بالمراقبة الإلكترونية، بل اكتفى بتعريف الاتصالات الإلكترونية فقط، كون المراقبة الإلكترونية تتمثل في مراقبة شبكة الاتصالات².

فالمراقبة الاتصالات الإلكترونية هي إذا إجراء يقوم به خبير في مجال المراقبة باستعمال تقنية المعلومات لمراقبة وتتبع كل ما يقوم به شخص مشتبه فيه من إرسال واستقبال لمكالمات أو تسجيلات صوتية أو كتابات أو صور و معلومات باستعمال وسيلة من وسائل تكنولوجيا و الاتصال في إحدى الجرائم المنصوص عليها في القانون، ومن ثم يمكن القول بأن المراقبة الإلكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها المراقب الإلكتروني والذي يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية وباستخدام برامج الكترونية³.

¹ - سارة معزوز، سلمه معزوز، "أساليب البحث و التحري الخاصة في جرائم الفساد"، "مجلة الباحث للدراسات الأكاديمية"، المجلد 9، العدد 3، جوان 2021، ص 49.

² - لينده بمحراث، إجراءات التحقيق الخاصة بالجرائم السيبرانية، يوم دراسي حول الجريمة السيبرانية، جامعة الأمير عبد القادر قسنطينة، يوم 20 أبريل 2022، ص 19.

³ - بنفس المرجع، ص 19.

هذا الإجراء تم استحدثه بموجب المادة 03 من القانون 04/09 السالف الذكر، أجاز تبعا لمستلزمات التحريات و التحقيقات القضائية الجارية في إطار هذا النوع من الجرائم اللجوء إلى وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها.

مما سبق من التعريفات التي ذكرناها نهتدي بأن المراقبة الإلكترونية هي إجراءات جمع الدليل الإلكتروني عن المشتبه فيه، ويقوم بها المراقب ذي كفاءة تقنية عالية في المجال الإلكتروني، ويستخدم في هذه المراقبة التقنية الإلكترونية عبر الشبكة الحاسوبية.

ثانيا: أحكام المراقبة الإتصالات الإلكترونية

مثل ماسبق وأشرنا بأن المشرع الجزائري سار على نهج التشريعات الأخرى التي سبقته وكرس الحق في الخصوصية، لذا وتفاديا للاعتداء على حرمة الحياة الخاصة في بعض الجرائم، نص في المادتين 3 و4 من القانون 04/09 السالف الذكر، على ضمانات قانونية فعالة لحماية الحرية الفردية، وحق الإنسان في سرية اتصالاته بمختلف أنواعها وتتمثل هذه الضمانات في :

أ- إباحة مراقبة الإتصالات الإلكترونية بنص القانون:

نصت المادة 3 من القانون 04/09 السالف الذكر، على إباحة مراقبة الإتصالات الإلكترونية كمايلي: "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في قانون الإجراءات الجزائية وفي هذا القانون، وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع و تسجيل محتواها في حينها و القيام بإجراءات التفتيش و الحجز داخل المنظومة المعلوماتية".¹

من خلال نص هذه المادة نجد أن المشرع عندما أشار أن إذا اقتضت ضرورة لحماية النظام العام أو مستلزمات التحري أو التحقيق أن تسري وفقا للقواعد العامة في قانون الإجراءات الجزائية وفي هذا القانون، أي يقصد من ذلك إتباع الشروط الواردة في نصوص المواد 65 مكرر 5 إلى مواد 65 مكرر 10، والتي تعتبر المراقبة سرية وتتم في إطار المراسلات السلوكية واللاسلكية، أما المراقبة الواردة في قانون 04/09 فهي مراقبة الاتصالات الإلكترونية.²

¹ - قانون رقم 04-09، السالف الذكر.

² - أسماء بوضياف، الحماية الجنائية للتجارة الإلكترونية، مذكرة لنيل شهادة ماستر، تخصص قانون الأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، الجزائر، 2020/2019، ص153.

و بالتالي فمراقبة الاتصالات الإلكترونية تكون في إطار الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، ولا تكون في باقي الجرائم الخطيرة الغير المحددة على سبيل الحصر، بل تكمن فقط بالنسبة لإجراء إعتراض المراسلات.

ب- الضرورة الملحة المرخصة لإجراء مراقبة الاتصالات الإلكترونية:

طبقا لنص المادة 4 يتبين أن لمقتضيات التحريات وللوقاية من وقوع بعض الجرائم هو السند الشرعي الذي يبرر المراقبة، ومن قبيل ذلك أن تتوفر معلومات عن إحتمال إعتداء على منظومة معلوماتية، تهدد النظام العام أو الدفاع أو مؤسسات أو الإقتصاد الوطني، أو حتى تمس بأمن الدولة ففي هذه الحالة لا بد من الترخيص بالمراقبة الإلكترونية.¹

ج- حصر القيام بإجراء مراقبة الاتصالات الإلكترونية في حالات معينة:

نصت المادة 4 الفقرة 1 من القانون 04/09 السالف الذكر، على الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية وهي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني.
- لمقتضيات التحريات و التحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الإلكترونية.
- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.

من خلال نص هذه المادة يتضح أن المشرع الجزائري أورد إجراء المراقبة الإلكترونية وقائيا من الجرائم التي تمس أمن وسلامة البلد، كجرائم الإرهاب أو التخريب، وكذا في حالة طلبات تنفيذ المساعدة القضائية، غير أن الحالة الثالثة من نفس المادة والتي تعني إمكانية اللجوء إلى إجراء المراقبة الإلكترونية في قضية مستعصية يصعب عليها الوصول إلى نتيجة، وهذا يؤدي إلى تعميم إستخدام هذه الآلية دون حد.²

د- لا يتم إجراء المراقبة الإلكترونية إلا بإذن السلطة القضائية المختصة:

طبقا لنص المادة 4 الفقرة 2 من القانون 04/09 السالف الذكر، والتي جاء فيها: "لا يجوز

¹ - أسماء بوضياف، مرجع نفسه، ص 153.

² - مرجع نفسه، ص 154.

إجراء عمليات المراقبة في الحالات المذكورة إلا بإذن مكتوب من السلطة القضائية المختصة.

وضحت المادة 41 من المرسوم الرئاسي 261/15 المؤرخ في 2015/10/08، كيف تحدد التشكيلة وتنظيمها وكيفية سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، وذلك يجعل القيام بإجراء مراقبة الاتصالات الإلكترونية كمهمة من المهام الموكلة إلى هذه الهيئة.¹

ثالثاً: حفظ المعطيات المتعلقة بحركة السير

يعد حفظ المعطيات المتعلقة بحركة السير من الإجراءات المستحدثة للبحث والتحري عن الجريمة الإلكترونية والتي جاء بها المشرع الجزائري في القانون رقم 04/09 السالف الذكر وفقد نص عليها في المادة 10 منه، ووضعه كالالتزام من التزامات مقدمي خدمة الانترنت، كما نص على هذا الإجراء كذلك ضمن المرسوم الرئاسي رقم 261/15، وهنا يظهر الحفظ كإجراء من إجراءات التحري.

أ- التعريف بمقدمي الخدمات:

عرف المشرع الجزائري مزودو الخدمات أو مقدمو الخدمة بموجب الفقرة "د" من نص المادة 2 من القانون 04/09 سالف الذكر، بأنه:

- أي كيان عام أو خاص يقدم لمستعملي خدماته ضمان القدرة على الاتصال بواسطة منظومة معلوماتية أو نظام للاتصالات.

- وأي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصالات المذكورة أو لمستعمليها".

ب- المقصود بحفظ المعطيات المتعلقة بحركة السير:

يمكن تحديد مقصود بحفظ المعطيات المتعلقة بحركة السير انه: "قيام مزود الخدمات بتجميع معطيات معلوماتية وحفظها وحيازتها في الأرشيف، وذلك بوضعها في ترتيب معين والاحتفاظ بها في المستقبل في انتظار إجراءات قانونية أخرى كالتفتيش وغيره".²

لكن تجدر الإشارة أن المشرع لم يحصرها في جميع المعطيات المعلوماتية وإنما حددها بمعطيات المرور أو كما سماها بحركة السير وقد عرفها بموجب الفقرة "هـ" بنص المادة 2

¹ - مرسوم رئاسي رقم 261/15، المؤرخ في 24 ذي الحجة عام 1436، الموافق لـ 08 أكتوبر سنة 2015، ج.ر.ج.ج، العدد 53، الصادرة في 2015/10/18.

² - رشيدة بوكري، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012 ص 448.

من نفس القانون" أي معطيات متعلقة بالاتصال عن طريق منظومة معلوماتية تنتجها هذه الأخيرة باعتبارها جزء في حلقة الاتصالات توضح مصدر الاتصال، والوجهة المرسل إليها، والطريق الذي يسلكه و وقت وتاريخ وحجم ومدة الاتصال ونوع الخدمة".¹

ويلاحظ في هذه الفقرة قد تضمنت مصطلحات غريبة نوعا ما عن القانون الجزائري، ومن ذلك "مصدر الاتصال" أي رقم هاتف مثلا، أو عنوان بروتوكول الانترنت أو بطريقة مماثلة تحديد هوية جهاز الاتصال الذي يقوم مزود الخدمة بتقديم خدماته من خلاله، "الوجهة المرسل إليها" ويشير إلى جهاز الاتصال الذي تتجه إليه الاتصالات المرسله، مصطلح "نوع الخدمة" ويشير إلى نوع الخدمة المستخدمة داخل شبكة (نقل الملف، بريد اليكتروني ...).²

يتبين أن المشرع الجزائري ألزم مقدمي الخدمات حفظ المعطيات بشكل يسمح بالتعرف على الأشخاص المساهمين في إنشاء المحتويات على الانترنت (المدونات، الإعلانات في مواقع البيع....) وذلك من أجل التبليغات المحتملة للسلطات القانونية أو في أي حالة طلب هذه الأخيرة لأجل التحريات أو المعاینات.

وبحسب القانون رقم 04/09 السالف الذكر ، فقد ألزم المشرع مزودي الخدمات بإزالة المعطيات التي يقومون بتخزينها وذلك بعد سنة واحدة ابتداء من تاريخ التسجيل، إلا انه بالنظر إلى نص المادة 10 الفقرة الأولى من قانون 04/09 السالف الذكر، نجد أن المشرع قد سمح بتسجيل المعطيات المتعلقة بمحتويات الاتصال ولكن بشرط أن يكون في حينه، وهو إجراء تسخير من طرف السلطات القانونية لمقدمي الخدمات المعنيين بجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات أيضا كانت (كالمكالمات الصوتية أو مكالمات الفيديو) وما يلاحظ هنا انه لم يحدد المدة ولا حتى السلطات المكلفة بتحريات تقوم بتسخير مقدمي الخدمات للقيام بهذا الإجراء الأخير، على عكس ما ذهب إليه المشرع الفرنسي.³

د- أصناف المعطيات الواجب حفظها:

لقد أوضح المشرع الجزائري أصناف المعطيات التي يجب على مقدمي الخدمات حفظها وذلك بموجب المادة 11 من نفس القانون رقم 04/09 السالف الذكر، حيث تنص على أن: "مع مراعاة طبيعة ونوعية الخدمات، يلتزم مقدم الخدمات :

أ- المعطيات التي تسمح بالتعرف على مستعمل الخدمة.

¹ - القانون 04/09، سالف الذكر.

² - رشيد بوكريء مرجع سابق ، ص 449.

³ - مرجع نفسه، ص 120.

- ب- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال .
- ج- الخصائص التقنية وكذا تاريخ ووقت ومدة كل اتصال.
- د- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها.
- هـ- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال و كذا عناوين المواقع المطلع عليها .
- بالنسبة لنشاطات الهاتف يقوم المتعامل بحفظ المعطيات المذكورة في هذه الفقرة من هذه المادة وكذا تلك التي تسمح بالتعرف على مصدر الاتصال وتحديد مكانه، تحدد مدة حفظ المعطيات المذكورة في هذه المادة بسنة واحدة من تاريخ التسجيل"

ج- جزاء الإخلال بحفظ المعطيات المتعلقة بحركة السير:

أوجب المشرع في نص المادة 10 في الفقرة 02 من القانون رقم 04-09 السالف الذكر على ما يلي: "و يتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين و كذا المعلومات المتصلة بها و ذلك تحت طائلة العقوبات المقررة للإفشاء أسرار التحري و التحقيق"¹، وفي حالة عدم التزامهم بحفظ هذه المعطيات فإن مسؤوليتهم الجزائية تقوم عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية.

تنص الفقرة 04 من المادة 11 من القانون 04-09 السالف الذكر على العقوبات المترتبة على الإخلال مقدمي الخدمات عن التزاماتهم و جاءت كالتالي: "دون الإخلال بالعقوبات الإدارية المترتبة على عدم احترام الالتزامات المنصوص عليها في هذه المادة، تقوم المسؤولية الجزائية للأشخاص الطبيعيين و المعنويين عندما يؤدي ذلك إلى عرقلة حسن سير التحريات القضائية،و يعاقب الشخص الطبيعي بالحبس من ستة(6) أشهر إلى خمس(5) سنوات و بغرامة من 50.000 دج إلى 500.000 دج .

يعاقب الشخص المعنوي بالغرامة وفقا للقواعد المقررة في قانون العقوبات"².

¹ - القانون 04-09، السالف الذكر.

² - القانون 04-09، السالف الذكر.

المبحث الثاني

إجراءات البحث و التحري المقررة في قانون الإجراءات الجزائية

إن تزايد الاعتماد على التقنيات الرقمية أفضى إلى عواقب وخيمة على الأفراد كما فتح المجال أمام المجرمين لارتكاب المزيد من الجرائم المصاحبة للتطور التكنولوجي والعملي، ولهذا عزز المشرع الجزائري من دور الضبطية القضائية وذلك بموجب تعديل قانون الإجراءات الجزائية في 2006، والذي فيه سطر صور متعددة للآليات التي تعمل على مكافحة الجرائم الخطيرة أو على الأقل التقليل من حدتها، ولهذا سوف نتعرض في هذا المبحث إلى إجراء التسرب الإلكتروني (المطلب الأول)، وإعترض المراسلات و تسجيل الأصوات والتقاط الصور (المطلب الثاني).

المطلب الأول

التسرب الإلكتروني

إن الانتقال من الجريمة التقليدية إلى إجرام نوعي يجعل عمل الشرطة القضائية في التحري وجمع الأدلة ضد مرتكبي الجرائم أصعب مما سبق، وهو ما فرض على المشرع استحداث أساليب تحر لها من الخصوصية ما يتناسب والوجه الجديد للإجرام، ومن بين هذه الإجراءات التسرب الإلكتروني، ويعد التسرب الإلكتروني أسلوب جديد مغاير عن التسرب في الجرائم العادية، فهو أسلوب يتناسب والبيئة الرقمية التي ينفذ فيها، ولذلك أستحدثه المشرع الجزائري للحد من الجرائم المستحدثة وتقديم يد العون للضبطية القضائية في تحرياتهما في الجرائم التي توصف بالخطيرة، لهذا سوف نتعرض في هذا المطلب إلى التعريف بالتسرب الإلكتروني (الفرع الأول)، ثم صور مساهمة المتسرب (الفرع الثاني)، وشروط التسرب الإلكتروني (الفرع الثالث).

الفرع الأول

تعريف التسرب الإلكتروني

الجرائم الإلكترونية أو المعلوماتية من بين الجرائم التي عدها المشرع الجزائري والتي يمكن فيها اللجوء لأسلوب التسرب الإلكتروني إذا دعت ضرورة التحقيق لذلك، والتسرب لغة مشتق من فعل تسرب أي دخل وانتقل خفية أو توغل¹، أما المشرع الجزائري فعرفه وفقا

¹ - تاجر كريمة، "التسرب الإلكتروني كآلية لمكافحة الجريمة الإلكترونية"، "المجلة النقدية للقانون والعلوم السياسية"، المجلد 19، العدد 02، كلية الحقوق و العلوم السياسية- جامعة تيزي وزو، 2024، ص 479.

للمادة 65 مكرر 12 من ق.ا.ج.ج على انه "قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه في ارتكابهم جنائية أو جنحة باتهامهم انه فاعل معهم أو شريك خاف"، حيث يعتبر التسلسل واحد من أهم أساليب البحث والتحري بل وأكثرها تعقيدا أو مجازفة لأنها تعتمد على مدى كفاءة وخبرة وفطنة وذكاء وحنكة الشخص المتسرب سواء كان ضابط أو احد أعوان الشرطة القضائية المقبل على العملية ويستخدم فيه مختلف الأساليب والأعياب والحيل من اجل كسب ود وثقة المشتبه فيهم وذلك في سبيل تحديد نوع ومدى العمل الإجرامي الممارس .

وأشار المشرع الجزائري إلى التسرب الإلكتروني كذلك في المادة 26 من قانون رقم 20/05، المتعلق بالوقاية من التمييز وخطاب الكراهية، التي تنص على التالي: "مع مراعاة أحكام قانون الإجراءات الجزائية، يمكن لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته لضابط الشرطة القضائية بالتسرب الإلكتروني إلى منظومة معلوماتية أو نظام للاتصالات الإلكترونية أو أكثر قصد مراقبة الأشخاص المشتبه في إرتكابهم لأي جريمة من الجرائم المنصوص عليها في هذا القانون، وذلك بإيهامهم أنه فاعل معهم أو شريك لهم..."¹

حيث يقوم ضابط أو عون الشرطة القضائية باختراق الجماعة الإجرامية تحت هوية مزيفة أو مستعارة بغية مراقبة الأشخاص و الاطلاع على مخططاتهم ما من شأنه أن يفيد التحقيق حول العصابة وأنشطتهم الإجرامية وكل ما له معلومة مفيدة حول ما يخص العصابة والتصرف في الوقت المناسب لكن دون أن يكون هذا التصرف تحريضا على ارتكاب الجريمة، فالتسرب من الناحية الأمنية هو تلك العملية المحضر لها والمنظمة قصد التوغل داخل وسط ما لمعرفة الحقيقة معرفة جيدة، من اجل الاستعلام عنه ومعرفة أدق التفاصيل فيه وخصوصية أسرارهِ حسب تطلعات الجهات الأمنية ويلاحظ مما سبق ذكره أن التسرب عملية معقدة ، تتطلب أن ينشأ المكلف بعملية التسرب اتصال بالأشخاص محل شبهة بالجريمة و إقامة علاقات معهم من اجل الوصول إلى الغاية المرجوة من العملية وعلى هذا فإن التسرب يركز على مبدئين:

أ-المبدأ العام: يستند على تقديم صورة على الوسط المراد التسرب فيه ويتوجب ذلك معرفة عموميات عن هذا الوسط مع توثيق هذه المعطيات .

¹ - قانون 05/20 ، مؤرخ في 18 أفريل 2020 ، يتعلق بالوقاية من التمييز وخطاب الكراهية، ج. ر. ج. ج، العدد 25، الصادر في 19 افريل 2020.

ب-المبدأ الخاص: يستند على تعميق التحري عن هذا الوسط ونشاطاته ومميزاته ووسائله وطبيعة الأشخاص المنتمين إليه، ليتم بعد ذلك دراسة الوظيفة العملية في هذا المجال بتوفير الوسائل البشرية والتقنية اللازمة.¹

وقد أطلق المشرع الجزائري على هذا الأسلوب مصطلح التسرب في قانون ا.ج.ج بينما أسماه "الاختراق" في المادة 56 من قانون قم 06-01 المتعلق بالوقاية من الفساد ومكافحته .

ويمكن تجسيد عملية التسرب في الجرائم الإلكترونية بإشراك ضابط أو عون الشرطة في محادثات غرف الدردشة أو حلقات النقاش حول "دعارة الأطفال"، أو يدور حول قيام احدهم باختراق شبكات أو بث فيروسات، فيتخذ المسرب أسماء مستعارة ويحاول الاستفادة حول كيفية اقتحام الهاكر لموقع ما حتى يتمكنوا من اكتشاف وضبط الجرائم .

الفرع الثاني

صور مساهمة المتسرب

وذلك حسب نص المادة 65 مكرر 12 من ق.إ.ج.ج لا يمكن أن يخرج العنصر المتسرب عن هذه الحالات الثلاثة وهي سواء كفاعل أساسي(1) أو كشريك في الفعل الإجرامي (2) أو خاف(3).

1-المتسرب كفاعل:

قدم المشرع تعريفا للفاعل في ق.ع. ج و ذلك حسب نص المادة 41 على أنه: "يعتبر فاعلا كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على ارتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي"، وعليه و استنادا لنص المادة 65 مكرر 12 سالفة الذكر من ق.إ.ج.ج. فإن العنصر المتسرب الذي يتولى مهمة القيام بعملية التسرب بإمكانه عن طريق التمويه ان يأخذ صورة فاعل أساسي في الجريمة، ولكن بشرط أن يقوم بالأفعال المنصوص عليها في المادة 65 مكرر 14 من ق.إ.ج.ج فقط دون أن تنجر وراء ذلك مسؤولية جزائية.²

فيمكن للعون المتسرب أن يرتكب أفعالا مادية تدخل في تشكيل الجريمة المتوغل فيها، ويوحي بها أنه يمثل مركزا مباشرا في تنفيذ العمل الإجرامي دون أن تشكل هذه

¹ - فاطمة الزهرة سماعيل، رمزية أمال صالح بلخوجة، نظام التسرب في قانون الإجراءات الجزائية، مذكرة لنيل شهادة الماستر، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2016/2015، ص05.

² - بوسقيعة أحسن، الوجيز في القانون الجزائي العام، ط 05، دار هومة للطباعة و النشر والتوزيع، الجزائر، ص152.

الأفعال تحريضا، لأنه لا يجوز قانونا للعون المتسرب بأي حال من الأحوال أن يكون فاعلا معنويا أي محرضا.¹

2- المتسرب كشريك:

وهي الصورة الثانية من صور التي يتخذها المتسرب، و طبقا لهذه الصورة فإن المتسرب يعتبر مساهما مساهمة مباشرة كونه شريك في ارتكاب الجريمة ، والمشرع الجزائري قدم تعريفا للشريك في نص المادة 42 من ق.إ.ج.ج على أنه: " يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا ولكنه ساعد بكل الطرق أو عاون الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك"، أي أن الشريك حتى ولو لم يشترك فالجريمة اشتراكا مباشرا إلا أنه يمكن تقوم في حقه المتابعة الجزائية إذا سهل و قدم يد المساعدة للمجرمين على القيام بأفعالهم الإجرامية . بأي شكل من أشكال المساعدة.²

3- المتسرب كخاف:

تعني كلمة خاف لغة: ما لا يرى وتعني كذلك إخفاء أي كتم و خبا، وهي الصورة الثالثة التي يتخذها المتسرب و ذلك بإيهام مرتكبي الجرائم بأنه واحد منهم وذلك من خلال إخفاء للأشياء التي تتم عملية اختلاسها أو تبديدها فيها وقد تم تحصيلها من خلال ارتكاب هذه الجرائم سواء كلياً أو جزئياً، وكما سبق وأن قدم المشرع الجزائري تعريفا لكل من الفاعل والشريك قدم كذلك تعريفا للخاف و ذلك في نص المادة 387 من ق.ع على أنه: "كل من أخفى عمدا أشياء مختلسة أو مبددة أو متحصلة من جنابة أو جنحة في مجموعها أو في جزء منها..." ، ومن هذا النص فإن جريمة الإخفاء تقوم عنصرين أساسيا هما:

- العلم باهته الأشياء بأنها مختلسة أو مبددة أو متحصلة من جنابة أو جنحة .
- حيازة أو إخفاء هاتيه الأشياء عمدا، لكن بالرجوع إلى نص المادة 65 مكرر 12 ق.إ.ج.ج يمكن للمتسرب أن يقوم بهذا الفعل دون أن تكون هناك متابعة جزائية.³

الفرع الثالث

الشروط التي تحكم عملية التسرب في الجرائم الإلكترونية

إن كون إجراء التسرب من أخطر أساليب البحث والتحري انتهاكا لحرمة الحياة الخاصة للأشخاص المشتبه فيهم من جهة وعلى خطورته للقائم بها من جهة أخرى ، و نظراً لأهميته

¹ - مرجع نفسه، ص153.

² - عبد الله أوهايبية، شرح قانون العقوبات(القسم العام)، د ط ، دار هومة، الجزائر، 2003، ص152.

³ - لدغم شيكوش زكرياء، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ، ورقلة، 2013/2012، ص83.

والأهداف المراد تحقيقها من جرائمها لفك شفرة الجرائم وفك خيوط شبكة العصابات أو الجماعات الإجرامية، ومن أجل إنجاز العملية وسيرها في ظروف سهلة تضمن أمن المتسرب وللوصول إلى الأهداف المسطرة دون التسبب في أية أضرار أو خسائر، لأن هاتيه العملية تتسم بالخطورة والمجازفة خاصة بالنسبة للشخص المتسرب وبالتالي تعريض حياته للخطر خاصة إذا ما أكتشف أمره، ولتجنب كل هذا أحاط المشرع الجزائري عملية التسرب بمجموعة من الشروط الشكلية (1) والموضوعية (2).

أولاً: الشروط الشكلية

نظراً لطبيعة عملية التسرب كإجراء منع المشرع اللجوء إليه في الحالات العادية، و بالنظر لما تتطلبه هذه العملية من حيطة وحذر وسرية نتيجة الخطورة البالغة على حياة المتسرب، لذا و حرصاً على حسن سير العملية في أحسن الظروف وضع المشرع الجزائري شروط شكلية استوجب العمل بها و يمكن إجمالها في:

أ- تقرير القيام بعملية التسرب:

يتعين على الفرد المكلف بتنسيق عملية التسرب، أن يحرر تقريراً يتضمن العناصر الضرورية لمعينة الجريمة محل التسرب، وكل المعلومات اللازمة لتنفيذ العملية، وقبل مباشرة عملية التسرب يقوم ضابط الشرطة القضائية بكتابة تقرير إلى وكيل الجمهورية وهذا حسب نص المادة 65 مكرر 13 من ق.إ.ج.ج الذي نص صراحة على أن ضابط الشرطة القضائية المكلف بتنسيق عملية التسرب هو المسؤول عن تحرير التقرير، ويجب أن يتضمن تقرير عملية التسرب ما يلي:

1- طبيعة الجريمة:

لا يتم اللجوء إلى التسرب إلا بصدد جريمة من الجرائم الخطيرة التي حددها المشرع والمذكورة في المادة 65 مكرر 05 الفقرة 02 من ق.إ.ج.ج، نصت على أن: إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو في التحقيق الابتدائي في جرائم المخدرات أو في الجرائم المنظمة العابرة للحدود الوطنية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أو الإرهاب، جرائم المتعلقة بالتشريع الخاص بالصرف وكذا الفساد..."

وانطلاقاً من المواد المنظمة لعملية التسرب التي جاء بها المشرع الجزائري، نستخلص إن التسرب لا يكون في جميع الجرائم و إنما في الجرائم التي جاءت على سبيل الحصر والتي توصف بالخطيرة و التي يكون التسرب فيها هو السبيل الوحيد للبحث و التحري فيها

وفك خيوطها، كما إن الطبيعة الخطرة لهذه الجرائم و الإجراءات على حد سواء يتطلب من العون المتسرب التحضير جيدا للعملية و التخطيط المسبق لها و الذي يتلاءم معها.¹

2- طبيعة عملية التسرب:

و ضرورة ذكر دواعي وأسباب اللجوء إلى إجراء التسرب، مع استعراض الخطوات أو النقاط التي سيتم إتباعها مع تحديد الفائدة المرجوة من هذا الإجراء في جمع المعلومات عن الجريمة والمجرمين، وذلك من أجل إقناع وكيل الجمهورية لمنح الإذن لهذا الإجراء، والذي يكون سببه هو البحث والتحري في الجرائم الخطيرة المذكورة على سبيل الحصر.²

3- تحديد عناصر الجريمة:

وذلك بأن يتم ذكر وتحديد جميع المعلومات المتعلقة بالجريمة و المجرمين وهي: ذكر هوية الأشخاص المشتبه فيهم مع ذكر أسمائهم الكاملة و كل ما يتعلق بهويتهم وأماكن إقامتهم والأماكن التي يرتادونها ، وتحديد المركبات المستعملة وأماكن التخزين.³

4- هوية ضابط الشرطة القضائية:

على الضابط الذي يحرر التقرير و المسؤول عنه أن يقوم بكتابة إسمه ولقبه و كافة المعلومات المتعلقة بهويته من صفته و رتبته و المصلحة التابع لها.

5- المدة الزمنية لعملية التسرب:

إن المشرع الجزائري أجاز لوكيل الجمهورية أو قاضي التحقيق الذي يمنح إذن مباشرة عملية التسرب أن يحدد المدة التي يراها تناسب نجاح العملية ، ولكن شرط أن لا تتجاوز مدة أربعة أشهر، ولكنه أعطى في المقابل صلاحية إعادة تمديد لأربعة أشهر أخرى إذا دعت ضرورة البحث والتحري ذلك ، كما يمكن تمديد مدة التسرب لمدة أربعة أشهر أخرى كأقصى حد للعملية، كما أجاز لوكيل الجمهورية أو قاضي التحقيق المشرف على العملية الذي رخص بالعملية أن يوقف العملية في أي وقت قبل انقضاء الإذن بالتسرب حسب ما تقتضيه مجريات العملية.⁴

¹-المرجع السابق، ص281.

²- فوزي عمارة، "اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و التسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية، العدد 33 ، جامعة منتوري قسنطينة ، جوان 2010، ص248.

³- مرجع نفسه، ص 250.

⁴لوجاني نورالدين، أساليب التحري و إجراءاتها وفقا لقانون 06-22 المؤرخ في 20 ديسمبر 2006، مداخلة أُلقيت في إطار يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، البزي ، 12 ديسمبر 2007، صص17، 16.

ب - الإذن :

إن الأصل في العمل الإجرائي هو الكتابة فلا يجوز للجهة القضائية المخولة و المشرفة على عملية التسرب أن تصدر الإذن شفاهيا ، وإنما يجب أن يكون محرراً وإلا كانت العملية تحت طائلة البطلان ، والإذن هو عبارة عن وثيقة رسمية أو ترخيص صادر عن وكيل الجمهورية أو قاضي التحقيق، هذا حسب ما تنص عليه المادة 5 مكرر 5 ق.إ.ج.ج ، كما يجب أن يحتوي الإذن على الجريمة التي تبرر وتسبب اللجوء إليه ، وكذا المدة الزمنية اللازمة للقيام بهذه العملية التي حددها المشرع الجزائي بأربعة أشهر قابلة للتمديد ، كما أن بإمكان الجهة القضائية المصدرة للإذن إيقاف العملية قبل انقضاء المدة المحددة له ¹.

لا يجوز و يعد مخالفاً للقانون كل ضابط أو عون شرطة قضائية يخوض عملية التسرب من تلقاء نفسه ودون الحصول على إذن مسبق من طرف السادة وكيل الجمهورية أو قاضي التحقيق حسب أحكام المادة 5 مكرر 11 ق.إ.ج.ج ، بل تتم العملية تحت المراقبة المباشرة للجهة المصدرة للإذن.

- **مكتوبا:** نعني بالكتابة صياغة الإذن و طباعته في شكل محرر، أي أن يكون مون و يحمل كافة الرسميات الخاصة بالجهة القضائية من رقم و تاريخ و توقيع و موضوع الإذن ...الخ.

- **التسبيب:** يجب على وكيل الجمهورية أو قاضي التحقيق ذكر السبب وراء منح الإذن، ويتعلق الأمر غالبا بالحاجة إلى التعمق في البحث والتحري في الجرائم المذكورة في المادة 65 مكرر 5 من ق إ ج ح.

ولقد أورد المشرع مجموعة من البيانات تذكر في الإذن وهي:

- الجريمة التي تبرر اللجوء إلى هذا الأسلوب.
- ذكر اسم الضابط المشرف على عملية التسرب وهويته الكاملة الذي تتم العملية تحت مسؤوليته (إسمه و لقبه، صفته، رتبته، المصلحة التي يتبعها).
- مدة عملية التسرب المرخص بها و التي تحدد بالأرقام و الأحرف.
- يجب أن يرفق الإذن بالملف القضائي المنجز ².

ثانيا: الشروط الموضوعية

كما هو معلوم أن عملية التسرب هي إجراء من إجراءات البحث و التحري المؤقتة و الخفية والتي لا تكون في جميع الجرائم بل في الجرائم التي جاءت على سبيل التحديد في المادة 65

¹-مرجع نفسه، ص 18.

²- شيخ ناجية، "إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة"، "مجلة معارف"، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، 2018، ص11.

مكرر 5 من ق.إ. ج. ج ، وتنحصر الشروط الموضوعية لعملية التسرب وفق الأحكام التي نظمها المشرع الجزائري فيما يلي :

1- دوافع اللجوء إلى عملية التسرب: نظرا لخطورة عملية التسرب وحساسيتها فإنه لا يتم التطرق إلى إجراء التسرب بمجرد وقوع إحدى الجرائم المحددة حصرا في القانون لتبرير العملية، بل يجب فضلا عن ذلك ان تكون هناك فائدة حقيقية ترجى من ورائها في كشف الحقيقة، فالعلة في ذلك أن هذه العملية إجراء استثنائي تمليه ضرورة كشف غموض الجريمة والعمل على ضبط الحياة.¹

وهو ما أكدته المشرع عندما استعمل في المادة 65 مكرر 11 عبارة: " عندما تقتضي ضرورات التحري أو التحقيق"، ليعترك لكل من وكيل الجمهورية وقاضي التحقيق السلطة التقديرية الكاملة في تقييم وتقدير مدى ضرورة اللجوء إلى إجراء التسرب، ولا سيما أن التسرب قد أجاز لعله ولأغراض خاصة وبصفة استثنائية، فتخلف تلك العلة يمنع قاضي التحقيق أو وكيل الجمهورية وبحسب الحالة في منح الإذن به وإلا عد متعسفا.²

2- سرية عملية التسرب:

لقد أمن قانون الإجراءات الجزائية الجزائري العنصر المتسرب وحفه بحماية خاصة و ذلك من أجل الحفاظ على روحه و سلامته وأمنه، حيث تعتبر السرية العامل الأساسي والرئيسي وضرورة الضروريات لنجاح العملية، بحيث يجب على المكلف بالتسرب أن يحيطها بالسرية التامة، من خلال منع كشف هويته الحقيقية عند أخذه هوية مستعارة تنفيذاً لعملية التسرب ، وذلك في أية مرحلة من مراحل الإجراءات، وتتأكد الرغبة الحقيقة والشديدة للمشرع في إحاطة العملية بالسرية التامة من خلال المادة 65 مكرر 16 من ق.إ. ج. ج التي نصت على جزاءات صارمة في حالة الكشف عن هوية ضابط أو أعوان الشرطة القضائية، والتي شددت هذه الجزاءات من حبس لمدة خمس سنوات إلى عشرة سنوات عند الاعتداء على أزواجهم وأبنائهم وأصولهم، وفي حالة تسبب الكشف في وفاة أحد هؤلاء الأشخاص، تكون عقوبة الحبس من عشرة إلى عشرين سنة، ناهيك عن الغرامات المالية الباهظة التي تصل إلى مليون دينار جزائري (1000000 دج).³

وبهذا منح المشرع المتسرب حق المحافظة على سرية هويته فلا يتم سماع أقواله أثناء الشهادة، ويحل ضابط الشرطة القضائية المكلف بالعملية محله بصفته شاهد على

¹ - آيت مولود سامية، "الضمانات المقررة لمشروعية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور في الجرائم الاقتصادية"، "المجلة النقدية للقانون والعلوم الإنسانية"، العدد 02، كلية الحقوق، جامعة مولود معمري تيزي وزو، 2015، ص320.

² - شيخ ناجية، "إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة"، "مجلة معارف"، العدد 25، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، 2018، ص10.

³ - مرجع نفسه، ص11.

العملية، وعدم جواز سماع المتسرب شخصياً كشاهد على العملية هذا من باب الحماية غير مباشرة للمتسرب، وتتمثل صورة السرية في استعمال هوية مستعارة، وعدم إيداع رخصة الإذن بالعملية في ملف الإجراءات.¹

3-نوع الجريمة:

المشرع الجزائري حصر عملية التسرب فقط على الجرائم الخطيرة و التي عددها في المادة 65 مكرر 5 و التي لا يجب أن تخرج عن نطاق الجرائم المذكورة في ذات المادة²، و التي نجد فيها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات على وجه الخصوص.

واللجوء إلى عملية التسرب لا يجوز قانوناً إلا إذا دعت إليه الضرورة وفي الجرائم التي الواردة على سبيل الحصر في نص المادة 65 مكرر 5 من ق.إ.ج.ج ولا يتم تنفيذها إلا بصدور إذن من الجهات المختصة المتمثلة في وكيل الجمهورية أو قاضي التحقيق.³

المطلب الثاني

إعتراض المراسلات و تسجيل الأصوات و التقاط الصور

أضحت الأساليب التقليدية في البحث والتحري عديمة الجدوى بسبب استغلال منفذي الإجرام التقنيات العلمية الحديثة في تنفيذ أغراضهم الإجرامية، مما دفع للإستعانة بالإجراءات الحديثة التي تبناها المشرع الجزائري بغيت البحث والتحري عن مرتكبيها، ومن هذه الإجراءات اعتراض المراسلات، وتسجيل الأصوات، والتقاط الصور، وهي وسائل أخذ بها المشرع الجزائري وأخضعها لمجموعة من الضوابط والشروط للموازنة بين متطلبات التحقيق وعدم التعدي على حرمة الحياة الخاصة للأفراد، ولذلك سنخرج في هذا المطلب على إعتراض المراسلات (الفرع الأول) و من ثم تسجيل الأصوات (الفرع الثاني) لتليها التقاط الصور (الفرع الثالث) وأخيرا الإجراءات الخاصة بها (الفرع الرابع).

الفرع الأول

إعتراض المراسلات

أولاً- تعريف اعتراض المراسلات: الاعتراض أو الاستيلاء بغتة لقد، اغفل المشرع الجزائري في ق.إ.ج تعريف اعتراض المراسلات، لأن وضع التعريفات ليس عمل المشرع

¹ - نورة هارون ، "الحماية القانونية للعون المتسرب: آلية فعالة في إنجاح عملية التسرب و مكافحة الجريمة"، "مجلة الدراسات القانونية المقارنة"، الجلد 07، العدد 01، كلية الحقوق والعلوم السياسية ، جامعة عبد الرحمن ميرة ، بجاية ، 2021، ص1978-1981.

² - المادة 65 مكرر 05 من ق.إ.ج.ج.

³ - شيخ ناجية، مرجع سابق، ص11،12.

و إنما هو من اختصاص الفقه، اعتراض المراسلات أو كما يدعوها البعض بالتصنت اكتفى المشرع الجزائري بتحديد إجراءات العملية المعمول بها من خلال نص المادة 65 مكرر 05 من ق.ج.ج حيث نجد أن المشرع الجزائري يقصد باعتراض المراسلات التعرض أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه المراسلات عبارة عن بيانات قابلة للإنتاج والتوزيع، التخزين، الاستقبال والعرض، وقد افرد لها مواد قانونية خاصة في إطار القانون 04/09 لمراقبة الاتصالات الإلكترونية مما لا يدعو للشك أن المراسلات المقصودة هنا هي المتعلقة بالهاتف الثابت والنقال ولكن بعد رقمنة كل وسائل الاتصال والإعلام يصعب التفرقة بين ما هو رقمي وما هو غير ذلك، وعلى هذا الأساس جمع المشرع كل الاتصالات في خندق واحد بموجب المادة 05 من المرسوم رقم 261/15 السالف الذكر.¹

كما عرف المشرع الجزائري المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية على أنها كل ترسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة عن طريق الأسلاك أو البصريات أو اللاسلكي الكهربائي أو أجهزة أخرى مغناطيسية.²

و بالرجوع إلى الفقه يمكن تعريف اعتراض المراسلات بأنه إجراء تحقيقي يباشر خلصة و ينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل غير مادي للجريمة، ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة التي تستخدمها الضبطية القضائية في مواجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية.³

وبناء على ما سبق ذكره إن اعتراض المراسلات هي: إجراء مراقبة الاتصالات الإلكترونية أثناء بثها، وليس الحصول على اتصالات الكترونية مخزنة، كما أنها سماع وتسجيل المحادثات الخاصة والشخصية التي تتم عن طريق المواصلات السلكية للهاتف الثابت والتيليغراف، واللاسلكية كالهاتف النقال و الانترنت و البريد الإلكتروني وغيرها من الوسائل التقنية الحديثة، وتتم هذه العملية بواسطة أجهزة تقنية ودون رضاهم وبناءا على إذن السلطة القضائية المختصة⁴، أو أنها إجراء تحقيقي يباشر خلصة و ينتهك سرية الأحاديث الخاصة، تأمر به السلطة القضائية في الشكل المحدد قانونا بهدف الحصول على دليل للجريمة،

¹ - دلال مولاي ملياني، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق و العلوم السياسية، جامعة أوبكر بلقايد، تلمسان، 2013/2014، ص 179.

² - القانون 2000/03 المؤرخ في جمادى الأولى عام 1421 الموافق لـ 5 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد و المواصلات السلكية

واللاسلكية، ج.ج.ج، العدد 48، الصادر في 2000.

³ - مرجع نفسه، ص 180.

⁴ - سارة عزوز، سلمة عزوز، مرجع سابق، ص 50.

ويتضمن من ناحية أخرى استراق السمع إلى الأحاديث، وهي تعتبر أيضا وسيلة هامة من الوسائل الحديثة للبحث والتحري تستخدمها الضبطية القضائية في مواجهة الإجرام الخطير وتتم عبر وسائل الاتصال السلكية واللاسلكية.¹

ثانيا- خصائص إعتراض المراسلات:

يتميز إعتراض المراسلات بمجموعة الخصائص والتي سنبينها فيما يلي:

1- إعتراض المراسلات يتم خلسة دون علم و رضا صاحب الشأن: هو عمل يتم دون رضا وعلم المشتبه وهو أهم خاصية فبعلم أصحاب الشأن تنتفي خاصية الاعتراض وهنا لا يمكن القول أننا أمام أسلوب الاعتراض فهذا الأخير يمحو خصوصية الاعتراض ويزيل السرية.²

2- إعتراض المراسلات إجراء يمس الشخص في حرمة الخاصة: المادة 46 " لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميها القانون.

سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة.

لايجوز بأي شكل المساس بهذه الحقوق دون أمر معلن من السلطة القضائية، ويعاقب القانون على انتهاك هذا الحكم.

حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي حق أساسي يضمنه القانون ويعاقب على انتهاكه".³

من خلال نص المادة نلاحظ أنها جاءت صريحة فيما يتعلق بحرية الحياة الخاصة وسرية المراسلات والاتصالات دون قيود، إلى أن إجراء إعتراض المراسلات ينتهك هذه الحرمة ويسترق السمع على المكالمات السلكية كانت أو اللاسلكية، هذا الاستثناء وضعه المشرع الجزائي بغية السير الحسن للتحريات والتحقيقات والحفاظ على الأمن العام، وهنا يعتبر إعتراض المراسلات إجراء يساعد دون شك الجهات القضائية والأمنية للوصول إلى أدلة ومعلومات كانت تعتبر شخصية ولا يمكن المساس بها تحت ذريعة الحرية الشخصية.⁴

3- العملية تستهدف الحصول على الدليل المادي: تعتبر تقنية التصنت على الأحاديث الهاتفية دليل غير مادي ينبعث من عناصر شخصية مما يصدر عن الغير من أقوال وأحاديث تقنع

¹-مرجع نفسه، ص51.

²- مارك نصر الدين، محاضرات في الإثبات الجنائي، ط 03، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2009، ص132.

³- قانون رقم 01-16 مؤرخ في 6 مارس 2016، يتضمن التعديل الدستوري، ج.ر.ج، العدد 14، صادرة بتاريخ 7 مارس 2016.

⁴- شريف محمد، مرنيش مختار، أساليب التحري والتحقيق الحديثة بين النظام و الاتهام ونظام البحث والتحري، مذكرة لنيل شهادة ماستر في الحقوق، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، 2015/2014، ص42..

القاضي بطريقة غير مباشرة تفيد في الكشف عن الجريمة، فتعتبر الأحاديث دليل معنوي غير مادي، فهدف إعتراض المراسلات هو إلتقاط الأدلة المعنوية بغيت تأكيد أدلة الاتهام.¹

4- تستخدم العملية أجهزة قادرة على إلتقاط الأحاديث: مع التطور التكنولوجي الذي شهده العالم في المدة الأخيرة أوجد معه تقنيات ووسائل تكنولوجية حديثة ذات فعالية كبيرة، بفضلها تستطيع اقتحام خصوصيات الأشخاص المشتبه بهم و إلتقاط الأحاديث الصوتية بدقة وجودة عالية، إلا أن استعمال هذه الوسائل دون أي ضمانات تقيدتها تشكل خطرا على حرية الأفراد فهي تتعارض أيضا مع أصول الديمقراطية.²

ثالثا- شروط إعتراض المراسلات:

نظرا لخطورة عملية اعتراض المراسلات وتعارضها مع حماية الحياة الخاصة ومصلحة المجتمع قيدها المشرع بشروط قانونية وهي ما سنذكرها تاليا:

1- ترخيص السلطة القضائية ومراقبتها لعملية التنفيذ:

طبقا للمادة 65 مكرر 5 من ق ا ج ج فإنه ليس في مقدور ضباط الشرطة القضائية اللجوء إلى أسلوب اعتراض المراسلات إلا بعد حصولهم على إذن مكتوب وصادر من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، فالسلطة القضائية هي وحدها هي وحدها المختصة بإصدار هذا الإذن وهو ما يعد ضمانا لازمة لمشروعية هذا الإجراء.

طبقا للمادة 65 مكرر 9 من ق ا ج المعدل و المتمم إن عملية تنفيذ إجراء اعتراض المراسلات تتم تحت رقابة السلطة القضائية التي أذنت به من خلال قيام ضباط الشرطة القضائية المؤذنون له أو المناب من طرف القاضي المختص بإعداد محضر كل عملية اعتراض المراسلات، وكذا عمليات وضع الترتيبات التقنية لهذا الغرض، ويذكر في هذا المحضر تاريخ وساعة بداية هذه العمليات والانتهاؤها منها، بمعنى لا يمكن لضباط الشرطة القضائية القيام بإجراء اعتراض المراسلات إلا بعد الحصول على إذن مكتوب ومسبب من طرف وكيل الجمهورية أو قاضي التحقيق في حالة فتح تحقيق قضائي، يحدد فيه نوع الجريمة التي اقتضت ضرورة التحري أو التحقيق القضائي وطبيعة المراسلة والاتصال

¹ - شريف مخمد، مرنيش مختار، مرجع نفسه، ص 42.

² - مرجع سابق، ص 133.

محل الاعتراض أو التصنت، على أن يتم هذا الإجراء تحت الإشراف المباشر للسلطة المصدرة للإذن.¹

2- تسبب اللجوء إلى اعتراض المراسلات:

يقصد به المبرر الشرعي و الضرورة الملحة التي تستدعي قيام بعملية اعتراض أو مراقبة المراسلات، حيث يشترط وكيل الجمهورية أو قاضي التحقيق المختص قبل منح الإذن بتنفيذ العملية المذكورة، تقدير وجودها وجديتها ودواعيها والفائدة المنتظرة منها في إظهار الحقيقة وكشف غموض الجريمة و الجنات مسبقاً.²

3- تحديد الجرائم محل اعتراض ومراقبة

اللجوء لإجراء اعتراض المراسلات الالكترونية لغرض تحقيق غير مسموح في كافة الجرائم وإنما في الجرائم التي حددها المشرع على سبيل الحصر في نص المادة 65 مكرر 5 من ق ا ج ج، وهي جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية، جرائم تبييض الأموال، أو الإرهاب، الجرائم المتعلقة بالصرف، جرائم الفساد والجرائم الماسة بأنظمة المعالجة الآلية.³

4- سرية الإجراءات وكتمان السر المهني

يعني انه ينبغي أن تنفذ عملية الاعتراض والمراقبة في سرية تامة ودون علم أو رضا المشتبه فيه وأصحاب المكان، لكن مع مراعاة عدم المساس بالسر المهني المقرر بنص المادة 45 فقرة 4 من ق ا ج ج، خاصة إذا تعلق الأمر بأماكن شغلها أشخاص ملزمون بكتمان السر المهني، مثل مكتب المحامي، مكتب المحضر القضائي، أو إذا تعلق الأمر بمن يحملون أسرار مهنية مثل القضاة، الأطباء، نواب البرلمان، فا رغم أن تلك الأماكن وهؤلاء الأشخاص غير مستثنين من إجراء الاعتراض إلا أنه يقتضي الأمر وجوب اتخاذ التدابير اللازمة لضمان احترام السر المهني الذي يخصها⁴، وعليه يمكن القول بان رغم الصعوبات و المخاوف الكثيرة حيال هذه الإجراءات المستحدثة إلا أن الواقع يثبت أن من الضروري والملح اللجوء إلى الاستعانة بهذا النوع من الإجراءات.

¹ - براهيمي جمال، "مكافحة الجرائم الإلكترونية في التشريع الجزائري"، "المجلة النقدية للقانون والعلوم السياسية"، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، ص141.

² - بن مكي نجا، السياسة الجنائية لمكافحة جرائم المعلوماتية، دط، دار الخلدونية، الجزائر، 2017، ص105.

³ - الأمر رقم 66-155، المتضمن لقانون الإجراءات الجزائية، المعدل المتمم، ج.ر.ج، المؤرخ في 18 صفر عام 1386، الموافق ل8 يونيو 1966.

⁴ - براهيمي جمال، مرجع سابق، ص142.

الفرع الثاني

تسجيل الأصوات

من بين إيجابيات التطور العلمي والتكنولوجي الذي شهده العالم هو إيجاد وتقديم وسائل وأجهزة تقنية حديثة تساهم وتساعد على كشف الجرائم وإظهار الحقيقة، ومن بين مخرجات هذا التطور هناك نجد وسائل وأجهزة التسجيل الصوتي، والتي شهدت قفزة نوعية حيث أضحت صغيرة الحجم وسهلة الحمل وبسيطة الاستعمال، لذلك أجاز المشرع الجزائري استخدام هذا التطور العلمي ووضع له إجراءات خاصة لتسجيل كل ما ينطق به الشخص المشتبه فيه أو شركائه أو الأحاديث التي تدور بينهم في الأماكن العامة أو الخاصة وذلك خدمة للعدالة ولذلك سنتعرض إلى تعريف التسجيل الصوتي (أولا) وشروط تسجيل الأصوات (ثانيا).

أولا- تعريف تسجيل الأصوات:

إن ثاني إجراء من الإجراءات الخاصة التي سنهما المشرع الجزائري إجراء التسجيل الصوتي الذي يتم اللجوء إليه بالإضافة إلى شرط الجرائم الخاصة لا بد من شروط معينة أخرى، ويقصد بتسجيل الأصوات بأنه حفظ الكلام أو الأحاديث التي يتفوه بها شخص أو عدة أشخاص مشتبه فيهم أو شركائهم بصفة سرية في مكان عام أو خاص، باستخدام جهاز أو وسيلة معدة لذلك بغية إعادة سماعها في وقت لاحق ونقله من مكان لآخر .

كما يمكن تعريف التسجيل الصوتي أنه: "عملية ضبط وحفظ الأصوات باستخدام أجهزة إلكترونية مختلفة، لإعادة سماعها عندما تستدعي الحاجة ذلك خاصة وأن الصوت يعد من الصفات المميزة لتحديد شخصية الإنسان، حيث يكون لكل شخص صوت مميز يختلف تماما عن صوت الآخرين مما يسمح بالتعرف على صاحبه".¹

والجدير بالذكر في هذا الشأن أن الأحاديث نوعان: عام وحديث خاص ومعياري التحديد فيهما إذا كان الحديث خاصا أو عاما مختلف فيه، فيبرز معيارين أحدهما شخصي (أ) والآخر موضوعي (ب) .

أ-المعيار الشخصي (طبيعة الحديث)

ذهب أنصار هذا الاتجاه إلى الاعتداد بموضوع الحديث ذاته كمعيار للتفرقة بين الحديث العام والحديث الخاص مباشر، فالعبرة هنا ليس بخصوص المكان أو عمومته وإنما بخصوصية

¹ - عبيزة منيرة، "التسجيل الصوتي كدليل للإثبات"، مجلة طبينة للدراسات العلمية الأدبية"، جامعة سطيف، المجلد 06، العدد 01، 2023، ص1602.

الحديث أي يقصد ذوي الشأن، وهذا القصد يستشف من موضوع الحديث ومن هيئة المتحدثين ودرجة علو صوتهم، بحيث يكون الحديث عام إذا كان بطريقة علنية و مسموعة من طرف الغير ولها علاقة بأمر عامة لا تخص المتحدث، ويعتبر الحديث خاص إذا كان يخص الحياة الشخصية للمتحدث بحيث يكون الموضوع ذا خصوصية يحرص صاحبه على إخفائه بغض النظر على المكان الذي يكون فيه فالعبرة ليست بالمكان إنما الحديث الذي يدور بين الطرفين.¹

ب - المعيار الموضوعي: (طبيعة المكان)

ذهب أنصار هذا الاتجاه إلى انه يجب الأخذ بطبيعة المكان الذي يدور فيه الحديث كمعيار للتفرقة، حيث يتخذ من مكان حدوثه قرينة على طبيعته و بالتالي يعتبر الحديث عاما إذا جرى في مكان عام متاح لكل من يرغب أن يستمع لما يدور فيه ويكون الحديث خاصا إذا ما تم في مكان خاص.²

وبالاستناد إلى نص المادة 65 مكرر 5 من ق.ا.ج. ج. يتبين أن المشرع الجزائري لم يولي أهمية للمكان الذي يتم فيه تسجيل الأصوات فقد يكون هذا الأخير في مكان عام أو خاص، واستنادا إلى ذلك فالمعيار الذي اعتمدته المشرع الجزائري هو معيار موضوعي، وهذا ما يتضح من عبارة "الكلام المتفوه به بصفة خاصة وسرية".

والمشرع الجزائري كما عودنا لم يقدم في ق.ا.ج. ج. تعريفا للتسجيل الصوتي مثل ما لم ينص على تعريف عملية اعتراض المراسلات، إنما أشار لها بنص المادة 65 مكرر 5 في الفقرة الثالثة " 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 عامة".³

ويأخذ حكم الحديث الخاص والسري ذلك الحديث الذي يجري في مكان خاص أو عام وكان شخصا وتضمن أدق التفاصيل والإسرار، أين يعبر الإنسان عن نفسه وينقل مكنوناته إلى المتحدث إليه وبغض النظر عن مكان التسجيل الذي قد يكون عاما كالشارع أو خاصا كالمسكن، والأداة التي يتم بها فالمهم في العملية هو الكلام المتفوه به الذي قد يشكل دليلا لإظهار الحقيقة.⁴

¹- عوض محمد عوض، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية، مصر، 2012، ص 404.

²- مرجع نفسه، ص 406.

³- مرجع نفسه، ص 407.

⁴- بشقاوي عبد الحق، بوقادوم يحيوي، "مشروعية الدليل الإلكتروني المستمد من التسجيل الصوتي بالهاتف النقال في الإثبات الجنائي"، "المجلة الجزائرية للأمن الإنساني"، المجلد 07، العدد 01، جامعة الجزائر 1، 2021، ص 167.

وتعتمد عملية التسجيل الصوتي على وضع الرقابة على المكالمات الهاتفية ونقل الأحاديث وتسجيلها، ويتم عن طريق وضع ميكروفونات حساسة تستطيع التقاط الأصوات وتسجيلها على أجهزة خاصة، كما يتم عن طريق التقاط الإشارات اللاسلكية، إلا أن هذه الترتيبات التقنية لا تكون إلا بإذن من وكيل الجمهورية الو قاضي التحقيق حسب الحالة وتحت مراقبته وإشرافه.

ثانيا- شروط تسجيل الأصوات:

لكي يكون التسجيل دليلا لإدانة المتهم لابد على القاضي أن يتأكد من أن الصوت المسجل يخص المتهم وأن لا يكون قد حدث تعديل بالتسجيل أو إجراء مونتاج على الشريط أو المقطع المسجل وأن يكون واضحا ذلك على النحو التالي:

1-التأكد بان الصوت المسجل يخص المتهم:

بما انه من السهل إجراء عملية المونتاج على شريط تسجيل وهو إدخال تغييرات وتعديلات ونقل عبارات من موضع إلى موضع آخر على الشريط، وبما أن المسألة على جانب كبير من الأهمية حيث يتوقف عليها قبول الدليل أو عدم قبوله ، بات من الضروري على قاضي التحقيق الاستعانة بخبير في الأصوات يكون رأيه استشاريا عملا بالقواعد العامة في الإجراءات الجزائية لاسيما و انه في بعض الحالات يكون من الصعب تحديد ما إذا كان الصوت يخص المتهم من عدمه نظرا لتشابه الأصوات، أو اختلاطها بالأصوات المحيطة بمكان التسجيل.¹

2- الحصول على التسجيل الصوتي دون إكراه: أي أن يحصل التسجيل الصوتي دون اللجوء إلى وسائل الإكراه المادي كالتعذيب أو الإكراه، وعدم الركون للغش أو التدليس أو الخداع في الحصول على التسجيل الصوتي فإ استخدام هذه الطرق من شأنه أن يجعل من الدليل المحصل باطلا ويفقد مشروعيته.²

3- الإذن ونوع الجريمة:

يشترط صدور إذن من القاضي قبل التسجيل يكون مسببا بوضوح يبين فيه أسباب صدور هذا أمر التسجيل أو قبول التسجيل، وأن تكون هناك جريمة قد وقعت قبل صدور الإذن، أما إذا كانت الجريمة لم تقع بعد فلا ضرورة لقبول الأمر بالتسجيل لأنه ينطوي على

¹ - بشقاوي عبدالحق، مرجع نفسه، ص 169.

² - مرجع نفسه، ص 170.

إعتداء واضح وصريح على حق الفرد في الخصوصية الذي كفله الدستور و القانون، كما أنه يتم حصر التسجيلات في الجرائم الخطيرة أو تلك التي لا يمكن إثباتها إلا بهذه الوسيلة.¹

3- تفرغ وتحريز التسجيلات:

لم يشر المشرع الجزائري صراحة لإجراء اعتراض المراسلات وتسجيل الأصوات والتقاط الصور إلى وضع التسجيلات أو شريط الصور أو إحراز مختومة إلا أنه بالنظر إلى نص المادة 18 ق.ج.ج تنص على موافاة وكيل الجمهورية بالأشياء المضبوطة، وبحكم المادة 45 من ق.ج.ج تغلق الأشياء المضبوطة و يختم عليها إذا أمكن ذلك، كما أن الأشرطة المسجلة تعتبر أدلة إثبات مادية أصلية ، تقتضي الشرعية الإجرائية حفظها بطريقة خاصة بوضعها في أحرار مختومة بما يضمن عدم التلاعب أو العبث في الحديث المسجل سواء بالحذف أو الإضافة و ضمها إلى ملف الإجراءات مع المحاضر التي تصف أو تنسخ محتواها لكشف الحقيقة.²

الفرع الثالث

إلتقاط الصور

إن المبدأ العام يمنع التقاط الصور خلسة وخفية دون إذن صاحبها، باعتبار تعدي على حرمة الحياة الخاصة، والذي يعتبر حق من الحقوق التي يحميها القانون في مواثيق حقوق الانسان و دساتير الدول، والمشرع الجزائري حذا حذو باقي الدول حيث نص في المادة 01/39 "لا يجوز انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه يحميها القانون".³

إلا إن هناك استثناء حيث أباح المشرع اللجوء إلى أسلوب التقاط الصور كأسلوب من أساليب التحري الخاصة وذلك بما تضمنته المادة 35 ومكرر فقرة 03 من ق.ج.ج إلى جانب اعتراض المراسلات وتسجيل الأصوات وعليه لتحديد مفهوم التقاط الصور وجب التطرق إلى تعريفه (1) ثم بيان التقنيات (2) و الوسائل المستخدمة وكذا شروطه (3).

أولا - تعريف التقاط الصور:

لم يتطرق المشرع الجزائري إلى تعريف عملية التقاط الصور وقد اكتفى بالإشارة إليها فقط بمصطلح "الالتقاط"، فهو أسلوب من أساليب البحث والتحري المستحدثة ويقصد بالتقاط الصور تلك العملية التي تستعمل في البحث والتحري عن الجرائم عن طريق الصورة

¹ - بشقاوي عبدالحق، مرجع سابق، ص162.

² - لوجاني نور الدين، مرجع سابق، ص8.

³ - أحمد غاي، ضمانات المشتبه فيه أثناء التحريات الأولية، دار الهومة، الجزائر، 2005، ص231.

والفيديو، فعذسة الكاميرا هي من أفضل الأساليب إثباتا للحالة، بما تنقله من صور حية و كاملة وصادقة لمكان أو لحدث معين أو واقعة معينة، رأى المشرع توظيفها كعين من العيون التي لا تغفل في خدمة القضاء و كشف الحقيقة.¹

كما عرف التقاط الصور بأنه: "تثبيت الصور على مادة حساسة، وتثبيت الصور يقصد به تركيزها بسرعة خاطفة ثم أخذها عن طريق جاز معد لذلك كي يتم استعمالها مستقبلا لغرض تحقيق مصلحة أو فائدة معينة"²، أما أجهزة المراقبة المتعددة ومتنوعة منها ما يتعلق بالرؤيا، المشاهدة وتسجيل الصورة وهي تمثل انتهاك خطيرا لحياة الأفراد الخاصة سواء في الأماكن الخاصة أو العامة.

لقد أجاز المشرع الجزائري من خلال نص المادة 65 مكرر 09 في ق.ا.ج.ج. بالتقاط الصور لشخص أو عدة أشخاص يتواجدون في مكان خاص، باستخدام أساليب علمية حديثة للحد من تفاقم معدلات الجريمة، فقد يستعان في التصوير بمختلف أجهزة المراقبة البصرية والتي تلتقط الصور والصوت معا، والتكنولوجيا في هذا المجال تطورت وسمحت بالتقاط صور أشخاص بدقة متناهية، بواسطة آلات التصوير المتعارف عليها أو الكاميرات الرقمية وأجهزة الفيديو أو حتى الأقمار الصناعية التي تسمح بالتقاط صور من مسافات بعيدة جدا.³

وهذا الإجراء يقوم أساسا على استخدام الكاميرات أو أجهزة خاصة تلتقط الصور والصوت لوضعية شخص أو عدة أشخاص مشتبه بأمرهم، على الحالة التي كانوا عليها وقت التصوير لغرض استخدام محتوى الفيلم كمادة إثبات ودليل مادي، أو بمعنى آخر مادة مرئية في المحاكم لضمان اتخاذ الإجراءات الوقائية لضبط المجرمين أو المشتبه فيهم، وهذا الإجراء يربط الأشخاص في زمان و في مكان وفي وقت واحد وخاصة مع التطور التكنولوجي والعلمي أصبح بإمكان استخدام وسائل حديثة وذات تقنية جيدة تساعد على التقاط الصور بجودة عالية فهناك أجهزة تعمل بالأشعة تحت الحمراء تلتقط صور الأشخاص ليلا بصورة دقيقة وواضحة وتحت جنحة الليل، حيث تستخدم هذه الأجهزة لنقل الصوت والصورة بشكل لا يلفت الانتباه، لتمكن ضباط الشرطة القضائية من سماع ورؤية ما يدور في حياة المشتبه فيه طوال مدة التحري و البحث.

¹ - نسرين حاج عابد الحفيظ، "الترصّد الإلكتروني كأسلوب قانوني للكشف عن جرائم الفساد الاقتصادي في القانون الجزائري"، "مجلة الدراسات القانونية"، المجلد 5، العدد 1، جامعة البليدة 2، الجزائر، 2022، ص 18، 14.

² - أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2015، ص 66.

³ - مرجع نفسه، ص 67.

ثانيا- شروط إجراء التقاط الصور:

لا تكون عملية التقاط الصور مشروعة إلا إذا توفرت على شروط موضوعية وأخرى شكلية والتي سنستعرضها فيما يلي:

1-الشروط الموضوعية :

- إجراء العملية بأمر مغل من السلطة المختصة : حتى تتم العملية في إطارها الشرعي وحسب مقتضيات القانون فإن وكيل الجمهورية أو قاضي التحقيق تتم العملية تحت إشرافهما و مراقبتهم المباشرة، وتنفيذ العملية حسب نص المادة 65 مكرر 8 و 65 مكرر 9 من تقنين بناء على انتداب من الجهة القضائية المختصة ، حيث أنه إذا قام أحد ضباط الشرطة القضائية بمباشرة أحد هاتيه الإجراءات دون إذن بذلك فإن الدليل المستمد يكون باطلا وتبطل جميع الإجراءات التي بنيت عليه.¹

- وقت إجراء العمليات و مكانها : لم يضع المشرع قيود زمنية ولا مكنية لهذه الإجراءات الخاصة، حيث أجازها بأي وقت من ليل أو نهار أو في أي مكان عام أو خاص، باستثناء السفارات والقنصليات الأجنبية ، حيث خول المشرع الجزائي بموجب استحداثه للنصوص الإجرائية الجزائية و المتعلقة بعملية بالتقاط الصور إمكانية إجراء هذا الأسلوب عبر كامل ربوع الوطن ويمكن أن يمتد إلى خارج الوطن في حالة ما كانت هناك اتفاقيات دولية تقضي بذلك، إضافة إلى عدم التقيد بالظرف الزمني حيث يمكن مباشرة إحدى العمليات موضوع البحث في أي ساعة من اليوم.²

- إجراء تمليه الضرورة :لا بد أن تكون هناك ضرورة ماسة تستدعي اللجوء إلى القيام بهذه الإجراءات،بالإضافة إلى وقوع جريمة من الجرائم المذكورة على سبيل الحصر في المادة 65 مكرر 05 من ق ج ج وكذا وجود دلائل قوية تفيد نسبتها إليها، حيث أن تتحقق الجهة القضائية المختصة من مدى فاعلية العملية في ظهور وكشف الجريمة محل التحقيق قبل إصدار الإذن، أين يكون من المستحيل اكتشاف مرتكبي الجريمة دون اللجوء لهذه العملية.³

2- الشروط الشكلية:

تفرض الشرعية الإجرائية ضرورة التقيد بمجموعة من القيود الشكلية المتمثلة في:

- مباشرة العملية بناء على إذن:حسب نص المادة 65 مكرر 05 من ق ج ج فإنه يجوز لقاضي التحقيق أن يرخص كتابيا لضابط الشرطة القضائية المختص وتحت إشرافه الدائم

¹ - فوزي عمارة، قاضي التحقيق، أطروحة دكتوراه ، جامعة الإخوة منتوري، قسنطينة ، 2010، ص239.

² -مرجع نفسه، ص 240.

³ - مرجع نفسه، ص 241.

بأن يقوم باعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية ووضع الترتيبات التقنية دون موافقة الشخص المعني من أجل القيام بـ: " إلتقاط وتثبيت وبث وتسجيل الكلام في سرية من طرف أي شخص وفي أي مكان عام أو خاص والتقاط الصور لكل شخص"¹، على أن يتضمن الإذن مايلي:

- ضرورة أن يكون الإذن مكتوبا دون اشتراط شكل معين.
- ذكر العناصر التي تسمح بالتعرف على الاتصالات المطلوب التقاطها.
- تحديد الإطار المكاني الذي سوف تتم في العملية.
- تحديد الجريمة التي تبرر اللجوء لهذا الإجراء.
- مدة إنجاز المهمة والتي لا يجب أن تتعد المدة المحددة قانونا بأربعة أشهر قابلة للتجديد ولكن ضمن نفس الشروط.
- استصدار الإذن للقيام بالتقاط الصور يكون حصرا في الجرائم التي اقترفت وليس الجرائم المستقبلية.²
- استئذان وكيل الجمهورية أو قاضي التحقيق قبل مباشرة العملية: إلتقاط الصور كغيره من الإجراءات التي سبق وأن ذكرناها تحتاج إلى إذن لصحتها، وحسب نص المادة 65 مكرر 05 من ق.إ. ج. ج. عند وقوع أحد الجرائم المذكور ضمن نفس المادة يجوز لوكيل الجمهورية أو لقاضي التحقيق أن يأذن باعتراض المراسلات وتسجيل الأصوات والتقاط الصور، بمعنى لابد من وجود إذن مسبق قبل البدء بهذه العمليات.³

الفرع الرابع

الإجراءات المتبعة لمباشرة عملية اعتراض المراسلات وتسجيل الأصوات والتقاط الصور

بعد حصول ضابط الشرطة القضائية على الإذن باعتراض وتسجيل الأصوات والتقاط الصور، فانه يقوم بتنفيذ هذه العملية وفق الإجراءات التي حددتها المواد 65 مكرر 5 المذكورة سابقا، المادة 65 مكرر 8 65 مكرر 9، المادة 65 مكرر 10 من ق.إ. ج. ج، وذلك

¹ - ميلودة عبدالرحمان، مرجع سابق، ص 1670.

² - مرجع نفسه، ص 1671.

³ - فوزي عمارة، مرجع سابق، ص 241.

بوضع الترتيبات القانونية (أولا) ثم تاليها تسخير الأعوان المؤهلين لدى مصلحة عمومية أو خاصة (ثانيا)، تحرير محضر عن العملية (ثالثا)، ونسخ ووصف وترجمة التسجيلات (رابعا).

أولا- وضع ترتيبات التقنية :

وتتمثل في توفير وتشغيل وتركيب التجهيزات الخاصة بمراقبة المحدثات أو الاعتراض عن المراسلات أو التصوير، من أجل التقاط الصور للأشخاص في الأماكن العامة أو الخاصة، أو التقاط الأصوات بالأشخاص والبث والتسجيل بالأماكن العامة والخاصة.¹

يتطلب وضع الترتيبات التقنية الدخول إلى المحلات السكنية دون علم أصحابها، وحتى خارج المواعيد المقررة في المادة 47 من ق 1 ج. ج والتي تنص على: "لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا ولا بعد الساعة الثامنة مساء إلا إذا طلب صاحب المنزل ذلك أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقررة قانونا".

إذ تنص المادة 65 مكرر 5 من ق 1 ج. ج في فقرتها الثانية على أنه: "يسمح الإذن المسلم بغرض وضع ترتيبات تقنية بالدخول إلى المحلات السكنية أو غيرها ولو خارج المواعيد المحددة في المادة 47 من هذا القانون وبغير علم ورضا الأشخاص الذين لهم حق على تلك الأماكن".²

ثانيا- تسخير الأعوان المؤهلين لدى مصلحة عمومية أو خاصة:

أعطى المشرع لضابط الشرطة القضائية صلاحية تسخير الأعوان العاملين بالمصالح والوحدات أو الهيئات المتخصصة في ميدان الاتصالات السلكية واللاسلكية سواء كانت تابعة للقطاع العام أو الخاص للتكفل بالجانب التقني، إذ تنص المادة 65 مكرر 8 من ق 1 ج. ج على أنه "يجوز لوكيل الجمهورية أو لضابط الشرطة القضائية الذي أذن له ولقاضي التحقيق أو ضابط الشرطة القضائية الذي ينييه أن يسخر كل عون مؤهل لدى مصلحة أو وحدة أو هيئة عمومية أو خاصة مكلفة بالمواصلات السلكية أو اللاسلكية للتكفل بالجوانب التقنية للعمليات المذكورة سالفا في المادة 65 مكرر 5 من ق 1 ج. ج ، ويكون تسخير هؤلاء الأشخاص بموجب "مقرر تسخيرة" يكلف العون بتنفيذها".³

¹ - سعدون فاطمة، السياسة الجنائية لمكافحة جرائم الإرهاب، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق ، جامعة الجزائر 1، 2014، صص 68-69.

² - مرجع نفسه ، ص ص 69-70.

³ - مرجع نفسه، ص-70، 69.

ثالثا- تحرير محضر عن العمليات:

أوجب القانون في المادة 18 من ق ا ج ج جميع الإجراءات التي يقوم بها مأمور الضبط القضائي في محاضر موقع عليها منه، كما تلتزم المادة 65 مكرر 9 من ق ا ج ج على أنه: "يحرر ضابط الشرطة القضائية المؤذن له أو المناب من طرف القاضي المختص محضرا عن كل عملية اعتراض وتسجيل المراسلات و كذا عن عمليات وضع ترتيبات تقنية وعمليات الالتقاط والتثبيت والتسجيل الصوتي أو السمعي البصري..."¹

ضابط الشرطة القضائية يقوم بتحرير محضرين الأول يتضمن الجوانب القانونية و يتعلق بعملية اعتراض وتسجيل الأصوات والتقاط الصور، أما المحضر الثاني فيتعلق بالجوانب التقنية من خلال تحديد الآلية المستعملة أو الجهاز ومكان تثبيته، وتوضع هذه المحاضر في ملف الإجراءات وللجهة القضائية السلطة التقديرية للأخذ بها.²

رابعا: نسخ ووصف وترجمة التسجيلات: نص عليها المشرع الجزائري في المادة 65 مكرر 10 من قانون ا.ج.ج على ما يلي: "يصف أو ينسخ ضابط الشرطة القضائية المؤذن له أو المناب المراسلات أو الصور أو المحادثات المسجلة و المفيدة في إظهار الحقيقة في محضر يودع بالملف".

من خلال نص هذه المادة يقوم ضابط الشرطة القضائية بوصف أو نسخ المراسلات أو صور أو المحادثات المسجلة والمفيدة في إظهار الحقيقة يودع بملف الإجراءات، وله أن يستعين بمترجم في حالة وجود عبارات بلغات أجنبية، إذ يسخر ضابط الشرطة القضائية للقيام بترجمتها.³

¹- طاهري حسين، الوجيز في شرح قانون الإجراءات الجزائية ، دار الخلدونية للنشر والتوزيع، الجزائر، 2005، ص31.

²- مرجع نفسه، ص31.

³- مرجع نفسه، ص32.

خاتمة

تعد الجريمة الإلكترونية من الجرائم التي ترتكب في كل ثانية في زمننا الحالي في شتى بقاع العالم، كما أنها في تطور وتزايد هائل هذا ما جعلها من الظواهر الخطيرة التي لها تأثير سلبي كبير على الفرد والمجتمع، خاصة في كون الأفراد يستغلون احترافهم في مجال المعلوماتية بأسلوب سيء، وتكمن هذه الإساءة في استعمال هذا التطور المعلوماتي في الوقوع في المحذور و التعدي على الممنوعات قانونيا، وهذا ما جعلنا نقوم بجهد و دراسة دقيقة لملامسة أكثر النقاط الهامة لهذا الموضوع بداية من التعرف على هذا النوع من الجرائم إلى الصعوبات التي تواجه المحققين في إثباتها والدوافع التي تجعل الشخص يرتكبها وصولا إلى مختلف الطرق التي وضعها المشرع للبحث والتحري عنها وكذا التصدي لها، وفي ذلك قام بإصدار ترسانة قانونية منها القانون 04-09 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، الذي كرس فيه إجراءات التحري التقليدية لهذه الجريمة، كما تولها في قانون الإجراءات الجزائية، و عدل البعض منها المتمثلة في إجراءات التحري المستحدثة، و هذا ما بيناه في مذكرتنا، فبعدا كل هذا البحث في الموضوع نصل إلى استخلاص عدة نتائج المتمثلة كالاتية:

1- عدم إجماع الفقهاء على تعريف موحد للجريمة الإلكترونية يعود أساسا إلى الاختلاف حول تحديد نطاق هذه الجريمة لذا نجد البعض منهم وسع نطاق تعريفها، كما نجد اتجاه آخر ضيق نطاقها.

2- تكريس المشرع الجزائري جهوده في محاولة إيجاد تعريف قانوني خاص بهذا النوع من الجرائم بحيث نجده إنحاز إلى التعريف الذي يحدد بأن كل جريمة يكون فيها الحاسب لألي تعتبر جريمة إلكترونية.

3- تتميز بخصائص تجعلها فريدة من نوعها منها صعوبة إثباتها، طريقة ارتكابها، امتدادها الجغرافي بحيث يمكن لمرتكبها أن يكون في بلد ما و النتيجة تتحقق في بلد آخر.

4- يتمثل مرتكبها بصفات تجعلهم من أخطر المجرمين في مجال الإجرام إذ يتمتعون بمهارات عالية تفوق الشخص العادي فأساس نجاح هذا النوع من الجرائم يعود إلى احترافهم في إستخدام الحاسب لألي و إتقانهم لكل وسائل المعلومات.

5- تدخل هذه الجريمة إلى عدة مجالات إذ قد تأخذ عدة أشكال فيمكن أن نجدها من الجرائم المادية التي تمس للأموال الدولة، أو الشخص، كما قد تكون من الجرائم الثقافية، السياسية و

الاقتصادية و أيضا تأخذ شكل الجرائم الجنسية(مواقع إباحية، تحرش، ابتزاز بصور، استدراج صغار دون سن الرشد...و غيره من الجرائم).

6-إن إجراء البحث و التحري في هذه الجريمة يأخذ صورة مختلفة تماما عن التحري في الجرائم التقليدية ففي هذا النوع من الجرائم يقوم بالبحث و التحري عنها رجال ضباط الشرطة، كما أن التحري عنها يعتمد على وسائل تقنية و مهارة عالية لدى المحقق لضمان الوصول إلى نتيجة.

7-جعل المشرع الجزائري إجراءات تحري كلاسيكية لتحري عن هذا النوع من الجرائم و ذلك في القانون 04-09، التي تتمثل في الإجراءات التي نجدها في الجرائم التقليدية و لكن مع تطويرها لتصل إلى مستوى الجرائم المعلوماتية و جعلها تتناسب مع طبيعتها الخاصة و التي تتمثل في إجراء التفتيش ،ضبط الدليل الإلكتروني...

8-إن إجراء التفتيش في البيئة المعلوماتية يتميز بعدة خصائص تميزه عن إجراء التفتيش العادي،و التي تتبين معنا بشروط الموضوعية و الشكلية التي وضعها المشرع للقيام بهذا الإجراء ،و كذا كيفية إجراءه في هذا النوع من الجرائم ،و إلى مدى يمكن لهذا الإجراء أن يطبق على المكونات المعنوية و المادية للحاسب لألي.

9-إجراء المعاينة هو من الإجراءات التي تساهم بشكل كبير في الكشف عن هذه الجرائم، إذ للإيجاد دلائل مفيدة يجب التنقل إلى مسرح الجريمة المرتكبة ،ورؤية المكان، فيقوم بهذا الإجراء فريق متخصص في التقنيات المعلوماتية.

10-ضبط الدليل الإلكتروني هو نتيجة التفتيش، أي عند القيام بالتفتيش نصل إلى نتيجة و هي ضبط دليل إلكتروني مفيد للإثبات في الجريمة، كما قد نجده يسمى بمصطلح آخر و هو حجز الدليل الرقمي،و الشرط المهم في هذا الإجراء هو الحرص على عدم الاعتداء على حياة الفرد و المجتمع عند القيام به.

11-إن المراقبة الإلكترونية من الإجراءات التي يلزم لها ترخيص من السلطة القضائية المختصة لكونها ماسة للحياة الفرد الخاصة، لذا قام المشرع الجزائري في المادة 04 الفقرة الأولى من القانون 04-09 بتبيان الحالات التي تسمح بلجوء إلى هذا الإجراء.

12-إن إجراء حفظ معطيات المتعلقة بحركة السير من أهم إجراءات التي استحدثها المشرع في القانون 04-09 ،بحيث يقوم فيه مزود الخدمات بتجميع معطيات المعلومات و حفظها في الأرشفة، فهذا الإجراء يساهم في عدم فقدان الدليل و ضمان تواجده في مكان موثوق.

13- قام المشرع الجزائري في قانون الإجراءات الجزائية الجزائري باستحداث أساليب لتحري في الجرائم المعلومات، المتمثلة في إعتراض المرسلات، تسجيل الأصوات و إلتقاط الصور، و كذا إجراء التسرب، و هذا لسبب و هو الالتحاق بالتطور الذي يحدث في هذا النوع من الجرائم وكذا ضمان و جود طرق لمكافحتها و حماية الفرد من أي خطر يوجهه.

في نهاية بحثنا نود أن نشير إلى بعض المقترحات التي يجب الالتفات إليها لوضع حد لهذا النوع من الجرائم و التأكد من مواجهتها بطريقة صحيحة المتمثلة في:

- يجب إستخدام كلمات مرور قوية و تغييرها بانتظام، مع تجنب مشاركة المعلومات الشخصية على الإنترنت، تحديث البرامج و التطبيقات باستمرار، استخدام برامج مكافحة الفيروسات .

- ضرورة خلق ثقافة لتثقيف بالجرائم الإلكترونية و التوعية من مختلف أساليب الاحتيال الإلكتروني، تهذيب مستخدمي الأنترنت و حثهم على الاستعمال الأمثل لهذا النوع من التقنيات.

- عقد دورات تدريبية و تكوينية للعاملين في مجال التحري و التحقيق لإعدادهم بشكل صحيح في مواجهة العالم الرقمي.

- تشجيع الجامعات و المراكز البحثية على تنظيم العديد من الندوات و المؤتمرات التي تعالج تطور الإجرام المعلوماتي و كيفية مكافحتها و الحد من أثارها.

- على المشرع الجزائري إبداء أهمية لتكثيف التعاون و التنسيق بين الدول، من أجل تطوير و توحيد التشريعات الجزائية، الموضوعية و الإجرائية التي تساهم في مكافحة الجرائم الرقمية.

قائمة المصادر والمراجع

I. باللغة العربية

أولاً: الكتب

1. أوهابية عبد الله، شرح قانون الإجراءات الجزائية الجزائري، ط 02، دار هومة، الجزائر، 2011.
2. ———، شرح قانون العقوبات (القسم العام)، د ط، دار هومة، الجزائر، 2003.
3. بالعليات إبراهيم، أركان الجريمة وطرق إثباتها في قانون العقوبات الجزائري، ط 01، دار الخلدونية، الجزائر، 2007.
4. بوحليط يزيد، الجرائم الالكترونية و الوقاية منها في القانون الجزائري، دار الجامعة الجديدة للنشر، مصر، 2019.
5. بوسقيعة أحسن، الوجيز في القانون الجزائي العام، الديوان الوطني للأشغال التربوية، الجزائر، 2002.
6. بوكر رشيدة، جرائم الاعتداء على نظم المعالجة الآلية في التشريع الجزائري المقارن، منشورات الحلبي الحقوقية، لبنان، 2012.
7. بيومي حجازي عبد الفتاح، مكافحة جرائم الكمبيوتر و الانترنت في القانون العربي النموذجين دراسة معمقة في القانون المعلوماتي، دار الفكر الجامعي، مصر، 2006.
8. حامد قشوش هدى، جرائم الحاسب الإلكتروني، د ط، دار النهضة العربية، مصر، د.س.ن.
9. بن مكي نجا، السياسة الجنائية لمكافحة الجرائم المعلوماتية، دار الخلدونية، الجزائر، 2017.
10. دباس الحميد محمد، ماركو إبراهيم نينو، حماية أنظمة المعلومات، دار حامد للنشر و التوزيع، عمان، 2007.
11. الرومي محمد أمين، جرائم الكمبيوتر و الإنترنت، د ط، دار المطبوعات الجامعية، مصر، 2004.
12. زيدان زبيحة، الجريمة المعلوماتية في التشريع الجزائري والدولي، د ط، دار الهدى للطباعة والنشر والتوزيع، الجزائر، 2011.
13. سعدي سليمة، بلال حجازي، جرائم المعلومات والشبكات في العصر الرقمي، دار الفكر الجامعي، الإسكندرية، 2017.
14. شيوا محمد سامي، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة الرابعة، دار النهضة، مصر، 1998.
15. طارق إبراهيم الدسوقي عطية، الأمن المعلوماتي، النظام القانوني للحماية المعلوماتية، د ط، دار الجامعة الجديدة، مصر، 2009.
16. طاهري حسين، الوجيز في شرح قانون الإجراءات الجزائية، دار الخلدونية للنشر والتوزيع، الجزائر، 2005.

17. **عبد الله حسين علي محمود**، سرقة معلومات المخزنة في الحاسب الآلي، دار النهضة العربية، مصر ، 2001.
18. **عبيد الكعبي محمد** ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت، د.ط، دار النهضة العربية، مصر، 2009.
19. **عفيفي كمال**، جرائم الكمبيوتر و حقوق المؤلف والمصنفات الفنية ودور الشرطة القضائية، ط 2 ، دراسة مقارنة، منشورات الحلبي القانونية، دمشق، 2007.
20. **عنازته محمد عبد الرحمن** ، القصد الجرمي في الجرائم الإلكترونية، دار الأيام للنشر و التوزيع، عمان، 2017.
21. **عوض محمد عوض**، المبادئ العامة في قانون الإجراءات الجنائية، دار المطبوعات الجامعية، مصر، 2012.
22. **غاي أحمد** ، ضمانات المشتبه فيه أثناء التحريات الأولية ، دار الهومة، الجزائر، 2005.
23. **فخري عبد الرزاق** ، الحديثي صلبى ، شرح قانون العقوبات القسم العام، د.ط، الناشر العاتك، مصر، 2008.
24. **قادري عبد الفتاح الشيهايوي** ، ضوابط التفتيش في التشريع المصري و المقارن، ط 25 ، منشأة المعارف، مصر ، د.س.ن.
25. **قارة أمال**، الحماية الجزائية للمعلوماتية في التشريع الجزائري، د.ط، دار هومة للطباعة و النشر والتوزيع، الجزائر، 2007.
26. **محمد الأسدي إلينا** ، مدى فاعلية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، دار حامد للنشر و التوزيع، عمان، 2015.
27. **محمد موسى مصطفى**، التحقيق الجنائي في الجرائم الإلكترونية، مطابع الشرطة، مصر، 2008.
28. **مروك نصرالدين**، محاضرات في الإثبات الجنائي، ط 03، الجزء الأول، دار هومة للطباعة والنشر والتوزيع، الجزائر، 2009.
29. **المناعة أسامة أحمد** ، الزغبى محمد جلال ، جرائم تقنية نظم المعلومات الإلكترونية، ط 3، دار النشر و التوزيع، عمان، 2014.
30. **هروال نبيلة هبة**، الجوانب الإجرائية للجريمة المعلوماتية، دون طبعة، دار الفكر الجامعي، الإسكندرية، دون سنة النشر.

ثانياً: الرسائل والمذكرات الجامعية:

1. أطروحات الدكتوراة:

1. **أمدور رجاء**، خصوصية التحقيق في مواجهة الجرائم المعلوماتية ، أطروحة مقدمة لنيل شهادة دكتوراه الطور الثالث ل . م د ، تخصص القانون الخاص، جامعة محمد البشير الإبراهيمي، برج بوعريرج، كلية الحقوق والعلوم السياسية، قسم الحقوق، السنة الجامعية 2021/2020.

2. براهيمي جمال، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه، تخصص قانون، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2018.
3. دلال مولاي ملياني، إشكالية الإثبات في جرائم الأنترنت في التشريع الجزائري، أطروحة دكتوراه تخصص قانون خاص، كلية الحقوق و العلوم السياسية، جامعة أوبكر بلقايد، تلمسان، الجزائر، 2013/2014.
4. عمر محمد أوبكر بن يونس، الجرائم الناشئة عن إستخدام الأنترنت، رسالة دكتوراه، كلية الحقوق، جامعة عين تمس، مصر، 2001.
5. فوزي عمارة، قاضي التحقيق، أطروحة دكتوراه، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة، الجزائر، 2010.
6. يحي بن إسماعيل، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة لنيل شهادة الدكتوراه العلوم في القانون الخاص، كلية الحقوق و العلوم السياسية، جامعة أوبكر بلقايد تلمسان، الجزائر، 2022.

2. المذكرات الجامعية:

أ - مذكرات ماجستير:

1. أمينة ركاب، أساليب التحري الخاصة في جرائم الفساد في القانون الجزائري، مذكرة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2015.
2. بن عقون حمزة، السلوك الإجرامي للمجرم المعلوماتي، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علم الإجرام وعلم العقاب، جامعة الحاج لخضر، باتنة، 2011-2012.
3. بن مهجع الغنزي سليمان، و سائل التحقق في جرائم نظم المعلومات، رسالة ماجستير في العلوم الشرطية، كلية الدراسات العليا بجامعة نيف التدريبية للعلوم الأمنية، السعودية.
4. بن ناصر السرحاني محمد، مهارات التحقيق الجنائي الفني في جرائم الحاسوب و الأنترنت، بحث مقدم لاستكمال متطلبات الحصول على درجة الماجستير، في قسم العلوم الشرطية، تخصص القيادة الأمنية، كلية الدراسات العليا، جامعة نيف العربية للعلوم الأمنية، السعودية، 2004.
5. سعدون فاطمة، السياسة الجنائية لمكافحة جرائم الإرهاب، مذكرة لنيل شهادة الماجستير في الحقوق، كلية الحقوق، جامعة الجزائر 1، 2014.
6. سعيداني نعيم، آليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص علوم جنائية، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2012-2013.
7. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجستير في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2013.

8. طارق عبد الرحيم الردايدة، التفتيش الإلكتروني في الجرائم الرقمية ، دراسة وصفية مقارنة، مذكرة ماجستير، ضمن تخصص امن نظم المعلومات والجرائم الرقمية، كلية الحقوق و العلوم السياسية ، جامعة الأميرة سمية للتكنولوجيا، الأردن 2017.
9. لدغم شيكوش زكرياء، النظام القانوني للتسرب في القانون الجزائري، مذكرة لنيل شهادة الماجستير في العلوم القانونية، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح ورقلة، 2013/2012.
10. مناصرة يوسف، جرائم المساس بأنظمة المعالجة الآلية للمعطيات، رسالة مقدمة لنيل شهادة الماجستير، في القانون الجنائي و العلوم الجنائية، قسم العلوم القانونية، كلية الحقوق و العلوم السياسية، جامعة الجزائر، السنة الجامعية 2008-2009.

ب- مذكرات الماستر:

1. بن عنطر سيهام، التحقيق الجنائي في الجرائم الالكترونية ،مذكرة لنيل شهادة الماستر، تخصص القانون الجنائي و العلوم الجنائية، كلية الحقوق، جامعة مولود معمري، تيزي وزو، الجزائر ، السنة الجامعية 2023.
2. بوبقرة خيرة، أليات البحث و التحري عن الجريمة المعلوماتية في القانون الجزائري ،مذكرة لنيل شهادة الماستر ،تخصص في القانون الجنائي و العلوم الجنائية ،قسم عام، كلية الحقوق و العلوم السياسية ،جامعة عبد الحميد بن باديس ،مستغانم ،السنة الجامعية 2020-2019.
3. بوضياف أسماء، الحماية الجنائية للتجارة الإلكترونية، مذكرة لنيل شهادة ماستر تخصص قانون الأعمال، قسم الحقوق ، كلية الحقوق والعلوم السياسية محمد خيضر بسكرة، الجزائر، 2020/2019.
4. شريف محمد، مرنيش مختار، أساليب التحري والتحقيق الحديثة بين النظام و الاتهام ونظام البحث والتحري، مذكرة لنيل شهادة ماستر في الحقوق، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون تيارت، 2015/2014.
5. عبد العزيز أحمد، خصوصية التحقيق في الجريمة المعلوماتية، مذكر مقدمة لنيل شهادة الماستر في الحقوق و العلوم السياسية، تخصص القانون الجنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية قسم الحقوق ،جامعة مولاي طاهر ، سعيدة، سنة 2021-2022.
6. فاطمة الزهرة سماعيل، رمزية أمال صالح بلخوجة، نظام التسرب في قانون الإجراءات الجزائية، مذكرة لنيل شهادة الماستر، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة ابن خلدون، تيارت، 2016/2015.
7. محمد بوعمره و سيد علي بنينال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة ماستر في العلوم القانونية ، تخصص قانون الأعمال، كلية الحقوق و العلوم السياسية ، جامعة أكلي محند أو لحاج البويرة ،2020-2019.

8. نواوي سليمة، دور الدرك الوطني في محاربة الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر في علوم الإعلام و الاتصال، تخصص اتصال وعلاقات عامة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف، المسيلة، 2019/2018.
9. وعلي بدر، المواجهة الإجرائية للجرائم المعلوماتية، مذكرة الماستر تخصص القانون الجنائي، كلية الحقوق و العلوم القانونية، جامعة محمد بوضياف المسيلة، 2018-2019.

ثالثا: مقالات:

1. ابتسام مناع، "جريمة الاعتداء الإلكتروني على الحياة الخاصة في التشريع الجزائري" مجلة الشريعة و الاقتصاد، المجلد الثامن، العدد 15، جامعة منتوري، قسنطينة، 2019، صص 319-324.
2. آيت مولود سامية، "الضمانات المقررة لمشروعية إعتراض المراسلات وتسجيل الأصوات والتقاط الصور في الجرائم الاقتصادية"، المجلة النقدية للقانون والعلوم الإنسانية، كلية الحقوق، جامعة مولود معمري تيزي وزو، العدد 02، 2015، صص 320، 321.
3. براهيم جمال، "مكافحة الجرائم الإلكترونية في التشريع الجزائري"، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، 2016، صص 141، 142.
4. بشقاوي عبد الحق، بوقادوم يحيوي، "مشروعية الدليل الإلكتروني المستمد من التسجيل الصوتي بالهاتف النقال في الإثبات الجنائي"، المجلة الجزائرية للأمن الإنساني، جامعة الجزائر 1، المجلد 07، العدد 01، 2021، صص 167، 168.
5. بن سولة نور الدين، "الجرائم الإلكترونية في ضوء التشريع الجزائري"، مجلة الحوار المتوسطي، المجلد التاسع، العدد 1، مارس 2018، صص 272، 273.
6. بن طالب ليندة، "التفتيش في الجرائم المعلوماتية"، مجلة العلوم القانونية و السياسية، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، الجزائر، العدد 22، جوان 2017، صص 494، 495.
7. بوضياف إسمهان، "الجريمة الإلكترونية و الإجراءات التشريعية لمواجهتها في الجزائر"، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، العدد 11، 09 مايو 2018 صص 352-357.
8. تاجر كريمة، "التسرب الإلكتروني كآلية لمكافحة الجريمة الإلكترونية"، المجلة النقدية للقانون والعلوم السياسية، كلية الحقوق و العلوم السياسية- جامعة تيزي وزو، المجلد 19، العدد 02، 2024، صص 479، 480.
9. تشنين صالح، "إجراءات التحري والتحقيق في جرائم الإعلام والاتصال في التشريع الجزائري"، مجلة الدراسات القانونية، جامعة عبد الرحمان ميرة، بجاية، العدد 01، 2014، صص 283، 284.

10. حاج عابد الحفيظ نسرين، "الترصد الإلكتروني كأسلوب قانوني للكشف عن جرائم الفساد الاقتصادي في القانون الجزائري" مجلة الدراسات القانونية، جامعة البليدة 2، الجزائر، المجلد 5، العدد 1، 2022، صص 14-18.
11. سعيد زيوش، "ظاهر الابتزاز الإلكتروني وأساليب الوقاية - قراءة سوسولوجية وأراء نظرية" مجلة العلوم الاجتماعية، العدد 22، جانفي 2017، صص 71، 72.
12. شيخ عبد الصديق، "الوقاية من الجرائم في ظل القانون 04-09 المتضمن لقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها" مجلة المعالم للدراسات القانونية و السياسية، المدية، العدد 15، 2020/06/01.
13. شيخ ناجية، "إجراء التسرب في القانون الجزائري: وسيلة لمكافحة الجرائم المستحدثة"، مجلة معارف، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو، 2018، صص 10، 11.
14. عبيزة منيرة، "التسجيل الصوتي كدليل للإثبات"، مجلة طبنة للدراسات العلمية الأدبية، جامعة سطيف، المجلد 06، العدد 01، 2023، صص 1602، 1603.
15. عثمانى صورية، مرابط، سعاد بن جديدي، "التحرش الجنسي بالأطفال المظاهر و المخاطر بين "متحرش و متحرش به"، دراسة حالة " مجلة دراسات في سيكولوجيات الانحراف، العدد 01، 30-12-2016، صص 82، 83.
16. عمارة فوزي، "اعتراض المراسلات و تسجيل الأصوات و التقاط الصور و التسرب كإجراءات تحقيق قضائي في المواد الجزائية" مجلة العلوم الإنسانية، جامعة منتوري قسنطينة، العدد 33، جوان 2010، صص 248، 249.
17. غريبي بشرة، "خصوصية المجرم المعلوماتي ودوافعه"، مجلة نومي روس الأكاديمية، العدد الثاني، جامعة أبوبكر بلقايد تلمسان، 01 جوان 2021، صص 108، 109.
18. محمد السعيد زناتي، "الجريمة المعلوماتية في ظل التشريع الجزائري و الاتفاقيات الدولية" مجلة اليزي للبحوث و الدراسات، العدد الثاني، المركز الجامعي اليزي، الجزائر، ديسمبر 2017، صص 34، 35.
19. المزروع يسعيد سالم و عزماني عبد الرحمان، "إجراءات التحقيق الجنائي في جرائم تقنيات المعلومات وفقا لتشريع الإماراتي" مجلة العلوم الاقتصادية و الإدارية القانونية، المجلة العربية للعلوم و نشر الأبحاث، العدد 13، المجلد الثاني، أكتوبر 2018، صص 111-124.
20. عزوز سارة، سلمه معزوز، "أساليب البحث و التحري الخاصة في جرائم الفساد"، مجلة الباحث للدراسات الأكاديمية، المجلد 9، العدد 3، جوان 2021، صص 49، 50.
21. ميلودة عبد الرحمان، "التصوير الخفي كإجراء تحقيق قضائي خاص"، دراسة مقارنة، مجلة الحقوق والحريات، جامعة الدكتور مولاي طاهر سعيدة، المجلد 10، العدد 01، 2022، صص 1669، 1670.
22. هارون وردة، "الحماية القانونية للعون المتسرب: آلية فعالة في إنجاح عملية التسرب و مكافحة الجريمة"، مجلة الدراسات القانونية المقارنة، كلية الحقوق و العلوم السياسية،

جامعة عبد الرحمن ميرة ، بجاية ، الجزائر، المجلد 07، العدد 01، 2021، ص ص 1978-1981.

رابعاً: نصوص قانونية

أ) دستور:

1. الدستور الجزائري لسنة 2020، ج. ر.ج.ج، العدد 82، صادر في 30 ديسمبر 2020.

ب) نصوص تشريعية:

❖ قوانين عادية:

1. القانون رقم 03/82، المؤرخ في 13 فبراير 1982، المتضمن لقانون الإجراءات الجزائية الجزائري، المعدل و المتمم، للأمر رقم 66-155، ج. ر.ج.ج، العدد 07، الصادر بتاريخ 16 فبراير 1982.
2. القانون رقم 04-15، مؤرخ في 10 نوفمبر 2004، المعدل و المتمم للأمر رقم 66-156، الصادر بتاريخ 08 جوان 1966، المتضمن قانون العقوبات، ج. ر.ج.ج، العدد 71.
3. القانون رقم 03/2000 المؤرخ في جمادى الأولى عام 1421 الموافق لـ 5 أوت 2000، يحدد القواعد العامة المتعلقة بالبريد والمواصلات السلوكية واللاسلكية، ج. ر.ج.ج، العدد 48، الصادر في سنة 2000.
4. قانون رقم 22/06 مؤرخ في 29 ذي القعدة 1427، الموافق لـ 20 ديسمبر 2006 المعدل و المتمم للأمر 66-155 المؤرخ في 8 1 صفر عام 1386 الموافق لـ 8 يونيو 1966، المتضمن قانون الإجراءات الجزائية، ج. ر.ج.ج، العدد 48.
5. القانون رقم 04-09، المؤرخ في 14 شعبان 1430 الموافق 5 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها، ج. ر.ج.ج، العدد 47، الصادر بتاريخ 16 أوت 2009.
6. قانون رقم 05/20، مؤرخ في 18 أفريل 2020، يتعلق بالوقاية من التمييز وخطاب الكراهية، ج. ر.ج.ج، العدد 25، الصادر بتاريخ 19 أفريل 2020.

❖ الأوامر التشريعية:

- أمر رقم 66-155، المؤرخ في 18 صفر عام 1386، الموافق لـ 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، المعدل المتمم بالقانون رقم 04-14، المؤرخ في 10 نوفمبر 2004، ج. ر.ج.ج، العدد 71.

❖ مراسيم رئاسية:

- المرسوم الرئاسي رقم 15-261 المؤرخ في 08 أكتوبر 2015 المتضمن تحديد تشكيلة و تنظيم كفاءات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال، ج. ر.ج.ج، عدد 53، في 08/10/2015.

خامسا: مداخلات

- 1 بن صولبح أمال، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام خطوة هامة نحو مكافحة الإرهاب الإلكتروني في الجزائر"، مداخلات الملتقى الدولي حول "الإجرام السيبراني المفاهيم و التحديات"، 11-12 أبريل 2017
- 2 لوجاني نور الدين، أساليب التحري و إجراءاتها وفقا لقانون 06-22 المؤرخ في 20 ديسمبر 2006، مداخلات أقيمت في إطار يوم دراسي حول علاقة النيابة العامة بالشرطة القضائية، إيزي، 12 ديسمبر 2007.
- 3 عبد الناصر محمود فرغلي، محمد عبيد سيف سعيد السماري، الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية، مداخلات تطبيقية، المؤتمر العربي الأول للعلوم الأدلة الجنائية و الطب الشرعي، جامعة نيف للعلوم الأمنية الرياض، 2017.

سادسا: محاضرات

- عثمان عي الدين، التحقيق في الجريمة الإلكترونية، محاضرة ملقى على طلبة سنة أولى ماستر، تخصص جريمة و أمن عمومي، كلية الحقوق و العلوم السياسية، جامعة العربي التبسي، تبسة.

II. باللغة الأجنبية:

- I. la preuve électronique , www.internt.juridique.net, consulté le 09. 052025

الفهرس

قائمة المحتويات	الصفحة
مقدمة	4-1

الفصل الأول

الإطار المفاهيمي للبحث والتحري عن الجريمة الإلكترونية

المبحث الأول: ماهية الجريمة الإلكترونية.....	38-6
المطلب الأول: أساسيات حول الجريمة الإلكترونية.....	15-6
الفرع الأول: تعريف الجريمة الإلكترونية.....	6
أولاً: تعريف الفقه للجريمة الإلكترونية.....	6
ثانياً: التعريف القانوني.....	8
الفرع الثاني: خصائص الجريمة الإلكترونية.....	9
أولاً: الجريمة الإلكترونية مرتبطة بالحاسب الآلي وشبكته.....	9
ثانياً: صعوبة اكتشاف الجريمة الإلكترونية.....	9
ثالثاً: صعوبة إثبات الجريمة الإلكترونية.....	10
رابعاً: جريمة سهلة وناعمة.....	10
خامساً: الامتداد الزمني والجغرافي (جريمة متعددة للحدود)	11
سادساً: صعوبة التحقيق الجنائي في الجرائم الإلكترونية.....	12
الفرع الثالث: دوافع ارتكاب الجريمة الإلكترونية.....	12
أولاً: الرغبة الأكيدة في الانتقام.....	12

12	ثانيا: الرغبة الأكيدة في تحدي وقهر النظام التقني المعلوماتي.....
13	ثالثا: الولع في جمع المعلومات وتعلمها.....
13	رابعا: السعي إلى تحقيق الربح.....
13	خامسا: ارتكاب الجرائم كوسيلة للتسلية والدعابة.....
14	سادسا: الدافع الديني.....
14	سابعا: الدافع السياسي والعسكري.....
14	ثامنا: دافع الإرهاب.....
26-14	المطلب الثاني: الأحكام الخاصة بالجرائم الإلكترونية.....
15	الفرع الأول: أركان الجريمة الإلكترونية.....
15	أولا: الركن الشرعي.....
15	ثانيا: الركن المادي.....
16	ثالثا: الركن المعنوي.....
17	الفرع الثاني: أطراف الجريمة الإلكترونية.....
17	أولا: الجاني أو المجرم المعلوماتي.....
19	ثانيا: المجني عليه في الجريمة الإلكترونية.....
20	الفرع الثالث: أشكال الجريمة الإلكترونية.....
20	أولا: الجريمة المادية.....
20	ثانيا: الجريمة الثقافية.....
20	ثالثا: الجرائم السياسية والاقتصادية.....
21	رابعا: الجرائم الجنسية.....

21.....	خامسا: جرائم حسب الأفراد.....
22.....	الفرع الرابع: تقسيم الجرائم الإلكترونية في التشريع الجزائري.....
22.....	أولا: الجريمة الإلكترونية المرتكبة باستخدام النظام المعلوماتي.....
25.....	ثانيا: الجريمة الإلكترونية الواقعة على النظام المعلوماتي.....
27.....	المبحث الثاني: ماهية البحث والتحري عن الجريمة الإلكترونية.....
27.....	المطلب الأول: مفهوم البحث والتحري عن الجريمة الإلكترونية.....
27.....	الفرع الأول: تعريف البحث والتحري عن الجريمة الإلكترونية.....
28.....	الفرع الثاني: خصائص البحث والتحري عن الجرائم الإلكترونية و شروطه.....
28.....	أولا: خصائص البحث والتحري عن الجريمة الإلكترونية.....
29.....	ثانيا: شروط البحث والتحري عن الجريمة الإلكترونية.....
30.....	الفرع الثالث: وسائل البحث والتحري عن الجريمة الإلكترونية.....
31.....	أولا: الوسائل المادية.....
31.....	ثانيا: الوسائل الإجرائية.....
32.....	المطلب الثاني: أجهزة البحث والتحري عن الجريمة الإلكترونية.....
33.....	الفرع الأول: المحقق في الجرائم الإلكترونية.....
33.....	أولا: تعريف المحقق الجنائي في الجرائم الإلكترونية.....
34.....	ثانيا: خصائص المحقق في الجرائم الإلكترونية.....
35.....	الفرع الثاني: الأجهزة المختصة بإجراء البحث والتحري في الجريمة الإلكترونية.....
35.....	أولا: الهيئات الفنية المختصة في البحث والتحري عن الجرائم الإلكترونية.....
36.....	ثانيا: جهازي الأمن الوطني والدرك الوطني.....

الفصل الثاني:

إجراءات البحث والتحري عن الجريمة الإلكترونية

- المبحث الأول: إجراءات البحث والتحري المقررة في القانون رقم 04-09.....40
- المطلب الأول: إجرائي التفتيش الإلكتروني والمعاينة.....41
- الفرع الأول: المقصود بالتفتيش الإلكتروني في الجرائم الإلكترونية.....42
- أولاً: تعريف التفتيش الإلكتروني.....42
- ثانياً: الشروط المتبعة لإجراء التفتيش الإلكتروني.....43
- الفرع الثاني: كيفية إجراء التفتيش في الجرائم الإلكترونية والسلطة المختصة به.....47
- أولاً: كيفية إجراء التفتيش في الجريمة الإلكترونية.....47
- ثانياً: السلطة المختصة بالإشراف على عمليات التفتيش.....49
- الفرع الثالث: إجراء المعاينة.....50
- أولاً: تعريف المعاينة والضوابط التي تتم فيها إجراء المعاينة.....50
- ثانياً: معاينة الجرائم الواقعة على المكونات المادية للحاسب.....53
- ثالثاً: معاينة الجرائم الواقعة على المكونات الغير مادية للحاسب.....54
- المطلب الثاني: ضبط الدليل الإلكتروني ومراقبة الاتصالات الإلكترونية.....54
- الفرع الأول: إجراء ضبط الدليل الإلكتروني.....55
- أولاً: تعريف ضبط الدليل الإلكتروني.....55
- ثانياً: إجراءات ضبط الدليل الإلكتروني.....56
- ثالثاً: أنواع الدليل الإلكتروني والصعوبة التي تواجه المحقق في ضبطه.....57
- الفرع الثاني: مراقبة الاتصالات الإلكترونية.....58

أولا: تعريف مراقبة الاتصالات الإلكترونية.....	59
ثانيا: أحكام مراقبة الاتصالات الإلكترونية.....	60
ثالثا: حفظ المعطيات المتعلقة بحركة السير.....	62
المبحث الثاني: إجراءات البحث والتحري المقررة في قانون الإجراءات الجزائية.....	65
المطلب الأول: التسرب الإلكتروني.....	65
الفرع الأول: تعريف التسرب الإلكتروني.....	66
الفرع الثاني: صور التسرب الإلكتروني.....	67
الفرع الثالث: الشروط التي تحكم عملية التسرب في الجرائم الإلكترونية.....	69
أولا: الشروط الشكلية.....	69
ثانيا: الشروط الموضوعية.....	72
المطلب الثاني: إعتراض المراسلات وتسجيل الأصوات والتقاط الصور.....	73
الفرع الأول: إعتراض المراسلات.....	74
أولا: تعريف إعتراض المراسلات.....	74
ثانيا: خصائص إعتراض المراسلات.....	75
ثالثا: شروط إعتراض المراسلات.....	76
الفرع الثاني: تسجيل الأصوات.....	78
أولا: تعريف تسجيل الأصوات.....	78
ثانيا: شروط تسجيل الأصوات.....	80
الفرع الثالث: إلتقاط الصور.....	81
أولا: تعريف إلتقاط الصور.....	82

ثانيا: شروط إجراء إلتقاط الصور.....	83
الفرع الرابع: الإجراءات المتبعة لمباشرة عملية إعتراض المراسلات وتسجيل الأصوات والتقاط الصور.....	85
أولا: وضع الترتيبات التقنية.....	85
ثانيا: تسخير الأعوان المؤهلين	85
ثالثا: تحرير محضر عن العمليات.....	86
رابعا: نسخ ووصف وترجمة التسجيلات.....	86
خاتمة.....	87-89
قائمة المراجع.....	90-97
فهرس المحتويات.....	98-103

الملخص:

العالم اليوم وفي ظل الثورة المعلوماتية والتطور التكنولوجي شهد ميلاد نوع جديد من الجرائم يعرف بالجرائم الإلكترونية، و مما زاد من حدة هذه الجرائم انتشار الانترنت، وذلك نتيجة للاستخدام السيئ للمعلوماتية أو الحاسوب الذي نتجت عنه عدة أضرار لا يمكن حصرها، وذلك لأنها تهدد أمن المعطيات من جهة و تمس بحرية الأفراد من جهة أخرى، ولأن الحماية الفنية مهما بلغت درجتها من التعقيد والصعوبة فهي لا تستطيع مواكبة الجريمة المعلوماتية ومقاومتها أمام التطور التقني الذي تشهده تقنية الاختراق، لذا من أجل مكافحة الجريمة الإلكترونية تطلب تكييف الإجراءات القانونية التقليدية و تعديلها، وإضافة آليات بحث و تجري متخصصة وفعالة مدعومة بتطوير التشريعات الوطنية ، تدريب الكوادر البشرية (قضاة، محققين، ضباط)، توفير التجهيزات التقنية اللازمة لجمع وتحليل الأدلة الرقمية.

الكلمات المفتاحية: الجريمة الإلكترونية، مجرم إلكتروني، الأساليب التقليدية، الأساليب الحديثة، التسرب الإلكتروني، مراقبة الاتصالات الإلكترونية.