الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

الرقم التسلسلي: .....

جامعة الشاذلي بن جديد –الطارف

كليّة الحقوق والعلوم السياسية

مذكرة بعنوان

التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري

مذكرة لاستكمال متطلبات الحصول على شهادة ماستر أكاديمي في تخصص

قانون جنائي وعلوم جنائية

اعداد الطالبتين

- حريزي زبيدة
- أونيسة رشاء

إشراف الأستاذة

د/مقدم رشا

لجنة المناقشة

الاسم واللقب	الرتبة	الهيئة المستخدمة	الصفة
د/ غرايبية خولة	أستاذ محاضر-ب	الشاذلي بن جديد -الطارف	رئيسا
د/ مقدم رشا	أستاذ محاضر-أ	الشاذلي بن جديد -الطارف	مشرفا ومقررا
د/ قريمس سارة	أستاذ مساعد -أ	الشاذلي بن جديد-الطارف-	ممتحنا

السنة الجامعية: 2025/2024

بسم الله الرحمن الرحيم

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد
UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): .....

الحامل لبطاقة التعريف الوطنية رقم: .....

الصادرة بتاريخ: .....

عن دائرة: .....

المسجل بقسم: .....

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

.....

.....

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06/11

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne Démocratique et Populaire

وزارة التعليم العالي والبحث العلمي

جامعة الشاذلي بن جديد - الطارف

كلية الحقوق والعلوم السياسية

قسم الحقوق

Minister de L'enseignement Supérieur

Et de La Recherche Scientifique

Université el tarf

Faculté de Droit et des Sciences Politiques

Département de Droit

جامعة الشاذلي بن جديد

UNIVERSITE CHADLI BENDJEDID

المرجع: القرار الوزاري رقم 1082 المؤرخ في 27 ديسمبر 2020 المحدد للقواعد المتعلقة بالوقاية من السرقة العلمية ومكافحتها

تصريح شرفي
خاص بالالتزام بقواعد النزاهة العلمية

أنا الممضي أدناه،

السيد (ة): حريز كريمة

الحامل لبطاقة التعريف الوطنية رقم: 110008245000005

الصادرة بتاريخ: 2019-11-20

عن دائرة: بوثلجة

المسجل بقسم: الحقوق

والمكلف بإنجاز مذكرة تخرج ماستر عنوانها:

التعسف في الحق في الشريعة والقانون دراسة مقارنة

أصرح بشرفي أني التزمت بمراعاة المعايير العلمية والمنهجية ومعايير الأخلاقيات المنهجية والنزاهة الأكاديمية المطلوبة في إنجاز البحث المذكور أعلاه.

التاريخ: 2025/06/11

إمضاء المعني

شكر و عرفان

شكر و عرفان

الحمد لله عزوجل ، وهو المستحق الثناء و الشكر دائما ، و الذي وفقني لإعداد هذا العمل و يسر لي إنجازه.

إلى من بلغ الرسالة و أدى الأمانة ، إلى نبي الرحمة و نور العالمين سيدنا محمد عليه أفضل الصلاة و السلام .

و عليه أتوجه بجزيل الشكر و الإمتنان إلى الأستاذة الكريمة "مقدم رشا" لقبولها الإشراف على هذه المذكرة و التي لم تبخل علينا بإرشاداتها القيمة و توجيهاتها لإثراء هذا العمل.

كما أشكر أعضاء اللجنة الموقرة لقبولهم مناقشة هذه المذكرة .

أتوجه بالشكر و التقدير أيضا إلى كل من ساعدنا من قريب أو من بعيد على إنجاز هذا العمل.

فأدعو الله أن يجازيهم خير الجزاء ، وأن يبارك في أوقاتهم.

إهداء

الحمد لله ما ضيع لي تعب ، و لا خيب لي سعي ، و لا نقص لي مجهود و لا ثبط لي حلم ، كان الله معي و لازال في كل سعي وراء النجاح فالحمد لله حتى ترضى و إذا رضيت و بعد الرضا.

أما بعد ، فإني أهدي هذا العمل أولا إلى نفسي ، التي لم تستسلم رغم التعب ، و سارت بخطى مثقلة بالحلم و الأمل ، أهديك هذا الإنجاز إعترافا بجهدك و إيمانا بحلمك الذي لم تتخلي عنه يوما.

إلى من أوصاني بهما الله برا و إحسانا والدي الكريمين ، اللذين كانا لي السند الذي لا يميل ، و الركن الذي لا ينهدم ، إليكما يا من غرستما في نفسي حب العلم و الإجتهاد ، و يا من سقيتماني من معين العطاء بلا حساب ، فمهما قلت و مهما سطرت ، ستظل حروفي عاجزة عن رد بعض فضلكما.

إلى أختي الغاليتين ، رفيقتا دربي و مصدر سعادتي ، كنتما الحضن الآمن و الإبتسامة التي تشجعني كلما تعبت ، شكرا لكل لحظة قرب و محبة. إلى العزيزين على قلبي تقي الدين وسندس، وجودكم إلى جانبي ودعمكم الصادق خلال هذه المرحلة كان من أجمل ما رافقني في رحلتي نحو التخرّج شكرا من القلب.

إلى زميلتي وشريكة دربي سلمى التي تقاسمت معي الجهد والسهر والعمل لإنجاز هذه المذكرة، لكِ كل الشكر والامتنان على إخلاصك وتفانيك، فلولا تعاونك لما اكتمل هذا العمل أدام الله صداقتنا و عطر قلبك بالفرح.

اللهم إجعل هذا العمل فاتحة خير لما هو قادم ، و وفقني لما فيه رضاك.

رشاء

الاهداء

الحمد الله حباً و شكرا و امتنان على البدء و الختام

" واخر دعواتهم ان الحمدالله رب العالمين"

لم تكن الرحلة قصيرة ولا الطريق محفوفا بالتسهيلات، لكنني فعلتها، فالحمدالله الذي يسر البدايات وبلغنا النهايات بفضله و كرمه .

اهدي هذا النجاح لنفسي الطموحة اولا ابتدت بطموح و انتهت بنجاح .

الى من احمل اسمه بكل فخر إلى من سعى طوال حياته لنكون افضل منه، الى من دعمني بلا حدود واعطاني بلا مقابل "ابي الغالي"

الى التي ساندتني والهمتني المواصلة مسيرتي وسهلت لي الشدائد بدعائها الى السراج الذي أنار لي الطريق "أمي الغالية" حفظها الله .

الى خيرة أيامي وصفوتها الى من كانوا لي سندا و دعما الى من غمروني بالحب و التوجيه إلى من هم السند و الكتف الذي لا يميل... اخوتي و اخواتي .

الى زميلتي التى تشاركنا لحظات التعب و الفرح طيلة مشوار هذا العمل، الى اصدقاء القربين إلى القلب .

وها نحن نختم هذا الجهد المتواضع بوجوه "ضاحكة مستبشرة"، حامدين الله على توفيقه راجين ان يكون ما قدمناه نوراً يضاف إلى مسيرتنا العلمية .

"حريزي زبيدة"

قائمة المختصرات:

المختصر	المعنى
ص	صفحة
ق ع	قانون العقوبات
د ط	دون طبعة
ط	طبعة
د س ن	دون سنة نشر
ق ع ج	قانون العقوبات الجزائري
ج ر ج	الجريدة الرسمية الجزائري

مقدمة

مقدمة

إن التطور الهائل الذي شهده كل من مجال تقنية المعلومات ومجال الاتصالات والاندماج المذهل الذي حدث فيما بعد، كان المحور الأساسي الذي قامت عليه تقنية المعلومات إذ أصبحت جميع القطاعات المختلفة تعتمد على أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتية، لما تتميز بين عنصرين السرعة والدقة في تجميع المعلومات وتخزينها ومعالجتها، ومن ثم نقلها وتبادلها بين الأفراد والشركات والمؤسسات المختلفة، داخل الدولة الواحدة أو بين عدة دول.

إلا أن هذا الجانب الإيجابي للتكنولوجيا المعلوماتية أفرز معه بعض الانعكاسات السلبية التي تولدت نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو قصد الإضرار بمصالح الأفراد والجماعات، فظهرت بذلك أنماط وصورة مستحدثة من الجرائم اصطلح الفقه على تسميتها بالجرائم الإلكترونية.

وقد انتشرت في الآونة الأخيرة وأصبحت ظاهرة جديرة بالنظر والإعتبار، ظاهرة الإجرام المستحدث الذي يتم عن طريق التكنولوجيا، ألا وهي الجريمة الإلكترونية، التي أصبحت ظاهرة تخترق المجتمع وتهدد دعائمه ولعله الجوهر والسبب الرئيسي لتجريم هذه الجريمة، وهو ما دعى المشرع الجزائري إلى سن التشريعات تتماشى مع المستجدات على الساحة الإجرامية.

أسفرت محاولات تطبيق النصوص التقليدية على هذه الأنماط الجديدة من الإجرام عن كثير من المشكلات القانونية، حيث يصعب في كثير من الأحيان العثور على أثر مادي للجريمة الإلكترونية، ولا يمكن أن تكتشف إلا بمحض الصدفة.

ويكاد من المستحيل تقدير مقدار الإجرام الإلكترونية التي تحدث في معظم الدول في جميع أنحاء العالم بسبب نقص التعريفات القانونية الموحدة للجريمة الإلكترونية وغموضها، ومع ذلك تشير الأدلة إلى أن معدلات الجرائم الإلكترونية أخذت في الزيادة مع استمرار معدلات الجرائم التقليدية.

وتكمن خطورة الجرائم الإلكترونية في كون العالم أصبح يعتمد أكثر فأكثر على الفضاء الإلكتروني، لاسيما في البنى التحتية المعلوماتية العسكرية، المصرفية، الحكومية، المؤسسات، الشركات العامة

والخاصة. ولاشك أن إزدياد الجرائم الإلكترونية والتي تشهد جزءا كبيرا منها اليوم، يرتبط بزيادة هذا الاعتماد على شبكات الإنترنت والحاسوب والبنى التحتية الوطنية الأساسية، وهو يعني إمكانية تطوير الجرائم الإلكترونية لتصبح سلاحا حاسما في النزاعات بين الدول في المستقبل وقد أوجدت هذه التطورات التكنولوجية فرصا لا تعد ولا تحصى للمجرمين لإرتكاب أشكال مختلفة من الجرائم عبر الفضاء الإلكتروني، وتطورت هذه الظاهرة الإجرامية في الآونة الأخيرة تطورا مذهلا سواء في أشخاص مرتكبيها أو في أسلوب إرتكابها، والذي يمثل في استعمال آخر ما توصل إليه العلم وتطويعه في خدمة الجريمة.

كما تتميز الجرائم الإلكترونية بصعوبة متابعتها حيث أنها في الغالب لا تترك أثرا، فليست هناك أموال أو ممتلكات مفقودة، ونظرا لخطورة هذه الجرائم وتنوعها وخصوصيتها جعلت من الإجراءات التقليدية لمكافحة الجريمة بصفة عامة عاجزة عن اكتشاف هذا النوع المستحدث من الجرائم وملاحقة مرتكبيها في حالة اكتشافها، فهي إجراءات لا تتوافق مع مسرح الجريمة الإلكترونية، الأمر الذي جعل مختلف التشريعات –من بينهم المشرع الجزائري– يستحدثون إجراءات أساسية ووسائل إثبات حديثة تواكب التطور الذي شهدته الجريمة الإلكترونية مما يستوجب تحول الدليل الجنائي من صورته التقليدية إلى صورته الرقمية الحديثة.

فأصبح من الضروري على جهات التحقيق الإعتماد على نوع جديد من الأدلة الإثبات الجنائي، والتي تعرف بالأدلة الجنائية الإلكترونية تلك التي تكتشف سر هذا النوع من الجرائم بما تفرضه من التحديات جديدة على القاضي الجنائي. حيث ساهمت الثورة التكنولوجية في مجال العولمة والاتصال في استحداث وسيلة تقنية حديثة سهلت عملية الإثبات الجنائي، ويتعلق الأمر بالدليل الإلكتروني، هذا الأخير أصبحت له مكانة خاصة ودور فعال في التصدي للجريمة وإثباتها ومعرفة مرتكبيها، بالرغم من هذه المزايا لهذا النوع الحديث من الأدلة الذي يشكل جزءا هاما من الحياة الخاصة بالأفراد.

تظهر **أهمية موضوع** دراستنا هذه من حيث حداثته وإندراجه ضمن القسم الإجرائي في القانون الجزائي، هو مجال لا يزال في طور الاستكشاف والتحليل على مستوى الفقه الجزائي. فقد اقتصرت معظم الدراسات المنشورة حول الجريمة الإلكترونية على الجوانب الموضوعية دون التعمق في مسألة إثبات

هذه الجرائم وتأثير خصائصها على الإجراءات القانونية المناسبة. وعلى الرغم من أن الجرائم الإلكترونية تعد من الظواهر الإجرامية التي نشأت حديثا نتيجة الثورة في تكنولوجيا المعلومات والاتصالات عن بعد، فهي تمثل مستجدات لم يكن القانون الجزائي سواء الموضوعي أو الإجرائي على دراية بها سابقا، ومن ثم فإن أي محاولة للتعامل مع هذا النوع من الجرائم إجرائيا –خاصة في سياق البحث – ستواجه إشكالات قانونية يجب أن تتناولها الدراسات القانونية بالشرح والتحليل.

كما تبرز **أهمية هذا البحث كذلك،** في كونه يركز على الجرائم الإلكترونية بإعتبارها جرائم جديدة أين لا يمكن أن تُطبق عليها نفس الإجراءات المتبعة في الجرائم التقليدية، مما يفرض خصوصية في تعامل جهات التحقيق معها، لاسيما أن التحقيق في هذه الجرائم يتم عادة في وقت قريب من وقوعها أو فور حدوثها، مما يتيح فرصة مناسبة لجمع الأدلة ذات الطابع الخاص، ويعتبر الدليل الإلكتروني الركيزة الأساسية لإثبات الجرائم الإلكترونية، إذ يتطلب جمعه وحفظه إجراءا دقيقا لضمان ملائمته وقبوله قانونيا، حيث أن التعامل السليم مع هذا النوع من الأدلة يضمن تحقيق العدالة ويجنب فقدانها أو تلفها.

يرجع اختيار موضوع مذكرتنا هذه الموسوم بعنوان "**التحقيق الجنائي في الجرائم الإلكترونية وإثباتها في التشريع الجزائري**" في حقيقة الأمر إلى **دوافع ذاتية ودوافع موضوعية، فالأسباب الذاتية** تكمن في إهتمامنا بمجال الجريمة الإلكترونية التي تندرج ضمن تخصصنا في الماستر القانون الجنائي والعلوم الجنائية، وما يلقاها من جرائم، إضافة إلى الرغبة الكبيرة في إثراء المعرفي الخاص بهذا الصنف من الجرائم الفتاكة والتي انتشرت في الآونة الأخيرة انتشارا كبيرا داخل المجتمعات العالمية ولاسيما في الجزائر، وهو ما يثير العديد من التساؤلات في الأذهان.

أما عن **الأسباب الموضوعية** فتكمن في طرح موضوع دراستنا للعديد من الإشكالات القانونية نظرا لكثرة استخدام التكنولوجيا والأنترنت في حياتنا اليومية، كما أنها تندرج تحت فئة الجرائم السبيرانية وتشمل عدة جرائم كالاحتيال الإلكتروني، السرقة الإلكترونية، التجسس وإختراق النظام الإلكتروني و غيرها من الجرائم السيبيرانية، والتي لابد من الوقوف عليها نظرا لحداثة الموضوع من الجانب الموضوعي لتجريم الأفعال والإعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات وكذا القواعد الإجرائية الحديثة التي

جاء بها قانون الإجراءات الجزائية المعدل والمتمم، والقانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما.

قد واجهنا خلال دراسة موضوع مذكرتنا هذه بعض **الصعوبات،** تمثلت أساسا في نقص المراجع المتخصصة في التحقيق الإلكتروني وتلك التي تدرس الإجراءات المستحدثة للتحقيق، بالإضافة إلى ندرة المراجع التي تُعنى الدليل الإلكتروني الذي يكاد يخلو من المراجع، ضف إلى ذلك صعوبة البحث في هذا الموضوع لاتصاله بالجانب العلمي التقني الذي يتعلق بالمعطيات الآلية الذي يتطلب في حقيقة الأمر دراسة ميدانية، خاصة وأن الإجتهاد القضائي محجف نوعا ما بخصوص هذا النوع من الجرائم.

نهدف من خلال دراسة موضوع " التحقيق الجنائي في الجرائم الأكترونية وإثباتها في التشريع الجزائري "، إلى:

- تحديد المفاهيم الأساسية المتعلقة بالجريمة الإلكترونية.
- تبيان وتحديد الإجراءات المتبعة في التحقيق الجنائي المتعلق بالجريمة الإلكترونية.
- النظر في مدى حجية الدليل الإلكتروني في الإثبات الجنائي وتكوين قناعة القاضي.

على ضوء ما تقدم ذكره يمكننا طرح **الإشكالية** التالية: **فيما تتمثل أساليب التحقيق والكشف عن الجرائم الإلكترونية في الجزائر ؟ وهل هي كافة لضبط وإثبات هذا النوع من الجرائم ؟**

للإجابة على الإشكالية المطروحة أعلاه اتبعنا **المنهج الوصفي التحليلي** كونه الأنسب لمثل هذه الدراسات، كونه يتطرق إلى **وصف** ظاهرة الجريمة الإلكترونية من خلال ذكر التعريف والخصائص والأركان الخاصة بكل جريمة من جهة، ومن جهة أخرى يُعنى بتحليل مختلف المفاهيم القانونية المتعلقة بالموضوع وشرح عدة قواعد قانونية من قانون الإجراءات الجزائية المعدل والمتمم والقانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما.

من أجل دراسة موضوع بحثنا بطريقة منهجية ومحكمة إرتأينا من خلال هذه الدراسة إلى تقسيم الموضوع إلى فصلين، **الفصل الأول** نعالج **فيه "ماهية التحقيق الجنائي في الجرائم الإلكترونية في**

التشريع الجزائري "، وقسمناه إلى مبحثين تناولنا في **المبحث الأول** " مضمون الجريمة الإلكترونية في التشريع الجزائري "، أما **المبحث الثاني** " أساليب البحث والتحري عن الجرائم الإلكترونية في الجزائر".

بينما خصصنا **الفصل الثاني** لدراسة **"الدليل الإلكتروني كأداة إثبات في الجرائم الإلكترونية"** قسمناه إلى مبحثين، **المبحث الأول** " ماهية الدليل الإلكتروني ومشروعيته "، أما **المبحث الثاني** "سلطة القاضي الجنائي في تقدير الدليل الإلكتروني".

الفصل الأول

ماهية التحقيق الجنائي للجريمة الإلكترونية في التشريع الجزائري

تمهيد

في خضم التطور التكنولوجي الهائل الذي يشهده عالمنا المعاصر وخاصة في مجال الإتصالات، فقد أسهمت هذه التكنولوجيا في تحسين العديد من المجالات، لكنها في الوقت ذاته أدت إلى ظهور تأثيرات سلبية، مما ساهم في إنتشار ظاهرة تعرف بالجريمة الإلكترونية التي تعد واحدة من أخطر الجرائم المعاصرة. وتتميز هذه الجرائم بخصائص تجعلها تختلف عن الجرائم التقليدية، مثل الدقة العالية والتقنية المتطورة المستخدمة في إرتكابها، فضلا عن صعوبة اكتشافها والتحقيق فيها .بناء على ذلك قمنا بتقسيم هذا الفصل إلى مبحثين:

-المبحث الأول: مفهوم الجريمة الإلكترونية.

- المبحث الثاني: الأجهزة المعنية بالبحث والتحري في الجريمة الإلكترونية.

المبحث الأول: مضمون الجريمة الإلكترونية

يعد التحقيق الجنائي أداة محورية في كشف ملابسات الجرائم على إختلاف أنواعها، وتقديم الأدلة الدامغة التي تثبت تورط مرتكبيها. فالتحقيق كما يوحي اسمه يهدف إلى إستجلاء الحقيقة كاملة وصولا إلى إدانة المتهم. وسعيا لإلقاء الضوء على التحقيق الجنائي في مجال الجرائم الإلكترونية، نتطرق إلى تحديد مفهوم الجريمة الإلكترونية من خلال المطلب الأول، ومن ثم نتطرق إلى تصنيفات الجرائم الإلكترونية في القانون الجزائري في المطلب الثاني.

المطلب الأول : مفهوم الجريمة الإلكترونية

إكتنفت الجريمة الإلكترونية عدة تعريفات متباينة، بين التصنيف والتوسيع، وإنعكس هذا التنوع على المصطلحات المستخدمة للإشارة إليها، فنجد من يستخدم " الإجرام المعلوماتي " أو " الإجرام السيبيراني "، بينما يفضل آخرون يفضلون استخدام مصطلح "الجرائم المعلوماتية"، كما ظهر مصطلح "جرائم إساءة إستخدام تكنولوجيا المعلومات والإتصال"، كمحاولة لمواكبة التطورات المتسارعة في هذا المجال، وقد تبناه مشروع القانون العربي النموذجي الموحد الصادر عن جامعة الدول العربية في عام 2004[1].

الفرع الأول: تعريف الجريمة الإلكترونية وأطرافها

تُصنف الجرائم الإلكترونية ضمن الجرائم المستخدمة التي نشأت في عصرنا الراهن، وإكتسبت هذه التسمية نظرا لإعتمادها على الحواسيب والتقنيات الإلكترونية في تنفيذها، إذ يقع الفعل الإجرامي في بيئة معلوماتية أو عبر إحدى الشبكات المعلوماتية.

ونتجة لذلك تباينت تعريفات الجريمة الإلكترونية وفقا لمعايير مختلفة، سواء بالإستناد إما على وسيلة إرتكابها أو موضوعها، أو على أساس المعرفة الفنية بإستخدام الحاسوب، وقد يجمع البعض بين أكثر من معيار في تعريفها. و هذا ما سوف نستعرضه في النقاط التالية:

[1] سهام بن عنطر، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة مومولود معمري-تيزي وزو، الجزائر، 2023، ص 5.

أولا: التعريف الفقهي للجريمة الإلكترونية

لقد إختلف الفقهاء حول تعريفهم للجريمة الإلكترونية، حيث إعتمد كل إتجاه على معيار معين في ذلك:

أ- تعريف الجريمة الالكترونية بالاستناد إلى معيار وسيلة إرتكابها: يرتكز أصحاب هذا الرأي في تعريف الجريمة الإلكترونية بالنظر إلى الطريقة التي تنفذ بها، ويؤكدون على ضرورة وقوعها عن طريق جهاز الكمبيوتر، فعرفوها بأنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب عن طريق الحاسب الآلي"[1]، أو هي:"كل فعل إجرامي يستخدم الحاسب الآلي في إرتكابه كأداة رئيسية".

كما عرفها الفقيه الألماني Tideman، بأنها:"كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب بإستخدام الحاسب" [2].

ب- تعريف الجريمة بالإستناد إلى المعرفة الفنية بإستخدام الحاسوب: يعتمد مؤيدو هذا الإتجاه على المعرفة الفنية أو التقنية بإستخدام الحاسوب، بمعنى آخر يعتمدون على معيار شخصي يتطلب أن يكون الفاعل على دراية بتقنيات المعلومات وإستخدام الحاسوب، حيث عرفوا هذا النوع من الجرائم، بأنها:" نشاط غير موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب والتي تقع عن طريقه"[3].

كما عرفها الفقيه دافيد توسون David Thopson، بأنها:" أي جريمة يتطلب لإقترافها أن تتوفر لدى المجرم فنيات باستعمال الحاسوب"[4].

ج- تعريف الجريمة الإلكترونية بالاستناد إلى موضوعها: يستند أنصار هذا الاتجاه في تعريفهم للجريمة الإلكترونية إلى وجوب أن يكون الكمبيوتر محلا للجريمة، أي يجب أن يتم الاعتداء على الحاسب

[1] حنان ريحان مبارك المنحكي، الجرائم المعلوماتية-دراسة مقارنة، الطبعة 1، منشورات الحلبي الحقوقية، بيروت-لبنان، ص 25.

[2] سامي علي حامد عياد، الجريمة المعلوماتية وجرائم الانترنت، دار الفكر الجامعي، الإسكندرية – مصر،2007، ص 38.

[3] نفس المرجع.

[4] نوال شاين، "الجريمة الإلكترونية في التشريع الجزائري: ماهيتها، موضوعها، خصائصها ومظاهر تحدياتها"، مجلة سوسولوجيا، جامعة الحاج لخضر-باتنة 1، الجزائر ، المجلد 06، العدد 02، 2022، ص 64.

الآلي أو نظامه، يشمل هذه الإعتداءات سرقة أو تقليد أو إتلاف أو تعطيل برنامج الحاسوب، بالإضافة إلى إفشاء محتوياته أو حذفها أو تغييرها أو تزويرها أو نسخ المعلومات المعالجة. حيث عرفوا الجريمة الإلكترونية، بأنها:" نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول للمعلومات المخزنة داخل النظام أو التي تحول عن طريقه، ويندرج هذا النوع تحت جرائم المعالجة الآلية للبيانات"[1].

أما بالنسبة **للتعريف القانوني للجريمة الإلكترونية**، إعتمد المشرع الجزائري مصطلح "الجرائم المتصلة بتكنولوجيا الإعلام والإتصال"، حيث عرفها بموجب نص المادة 02 من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، بأنها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو تسهيل إرتكابها عن طريق منظومة معلوماتية، أو نظام الإتصالات الإلكترونية"[2].

من خلال هذا التعريف، يتضح بأن المشرع الجزائري إعتمد على معيار دور النظام المعلوماتي لتحديد معالم الجريمة، حيث أطلق على الجرائم الموجهة ضد النظام المعلوماتي اسم "جرائم المساس بأنظمة المعالجة الآلية للمعطيات"، كما هو موضح في قانون العقوبات[3]، من نص المادة 394 مكرر إلى نص المادة 394 مكرر 07، وقد ترك المجال مفتوحا لأي جريمة أخرى قد ترتكب عبر منظومة معلوماتية ونظام الإتصالات الإلكترونية.

وفقا للمشرع الجزائري يمكن أن تتحقق الجريمة الإلكترونية بمجرد وقوع الجريمة أو تسهيل إرتكابها عبر منظومة معلوماتية أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف شاملا لعدد كبير من الجرائم كما يتضمن هذا التعريف تكرار لمفهوم نظام الإتصالات الإلكترونية، الذي يندرج ضمن مصطلح

[1] أحمد خليفة الملط، الجرائم المعلوماتية-دراسة مقارنة، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية-مصر، 2006، ص ص: 85 و86.

[2] القانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد رقم 47، ص 5.

[3] القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2001، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 08 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية، العدد رقم 71، 1966.

المنظومة المعلوماتية[1]، وقد أحسن المشرع في تعريفه، حيث جعله شاملا يضم جميع الوسائط الإلكترونية على عكس التعريفات الفقهية التي إقتصرت على الحاسب.

ثانيا: أطراف الجريمة الإلكترونية

لتحقيق أي جريمة بشكل عام يتطلب وجود شخص أو طرف يقوم بالنشاط الإجرامي والذي يعرف بالمجرم، بالإضافة إلى وجود الطرف المستهدف من هذا النشاط والذي يطلق عليه الضحية. وينطبق هذا الأمر أيضا على الجرائم الإلكترونية، حيث يتواجد ما يعرف بالمجرم الإلكتروني وكذلك الضحية في هذا النوع من الجرائم.

أ-المجرم الإلكتروني: إستنادا إلى مبدأ أن الجريمة تتطور بإستمرار وأن الإجرام لا يعرف حدودا، فقد أدى التقدم التكنولوجي في مجالات الإتصال والمعلوماتية إلى ظهور نوع جديد من المجرمين يعرف بـ" المجرم الإلكتروني "، حيث يتميز هذا النوع من المجرمين عن المجرمين التقليديين من حيث الخصائص والدوافع، إذ يتمتع المجرم الإلكتروني بعدد من الميزات التي يستخدمها لإرتكاب الجرائم الإلكترونية وتختلف هذه الميزات بإختلاف مستوى خبرة المجرم سواء كان مبتدئا أو محترفا في هذا المجال. ومن أبرز هذه السمات يمكن الإشارة إلى الذكاء المعلوماتي الذي يمتلكه المجرم الإلكتروني وتخصصه في هذا مجال الإجرام المعلوماتي[2]، كما أن دوافع المجرم الإلكتروني تتنوع بناءً على مستوى وعيه ونوعه.ومن بين أنواع المجرمين الإلكترونيين نجد:

1- القراصنة: يمكن تصنيفهم إلى صنفين:

1-1-الهاكرز Hackers: هي طائفة من المتطفلين يتحدون إجراءات أمن النظام والشبكات، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية، وإنما ينطلقون من دوافع التحدي وإثبات المقدرة، فإصطلاح الهاكرز مرادف في الغالب لهجمات التحدي.

[1] عائشة نايدي، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، تخصص قانون إداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دارية -أدرار، الجزائر، 2017/2016، ص 09.

[2] سهام بن عنطر، المرجع السابق، ص 10.

كما يعرف الهاكرز بأنهم الأشخاص اللذين يخترقون جهازك، فيستطعون مشاهدة ما به من ملفات أو سرقتها أو تدمير جهازك أو التلصص أو مشاهدة ما تفعله على شبكة الإنترنت.

فمن خلال الدخول إلى أنظمة الحاسبات الآلية غير المصرح لهم بالدخول إليها وكسر الحواجز الأمنية الموضوعة لهذا الغرض، يكون الهدف الأساسي لهذا النوع من الشباب هو إثبات الذات أو الفضول، حيث يعتبر ذلك محفزا أساسيا لهم[1].

1-2-الكراكز Chackers: إصطلاح الكراكز مرادف للهجمات الحاقدة والمؤذية، وهم الأشخاص الذين يقمون بالتسلل إلى أنظمة المعالجة الآلية للإطلاع على المعلومات المخزنة بها وإلحاق الضرر أو العبث بها أو سرقتها[2].

وتعد هذه الطائفة الأخطر من بين مجرمي المعلوماتية، حيث تهدف إعتداءاتهم بالأساس إلى تحقيق الكسب المادي لهم أو للجهات التي كلفتهم وسخرتهم لإرتكاب جرائم الحاسوب، كما تهدف إعتداءات بعضهم إلى تحقيق أغراض سياسية والتعبير عن موقف فكري أو نظري أو فلسفي، وأفراد هذه الطائفة يتسمون بالتكتم خلافا للطائفة الأولى، فلا يتبادلون المعلومات بشأن أنشطتهم بل يطورون معارفهم الخاصة ويحاولون ما أمكن عدم كشف طرقهم التقنية لإرتكاب جرائمهم[3].

2- الحاقدون: يحرك أنشطة هذه الفئة الرغبة بالإنتقام والثأر كأثر لتصرف صاحب العمل معهم أو لتصرف المنشأة المعنية معهم عندما لا يكونون موظفين فيها، وتغلب على أنشطتهم من الناحية التقنية استخدام تقنيات زراعة الفيروسات والبرامج الضارة وتخريب النظام[4].

---

[1] شفيقة خنيفر، الجريمة الإلكترونية (الواقع والتحديات)، مداخلة ملقاة في يوم دراسي، حول:" الاجرام الإلكتروني كفاءات ضائعة في عالم التقنية"، جامعة محمد الشريف مساعدية -سوق أهراس، الجزائر، 2022،ص 07.

[2] نفس المرجع.

[3] فاطمة شرويلي، فضيلة ديدي، آليات مكافحة الجريمة الإلكترونية، مذكرة ماستر، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة صالحي أحمد-النعامة، الجزائر، 2023/2022، ص 21.

[4] المرجع نفسه، ص 08.

3- الهواة The kids: من يرتكبون هذه الجرائم بغرض التسـلية دون أن تكون لديهم نية إحداث أضرار بالمجني عليهم، وتتميز هذه الفئة بصغر سنهم ونبوغهم في علوم الحاسوب، إلا أن خطورتهم تكمن في أنهم قد يكونوا نواة جيدة للتحول إلى قرصان محترف[1].

يظهر من خلال نص المادة 394 مكرر 4 من قانون العقوبات المعدل والمتتم، أن المجرم في هذه الجريمة قد يكون شخصا طبيعيا -كما قد سبق وأن ذكرنا-، كما قد يكون شخصا معنويا، حيث نصت على أنه:" يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم ..". وهذا الأخير يتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات.

ب-الضحية الإلكترونية: بعد أن أصبحنا على دراية بالمجرم الإلكتروني كأحد أطراف الجريمة الإلكترونية، سننتقل إلى الطرف الآخر ألا وهو الضحية، يجب أن ندرك أن تأثير هذه الجريمة لا يقتصر على الشخص المتضرر فقط بل يمتد ليشمل جميع من تضرروا من الجريمة الإلكترونية. فقد يقع ضحية لجريمة إلكترونية أشخاص طبيعية أو أشخاص معنوية[2]، حيث يشمل هذا النوع الأخير المؤسسات والشركات سواء كانت عامة أو خاصة. وعلى هذا الأساس سوف نتطرق إلى التعرف على هاتين الفئتين من ضحايا الجريمة الإلكترونية كما يلي:

1-الضحية الشخص الطبيعي في الجريمة الإلكترونية: ازدادت حالات الاعتداء الناجمة عن الجريمة الالكترونية مع زيادة إستخدام الأفراد للحواسيب والأجهزة الذكية خاصة مع الإقبال المتزايد على الخدمات التي توفرها شبكة الإنترنت، الذي يصل أحيانا إلى حد الإدمان، حيث أصبح سهلا على المجرم الإلكتروني اصطياد ضحياه من خلال قرصنة حواسيبهم أو هواتفهم عن طريق اختراق البريد الالكتروني أو الحسابات التي ينشئها الأفراد على شبكات التواصل الإجتماعي، مما يؤدي إلى تشهير

[1] سهام بن عنطر، المرجع السابق، ص 11.

[2] أنظر القانون رقم 04-15 المؤرخ في 25 ديسمبر 2004، المعدل و المتمم للأمر رقم 66-156 المؤرخ في 08 جوان 1996، المتضمن قانون العقوبات.

الأفراد من خلال نشر صورهم وإتاحتها للجمهور مقابل الحصول على مكاسب قد تكون في أغلب الحالات مالية[1].

والملاحظ أنه في كثير من الحالات لا يبادر الضحايا إلى الإبلاغ عن هذه الجرائم خشية على سمعتهم داخل الأسرة والمجتمع، الأمر الذي لا يساعد على مكافحة الجريمة الإلكترونية ويجعل الجناة يفلتون من العقاب، بل إن عزوف الضحايا عن التبليغ يشجع الجناة على مواصلة نشاطهم الإجرامي من خلال إستمرارهم ومواصلتهم في إصطياد ضحايا آخرين.

في بعض الأحيان وبعد تردد قد يبادر بعض الأفراد إلى التبليغ عن هذه الجرائم لكن بشكل متأخر، هذا التأخير يعيق جهات التحقيق عن تتبع الجاني، خاصة أن الجرائم الإلكترونية تتطلب سرعة في إتخاذ الإجراءات بسبب طبيعتها وخصائصها التي تشكل عقبة أمام جهات التحري والتحقيق.

2- الشخص المعنوي كضحية في الجريمة الإلكترونية: تشكل الجرائم الإلكترونية تهديدا كبيرا للأشخاص المعنوية، سواء كانت حكومية أو خاصة فهي تستهدف عددا من الضحايا في آن واحد وتؤثر على مصالح حيوية للدولة، خاصة إذا ما تعلق الأمر بمنشآت حساسة كتلك المتعلقة بالدفاع والأمن الوطنيين.

إن ما ذكرناه سابقا بخصوص إحجام الأفراد أو الأشخاص الطبعيين عن التبليغ لدى وقوعهم ضحايا لجريمة الكترونية ما، فإنه ينطبق كذلك على تلك الحالات التي يكون فيها الضحايا من الأشخاص المعنويين، حيث تبرز في هذا السياق المؤسسات المالية والبنوك كأكثر الأشخاص المعنوية عزوفا عن التبليغ وذلك خشية فقدان العملاء والزبائن بها، فتفقد بالتالي سمعتها وقيمتها بين المنافسين لذلك تعمدت الكثير من البنوك إلى التستر على تلك العمليات التي تتعرض لها أنظمتها المعلوماتية من قرصنة وإتلاف وتجسس وغيرها من الجرائم الإلكترونية[2].

[1] إسماعيل بن يحي، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، تخصص القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد – تلمسان، الجزائر، 2021/2020، ص ص: 34 و35.

[2] نفس المرجع، ص ص: 35 و36.

الفرع الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بخصائص وصفات تميزها عن غيرها من الجرائم الأخرى التقليدية، ومن بين أهم الخصائص نذكر مايلي:

أولا: الجريمة الإكترونية جريمة عابرة للحدود

أعطى إنتشار شبكة الانترنت إمكانية ربط الأعداد الهائلة من أجهزة الحاسوب بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، لذلك فإن من السهولة أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر، وهذا ما يظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها، حيث أن التشريعات الداخلية متفاوتة بين كل دولة من دول العالم وتظهر العديد من المشاكل حول صاحب الإختصاص القضائي لهذه الجريمة وإشكالات أخرى متعلقة بإجراءات الملاحقة القضائية[1].

ثانيا: صعوبة إثبات الجريمة الإلكترونية

إكتشاف الجريمة الإلكترونية أمر ليس بالسهل و لكن حتى في حال إكتشاف وقوع هذه الجريمة و الإبلاغ عنها فإن الإبلاغ عنها أمر يحيط به الكثير من الصعاب، فالجريمة الإلكترونية تتم في بيئة غير تقليدية حيث تقع خارج إطار الواقع الملموس لتقوم أركانها في بيئة الحاسوب والإنترنت مما يزيد الأمور أكثر تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة مما يطيل إجراءات إثباتها[2].

ثالثا: الجريمة الإلكترونية أقل عنفا وجهدا في التنفيذ

لا تتطلب الجرائم الإلكترونية عنفا للتنفيذها، بل تُنفذ بأقل جهد ممكن مقارنة مع الجرائم التقليدية التي تتطلب نوعا من الجهد العضلي، الذي قد يكون في صورة ممارسة العنف والإيذاء. وعلى هذا

[1] أمحمد اقبلي , عبابد العمراني الميلودي , القانون الجنائي الخاص المعمق في الشروح , ط1, 2020.

[2] نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 2، دار الشفافة، عمان، 2010، ص 56.

الأساس تتميز هذه الجرائم بأنها جرائم هادئة أو الناعمة، حيث لا تحتاج إلى عنف وكل ما تحتاج إليه هو عامل الخبرة، الذكاء والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني في إرتكاب الأفعال غير المشروعة[1].

رابعا: الجريمة الإلكترونية جريمة مستحدثة

الجريمة الإلكترونية جريمة مستحدثة، بل أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، بحيث ظهرت تبعا للتطور الهائل في مجال التقنية العالمية، وهو ما جعل أمر تحديد هذا النمط من الإجرام وإدراجه ضمن طائفة الجرائم التقليدية المعروفة تكتنفه صعوبات ترجع إلى الطبيعة الخاصة بإعتبارها إتصال المعلومات[2].

خامسا: قلة الإبلاغ عن الجرائم الإلكترونية

لا يتم التبليغ عن الجرائم الإلكترونية في الغالب، لذا نجد أن معظم الجرائم الإلكترونية تم إكتشافها بمحض الصدفة، بل وبعد وقت طويل من إرتكابها، وقد يرجع عدم الإبلاغ عن هذه الجرائم إلى عدة أسباب منها عدم إكتشاف الضحية لها، خشية من التشهير حيث هذه الجرائم لا تترك أثرا ماديا ملموسا بعد إرتكابها فليست هناك أموال أو مجوهرات مفقودة، وإنما هي أرقام تشفير في السجلات[3].

الفرع الثالث: أركان الجريمة المعلوماتية

تتمثل الجريمة الإلكترونية في الفضاء الإفتراضي كمسرح لإرتكابها مما يمنحها خصائص مميزة، إلا أن ذلك لا يعني وجود أوجه التشابه بينها وبين الجريمة التقليدية أو المادية فهي تشترك في العنصر الأساسي المتمثل في الفعل غير المشروع، حيث يقوم الجاني بتنفيذ هذا الفعل. ومن خلال هذا الشبه نتسائل عن شرح الأركان التي تقوم عليها هذه الجريمة[4].

---

[1] شوقي يقشب تمام، الجريمة المعلوماتية دراسة تأصيلية مقارنة، الطبعة 1، مطبعة الرمال، الوادي-الجزائر، 2019، ص ص: 29 و30.

[2] امحمد اقبلي، المرجع السابق، ص 287.

[3] سعدات محمود فتوح محمد، خصائص الجريمة المعلوماتية وصفات مرتكبيها في ظل مجتمع معلوماتي، انظر الرابط: http//www noor-book.com.

[4] عمار حشمان، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرباح-ورقلة، الجزائر، 2019/2018، ص 12.

أولا: الركن الشرعي للجريمة الإلكترونية

تدخل المشرع لتجريم الأفعال غير المشروعة والضارة بنص قانوني، فالمشرع الجزائري من خلال القانون رقم 04-15 المؤرخ في 10 نوفمبر 2004 أدرج قسما خاصا لحماية أنظمة المعالجة الآلية للمعطيات ضمن القسم السابع مكرر بمحتوى المادة من 394 مكرر الى 394 مكرر 7. هذا التشريع يعكس إهتمام المشرع بحماية البيانات الشخصية وحمايتها من الإعتداءات، التي قد تحدث بإستخدام وسائل التكنولوجيا الحديثة. كما أقر المشرع الجزائري حماية خاصة للأفراد من خلال القانون رقم 06- 23 المؤرخ في 20 ديسمبر 2006 الذي يتضمن تعديل المادة 303 من قانون العقوبات بهدف مواجهة الاستخدام السيء للتكنولوجيا والتعدي على الحياة[1].

ثانيا: الركن المادي للجريمة الإلكترونية

يشير الركن المادي للجريمة الإلكترونية إلى العناصر الملموسة التي تشكل الجريمة وتعتبر جزءا أساسيا في تحديد طبيعة الجريمة الإلكترونية، حيث يتكون الركن المادي من عدة عناصر أساسية، هي:

أ- **السلوك الإجرامي**: يتمثل في الأفعال التي يقوم بها الجاني مثل دخول الغير إلى أنظمة المعلومات أو التلاعب بالبيانات، وهذا السلوك يمكن أن يكون عن طريق الإختراق أو إتلاف المعلومات.

ب- النتيجة الإجرامية: وهي الآثار التي تحدث نتجة الفعل الإجرامي، مثل إتلاف البيانات أو تعطيل النظام المعلوماتي، في بعض الحالات قد تكون هذه النتيجة شكيلة، حيث تتحق الجريمة بمجرد القيام بالفعل دون الحاجة إلى تحقق أي ضرر مادي.

ج- العلاقة السيئة: يجب أن يكون هناك ترابط بين الفعل والنتيجة، حيث يؤدي السلوك الإجرامي إلى حدوث ضرر أو تأثير سلبي على النظام المعلوماتي.

وبشكل عام، يعتبر الركن المادي أساسيا لفهم الجرائم الإلكترونية، حيث يتطلب وجود بيئة رقمية

[1] إيمان بغدادي، أثر تعديل العقوبات الجزائرية في التصدي للجريمة المعلوماتية، مجلة الأفاق والدراسات، المركز الجامعي إليزي، الجزائر، العدد 04، 2019، ص 188.

ووسائل تقنية لتنفيذ الأفعال الإجرامية [1].

ثالثا : الركن المعنوي للجريمة الإلكترونية

إن الركن المعنوي في الجريمة هنا هو عبارة عن القصد الجنائي بعنصريه العلم والإرادة، فالفاعل لابد له من أن يكون على علم بأنه يقوم بفعل الدخول والبقاء غير المشروع في النظام المعلوماتي، ولابد من أن تكون إرادته متجهة لإرتكاب هذا الفعل[2].

كما إشترط المشرع توافر القصد الجنائي العام في جريمة إتلاف المعلومات، حيث يكفي علم الجاني بأنه يقوم بأعمال من شأنها أن تؤدي إلى تغيير الحالة التي كانت عليها المعلومات والمعطيات بمحوها أو إتلافها وأن تتجه إرادته إلى تحقيق ذلك، وبالتالي نجد أن معظم جرائم المعلوماتية إشترط فيها المشرع القصد الجنائي العام، حيث إكتفى بضرورة توافر القصد الجنائي العام لوحده لتوافر الركن المعنوي[3].

المطلب الثاني: تصنيفات الجرائم الإلكترونية في التشريع الجزائري

شهدت الجريمة الإلكترونية تباينا في تقسيماتها بسبب الإختلاف في تسميتها، حيث إستند كل إتجاه على معيار معين، فالبعض يصنفها حسب الأسلوب المتبع في إرتكابها، بينما يستند آخرون إلى دوافع إرتكابها، أو يعتمدون على تعدد محل الإعتداء أو تعدد الحق المعتدى عليه.

أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الإلكترونية إلى نوعين الأول يشمل الجرائم التي ترتكب بواسطة النظام المعلوماتي، والتي نص عليها المشرع دون تحديدها، و التالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الإعلام والإتصال (الفرع الأول)، أما الفرع الثاني من الجرائم يتمثل في تلك الجرائم

[1] ارتياس نذير، الجريمة الإلكترونية وحجة الدليل الرقمي في الإثبات الجنائي، الطبعة 1، المركز المغاربي، شرق أدنى للدراسات الاستراتجية، المملكة المتحدة –بريطانيا، جانفي 2024، ص 57.

[2] المحاضرة الثانية والثالثة، الجرائم الماسة بأنظمة المعالجة الآلية، انظر عبر الموقع .http// tele enc .umiv-oeb.bg

[3] امين بوشرة، سهام موسى، إطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة ماستر، تخصص قانون علوم جنائية، جامعة عبد الرحمان ميرة-بجاية، 2018/2017، ص 42.

الواقعة على النظام المعلوماتي، وقد حددها المشرع بموجب قانون العقوبات (الفرع الثاني). و هذا ما سيتم توضيحه في الفرعيين المواليين[1].

الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي

يشمل هذا التصنيف أهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الآلي في هذه الطائفة من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعف لجسامتها[2]. وهي أنواع تتمثل في الجرائم الإلكترونية الواقعة على الأشخاص، الجرائم الواقعة على الأموال والجرائم الواقعة على الأسرار. وسنوضح كل منها كالآتي:

أولا: الجرائم الإلكترونية الواقعة على الأشخاص بواسطة النظام المعلوماتي

يطلق بعض الفقهاء على هذا النوع من الجرائم مصطلح الإعتداء على جريمة الحياة الخاصة للأفراد بإعتبارها حق حماية الحياة الخاصة، ومن أهم الحقوق وذلك لما له من إرتباط وثيق بحرية الفرد[3].

كذلك هي الجرائم التي تنال بالاعتداء أو تهدد بالحظر الحقوق ذات الطابع الشخصي البحت، أي الحقوق اللصيقة بالشخص والتي تعتبر من بين المقومات الشخصية وتخرج عن دائرة التعامل الإقتصادي. ومن أهم الحقوق الحق في الحياة، الحق في سلامة الجسم، الحق في الحرية والحق في صيانة الشرف، ومن بين الجرائم التي تقع على الأشخاص منها: جريمة المضايقة والملاحقة، جريمة إنتحال الشخصية، وجرائم التشهير وتشويه السمعة[4].

---

[1] عائشة نايري، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، تخصص قانون إداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دراية-أدرار، الجزائر، 2017/2016، ص 24.

[2] سفيان سوير، جرائم المعلوماتية، رسالة ماجستير، تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم الساسية، جامعة أبو بكر بلقايد-تلمسان، الجزائر، 2011/2010، ص 33.

[3] مولاي براهيم عبد الحكيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، الجزائر، العدد 23، 2015، ص 216.

[4] عمار حشمان، المرجع السابق، ص 05.

ثانيا: الجرائم الواقعة على الأموال بواسطة النظام المعلوماتي

تستهدف أكثر تلك الجرائم تحديد عناصر الخدمة المالية ويكون الطمع وراء إرتكابها هو الحصول والإستيلاء على تلك الأموال، وفكرة المكسب السريع التي تحرك مرتكبها وقد ترتكب أحيانا لمجرد قهر نظام منشأة مثلا، وتخطي حواجز الحماية أو بدافع الإنتقام من صاحب تلك المنشأة أو أحد عناصرها كالسطو، السرقة، التحويل الإلكتروني غير المشروع للأموال، جريمة غسيل الأموال وقرصنة الحسابات الشبكية غير المشروعة[1].

ثالثا: الجرائم الإلكترونية الواقعة على الأسرار

تقع هذه الجرائم باستعمال النظام المعلوماتي لإفشاء الأسرار، سواء كانت الأسرار عامة أو خاصة تتعلق بالأفراد والمؤسسات المختلفة، يأخذ هذا النوع من الجرائم صورتين رئيسيتين: الأولى تتعلق بالجرائم الواقعة على أسرار الدولة[2]، حيث أتاحت الإنترنت للعديد من الدول فرصة التجسس على دول أخرى من خلال الحصول على الأسرار العسكرية والاقتصادية، خاصة في الدول التي تشهد نزاعات[3]، والصورة الثانية تتعلق بالجرائم الواقعة على أسرار المهنة، حيث يهدف إرتكاب هذه الجريمة إلى سرقة المعلومات بغرض التشهير بشخص أو جماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الأمر أو استخدامها للضغط على أصحابها من أجل إقناعهم بفعل شيء أو الإمتناع عن فعله[4].

وقد حرص المشرع الجزائري على حماية هذه الأسرار من خلال الباب الأول المتعلق بالجنايات والجنح ضد الشيء العمومي من نصوص المادة 21 إلى 96 مكرر من قانون العقوبات المعدل والمتمم، بالإضافة إلى نص المادة 394 مكرر 3، التي تنص على:" تضاعف العقوبات المنصوص عليها في هذا القسم

---

[1] بوديسة بجاد عبد الرؤوف ، االيات التحري عن الجريمة الالكترونية في القانون الجزائري، مدكرة ماستر في لقانون،تخصص قانون اعلام الي و انترنت، ص ص 28 و 29

[2] عائشة نايري، المرجع السابق، ص 26.

[3] يوسف صغير، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، تخصص القانون الدولي للأعمال، جامعة مولود معمري-تيزي وزو، الجزائر، 2013، ص 54.

[4] عائشة نايري، المرجع السابق، ص 26.

إذا استهدفت الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الإخلال بتطبيق عقوبات أشد "[1].

الفرع الثاني: الجرئم الواقعة على النظام المعلوماتي

يمس هذا النوع من الجرائم إما المكونات المادية للنظام المعلوماتي كالكابلات أو المكونات المعنوية (البرامج)، حيث يستلزم معرفة فنية عالية في مجال البرمجة وتقع هذه الجرائم إما على البرامج التطبيقية أو برامج التشغيل[2].

من أجل سد الفراغ الذي عرفه التشريع الجزائري في هذا المجال جاء القانون رقم 05- 15 الصادر في 10 نوفمبر 2004، المتضمن تعديل قانون العقوبات بتجريم كل أنواع الإعتداءات التي تستهدف أنظمة المعالجة الآلية للمعطيات، وقد ورد في النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات، وذلك في المادة 394 مكرر 07. وتأخذ صور الإعتداء صورتين وهما الدخول والبقاء في منظومة المعلومات (أولا)، كما تضمن صورة أخرى ألا وهي جريمة المساس بمنظومة معلوماتية (ثانيا)[3]. وهذا ما سنتاوله في النقاط التالية:

أولا: جريمتي الدخول والبقاء غير المشروعان في منظومة المعلومات

تنص المادة 394 مكرر من قانون العقوبات المعدل والمتمم، على أنه:" ...حيث يعاقب على الدخول إلى النظام أو البقاء غير المشروع في المنظومة المعلوماتية دون علم الضحية"[4].

[1] القانون رقم 04- 15 المؤرخ في 10 نوفمبر 2001، يعدل ويتمم الأمر رقم 66-156 المؤرخ في 08 جوان 1996، المتضمن قانون العقوبات، الجريدة الرسمية، العدد 71.

[2] عبد القادر فلاح، نادية آيت عبد المالك، "التحقيق الجنائي في الجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف-المسيلة، الجزائر، المجلد 04، العدد 02، 2019، ص 1697.

[3] عائشة نايري، المرجع السابق، ص 27.

[4] عبد القادر فلاح، نادية آيت عبد المالك، المرجع السابق، ص 1694.

إذ نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فإن العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء، بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع، إما محو أو تغيير في المعطيات الموجودة في النظام[1].

ثانيا: جريمة المساس بمنظومة معلوماتية

تنص المادة 394 مكرر 01 من قانون العقوبات المعدل والمتمم، على متابعة كل شخص يقوم بإدخال معطيات في نظام المعالجة الآلية أو يحذف أو يعدل هذه البيانات باستخدام الغش، ويتجلى هذا السلوك الإجرائي في ثلاثة صور، هي: الإدخال، المحو، التعديل، ولم يشترط المشرع إجتماع هذه الصور بل يكفي أن يصدر عن الجاني إحداهما فقط ليتوافر الركن المادي، تتضمن أفعال الإدخال، الإزالة، التعديل والتلاعب بالبيانات الموجودة في نظام المعالجة الآلية، سواء بإضافة بيانات جددية غير صحيحة أو محو أو تعديل بيانات موجودة مسبقا، هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الآلية، مثل إدخال فيروسات المعلوماتية في البرامج من أجل إتلافها[2].

[1] عائشة نايري، المرجع السابق، ص ص: 27 و28.

[2] نفس المرجع، ص 29.

المبحث الثاني: أساليب البحث والتحري عن الجرائم الإلكترونية في التشريع الجزائري

تعتبر مرحلة جمع المعلومات والمعطيات من أهم المراحل في الدعوى الجزائية، حيث تسبق المحاكمة وتتيح التعرف على من إرتكب الفعل ويطلق على هذه المرحلة التحقيق.

فالتحقيق هو مجموعة من الإجراءات التي تستهدف التنقيب والكشف عن الأدلة بشأن الجريمة التي إرتكبت ثم مدى كفايتها لإحالة المتهم للمحاكمة[1]، هذا الإجراء يقوم به المحقق وهو بذلك الشخص الذي عهد إليه قانونا بإتخاذ كافة الإجراءات القانونية والوسائل المشروعة فيما يصل علمه من جرائم يهدف الكشف عن غموضها وضبط فاعلها وتقديمه للمحاكمة[2]، وقد عبر عنه المشرع الجزائري بقاضي التحقيق في نص المادة 68 من قانون الإجراءات الجزائية المعدل والمتمم[3].

يتم التحقيق في الجريمة الإلكترونية بمجموعة من الصفات منها السرية، حيث يتم حماية مجريات التحقيق من إطلاع الغير وفقا لما نصت عليه المادة 11 من قانون الإجراءات الجزائية المعدل والمتمم، بالإضافة إلى ذلك يتم التدوين لجميع إجراءات التحقيق محاضر مصادق عليها في محضر رسمي، مما يجعلها حجة في الإثبات، ويبدأ التحقيق بوضع خطة للتحقيق حيث يشرع المحقق بجميع الإستدلالات، ويتلقى الدعم من فريق مؤهل في الجرائم الإلكترونية.

يتطلب التحقيق في هذا النوع من الجرائم وسائل مادية وبشرية للبحث والتحري وضبط مرتكبها[4]، حيث تتميز آليات البحث والكشف عن الجرائم الإلكترونية بخصوصية تميزها عن باقي الجرائم الأخرى التقليدية. لذا سنتطرق إلى الأجهزة المختصة بالبحث والتحري (المطلب الأول)، ثم إجراءات البحث والتحقيق (المطلب الثاني).

---

[1] عبد القادر فلاح، نادية آيت عبد المالك، المرجع السابق، ص 1694.

[2] خالد ممدوح ابرهيم، فن التحقيق الجنائي والجرائم الإلكترونية، الطبعة 1، دار الفكر الجامعي، الإسكندرية–مصر، 2009، ص 87.

[3] الأمر رقم 66–155 المؤرخ في 8 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية، العدد رقم 71، 1966، المعدل والمتمم.

[4] عبد القادر فلاح، نادية آيت عبد المالك، المرجع السابق، ص 1695.

المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجرائم الإلكترونية في الجزائر

يمكن القول أن المحقق هو من يتولى التحقيق من رجال الضبطية القضائية أو من أعضاء النيابة العامة أو قضاة التحقيق، ويلحق بالتحقيق الجنائي الباحث الجنائي الذي يكون غالبا من الشرطة القضائية الذي يخول لهم القانون مهمة جمع الإستدلالات عن المشتبه بهم[1].

سنحاول من خلال هذا المطلب أن نستعرض أبرز الهيئات والوحدات المختصة في مجال مكافحة الجرائم الإلكترونية، حيث سنتناول الأجهزة الأمنية التابعة لسلك الأمن الوطني والتابعة لقيادة الدرك الوطني (الفرع الأول)، إضافة إلى الهيئة الوطنية التابعة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال (الفرع الثاني).

الفرع الأول: البحث والتحري عن الجرائم الإلكترونية في الضبطية القضائية

يتمتع جهاز الضبطية القضائية بالولاية العامة في البحث والتحري عن الجرائم بمختلف أنواعها وأشكالها، ومع ذلك تعهد بعض القوانين الخاصة بهذا الدور استثنائيا، إلى جهات وهيئات معنية بسبب خبرتها في مجال معين، حيث تعتبر الأكثر قدرة على كشف الجرائم التي تقع ضمن حدود إختصاصها الفني أو التقني. والواقع أن ذلك لا يحول دون ضرورة تنسيق الجهود مع جهاز الضبطية القضائية التقليدي من أجل ضمان تحقيق أكبر قدر من الفعالية في مجال الضبط القضائي.

ومن اجل اشراك مزودي الانترنات و الاتصالات الثابتة و المتنقلةفي مجال مكافحة الجرائم الالكترونية يلزم القانون 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال مكافحتها ، هؤلاء بتقديم المساعدة للسلطات المختصة في مجال جمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات حينها .

[1] ابتسام بوبعاية، التحقيق في الجريمة الإلكترونية، مذكرة ماستر، تخصص قانون الإعلام الآلي والانترنت، جامعة محمد البشير الابراهيمي-برج بوعريريج، الجزائر، 2022/2021، ص 31.

أولا: البحث والتحري عن الجرائم الإلكترونية على مستوى جهاز الشرطة

في تجسيد سياسية أمنية فعالة تضع مديرية الأمن الوطني كافة الإمكانيات البشرية والتقنية المتاحة لديها لتصدي لكل أنواع الجرائم ولاسيما المستحدثة منها كالجرائم المعلوماتية، والتي تعتبر نتاج التطور الحاصل على المستوى الدولي الوطني في مجال تكنولوجيا الإعلام والإتصال، وذلك بهدف حماية المصلحة العامة وكذلك المصالح الخاصة المرتبطة باستعمال هذا النوع من التكنولوجيا.

أ- على المستوى المركزي: بادرت المديرية العامة للأمن الوطني إلى تحديث هيكلها بغية إنشاء وحدات متخصصة تعمل كل منها على مكافحة نوع معين من الجرائم دون سواها، لذلك قامت المديرية العامة للشرطة القضائية بإنشاء مصلحة مختصة في مكافحة الجريمة الإلكترونية سميت بنيابة مديرية مكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، بالإضافة إلى ذلك تم إنشاء مديرية الشرطة العلمية والتقنية التي توفر مصالح علمية مختصة لتسهيل أعمال البحث والتحري والتحقيق بشأن الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، وتعتبر هذه الوحدة هي المركز المركزي للشرطة العلمية ومقرها الجزائر العاصمة.

يتولى كل المخبر المركزي مهام البحث والتحقيق وتحليل الأدلة الجنائية بمختلف أنواعها، لأجل ذلك يضم المخبر دائرة تقنية تتولى مهام البحث والتحقيق وتحليل الأدلة الجنائية الناتجة عن الجرائم التي تستعمل فيها الأسلحة والقذائف بمختلف أنواعها، وكذلك جرائم التزوير، إضافة إلى الجرائم الإلكترونية وتباشر الإجراءات الخاصة بكل جريمة على مستوى دائرة مستقلة عن الأخرى[1].

ب-على المستوى الجهوي: أنشأت المديرية العامة للأمن الوطني مخبرين جهويين بكل من قسنطينة ووهران، تحتوي على فروع تقنية من بينها خلية الإعلام الآلي وفرق مختصة مهمتها التحقيق والكشف

[1] عمار حشمان , المرجع السابق , ص 38.

عن جرائم الإنترنت، بالإضافة إلى ثلاث مخابر أخرى قيد الإنجاز على مستوى ولاية ورقلة وبشار وتمنراست، لأجل تعميم هذا النشاط على كافة ربوع الوطن[1].

يظهر المخبر الجهوي للشرطة العلمية على مستوى قسنطينة ووهران مخبرا خاصا يتولى مهمة التحقيق في الجريمة الإلكترونية تحت اسم "دائرة الأدلة الرقمية والآثار التكنولوجية"[2]. والتي لم تكن عند استحداثها سنة 2004 سوى قسم غير أن الإرتفاع المحلوظ لعدد القضايا الناتجة عن الجرائم المعلوماتية، بسبب الإنتشار المتزايد لتقنيات المعلوماتية عجل بترقيتها إلى دائرة تضم ثلاث أقسام فرعية، وذلك بالإستعانة بأجهزة مادية للكشف عن الجرائم الإلكترونية. وتتمثل هذه الأقسام في ما يلي:

1-قسم استغلال الأدلة الرقمية الناتجة عن الحواسيب والشبكات.

2-قسم استغلال الأدلة الناتجة عن الهواتف النقالة.

3 - قسم تحليل الأصوات[3].

تضم الدائرة في صفوفها ثمانية أعضاء محققين أربع (4) منهم عناصر شرطيون رسميون يتمتعون بصفة ضابط شرطة قضائية، والبقية هم أعوان شبيهون، يحمل كل منهم بشهادة جامعية في تخصص الإعلام الآلي، إضافة إلى إلمامهم بالجانب القانوني، ومما يزيد من فعاليتهم في مجال مباشرتهم لمختلف إجراءات البحث والتحقيق في الجرائم المعلوماتية هو خضوعهم بصفة دورية لدورات تكوينية لأجل الإطلاع على كل المستجدات القانونية منها في مجال الإجرام المعلوماتي[4].

تضمن مخابر الشرطة عملا تقنيا شاملا لمختلف أجهزة الشرطة والجهات القضائية في مجال التحريات الإلكترونية، إذ يتم ذلك من خلال البحث عن البيانات المشبوهة والمعلومات الرقمية بجميع أشكالها،

[1] حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة 1، الجزائر، 2016/2015، ص 177.

[2] عبد القادر فلاح، نادية آيت عبد المالك، المرجع السابق، ص 1996.

[3] عمار حشمان، المرجع السابق، ص 39.

[4] نفس المرجع.

مثل: الملفات، الرسائل الإلكترونية، البرامج والصور...، يستخدم في هذا البحث برامج ووسائل خاصة تمكن من استرجاع البيانات المحذوفة والإطلاع على محتوى كل الوسائط الرقمية.

تلعب هذه الدائرة دورا حاسما في كشف أسرار الجرائم الإلكترونية من خلال مختلف الإجراءات التي تباشرها إما أثناء مرحلة البحث والاستدلال أو أثناء مرحلة التحقيق القضائي.

فمن خلال مرحلة البحث والتحري يستجيب أعضاء الدائرة إلى الطلبات المقدمة من عناصر الشرطة التابعة لفرق مكافحة الجرائم المعلوماتية الموزعة على كل مديريات الأمن الوطني أو الطلبات التي يوجهها وكيل الجمهورية أو قاضي التحقيق في شكل إنابة قضائية، من أجل دعمهم ومساندتهم أثناء مرحلة المعاينة لمسرح الجريمة وكذلك لحجز الأدلة المتواجدة عليها[1].

إما أثناء مرحلة التحقيق القضائي يقتصر دور المخابر على دور الخبير، حيث يعدون تقارير خبرة بناء على طلبات وكيل الجمهورية وبالخصوص قاضي التحقيق، ينجر على ذلك بعد قيام المحقيقين بتحليل الأدلة المحجوزة والعمل على استخراج الأدلة الإلكترونية منها، مثل: تحليل محتوى الأقراص الصلبة للحواسيب المستخدمة في الجريمة أو حواسيب الضحايا، وكذلك كل دعامات التخزين الإلكترونية بمختلف أنواعها وأشكالها، كما يتم تحديد المواقع الجغرافية وعناوين المجرمين باستخدام وسائل مادية خاصة متطورة ذات جودة عالية[2].

وفي الأخير فإن ما يمكن قوله بهذا الخصوص أن المديرية العامة للأمن الوطني تولي أهمية بالغة في مجال مكافحة الإجرام المعلوماتي.

ثانيا: البحث والتحري عن الجرائم الإلكترونية على مستوى الدرك الوطني

تعمل مؤسسة الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية والإجرام، الكائن بمقره ببوشاوي التابع لقيادة الدرك الوطني العامة قسم الإعلام والإلكترونيك، الذي

[1] حسين ربيعي، المرجع السابق، ص 180.

[2] نفس المرجع.

يختص بالتحقيق والكشف عن الجرائم الإلكترونية، وهي هيئة ذات إختصاص وطني مهمتها التصدي للجريمة الإلكترونية[1].

حيث يخضع الدرك الوطني لتنفيذ مهامه في مجال الحفاظ على الأمن الوطني والنظام العام ومحاربة الجريمة بكافة أنواعها، كم خلال وحدات متنوعة وعديدة على مستوى القيادة العامة أو على مستوى القيادات الجهوية والمحلية[2]. نذكر منها:

أ- المعهد الوطني للأدلة وعلوم الإجرام: وهو جهاز تابع للدرك الوطني أنشئ سنة 2004 بموجب مرسوم رئاسي رقم 04-183، يتكون من إحدى عشرة 11 دائرة متخصصة من عدة مجالات تضمن الخبرة، التكوين، التعليم، تقديم المساعدات التقنية، البحوث، الدراسات، التحاليل وتقديم كل دليل إلكتروني وتماثلي للعدالة، كما تقدم مساعدة للمحقيقين في التحقيقات المعقدة[3].

حيث يعمل المعهد الوطني للأدلة الجنائية وعلم الإجرام الذي يختص بالتحقيقات في الجرائم الإلكترونية، على القيام بتحليل الأدلة الخاصة بالجرائم وذلك بتحليل الدعمات الإلكترونية، إنجاز المقارنات الهاتفية، تحسين التسجيلات الصوتية، الفيديوهات والصور، وذلك لتسهيل استغلالها. بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي ومكافحتها[4].

إن الوظيفة الأساسية للوحدة هي خدمة العدالة ودعم وحدات التحري في إطار مهام الشرطة القضائية في مجال مكافحة شتى أنواع الجرائم بما فيها الجريمة المعلوماتية[5].

---

[1] عبد القادر فلاح، آيت عبد المالك نادية، المرجع السابق، ص 1996.

[2] ايمن صالح بن قسمية، نور الدين عيسى، دور الضبطية القضائية في البحث والتحري في الجرائم الإلكترونية، مذكرة ماستر، تخصص قانون جنائي وعلوم الجنائية، جامعة عمار ثليجي-الأغواط، الجزائر، 2022/2021، ص41.

[3] عبد الرؤوف بوديسة بجاد، المرجع السابق، ص 27.

[4] أيمن صالح بن قسمية، نور الدين عيسى، المرجع السابق، ص 42.

[5] نفس المرجع، ص 48.

الفرع الثاني: مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية

إتخذ المشرع الجزائري لمكافحة الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال مجموعة من التدابير سواء وقائية أو عقابية، وقد أنشأ المشرع هيئة إدارية تكلف بالوقاية والتحري عن الجرائم المتصلة بتكنولوجيا الإتصال وهذا في الجرائم الخطيرة والتي تمس بأمن الدولة عموما أو توصف بالجرائم الإرهابية، وفي إطار الكشف عن هذه الجرائم أجاز المشرع لهذه الهيئة التعاون مع الشرطة القضائية[1]. ومن هنا سوف نتطرق إلى تعريفها (أولا)، ثم إختصاصها (ثانيا) وأخيرا تشكيلها.

أولا: تعريف مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية

تعتبر الهيئة كما إصطلح عليها في صلب نصوص المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها[2]، حسب أحكام المواد من 01 إلى 04 منه، بأنها سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي وتوضع لدى الوزير المكلف بالعدل، ويقع مقرها بالجزائر العاصمة، حيث تتولى الهيئة المهام المنصوص عليها في المادة 14 من القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتعلقة بتكنولوجيا الإعلام والإتصال ومكافحتها، وذلك تحت رقابة السلطة القضائية وطبقا لأحكام قانون الإجراءات الجزائية المعدل والمتمم[3].

وتم إنشاء هذه الهيئة بموجب نص المادة 13 من القانون رقم 09-04 المتضمن القواعد الخاصة بالجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، والتي جاء فيها:" تنشأ هذه الهيئة

[1] سهيلة بوزرة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها بين سرية المعطيات الإلكترونية ومكافحة الجرائم الإلكترونية "، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، المجلد 17، العدد 02، 2022، ص 560.

[2] المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد رقم 53، 2015.

[3] عمار حشمان، المرجع السابق، ص 33.

الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها وتحدد تشكيلة الهيئة كيفيات سيرها عن طريق التنظيم "[1].

ثانيا: إختصاصات مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية

بينت الفقرة الثانية من المادة 04 من المرسوم الرئاسي رقم 15-267 المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، المهام الأساسية التي تكلف بها الهيئة، وهي على سبيل الحصر هذه مهام الهدف منها الوقاية من الجرائم المعلوماتية ومكافحتها من خلال الاسهام في أعمال البحث والتحقيق. ومن أبرز مهام هذه الهيئة [2]:

- اقتراح عناصر استراتيجية وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الاعلام و الاتصال ومكفحتها.
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها.
- مساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة جرائم المتصلة بتكنولوجيا الإعلام والإتصال.
- ضمان المراقبة الوقائية للإتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والمساس بأمن الدولة تحت السلطة المختصة باستثناء أي هيئات أخرى.

ثالثا: تشكيلة مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية

في ظل المرسوم الرئاسي رقم 15- 261 كانت الهيئة تضم مجموعة من الهياكل، تمثلت في: لجنة المديرية ومديرية عامة، مديرية المراقبة الوقائية واليقضة الإلكترونية، مديرية التنسيق التقني، مركز العمليات التقنية، ملحقات جهوية[3].

[1] سعاد بوخلفة، مكافحة الجرائم الإلكترونية في التشريع الجزائري، مداخلة مقدمة ضمن أعمال الملتقى الوطني، بعنوان:" الجرائم الإلكترونية في المجتمع الجزائري"، جامعة يحي فارس-المدية، الجزائر، المنعقد بتاريخ 15 مارس 2022، ص 124.

[2] عمار حشمان، المرجع السابق، ص 33.

[3] إلهام خرشي، "النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها"، المجلة القانونية والسياسية، جامعة محمد لمين دباغين-سطيف، الجزائر، المجلد 04، العدد 01، 2022، ص 63.

أ– اللجنة المديرة: تتشكل من وزير العدل كرئيس لجنة، والوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيا الإعلام والإتصال، وقائد الدرك الوطني، المدير العام للأمن الوطني، ممثلا عن رئيس الجمهورية، وآخر عن وزارة الدفاع يعنينان بموجب مرسوم رئاسي[1].

تُكلف لجنة المديرية بتوجيه عمل الهيئة، الإشراف عليها، مراقبتها ودراسة كل مسألة تخضع لمجال إختصاص الهيئة، دراسة مشروع النظام الداخلي للهيئة والمصادقة عليه، دراسة التقرير السنوي لنشاطات الهيئة والمصادقة عليها، وإبداء الرأي في كل مسألة تتصل بمهام الهيئة.

ب– المديرية العامة: يترأسها مدير عام يعين بموجب قرار رئاسي من دون تحديد وضبط تشكيلتها[2]. ومن صلاحيات المدير العام السهر على حسن سير الهيئة والسهر على تنفيذ برنامج عملها، تبسيط نشاطات هياكل الهيئة، تنسيقها، متابعتها ومراقبتها، تحضير إجتماعات لجنة المديرة والسهر على القيام بإجراءات التأهيل وأداء اليمين فيما يخص المستخدمين المعينين في الهيئة.

ج– مديرية المراقبة الوقائية واليقظة الإلكترونية: تكلف على وجه الخصوص بتنفيذ عمليات المراقبة الوقائية للإتصالات الإلكترونية من أجل الكشف عن الجرائم، إرسال المعلومات المتحصل عليها من خلال المراقبة الوقائية إلى السلطات القضائية، تنفيذ طلبات المساعدة القضائية الأمنية في مجال تدخل الهيئة وجمع المعطيات المفيدة، تنظيم أو المشاركة في عمليات التوعية حول استعمال تكنولوجيات الإعلام والإتصال، وحول المخاطر المتصلة بها.

د–مديرية التنسيق التقني : تُكلف بإنجاز الخبرات القضائية في مجال إختصاص الهيئة وتكوين قاعدة المعطيات التحليلة لإجرام المتصل بالقيام بمبادرة منها أو بناء على طلب اللجنة المديرة، تسير منظومة الإعلام للهيئة وإدارتها[3].

---

[1] حميدة بوادي، فطيمة بن سالم، الهيئة الوطنية للجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، مذكرة ماستر، تخصص إعلام آلي وإنترنت، جامعة البشير الابراهيمي–برج بوعريرج، 2023/2022، ص 21.

[2] نفس المرجع، ص 22.

[3] أنظر نص المادة 12 من المرسوم الرئاسي رقم 15–261 المؤرخ في 8 أكتوبر 2015، المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

هـ–مركز العمليات التقنية: يقوم بالمنشآت، التجهيزات، الوسائل المادية وكذا المستخدمين التقنيين، الضرورية لتنفيذ العمليات التقنية لمراقبة الإتصالات الإلكترونية. ويتبع هذا المركز مديرية المراقبة الوقائية واليقظة الإلكترونية[1].

و–الملحقات الجهوية: يتم تشغيلها من طرف مديرية المراقبة الوقائية واليقظة الإلكترونية التي تتبعها[2].

المطلب الثاني: إجراءات التحقيق في الجرائم الإلكترونية في الجزائر

تنقسم الإجراءات القانونية من أجل الكشف عن الجريمة الإلكترونية إلى إجراءات تقليدية (الفرع الأول)، وإجراءات مستحدثة للكشف عن الجريمة الإلكترونية (الفرع الثاني).

الفرع الأول: إجراءات التحري المألوفة والتقليدية في الجرائم الإلكترونية في الجزائر

تتضمن إجراءات التحري التقليدية للكشف عن الجريمة الإلكترونية جميع الإجراءات الموجودة في الجرائم التقليدية، مثل المعاينة، التفتيش والضبط. وعليه سنبرز هذه الإجراءات فيمايلي:

أولا: المعاينة في الجرائم الإلكترونية

عند التكلم عن إجراءات التحري التقليدية للكشف عن الجرائم الإلكترونية أول ما يجب دراسته هو معاينة مسرح الجريمة الإلكترونية، فبعد إقتراف الجريمة يخلف الجاني عادة آثار تعمل كدليل يساعد جهات التحقيق في التعرف على هوية الجاني، هذه الآثار وإن كانت ذات طبيعة مادية في الجرائم التقليدية إلا أنها في الجريمة الإلكترونية تكتسي طبيعة خاصة.

[1] أنظر نص المادة 13 من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

[2] أنظر نص مادة 14 من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها.

ومن أجل الإستفادة من هذه الأثار التي تركها الجاني يجب على جهات التحقيق التحرك بسرعة لمعاينة كل ما يتعلق بالجريمة، حيث تعتبر المعاينة إجراء حاسما يدعم جهود سلطات التحقيق في كشف عن الحقيقة[1].

إذ يُقصد بالمعاينة رؤية محل إرتكاب الوقائع الجنائية وإثبات حالتها بالشكل الذي تركها له الجاني عقب إرتكاب الجريمة. والمعاينة هي إثبات مادي ومباشر لحالة الأشخاص، الأشياء والأمكنة ذات الصلة بالحادث[2].

بالإضافة إلى أنها إجراء يتطلب سرعة الإنتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها.

نص المشرع الجزائري ضمن نص المادة 79 من قانون الإجراءات الجزئية المعدل والمتمم، على المعاينة كونها إجراء من إجراءات التحقيق، بقوله:" يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته، ويستعين قاضي التحقيق دائما بكاتب التحقيق ويحرر محضرا بما يقوم به من إجراءات ".

ويقصد بالمعاينة في الجريمة الإلكترونية معاينة الآثار والبصمات الإلكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الإنترنت، وتشمل الرسائل المرسلة منه والتي يستقبلها، وكافة الإتصالات التي تمت من خلال الكمبيوتر والشبكة العالمية. ويرى البعض أن أهمية المعاينة تتضاءل في الجريمة الإلكترونية وذلك لندرة تخلف آثار مادية عن إرتكاب الجريمة الإلكترونية، كما أن طول الفترة بين وقوع الجريمة وإرتكابها، وبين اكتشافها يكون له التأثير السلبي على الآثار الناجمة عنها بسبب البحث أو المحو أو التلف لتلك الآثار[3]. ولمعاينة مسرح الجرائم الإلكترونية يجب التفرقة بين حالتين:

[1] إسماعيل بن يحي، المرجع السابق، ص 175.

[2] خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، الطبعة 1، دار الفكر الجامعي، الإسكندرية-مصر، 2009، ص ص: 147 و148.

[3] إسماعيل بن يحي، المرجع السابق، ص 176.

أ–معاينة الجرائم الواقعة على المكونات المادية للحاسوب (Hardware): التي قد تتمثل في شاشة العرض، مفاتيح التشغيل، الأقراص وغيرها من مكونات الحاسوب ذات الطابع المادي المحسسوس، فهي لا تثير أية مشكلة بحيث يمكن لمأمور الضبط القضائي معينتها والتحفظ على الأشياء التي تعد أدلة مادية للكشف عن الجريمة[1].

ب–معاينة الجرائم الواقعة على المكونات غير المادية أو بواسطتها (Software): كتلك الواقعة على برامج الحاسوب وبياناته، هذه المكونات تثير صعوبات عديدة تحول دون فاعلية المعاينة أو فائدتها. وهذه الصعوبات تتلخص فيمايلي:

–قلة الآثار المادية المرتبة عن الجرائم التي تقع على المكونات غير المادية للحاسوب.

–الأعداد الكبيرة من الأشخاص الذين يترددون على مسرح الجريمة من خلال المدة الزمنية التي غالبا ما تكون طويلة، وذلك بين إقتراف الجريمة والكشف عنها، الأمر الذي يمنح فرصة لإحداث تغيرات أو العبث بالآثار المادية أو زوال بعضها، مما يؤدي إلى غموض الدليل من المعاينة.

لالمعاينة في الجرائم المعلوماتية أشكال مختلفة بحسب نوعية الجريمة المرتكبة، على أن هناك طرق عامة تتوافق مع طبيعة الإتصال بالإنترنت أو الوسيلة المستخدمة، مثلا: وسيلة تصوير شاشة الحاسوب التي تكون بواسطة آلة تصوير تقليدية عن طريق إستخدام برمجة حاسوب متخصصة في أخذ الصورة لما يظهر على الشاشة، وهذا ما يصطلح عليه " تجميد مخرجات الشاشة "[2].

ثانيا: التفتيش في البيئة الإلكترونية

لم يحدد المشرع الجزائري تعريفا دقيقا للتفتيش، بل إعتبره إجراءً من إجراءات التحقيق وأحاطه بضوابط صارمة نظرا لأهميته في كشف الأدلة من جهة، وخطورته فيما يترتب عليه مساس بحرية الأشخاص

[1] آمنة امحمدي بوزينة، إجراءات التحري الخاصة في مكافحة الجرائم المعلوماتية، مداخلة مشارك بها في الملتقى الوطني حول:" آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، الجزائر العاصمة، 29 مارس 2017، ص 61.

[2] ابتسام يومايلة، مناهج التحقيق الجنائي في ظل تفشي الجريمة الرقمية، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة قاصدي مرباح–ورقلة، ص ص: 45 و46.

وكرامتهم من جهة أخرى[1]، ويُظهر الدستور الجزائري إهتماما خاصا بهذا الإجراء من خلال نص المادة 48 منه، والتي تنص على مايلي: " ...لا تفتيش إلا بمقتضى القانون، وفي إطار إحترامه.

لا تفتيش إلا بأمر مكتوب صادر عن السلطة القضائية المختصة"[2].

كما نصت المادة 5 في فقرتها الأولى من القانون رقم 09- 04 المتضمن لقواعد خاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، على: " يجوز للسلطات القضائية المختصة وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية وفي الحالات المنصوص عليها في المادة 04 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى: منظومة معلوماتية أو جزء منها وكذا المعطيات المخزنة فيها ومنظومة التخزين المعلوماتية ".

ويمكن تعريف التفتيش، بأنه عبارة عن إجراء من إجراءات التحقيق التي تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها في فعل يتمتع بحرمة المسكن أو الشخص، وذلك بهدف إثبات إرتكابها أو نسبتها إلى متهم وفقا لإجراءات قانونية محددة[3].

أ-تفتيش نظم المعلوماتية: تنصب عملية التفتيش على المكونات المادية بأوعيتها المختلفة للبحث في أي شيء يتصل بجريمة معلوماتية ما للكشف عنها، ويدخل في نطاق التفتيش التقليدي وفقا للإجراءات القانونية المعمول بها، إلا أن هناك حالات خاصة للتفتيش في هذه المكونات، وهي[4]:

- **الحالة الأولى:** في حالة ما إذا كانت المكونات موجودة في مكان خاص كمسكن المتهم أو أحد ملحقاته، فإنها تأخذ نفس الأحكام المقررة لتفتيش المسكن وبنفس الضمانات المقررة قانونا في مختلف التشريعات.

[1] نفس المرجع، ص 41.

[2] الدستور الجزائري لسنة 1996، المعدل والمتمم بموجب المرسوم الرئاسي رقم 20-442 المؤرخ في 30 ديسمبر 2020، الجريدة الرسمية، العدد رقم 82، 2020.

[3] علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية-دراسة مقارنة، دار الكتب والوثائق القومية، مصر، 2012، ص 38.

[4] آمنة أمحمدي بوزينة، المرجع السابق، ص 62.

- **الحالة الثانية:** إذ كانت مكونات الحاسوب المادية منعزلة عن غيرها من أجهزة الكمبيوتر أم أنها متصلة بجهاز أو نهاية طرفية في مكان آخر كمسكن غير مسكن المتهم ، بحيث إذا كانت هناك بيانات مخزنة في أوعية هذا النظام الآخر، فإن عملية الكشف تصبح صعبة جدا، وربما مستحيلة، لذلك تتم عملية تفتيش هذه الأجهزة المرتبطة بأجهزة في أماكن أخرى أين يتعين مراعاة القيود والضمانات التي يوجبها المشرع لتفتيش هذه الأماكن.

وقد حذا المشرع الجزائري حذوا معظم التشريعات المعاصرة بأن أقر نص المادة 65 مكرر ومايليها من قانون الإجراءات الجزائية التي تسمح إذا إقتضت ضرورة التحري أو التحقيق في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، بإعتراض المراسلات، تسجيل الأصوات وإلتقاط الصور[1].

- **الحالة الثالثة:** إذا وجدت مكونات الحاسوب المادية (في حالة الحاسوبات الآلية المحمولة) في الأماكن العامة بطبيعتها كالمطاعم والسيارات العامة كسيارات الأجرة مثلا، فإن تفتيشها لا يكون إلا في الحالات التي يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها في هذه الحالات[2].

ب- تفتيش نظم الحاسوب المنطقية والمعنوية: تُعرف الكيانات المنطقية للحاسب، بأنها:"مجموعة من البرامج و لأساليب والقواعد والأوامر المتعلقة بتشغيل وحدة معالجة البيانات "[3].

وقد حذا المشرع الجزائري في نص المادة 47في فقرتها الرابعة من قانون الإجراءات الجزائية المعدل والمتمم، حذو التشريعات المقارنة بإمكانية التفتيش والضبط على المكونات المعنوية للحاسوب، بنصه على أنه:" إذا تعلق الأمر بجريمة ماسة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم

[1] آمنة أمحمدي بوزينة، المرجع السابق، ص 63.

[2] عمار حشمان، المرجع السابق، ص 50.

[3] جمال براهيمي، التحقيق الجنائي في الجريمة الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، 2018، ص 17.

بأية عملية تفتيش أو حجز ليلا ونهارا أو في مكان على إمتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

ج- القواعد الشكلية لتفتيش نظم المعلومات: تتضمن هذه القواعد ما يلي:

1-إجراء التفتيش بحضور أشخاص معينين بالقانون: يتم التفتيش بحضور المتهم أو من يمثله بالإضافة إلى ضابط الشرطة القضائية القائم بالتفتيش، إذا تعذر حضور المتهم أو من يمثله يتم التفتيش بحضور شاهدين من غير الموظفين الخاضعين لسلطته. ومع ذلك هناك استثناء في جرائم أنظمة المعالجة الآلية للمعلومات، حيث لا تطبق هذه الأحكام وفقا لنص المادة 45 من قانون الإجراءات الجزائية المعدل والمتمم.

2- إعداد محضر خاص بالتفتيش: يكون ذلك بتكليف القائم بالتفتيش بإصطحاب كاتب يحرر محضرا خاصا بالتفتيش والضبط وتسجيل جميع وقائع التحقيق بالتفصيل مع ذكر البيانات والأشياء والوثائق التي تم ضبطها بدقة وحرص.

3- إجراءات تنفيذ تفتيش نظم الحاسوب الآلي وميعاده: تتميز إجراءات تفتيش نظم الحاسوب الآلي بخصوصية معينة بسبب دقة التعامل مع الأجهزة والبرامج، ولكي يتم على أأمل وجه يجب تحديد نوع النظام المراد تفتيشه، ويتطلب ذلك أن يكون القائم بالتفتيش على دراية بعلوم الإعلام الآلي حتى يتسنى له معرفة نظم الحاسوب المراد تفتيشها والإستعانة بخبراء النظام في عملية إجراء التفتيش، ومعرفة إمكانية الحصول على كلمة السر للدخول إلى النظام المراد تفتيشه وتحديد مكان تحليل نظم الحاسوب الآلي[1].

بالإضافة إلى تحديد هوية أعضاء فريق التفتيش، يجب على القائم بالتفتيش إتخاذ الخطوات التالية عند تنفيذ إذن التفتيش، والتي تتلخص فيمايلي[2]:

[1] عمار حشمان، المرجع السابق، ص 51.

[2] آمنة امحمدي بوزينة، المرجع السابق، ص 66.

- **تأمين حماية مسرح الجريمة:** بفصل القوة الكهربائية عن موقع المعاينة وأجهزة شبكة الإنترنت لمنع أي تدخل من قبل الجاني.
- **إبعاد المتهم عن مكان النظام:** إذا كان المتهم قريبا، يجب أخذ الحيطة لمنع دخوله عن بعد إلى النظام المعلوماتي.
- **الدخول إلى الموقع ببطئ:** لمنع تشويه أو إتلاف الأدلة.
- **عدم لمس لوحة المفاتيح:** لتجنب تشغيل برامج إحتيالية.
- **العناية بالملاحظات وكلمات السر ورموز التشفير:** لضمان الكشف عن الجريمة المراد إثباتها.

إن في نطاق تفتيش نظم الحاسوب نجد أن المشرع الجزائري لم يحدد مدة معينة لتنفيذ إجراء التفتيش، غير أن الرأي الغالب في مجال تفتيش النظم المعلوماتية هو عدم تقييد المحقق بمدة زمنية معينة، بل يجب تركها للسلطة التقديرية له، لأن الوقت الذي تكثر فيه الجرائم الإلكترونية هو ليلا، لسهولة الإتصال ومجانيته في ذلك الوقت في بعض الخالات بالإضافة إلى سهولة الدخول إلى المواقع المستهدفة بسبب قلة المستخدمين في ذلك الوقت، كما تم النص عليها في الفقرة الثالثة من المادة 47 من قانون الإجراءات الجزائية المعدل والمتمم[1].

ثالثا: ضبط الأدلة في الجرائم الإلكترونية

يُعتبر الضبط من إجراءات جمع الأدلة، وهو النتيجة الطبيعية التي ينتهي إليها التفتيش والأثر المباشر الذي يسفر عنه، ويقصد به وضع اليد على الأشياء المتعلقة بجريمة وقعت والتي تفيد في كشف الحقيقة عنها وعن مرتكبيها، ووضعها في أحراز مختومة و لتقدم إلى الجهة القضائية المختصة كدليل إثبات.

إن تحصيل الأدلة في الجرائم الإلكترونية قد يرتبط بعناصر مادية كجهاز الحاسب الالي وملحقاته، كالأقراص الصلبة، الأشرطة الممغنطة، الطباعة، البرامج اللينة، المراشد والبطاقات الممغنطة، بطاقات الائتمان والمعدات المستعملة في شبكة الإنترنت مثل المودم، ففي هذه الحالات لا يطرح ضبط هذه

[1] نورة طرشي، مكافحة الجريمة المعلوماتية، رسالة ماجستير، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة ين يوسف بن خدة-الجزائر 1، الجزائر، 2012/2011، ص 126.

المكونات المادية أي إشكال قانوني أو عملي لإمكانية إخضاعها لإجراءات الضبط والتحريز التقليدية، وقد يرتبط الدليل بالمكونات المعنوية للحاسب، كمختلف البرامج والبيانات المعالجة آليا والمراسلات والإتصالات الإلكترونية التي يجري تبادلها عبر شبكة الانترنت والبريد الإلكتروني[1].

رابعا: الخبرة التقنية في مجال الجرائم الإلكترونية

تعتبر الاستعانة بالخبراء من بين الإجراءات التي يلجأ إليها القضاء، وسلطات التحقيق على حد سواء، و ذلك ما إستعصى عليهم الامر، ومن بين هذه المجالات التي تستدعي اللجوء إلى الخبرة نجد الجريمة الإلكترونية، حيث أنه لا يستطيع التعامل مع هذه الجريمة إلا الأشخاص ذو دراية وخبرة في مجال الإلكترونيات[2].

أ-أنواع الخبراء الإلكترونيين: الخبير في الجريمة الإلكترونية هو الفني المتخصص وصاحب الخبرة التقنية الإلكترونية وشبكتها قد يلاحظ أو يسمع أو يدرك معلومات هامة باستخدام حواسه مما يساعد على الدخول إلى نظام المعالجة الآلية الرقمية للبيانات إذا دعت مصلحة التحقيق إلى البحث عن دليل رقمي إلكتروني داخله. ويعتبر خبراء إلكترونين كل من:

1-المبرمجون: الذين يصممون ويطورون البرامج المستخدمة في نظم الحاسوب.

2-المحللون: وهم الأشخاص الذين يضعون خطوات العمل ويقومون بتجميع بيانات نظام معينة لتحليلها.

3-مهندسوا الصيانة والإتصالات: المسؤولون عن صيانة البنية التحتية للشبكات والأنظمة الإلكترونية.

4-مشغلو الحاسوب الآلي: الذين يقومون بتشغيل نظم الحاسوب وتحديثها.

[1] جمال براهيمي، المرجع السابق، ص ص: 46 و47.

[2] ابتسام يومايلة، المرجع السابق، ص 44.

5–مدير النظام المعلوماتي: المسؤول عن إدارة وتشغيل نظم المعلومات في المنظمة.

ب– أهمية الخبرة في البحث عن الدليل الإلكتروني: إهتم المشرع الجزائري بتنظيم أعمال الخبرة في نصوص المواد من 143 إلى 156 من قانون الإجراءات الجزائية المعدل والمتمم، وإعتبرها من إجراءات البحث عن الدليل، حيث نصت المادة 143 على أنه:" لجهات التحقيق أو الحكم عندما تعرض لها مسألة ذات طابع فني أن تأمر بندب خبير إما بناء على طلب النيابة العامة وإما من تلقاء نفسها أو من الخصوم...".

كما أشار المشرع الجزائري في المادة 05 الفقرة الأخيرة من القانون رقم 09- 04 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، أنه:" يمكن للسلطة المكلفة بتفتيش المنظومات المعلوماتية تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو التدبير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها".

الفرع الثاني: إجراءات التحري المستحدثة في الجرائم الماسة بأنظمة المعالجة الآلية للبيانات

في سبيل مكافحة جرائم الفساد نص المشرع على مجموعة من أساليب التحري تضاف إلى تلك الأساليب التقليدية وتمثل الهدف من هذه الأساليب في الكشف عن الجرائم واستئصال الفساد ردع المفسدين[1].

أولا: التسرب الإلكتروني

نتطرق أولا إلى مفهوم التسرب الالكتروني، ومن ثم إلى شروطه (ثانيا) وأخيرا إلى صوره (ثالثا).

أ–تعريف التسرب: عرف المشرع الجزائري التسرب من خلال نص المادة 65 مكرر 12 من قانون الإجراءات الجزائية المعدل والمتمم، والتي جاء فيها:" يقصد بالتسرب قيام ضابط أو عون الشرطة

[1] محمد أمين بن حديفة، وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية، مذكرة ماستر، قانون قضائي، جامعة عبد الحميد بن باديس–مستغانم، الجزائر، 2020/2019، ص 32.

القضائية، تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية، بمراقبة الأشخاص المشتبه في إرتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك أو خاف".

ب- شروط التسرب: يشترط في التسريب شروط موضوعية وأخرى شكلية، نوضحها فيما يلي:

1- الشروط الموضوعية: هناك شرطين موضوعين لإجراء التسرب هما:

1-1 – عنصر التسبيب: يُعد عنصر التسبيب ضمانة هامة كونه تتضح من خلاله الأسباب المبررة التي دفعت بوكيل الجمهورية لإصدار الأمر بإجراء التسرب، وذلك تحت طائلة بوطلان الإذن وكل الإجراءات أي مفاده تبيان المبررات وكذلك الحجج التي بموجبها منحت الجهة القضائية الإذن بالتسرب لضابط الشرطة القضائية[1].

1-2- تحديد نوع الجريمة: يتوجب تبيان نوع الجريمة التي بموجبها تم طلب إجراء التسرب بهدف التحقيق فيها مع ضرورة أن تكون هذه الجرائم من ضمن الجرائم الخطيرة، وهي محددة على سبيل الحصر بموجب نص المادة 65 مكرر05 من قانون الإجراءات الجزائية المعدل والمتمم، وهي جرائم المخذرات، الجريمة العابرة للحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم الأموال، الجرائم المتعلقة بالصرف وكذلك جرائم الفساد[2].

2- الشروط الإجرائية لإجراء التسرب: خول المشرع الجزائري لوكيل الجمهورية إلى جانب إدارته الأعمال الضبطية القضائية سلطة منح الإذن لضباط الشرطة القضائية لأجل مباشرة التسرب الإلكتروني. والحصول على إذن من السلطة المختصة تجعل من صفة الإنتهاك عملا مباحا[3].

---

[1] نوال مجذوب، "آليات الإجرائية للكشف عن الجريمة المعلوماتية"، مجلة البحوث القانونية والاقتصادية، مركز الجامعي-مغنية، الجزائر، المجلد 06، العدد 04، 2023، ص 201.

[2] نفس المرجع.

[3] سمير خليفي، " التسرب الإلكتروني: إجراء لمكافحة الجرائم المخذرات عبر الوسائط الإلكترونية في ظل انتشار جائحة كورونا"، مجلة المحلل القانوني، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج-البويرة، الجزائر، المجلد 04، العدد 02، ديسمبر 2020، ص 85.

ولابد أن يحدد الإذن مدة عملية التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر، ولا يمكن أن تجدد عملية حسب مقتضيات التحري أو التحقيق[1].

ج- صور التسرب: نصت المادة 65 مكرر 12 من قانون الإجراءات الجزائية المعدل والمتمم، على تعريف عملية التسرب، كما جاء في آخر الفقرة منها على كيفية تنفيذ هاته العملية، وذلك بأن يوضع الجماعة الإجرامية بأنه مساهم في جريمة سواء كفاعل أساسي أو شريك أو خاف. لهذا تعتبر هذه الصورة تنفيذا لهذه العملية من أساسيات عملية التسرب، وهي كالآتي[2]:

1- المسرب كفاعل: الفاعل هو ما جاء بيانه في نص المادة 41 من قانون العقوبات المعدل والمتمم[3]، حيث يعتبر الفاعل كل من ساهم مساهمة مباشرة في تنفيذ الجريمة أو حرض على إرتكاب الفعل بالهبة أو الوعد أو التهديد أو إساءة استعمال السلطة أو الولاية أو التحايل أو التدليس الإجرامي.

2- المسرب كشريك: يقصد بالشريك في الجريمة حسب نص المادة 42 من قانون العقوبات، أنه:"يعتبر شريكا في الجريمة من لم يشترك اشتراكا مباشرا، ولكنه ساعد بكل الطرق أو عاون الفاعل أو الفاعلين على إرتكاب الأفعال التحضيرية أو المسهلة أو المنفذة لها مع علمه بذلك"[4].

ثانيا: المراقبة الإلكترونية

إن الخوض في مسألة المراقبة الإلكترونية يتطلب منا أولا التعرض إلى تعريفها، ومن ثم إلى حالات اللجوء إليها (ثانيا).

---

[1] هدى زوزو، "التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائرية"، مجلة الدفاتر السياسية والقانونية، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة-الجزائر، العدد 11، جوان 2014، ص 119.

[2] عبد الرحمان كوداد، عملية التسرب على ضوء التشريع الجزائري، مذكرة ماستر، تخصص علم الإجرام، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر-سعيدة، الجزائر، 2017/2016، ص 43.

[3] أنظر نص المادة 41 من الأمر رقم 66-156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات المعدل والمتمم.

[4] شمس الدين مهدي، النظام القانوني للتسرب في قانون الجزائر، مذكرة ماستر، تخصص قانون جنائي، جامعة محمد خيضر-بسكرة، 2014/2013، ص 73.

أ- تعريف المراقبة الإلكترونية: تتمثل المراقبة في كشف الجرائم قبل وقوعها وتلعب دورا كبيرا في الكشف عن الجرائم الإلكترونية، وهي وضعية هامة في وسائل الإرشاد الجنائي. ويقصد بالمراقبة الأمنية التي محلها الإتصالات الإلكترونية التي عرفها المشرع الجزائري[1].

نص القانون رقم 09- 04 المؤرخ في 05 أوت 2009، والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، في نص المادة 03 على ما يلي:" مع مراعاة الأحكام القانونية التي تضمن سرية المرسلات والإتصالات يمكن لمقتضيات حماية النظام العام أو لمستلزمات التحريات أو التحقيقات القضائية الجارية فيها للقواعد المنصوص عليها في قانون الإجراءات الجزائية ..."[2].

ب-حالات اللجوء إلى المراقبة الإلكترونية للاتصالات: نصت المادة 04 من قانون رقم 09-04 المؤرخ في 05 أوت 2009، والمتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، على الحالات التي يمكن اللجوء إلى إجراء المراقبة الإلكترونية فيها، وهي:

- الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، فهي وظيفة المشرع الجزائري مستوى من مستويات السياسية الجنائية، وهو المستوى الوقائي على غرار المستويين التجريمي والعقابي[3].
- في حالة توفر معلومات عن إحتمال إعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني[4].

---

[1] عبد الرؤوف بوديسة بجاد، المرجع السابق، ص 58.

[2] محمد امين بن حديفة، المرجع السابق، ص 58.

[3] عبد الحليم بن بادة، المراقبة الإلكترونية كإجراء لإستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني، المجلة الأكادمية للبحث القانوني، جامعة عبد الرحمان ميرة-بجاية، المجلد 10، العدد 43، 2019، ص 396.

[4] كريم معروف، سعاد بن حليمة، "الإجراء المستحدث في البحث والتحقيق للكشف عن الجرائم التي ترتكب في الفضاء الإلكتروني (دراسة تحليلية وصفية وفق ما جاء به المشرع الجزائري)"، مجلة الدراسات الاستراتجية والعسكرية، المركز الديمقراطي العربي، برلين-ألمانيا، العدد 13، ديسمبر 2021، ص 08.

- مقتضيات التحري والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى مراقبة إلكترونية[1].

ثالثا: إعتراض المراسلات

نستعرض من خلاله تعريف إعتراض المراسلات، ثم من تنطرق إلى خصائص هذا الإجراء والشروط الواجب توافرها لإتخاذه.

أ- تعريف إعتراض المراسلات: من نص المادة 65 مكرر 05 من قانون الإجراءات الجزائية المعدل والمتمم، إن المقصود بإعتراض المراسلات هو إعتراض أو تسجيل المراسلات التي تتم عن طريق قنوات أو وسائل الإتصال السلكية واللاسلكية، وهاته المراسلات عبارة عن بيانات قابلة للإنتاج، التوزيع، التخزين، الإنتقال والعرض[2]. وبالتالي حصر المشرع الجزائري المراسلات في شكل كتابي فقط، إلى أن جاء القانون رقم 09- 04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و لإتصال ومكافحتها، والذي جاء فيه من خلال نص المادة الثانية الفقرة السادسة منها، أنه:" أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو رموز أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية "[3].

ب- خصائص إعتراض المراسلات: من بين خصائص إعتراض المراسلات، ما يلي:

1- إعتراض المراسلات يتم خلسة دون علم ورضى صاحب الشأن: إن إعتراض المراسلات إجراء يتم من دون علم ورضى المشتبه فيه، وهي أهم خاصية، فعندما يعلم أصحاب الشأن بتلقي خاصية

[1] نفس المرجع.

[2] محمد شرف، مختار خرشبن، أساليب التحري والتحقيق الحديث من النظام الاتهامي ونظام البحث والتحري، مذكرة ماستر، تخصص علوم جنائية، جامعة ابن خلدون-تيارت، الجزائر، 2015/2014، ص 39.

[3] عبد النور سعداني، ليندة بومحراث، إجراءات البحث والتحري في الجرائم الإلكترونية، مداخلة مقدمة ضمن أعمال الملتقى الوطني بعنوان:" الجرائم الإلكترونية في المجتمع الجزائري "، جامعة يحي فارس-المدية، الجزائر، المنعقد بتاريخ 15 مارس 2022، ص 144.

الإعتراض –وهنا لا يمكننا القول أن أمام أسلوب لإعتراض– فهذا الأخير يمحوا خصوصية الإعتراض ويزيل السرية[1].

2– إعتراض المراسلات إجراء يمس حق الشخص في سرية الحديث: إن إعتراض المراسلات إجراء يمس بحق الانسان في سرية حديثه رغم أن نص المادة 47 من الدستور تنص على حرية الحياة الخاصة وتحمي سرية المراسلات والإتصالات الخاصة دون أي قيود، وذلك بقولها:" 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 معلل من السلطة القضائية.

حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي.

يعاقب القانون على كل إنتهاك لهذه الحقوق".

إلا أن إجراء الإعتراض والمراسلات ينتهك هذه الحرمة ويسرق السمع على المكالمات، وهذا الإسناد وضعه المشرع بغية السير الحسن لتحريات والتحقيقات[2].

3– تستهدف عملية إعتراض المراسلات على دليل غير مادي: تعتبر تقنية التنصت على الأحاديث الهاتفية دليل غير مباشر ينبعث من عناصر شخصية مما يصدر عن الغير من أوقوال وأحاديث تقنع القاضي بطريقة غير مباشرة تفيد في الكشف عن الجريمة، فتعتبر الأحاديث دليل معنوي غير مادي، فهدف إعتراض المراسلات هو إلتقاط الأدلة المعنوية بغية تأكيد أدلة الإتهام[3].

[1] مختار خداوي، إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري، مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة الطاهر مولاي–سعيدة، الجزائر، 2016/2015، ص 32.

[2] سارة قادري، أساليب التحري الخاصة في قانون الاجراءات الجزائية، مذكرة ماستر، تخصص قانون أعمال، جامعة قاصدي مرباح–ورقلة، الجزائر، 2014/2013، د ص.

[3] نفس المرجع.

4- تستخدم إعتراض المراسلات أجهزة قادرة على إلتقاط الأحاديث : مع مضى عهد إستراق السمع من وراء الأبواب والنوافذ وتطور عهد التكنولوجيا الحديثة، أصبح من الضروري إيجاد تقنيات جديدة ذو فاعلية كبيرة لإقتحام خصوصيات الأشخاص المشتبه بهم، وخصوصا مع التطور الذي عرفته العمليات الإجرامية التي شكلت قلقا رهيبا في أوساط المجتمع، لذا تستلزم عملية إعتراض المراسلات إستخدام أجهزة ذو تقنية واسعة قادرة على إلتقاط الأحاديث الصوتية بدقة وجودة عالية[1].

ج-الشروط الموضوعية لإعتراض المراسلات: يشترط في إجراء إعتراض المراسلات الشروط الموضوعية التالية:

1- **التسبيب:** يعتبر التسبيب أساس العمل القضائي، ومن ثم كان لزاما عند إصدار الإذن بإجراء عمليات الإعتراض أو إلتقاط والتسجيل سواء من طرف وكيل الجمهورية أو قاضي التحقيق، إظهار الأدلة القانونية والموضوعية بعد تقدير جميع العناصر المعروضة عليه من طرف ضابط الشرطة القضائية.

2- نوع الجرائم: حصرت المادة 65 مكرر من قانون الإجراءات الجزائية المعدل والمتمم، إجراء الإعتراض، الإلتقاط والتسجيل في جرائم المخذرات، الجريمة المنظمة العابرة للحدود، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات، جرائم تبيض الأموال، جرائم الإرهاب، جرائم الصرف أو جرائم الفساد. وتجدر الإشارة إلى أنه يترتب على تخلف أحد شروط عمليات الإعتراض والالتقاط والتسجيل بطلان الإجراء[2].

د- الشروط الشكلية لإعتراض المراسلات: يشترط في إجراء إعتراض المراسلات الشروط الشكلية التالية:

[1] صالح شنين، اعتراضات المراسلات و سجيل أصوات وإلتقاط الصور في قانون إجراءات الجزائية الجزائري، مذكرة ماستر، كلية الحقوق، جامعة عبد الرحمن ميرة-بجاية، الجزائر، د س ن، ص 96.

[2] نفس المرجع.

1- الإذن بإعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور: من الناحية القانونية لا يحق لقاضي التحقيق إصدار إذن بإجراء هذه العمليات وفقا لشكل معين، وإذا كان قد إشترط أن يكون مكتوبا ومتضمنا كل العناصر التي تسمح بالتعرف على الإتصالات المطلوبة إلتقاطها والأماكن المقصودة سكنية كانت أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير مع الإشارة إلى مدة إنجاز هذه العمليات، على أن يكون أقصاها أربعة (4) أشهر قابلة للتجديد[1]، وذلك وفقا لنص المادة 65 مكرر 7 من قانون الإجراءات الجزائية االمعدل والمتمم.

تنص المادة 65 مكرر 7 من قانون الإجراءات الجزائية االمعدل والمتمم، على:" يجب أن يتضمن الإذن المذكور في المادة 65 مكرر 5 أعلاه، كل العناصر التت تسمح بالتعرف على الاتصالات المطلوب التقاطها والأماكن المقصودة سكنية أو غيرها والجريمة التي تبرر اللجوء إلى هذه التدابير ومدتها.

يسلم الإذن مكتوبا لمدة أقصاها أربعة (4) أشهر قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكلية والزمنية".

الملاحظ على نص المادة المذكور أعلاه، أنها قصرت الإذن على تدابير إعتراض المراسلات المطلوب إلتقاطها دون التسجيل الصوتي أو السمعي البصري، وأن المشرع الجزائري لم يراع العامل الزمني، إذ لم يحدد مرات قابلية هذا الإذن بهذه العمليات توقيفها قبل الموعد المحدد في الإذن[2].

2- ضرورة تدوين محضر العمليات: إن طبيعة عمليات الإعتراض وتسجيل وإلتقاط الصور لا ينتظر بلوغ مرحلتها النهائية لتحرير محضر بشأنها، فهناك ضباط الشرطة القضائية المكلفين يقيام العمليات عليهم بتحرير محاضر على كل مرحلة على حدى، إذ يحرر بشكل مفصل محضر دخول

[1] محمد شرف،مختار خرشبن، المرجع السابق، ص53.

[2] فوزي عمارة، "إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية ،كلية الحقوق، جامعة الإخوة متنوري-قسنطينة1، الجزائر، العدد 33، جوان 2010، ص 241.

المساكن ومحضر إلتقاط الصور ومحضر عملية الإعتراض، ويشمل كل محضر من هذه المحاضر على تاريخ وساعة بداية العملية وكذا تاريخ الإنتهاء منها[1].

كما أوجب المشرع في نص المادة 65 مكرر 10 وصف أو نسخ المراسلات والصور أو المحادثات المسجلة والمعيدة في إظهار الحقيقة كمرافقات تودع بالملف، ونسخ وترجمة المكالمات التي تتم باللغة الأجنبية عند الإقضاء بمساعدة مترجم يسخر لهذا الغرض ولايكون لهذه المحاضر قوة إثبات إلا إذا كانت صحيحة[2].

رابعا: الحفظ وإفشاء العاجلان للمعطيات الإلكترونية

يُعد الحفظ والإفشاء من الإجراءات المستخدمة للكشف عن الجريمة المعلوماتية والوصول إلى الدليل الرقمي، ونصت المادة 10 من قانون 09- 04 المتعلق بالوقاية من الجرائم المتلعلقة بتكنولوجيا الإعلام والإتصال ومكافحتهما[3]، على أنه:" يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الإتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحقيقين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق".

ومن ثم هناك نوع من المعطيات يجب أن تكون محل حفظ، حيث حددت المادة 11 من قانون رقم 09- 04 المتعلق بالوقاية من الجرائم المتلعلقة بتكنولوجيا الإعلام والإتصال ومكافحتهما، معطيات

[1] رمزي بوشالة، التنصت على المكالمات وإلتقاط الصور بين التجريم والإباحة، مذكرة ماستر، تخصص قانون جنائي للأعمال، كلية الحقوق، جامعة العربي بن مهدي-أم البواقي، الجزائر، 2015/2014، ص 24.

[2] صالح شيشن، المرجع السابق، ص 68.

[3] عائشة نايري، المرجع السابق، ص 52.

المرور التي يتعين على مقدم الخدمات التحفظ عليها بناءا على طلب من السلطة القضائية المختصة. والتي تجسدت فيما يلي[1]:

-المعطيات التي تسمح بالتعرف على مستعملي الخدمة،

-المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال،

-الخصائص التقنية وكذا تاريخ ووقت ومدة كل إتصال،

-المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة ومقدميها،

- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الاتصال وكذا عناوين المواقع المطلع عليها.

[1] نوال مجدوب، المرجع السابق، ص 204.

خلاصة الفصل

إن مفهوم الجريمة الإلكترونية يقوم على أسس قانونية وفقهية، تلك التي يقوم عليها التحقيق الجنائي في هذا المجال الحديث والمعقد. حيث تطرقنا إلى تعريف الجريمة الإلكترونية من الناحيتين الفقهية والقانونية وبيّنا أطرافها وخصائصها وأركانها، إن دراسة تصنيفات و أساليب البحث والتحري عن هذه الجرائم تحتاج إلى صب التركيز على الأجهزة المختصة في الجرائم، مثل الضبطية القضائية ومركز الوقاية من جرائم الإعلام والاتصال، ومن ثم التطرق إلى الإجراءات المتبعة في التحقيق سواء التقليدية أو المستحدثة التي تتناسب مع طبيعة الجرائم الالكترونية.

الفصل الثاني

الدليل الإلكتروني كأداة إثبات في الجرائم الالكترونية

تمهيد

في ظل التطور التكنولوجي المتسارع والإنفتاح الرقمي غير المسبوق، أصبحت الجرائم الإلكترونية تمثل تحديا متناميا ذا أبعاد أمنية وقانونية بالغة التعقيد يهدد أفراد ومؤسسات على حد سواء، ولم تعد هذه الجرائم تقتصر على إختراق الأنظمة و رقة المعلومات بل توسعت لتشمل أنماطا أكثر تطورا كجرائم الإبتزاز الإلكترونية، الإحتيال المالي، إنتحال الهوية وغيرها من الأفعال الإجرامية التي باتت تشكل ظواهر مقلقة في الفضاء السبيراني.

وفي مواجهة هذا التحدي المتصاعد أصبح من الضروري أن يضطلع المشرع الجزائي بدور محوري في مواكبة هذا الواقع، من خلال وضع نصوص قانونية توضح كيفية التعامل مع هذه الجرائم الناشئة ويحدد السبل القانونبة و الإجرائية لاثباتها جنائيا، خاصطا بالنظر الى التعقيد للرسائل الوقائية المستخدمة في إرتكابها. ومن هذا المنطلق يبرز مفهوم الأدلة الإلكترونية كوسيلة أساسية في التصدي لهذه الجرائم. إذ يهدف إلى توفير مرجعية قانونية وتقنية لتعزيز الوعي بمخاطر الجريمة الإلكترونية وتقديم آليات ناجحة للإبلاغ عنها بما يساهم في ترسيخ الأمن السبيراني وتهيئة بيئة رقمية أكثر أمنا.

ولهذا سيتم في هذا الفصل التطرق إلى الدليل الإلكتروني كأداة إثبات في الجرائم الالكترونية، حيث تم تقسيمه إلى:

- **المبحث الأول: ماهية الدليل الإلكتروني ومشروعيته.**
- **المبحث الثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني.**

المبحث الأول: ماهية الدليل الإلكتروني ومشروعيته

يعد الدليل الإلكتروني الركيزة الأساسية في إثبات الجرائم الالكترونية بإعتباره الوسيلة الوحيدة الرئيسية للكشف عنها، ولا شك أن هذا النوع من الأدلة جاء مواكبا للتطورات التكنولوجية والتقنية من جهة، ومساهما في مكافحة الجريمة الإلكترونية من جهة أخرى، مما يجعل من الضروري على أجهزة العدالة التعامل معه كدليل مستحدث وفعال لمواجهة هذا النوع من الجرائم. لذلك سوف يتم تحديد مضمون هذا الدليل من خلال تعريفه، ذكر خصائصه وأنواعه في (المطلب الأول)، ومن ثم تسليط الضوء على مشروعية هذا الدليل في (المطلب الثاني).

المطلب الأول: مفهوم الدليل الإلكتروني

إختلفت الآراء حول الدليل الإلكتروني، إلا أنه يقصد به عموما الأدلة المستخرجة من الأنظمة الحاسوبية والوسائط الإلكترونية والتي يعتمد عليها بغرض الإثبات. ونتناول في هذا المطلب تعريف الدليل الإلكتروني (الفرع الأول) وخصائصه (الفرع الثاني) وأنواعه (الفرع الثالث).

الفرع الأول: تعريف الدليل الإلكتروني

قبل التطرق إلى تعريف الدليل الإلكتروني من الضروري أولا التعريف بمصطلح " **الدليل** "، وكذا "**الإلكتروني**" ككل كلمة على حدا.

أولا: تعريف مصطلح الدليل

أ–تعريف الدليل لغة: يقصد به المرشد وما يستند به، والدليل الدال والجمع أدلة ودلالات، والدليل ما يستدل به دال أيضا، وقد دله على طريق يدله بالضم دلالة بفتح الدال وكسرها ودلوها بالضم والفتح الأعلى، وفلان دل فلاف أي يثق به[1].

1- المعجم الوجيز، مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم، مصر، 2004، ص 234.

ب– تعريف الدليل اصطلاحا: فهو الذي يلزم من العلم بسبب آخر، وغايته أن يتوصل العقل إلى تصديق اليقين بما كان يشك في صحته، أي التوصل إلى المعرفة الحقيقية، وأيضا يقصد بالدليل ما يمكن التوصل إلى معرفة الحقيقة[1].

ج– التعريف التشريعي للدليل: الدليل في إصطلاح القانون هو ما يلزم من العلم به، العلم بشيء آخر، فإذا أعلم المدعي القاضي بحجته على دعواه لزم من علم القاضي بتلك الحجة مع إقناعه بها، بهدف علمه بصدق دعوى المدعي فيما دعاه[2].

قال تعالي: {ألم ترى إلى ربك كيف مد الظل ولو شاء لجعله ساكنا ثم جعلنا الشمس عليه دليلا}[3]. الاية 49 من سورة الفرقان.

ثانيا: تعريف مصطلح الالكتروني

أ– تعريف الالكتروني لغة: اسم منسوب إلى إلكترون ويوصف به ما كان تابعا لمجال الإلكترونيك فيقال حاسب الكتروني، ومجهر إلكتروني، البرمجة الإلكترونية، بريد إلكتروني[4].

ب–تعريف الالكتروني إصطلاحا:

ثالثا: تعريف الدليل الإلكتروني

1– جلال فضل محمد العودي، الدليل الإلكتروني وسلطات القاضي الجنائي في تقديره، قانون جنائي، ص 29، انظر عبر الرابط www Noor – book com https

2– عبيدة بلعابد، "الدليل الرقمي بين حتمية الإثبات و حق في خصوصية المعلومات"، مجلة الآفاق العلمية، جامعة أمين العقال الحاج موسى اق خموك– تمنراست، الجزائر، العدد 01، 2019، ص 137

3– الآية 99 من سورة الفرقان.

4– أحمد مختار عمر وآخرون، معجم اللغة العربية المعاصرة، عالم الكتب، جزء1، الطبعة 1، القاهرة–مصر، 2008، ص 764.

يُعرف الدليل الإلكتروني، بأنه:" الدليل الذي يحدد له أساس في العالم الإفتراضي ويقود إلى الجريمة، أو هو تلك المعلومات التي يقبلها المنطق والعقل ويعتمدها العلم ويتم الحصول عليها بإجراءات قانونية وعلمية بترجمة آليات البيانات الحسابية المخزنة في أجهزة الحاسب الآلي"[1].

كما يعرف بأنه:" الأخذ من أجهزة الكمبيوتر ويكون في شكل مجالات أو نبضات مغناطيسية، أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة، وهي مكون رقمي لتقديم معلومات في أشكال متنوعة، مثل: النصوص، الأصوات، الصور،الأشكال، أو الرسوم. وذلك من أجل إعتماده أمام أجهزة إنفاذ وتطبيق القانون"[2].

إذن الدليل الإلكتروني هو المعلومات المخزنة أو المنقولة بصفة رقمية ويعتمد عليها في التحقيقات وأمام المحكمة، إما بالإدانة أو بالبراءة.

الفرع الثاني: خصائص الدليل الإلكتروني

يتميز الدليل الإلكتروني بعدة خصائص تميزه عن باقي الأدلة التقليدية، وأهمها الدليل الإلكتروني، وهو الواقعة التي تبين عن وقوع جريمة أو فعل غير مشروع وهذه الواقعة منبتها علمي من حيث أن مبنى العالم الإفتراضي علمي، وهذه الخاصية مفادها أن الدليل الإلكتروني لا يمكن الحصول عليه والإطلاع على فحواه إلا باستخدام الأساليب العلمية[3].

وإنطلاقا من هذه الخاصية يمكن القول أنه لا يمكن الحصول على الدليل الجنائي الإلكتروني أو الإطلاع عليه سواء باستخدام الوسائل والأساليب العلمية، ويعود ذلك للمنشأ الذي تَكَوَنَ فيه هذا الدليل[4].

1- نور هدى محمودي، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، جامعة الحاج لخضر- باتنة1، الجزائر، العدد 11، 2017، ص 911.

2- نفس المرجع.

3- أمال لصامي، جميلة بن طالب، حجية الدليل الإلكتروني في إثبات وحق التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي، جامعة مولاي الطاهر-سعيدة، الجزائر، 2022/2021، ص 20.

4- فؤاد أوساسي، دور الدليل الإلكتروني في الإثبات الجنائي، مذكرة ماستر، تخصص قانون جنائي، جامعة زيان عاشور-الجلفة، الجزائر، 2020/2019، ص 8.

أولا: الدليل الإلكتروني ذو طابع تقني ومتطور

يعتمد الدليل الإلكتروني على تقنية المعلوماتية المتطورة متمثلة في نبضات كهربائية أو مغناطسية عالية الدقة لا تحتمل الخطأ، فهو لا يوجد في واقع مادي ملموس بل يجد أساسه في بيئة رقمية ذات طبيعة ديناميكية تتميز بالسرعة الفائقة التي تتخطى حدود الزمان والمكان[1].

لا إختلاف عن إعتبار الدليل الإلكتروني دليلا متطورا بطبيعته، فهو يمتاز بتطور تلقائي تبعا لتطور البيئة الرقمية التي تعتمد أساسا على التجديد. ويرجع هذا إلى تطور الثورة التكنولوجية خاصة في مجال الإتصالات وأجهزة التواصل[2].

ثانيا: الدليل الإلكتروني يصعب التخلص منه

تُعد هذه الخاصية من أهم الخصائص التي يتميز بها الدليل الإلكتروني عن الأدلة التقليدية الأخرى، إذ أنه يمكن التخلص بسهولة من الأدلة التقليدية الأخرى، حيث يمكن بسهولة التخلص من الأدلة الأخرى كالأوراق، السلاح، الأموال المزورة بإتلافها وحرقها، أما الدليل الإلكتروني بشكل خاص وكل ما يتعلق بتكنولوجيا المعلومات بشكل عام، فإنه كلما حدث إرتباط أو إتصال أو وسيلة تقنية المعلومات، فإنه يصعب التخلص من ذلك ولو استخدمت أدوات الحذف والإلغاء[3].

1- طارق قادري، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، الطبعة 1، المملكة المتحدة-بريطانيا، جانفي 2024، ص 141.

2- عبيدة بلعابد، المرجع السابق، ص 138.

3- جلال فضل محمد العودي، المرجع السابق، ص 34.

حيث يتميز الدليل الإلكتروني بصعوبة محوه وتحطيمه، اذ حتى بمحاولة إصدار أمر بإزالة ذلك الدليل فمن الممكن إعادة إظهاره من خلال ذاكرة الآلية التي تحتوي على ذلك الدليل، ويعتمد على استخدام أجهزة خاصة تقوم بتجميع وتحليل محتواه، ولذلك فكل ما لا يمكن تحديد وتحليل محتواه بواسطة تلك الأجهزة لا يمكن إعتباره دليلا إلكترونيا[1].

ثالثا: الدليل الإلكتروني دليل قابل للنسخ

أهم ما يميز الدليل الجنائي الإلكتروني قابليته للنسخ، وتكون النسخ مستخرجة ذات قيمة بمثابة الدليل الأصلي مما يسهل للمحقق المحافظة على النسخ الأصلية من التلف أو الفقد أو التلاعب بها فيسهل إثباتها أمام القضاء[2]. وذلك من خلال نسخ الدليل لنسخ تكون طبق الأصل ولها ذات الحجية الثبوتية، فالوثيقة المحفوظة على هيئة مستند في جهاز الحاسب الآلي يمكن نسخها بسهولة من الأصل وتقديم الملف كدليل إثبات يكون لتلك النسخة ذات القيمة العلمية والحجية التي يمتلكها الأصل[3].

رابعا: الدليل الإلكتروني ذو طبيعة ثنائية

تُعتبر الطبيعة الثنائية التي يختص بها الدليل الإلكتروني إمتدادا للطبيعة التقنية لهذا الأخير، وأيضا إمتداد للبيئة الإفتراضية التي تكون فيها. لذا فالمعلومات والبيانات التي تشكل دليلا جنائيا رقميا تكون في الأصل شكلا ثنائيا أو رقميا، ومراد ذلك أن الحاسب الآلي أو أي جهاز آخر له نفس خصائصه يقوم باستقبال هذه البيانات والمعلومات ويقوم بتحويلها إلى أرقام ثم معالجتها[4].

1- حنان ميمون، عارف ناصري، سلطة القاضي في تقدير الدليل الرقمي، مذكرة ماستر، قانون إعلام آلي، جامعة محمد البشير الابراهيمي- برج بوعريريج، الجزائر، 2023/2022، ص 12.

2- فيصل الغامدي، الأدلة الرقمية وحجيتها في إثبات النظام السعودي، مجلة العربية للنشر العلمي، المجلد 07، العدد 69، 2024، ص 102.

3- مسعد بن المعمري، الدليل الإلكتروني لإثبات الجريمة الالكترونية، ملحق خاص، العدد 03، جزء 02، أكتوبر 2018، ص 201.

4- مسعود نطوي، " خصوصية الدليل الإلكتروني "، مجلة الفكر القانوني والسياسي، جامعة عمار ثلجي-الأغواط، الجزائر، المجلد 07، العدد 01، ص 1065.

فمضمون الطبيعة الثانية للدليل الإلكتروني هو إختزال البيانات أو المعلومات كالنصوص أو الصور أو الصوت أو أي معلومة أخرى إلى رموز ثنائية، وهذه الرموز الثنائية تتكون من سلسلة من رقم الصفر (0) ورقم واحد (1)، ومثال ذلك أن الحرف (أ) يقابله في البيئة الافتراضية (110 11000) و هكذا يتم الترميز من خلال طرق الترميز نقل وتمثيل البيانات المختلفة[1].

المطلب الثاني: مشروعية الدليل الإلكتروني

تُعرف المشروعية بأنها سيادة القانون أو هي مطابقة أي تصرف أو أي عمل قانوني للقانون، سواء كان التصرف أو العمل في مجال القانون العام أو في أي مجال القانون الخاص، ويقصد بمشروعية الدليل الإلكتروني أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الاستناد إليه[2]. إذ تختلف مشروعية الأدلة في النظم القانونية في موقفها من حيث الأدلة.

إذا تتمثل مشروعية الدليل الإلكتروني إما في النظم الحر (الفرع الأول)، أو مشروعية الدليل الإلكتروني المقيد (الفرع الثاني).

الفرع الأول: مشروعية الدليل الإلكتروني في النظام الحر

في نظام الإثبات الحر لا يحدد القانون أدلة الإثبات ووسائله بل يترك للقاضي الحرية في أن يؤسس حكمه على أي دليل وفقا لإقتناعه الشخصي دون أن يفرض عليه أي دليل يعينه والإعتراف له، فالقاضي حر في أن يستعين بكل طرق الإثبات للبحث عن الحقيقية وهو حر في وزن وتقدير كل دليل[3].

1- أسامة حسن محي الدين عبد العال، " حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)"، مجلة البحوث القانونية والاقتصادية، العدد 76، 2021، ص ص: 644 و645.

2- حنان ميمون، عارف ناصري، المرجع السابق، ص 37.

3- شهيرة مزعاء، عيسى حداد، " حجية الدليل الإلكتروني أمام القضاء الجزائي"، دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي مرسلي عبد الله- تيبازة، الجزائر، المجلد 07، العدد 02، 2023، ص 250.

وهذه الحرية تؤمن للقاضي الجنائي القيام بدور إيجابي في عملية البحث عن الحقيقة بشأن الجريمة المعروضة أمامه على ثلاث جوانب فهو يقوم بدور إيجابي في جمع الأدلة التي تقربه من كشف الحقيقة،كما له الحرية في قبول أي دليل يفيد في أمر الدعوى المطروحة أمامه وفقا لإقتناعه[1].

الفرع الثاني: مشروعية الدليل الإلكتروني في النظام المقيد

يُعد نظام الإثبات القانوني أو المقيد هو السائد في النظام الإنجليزي، وفي هذا النظام تكون الأدلة محصورة ومحددة سلفا من قبل المشرع بل إن قوتها الدليلية محددة ولا يجوز للقاضي أن يخرج عليها أو يبين حكمه على خلافها[2].

فهو النظام الذي يقوم على قواعد وطرق محددة ومنظمة للإثبات، لا يمكن أن يقوم الأطراف بإثبات دعواهم إلا من خلالها، وبذلك تكون السلطة ناظر الدعوى قاصرة لا تستطيع الحكم إلا من خلال الوسائل التي حددها المنظم أو المشرع للإثبات حتى و إن ثبت أمامه فعلا الحق المدعى به[3].

حيث أن القانون قيد القاضي بقائمة من الأدلة التي حددت قيمتها الإثباتية وهذا النظام ينتمي إلى النظم ذات الثقافة الانجلوسكسونية، مثل: الولايات المتحدة الأمريكية و لذا فإن النظم التي تتبنى هذا النظام لا يمكن في ظلها الإعتراف بالدليل الرقمي[4].

1- محمد محمد عبد الظاهر موسى، "القيمة الثبوية للدليل الرقمي وضوابط إقناع القاضي الجنائي"، مجلة البحوث القانونية والإقتصادية، جامعة بن يوسفي، المجلد 36، العدد 2، يوليو 2006، ص 265.

2- عباس بوسندة، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه، تخصص علوم جنائية، جامعة جيلالي اليابس- سيدي بلعباس، الجزائر، 2013/ 2014، ص 267.

3- فيصل ماطوف العصاف، سليمان العجاني، " ماهية الدليل الرقمي في النظام السعودي-دراسة مقارنة"، مجلة الدولية للدراسات القانونية والسياسية، مركز كيدني للبحث والتطوير، لندن-المملكة المتحدة، 15 أفريل 2023، ص 53.

4- حكيم محمد عثمان، "حجية الدليل الإلكتروني في مجال الإثبات الجنائي وموقف المشرع الليبي "، مجلة الحق، ليبيا، العدد 07، 2014، ص 105.

وما يعاب على نظام الإثبات القانوني تقيده للقاضي على نحو يفقده سلطته في الحكم بما يتفق مع الواقع، فيحكم في الكثير من الأحيان بما يخالف قناعته التي تكونت لديه من أدلة لا يعترف بها ذلك النظام فيصبح القاضي كآلة في إطاعته لنصوص القانون[1].

وبالرغم من أن هذا النظام وضع لحماية المتهمين من التعسف واستبداد القضاء، إلا أنه أخرج القاضي من وظيفته الطبيعية وسمح للمشرع أن يتدخل في نطاق لا يملكه، حيث قام بتقنين اليقين في قواعد عامة محددة على الرغم من أن هذا اليقين مسألة واقع ترتبط بظروف كل قضية وتترك لتقدير قاضي الموضوع، وغلب مصلحة على مصلحة أخرى في حين كان يجب عليه أن يقيم موازنة معتدلة بين حق الإنسان في البراءة وحق المجتمع في العقاب[2].

ومنها إعتمد المشرع الجزائري في الإثبات على مبدأ حرية الإثبات كأصل ونظام الأدلة القانونية كاستثناء من الأصل[3]. فنصت المادة 212 في فقرتها 1 من قانون الإجراءات الجزائية المعدل والمتمم، على أنه:" يجوز إثبات الجرائم بأي طريق من طرق الإثبات ما عدا الأحوال التي ينص عليها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص".

كذا نص المادة 307 من نفس القانون، التي نصت على:" ... إن القانون لا يطلب من القضاة أن يقدموا حسابا عن الوسائل التي بها وصلوا إلى تكوين إقتناعهم ..."[4].

وبتطور دور الإثبات العلمي وظهور الدليل الرقمي جعل القاضي في هذا النظام يضطر إلى التعامل مع الأدلة المستحدثة بغية اكتشاف الجرائم، ونتيجة لهذا المبدأ فإن القاضي غير مقيد بالأدلة التي يقدمها

1- خالد ضو، " حجية الدليل الإلكتروني وشروط قبوله والإثبات الجنائي "، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية ،جامعة بن يوسف بن خدة-جامعة الجزائر 1، الجزائر، 2022، ص 206.

2- أسامة حسن محي الدين العال، المرجع السابق، 624.

3- فؤاد اوساسي، المرجع السابق، ص 55.

4- كلثوم فراوي، " مشروعية الدليل الإلكتروني في الإثبات الجنائي "، مجلة طبنة للدراسات العلمية والاكاديمية، المركز الجامعي سي الحواس-بريكة، الجزائر، المجلد 05، العدد 01، 2022، ص 989.

أطراف الدعوى لأنه من حقه أن يبادر بنفسه لإتخاذ جميع الإجراءات بحثا عن الأدلة اللازمة لتكوين إقتناعه[1].

وفي سبيل ذلك يوجه أوامره إلى مزود خدمة الإنترنت من أجل جمع الأدلة الرقمية كعناوين المواقع التي إطلع عليها المتهم والملفات والحوارات، كما يأمر مشغل النظام بتقديم المعلومات اللازمة لإختراق النظام والولوج إلى داخله، كما أن للقاضي الجنائي وفق هذه التشريعات أن يتأكد أولا من قبول الدليل ومدى صحته ومصداقيته[2].

الفرع الثالث: أنواع الدليل الإلكتروني

يتخذ الدليل الإلكتروني أشكالا متعددة مما يمثل مجموعة من البيانات، والتي يمكن الإعتماد عليها كوسيلة لإثبات الجرائم الإلكترونية. أما عن أنواع الدليل الإلكتروني كدليل إثبات من عدمه يمكن تقسيمه لنوعين رئيسيين:

أولا: الأدلة المعدة لتكون وسيلة إثبات

تنقسم الأدلة الجنائية الإلكترونية إلى قسمين، القسم الأول يتمثل المعلومات والبيانات المنشئة تلقائيا من طرف الحاسب الآلي، وأما القسم الثاني يتمثل في المعلومات والبيانات ذات الطبيعة المختلطة[3].

أ-**المعلومات أو البيانات المنشئة تلقائيا من طرف الحاسب الآلي**: وهي جميع المعلومات والبيانات الرقمية التي تم إنشاؤها بواسطة جهاز الحاسب الآلي أو أي جهاز آخر ولا دخل للمستخدم في إنشائها، أو السجلات التي تعتبر من مخرجات جهاز الحاسب الآلي، مثل: فواتير البطاقات البنكية المعدة آليا[4].

1- محمد بن فردية، الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي-دراسة مقارنة، المجلة الأكادمية للباحث القانوني، جامعة عبد الرحمن ميرة-بجاية، الجزائر، المجلد 09، العدد01، 2014، ص 282.

2- نفس المرجع.

3- فؤاد أوساسي، المرجع السابق، ص 12.

4- نفس المرجع.

ب–المعلومات والبيانات ذات الطبيعة المختلطة: وهي البيانات التي تم إنشاء جزء منها بواسطة الحاسب الآلي أما الجزء الآخر يحفظ بإدخال أي معلومات ذات طبيعة مختلطة تحفظ عادة للإحتجاج بها لاحقا[1].

لذا تكمن أهمية النوعين السابق ذكرهما في كونها أعدا سلفا بغرض استخدمهما كوسيلة لإثبات بعض الوقائع التي تتضمنهما، ولهذا يتم حفظ هذه المعلومات والبيانات الرقمية للاحتجاج بها لاحقا، قصد التقليل من إمكانية فقدانها كما يسهل الحصول عليها عند الحاجة[2].

ثانيا: الأدلة غير المعدة لتكون وسيلة إثبات

هذا النوع من الأدلة الإلكترونية ينشأ دون إرادة الشخص، فهو يعد أثر يتركه الشخص دون أن يكون قاصدا وجوده[3]. وسمي هذا النوع بالبصمة الإلكترونية أو الآثار المعلوماتية الإلكترونية وهي تتجسد في الآثار التي يتركها مستخدم الشبكة المعلوماتية، بسبب تسجيل الرسائل المرسلة منه أو التي يستقبلها وهو لم يعد أساسا للحفظ من قبل من صدر منه، غير أن الوسائل الفنية الخاصة تتمكن من ضبط هذه الأدلة ولو بعد فترة زمنية من نشوؤها[4]. مثال ذلك: البيانات والمعلومات المضمنة في ملفات الولوج lag files، والتي تحتوي على معلومات كتاريخ ووقت التحميل أو إرسال ملفات المستخدم.

وتكمن أهمية هذا النوع من الأدلة على أنه قد يحتوى على معلومات تساعد في الكشف عن هوية مرتكب الجريمة بواسطة تقنيات وبرامج خاصة[5].

1– هاجر طباخ، صبرينة مقلاتي، الأدلة الرقمية ودورها في الإثبات الجنائي، مذكرة ماستر، تخصص إعلام آلي وإنترنت، جامعة محمد البشير الابراهيمي–برج بوعريريج، الجزائر، 2024/2023، ص 17.

2– نعيم سعيداني، آليات التحري عن الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجستير، تخصص علوم جبائية، جامعة الحاج لخضر–باتنة1، الجزائر، 2013/2012، ص 129.

1– مسعود ين حميد المعمري، " الدليل الإلكتروني لإثبات الجريمة الإلكترونية "، مجلة القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي، عدد خاص، الجزء 2، العدد 3، 2018، ص 203.

2– عائشة عبد الحميد، "الدليل الرقمي كحجية للإثبات أمام القاضي الجزائري في المعاملات الإلكترونية "، مجلة صوت القانون، جامعة الجيلالي بونعامة – خميس مليانة، الجزائر، المجلد 07، العدد 01، ماي 2020، ص 485.

3– هاجر طباخ، صبرينة مقلاتي، المرجع السابق، ص 18.

المبحث الثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني

يعتبر الدليل الجنائي الوسيلة القانونية التي يعتمد عليها القاضي للوصول إلى الحقيقة، حيث يمتلك سلطة واسعة في تقدير الأدلة، حتى وإن كانت علمية ولا يجوز له أن يبنى قراره إلا على الأدلة المقدمة له والمشروعة. ويعد الدليل الإلكتروني من أهم وسائل الإثبات في الجرائم الإلكترونية ضمن البيئة الإفتراضية مما يمنحه مزايا تميزه عن غيره من الأدلة، إلا أن استخراج هذا النوع من الأدلة يواجه العديد من الصعوبات سواء من حيث طبيعته التكوينية أو الإجراءات المتبعة في استخلاصه. ولدراسة هذا الأمر نقسم مبحثنا إلى مطلبين: شروط قبول الدليل الإلكتروني في المطلب الأول، وصعوبات استخلاص الدليل الإلكتروني في المطلب الثاني.

المطلب الأول: شروط قبول الدليل الإلكتروني

لا يمكن الإعتماد على الدليل الإلكتروني كوسيلة إثبات في الجرائم الإلكترونية إلا إذا استوفى مجموعة من الشروط، والتي تسمح بقبوله كدليل قانوني في تلك الجريمة، وهي أن يكون مشروعا (الفرع الأول)، وأن يطرح الدليل للمناقشة (الفرع الثاني)، وأن يبلغ القاضي الإقناع درجة اليقين (الفرع الثالث).

الفرع الأول: شرط مشروعية الدليل الإلكتروني

الدليل الرقمي يجب أن يكون مشروعا أي أن إجراءات جمع الأدلة الإلكترونية المتحصل عليها من الحاسب الآلي إذ خالفت قواعد الإجراءات التي تنظم كيفية الحصول عليها، فإنها تكون باطلة و لا تصلح أن تكون أدلة تبنى عليها الإدانة في المواد الجزائية[1].

كما أوصى المؤتمر الدولي الخامس عشر (15) للجمعية الدولية لقانون العقوبات في مجال حركة اصلاح الإجراءات الجنائية وحماية الإنسان، بمجموعة من التوصيات منها التوصية رقم 18 التي نصت على أن كل الأدلة التي يتم الحصول عليها عن طريق إنتهاك حق أساسي للمتهم، والأدلة الناتجة عنها تكون باطلة ولا يمكن التمسك بها أو مراعاتها في أي مرحلة من مراحل الإجراءات[2].

ومعنى ذلك أن تكون الوسائل والأدوات تمت بشكل قانوني ومشروع، حيث أن الدليل لا يكون مشروعا ومقبولا في عملية الإثبات التي تتم من خلالها إخضاعه للتقدير، إلا إذا أجريت عملية البحث عنه أو الحصول عليه وكذا عملية تقديمه إلى القضاء أو إقامته بالطرق التي وضعها القانون، والتي تكفل تحقيق توازن عادل بين حق الدولة في العقاب وحق المتهم في توفير الضمانات الكافية لإحترام كرامته[3].

1- مبارك بن الطيب، محمد رحموني، " شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية "، مجلة القانون والعلوم السياسية، المركز الجامعي صالحي أحمد-النعامة، الجزائر، المجلد 05، العدد 02، 2019، ص 27.

2- شهيرة مرغاد، عيسى حداد، المرجع السابق، ص 310.

3- أسامة حسين محي الدين عبد العال، المرجع السابق، ص 682.

ويقصد بمشروعية الدليل الإلكتروني أن يعترف المشرع بهذا الدليل من خلال تصنيفه في قائمة الأدلة القانونية التي يجيز القانون فيها للقاضي الاستناد إليه في تكوين عقيدته[1].

الفرع الثاني: شرط مناقشة الدليل الإلكتروني

بني بهذا الضابط وجوب استخلاص القاضي لقناعته من الأدلة القضائية، أي تلك التي طرحت في جلسة بحضور الخصوم وبصورة علانية، وهذا الضابط بمبدأ حرية القاضي في الإقتناع يحقق العدالة ويكشف الحقيقة ويضمن الدفاع من خلال فتح الباب المناقشة أمام الخصوم فيما يخص ما يقدم من الأدلة[2].

ولا يمكن للقاضي أن يبني حكمه على دليل لم يطرح أمامه في الجلسة لأنه ليس حرا في تكوين عقيدته من أي دليل حتى ولو لم يطرح في المناقشة في الجلسة، ولذا يجب أن يستند القاضي في حكمه بالإدانة إلى دليل عرض في الجلسة على الخصوم وتمت مناقشته، كما يجب أن يكون لهذا الدليل أصل في أوراق الدعوى، فإذا لم يكن كذلك كان الحكم معيبا[3].

وهذا يعني أن الحكم الذي يبنى على دليل لم يطرح للمناقشة ولم تمنح للخصوم إمكانية مناقشته يعتبر حكما باطلا[4]، وهو ما أشار إليه المشرع الجزائري في نص المادة 212 الفقرة 2 منها من قانون الإجراءات الجزائرية المعدل والمتمم، على أنه:" ...ولا يسوغ للقاضي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريا أمامه".

ومنه يجب أن تناقش كل الأدلة المتحصل عليها من جرائم الحاسوب والإنترنت سواء كانت مطبوعة أم بيانات معروضة على شاشة الحاسوب، أم كينات مدرجة في حاملات البيانات، أم إتخذت أشرطة

1- نعيم سعيداني، المرجع السابق، ص 208.

2- حنان ميمون، عارف ناصري، المرجع السابق، ص 34.

3- سامية بلجراف، " سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي"، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي- الشلف، الجزائر، المجلد 07، العدد 01، 2012، ص 687.

4- طارق قادري، المرجع السابق، ص 149.

وأقراص مضغطة أو ضوئية أو مصغرات فلمية، كل هذه ستكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[1].

وبعد المناقشة يكون القاضي حرا في الإجتهاد في الحكم في الجرائم الإلكترونية وعدم الاعتماد على رأي الغير، إلا إذا كان هذا الغير من الخبراء وقد إرتاح ضميره إلى التقرير المحرر منه وقرر الاستناد إليه ضمن حكمه، وبناءً عليه يكون متولدا من عقيدته وليس من تقرير الخبير[2].

وضبط وضعية الدليل الإلكتروني ترتب عليه نتائج، من أهمها عدم جواز أن يقضي القاضي الجنائي بناءً على علمه الشخصي أي عدم استناده على معلومات الشخصية التي قد يكون قد حصل عليها من خارج نطاق الدعوى العمومية المطروحة أمامه[3].

أما النتيجة الثانية فهي عدم جواز أن يقضي القاضي بناء على رأي الغير، فالقاضي الجنائي يجب أن يستوفي قناعته بنفسه من التحقيق في الدعوى ولا يعتمد على رأي الغير. وهي نتيجة مهمة تترتب على قاعدة وجوب مناقشة الدليل. وتأسيسا على ذلك لا يجوز للمحكمة أن تعتمد على أدلة ووقائع استقصتها من أوراق قضية أخرى ما لم تكن مضمون الدعوى الذي تفصل فيها[4].

وفي الأخير تبين لنا أن إجماع التشريعات الإجرائية في مختلف النظم القانونية على وجوب عرض الدليل المقدم في دعوى المناقشة وفي حالة عرضه للمناقشة يتم نقض هذا الحكم، وذلك بسبب مخالفة وجوب مناقشة الأدلة.

1- سامية بلجراف، مرالجع السابق، ص 35.

2- نور هدى محمودي، المرجع السابق، ص 28.

3- جليلة بلعملي، صالح مزري، الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة قاصدي مرباح – ورقلة، الجزائر، 2021/ 2022، ص 37.

4- حفيظة عباشي، " سلطة القاضي الجزائي في تقدير الدليل الإلكتروني وفق التشريع الجزائري"، مجلة القانون والعلوم السياسية، جامعة مولاي الطاهر-سعيدة، الجزائر، المجلد 09، العدد 01، 2022، ص 556.

الفرع الثالث: شرط يقينية الدليل الإلكتروني

إن الهدف الذي تسعى إليه كافة التشريعات الإجرائية هو ان يصيب القاضي الحقيقية في حكمه سواء بالبراءة أو الإدانة، والحقيقة لا يمكن الوصول إليها إلا باليقين، فالقاضي لا يبني حكمه ويؤسس إقتناعه إلا بناءً على الأدلة التي طرحت أمامه وخضعت للمناقشة أمام الخصوم[1].

تكمن أهمية يقينية الأدلة الجنائية في إتصاله المباشر لما سيؤول إليه حكم القاضي في الدعوى العمومية[2]، لذا سنتطرق إلى مفهوم مبدأ يقينية الدليل الجنائي الإلكتروني (أولا) ثم القواعد التي تحكمها (ثانيا).

أولا: مفهوم مبدأ يقينية الدليل الإلكتروني

اليقين بصفة عامة هو عبارة عن حالة ذهنية أو عقلانية تؤكد وجود الحقيقة، ويتم الوصول إليها عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال ما يعرض عليه من وقائع الدعوى، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التوكيد[3].

لذا عندما يصل القاضي إلى درجة اليقين، فإنه يصبح في هذه المرحلة مقتنعا بالحقيقة لأن اليقين هو الأصل ووسيلة لإقتناع القاضي بالحقيقة وهو ثمرة اليقين وليس اليقين ذاته[4].

وأما اليقين في مجال الأدلة الجنائية الرقمية، فإنه يشترط في هذا النوع من الأدلة مثل باقي الأدلة الجنائية الأخرى، بحيث تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، وذلك أنه لا مجال لدحض قرينة البراءة وإفتراض عكسها إلا عندما يصل إقتناع القاضي إلى حد الجزم واليقين[5].

1- جليلة بلعملي، صالح مزري، المرجع السابق، ص 33.

2- فؤاد أوساسي، المرجع السابق، ص41.

3- نصر الدين مبروك، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، الطبعة 2، دار الهدى، الجزائر، د س ن، ص 491.

4-نفس المرجع.

5-جليلية بلعملي، صالح مزري، المرجع السابق، ص ص 33 و34 .

ويمكن الوصول إلى اليقين في هذه الحالة من خلال ما يعرض من أدلة رقمية بمختلف أنواعها وأشكالها، وينطبع في ذهن القاضي من تصورات واحتمالات تحدد قوتها الاستدلالية على صدق نسبة الجريمة المعلوماتية إلى شخص معين من عدمه[1].

وفي حالة عدم قدرة أدلة الإدانة على إحداث اليقين يترتب عليه استمرار حالة البراءة التي يكفي لتأكيد وجودها مجرد الشك في ثبوت الادانة، وذلك لأنها إثبات على خلاف الأصل الذي لا يمكن إثبات عكسه إلا بمقتضى حالة من اليقين في نتائجها مع تلك المسلم بوجودها نتيجة لمبدأ إفتراض البراءة[2].

ثانيا: القواعد التي تحكم مبدأ يقينية الأدلة الجنائية الإلكترونية

نظرا للطابع التقني الذي يميز الدليل الجنائي، تم وضع قواعد محددة من قبل المختصين لضمان يقينيته، وذلك من خلال استخدام وسائل خفية تتناسب مع طبيعة هذا الدليل تتيح فحصه والتأكد من سلامته وصحة الإجراءات المتبعة في الحصول عليه[3].

أ-تقييم الدليل الجنائي الرقمي من حيث سلامته من العبث: تعد صلاحية الأدلة الجنائية الرقمية المستخلصة من سلامتها من الركائز الأساسية التي يقوم عليها التحقيق الجنائي، وبناءً عليه تهدف عملية تقييم الدليل الجنائي الإلكتروني إلى التأكد من خلوه من العبث، وذلك عبر إتباع مجموعة من الأساليب أبرزها استخدام تقنية التحليل التناظري الإلكتروني التي تعتبر من الوسائل الفعالة للكشف عن مصداقية الدليل الإلكتروني من خلال مقارنة النسخة الأصلية المقدمة إلى القضاء بالنسخة المستخرجة[4].

1-علي حسن احمد الفوالبة، التفتيش الجنائي في نظم الحاسوب-دراسة مقارنة، الطبعة 1، عالم الكتب الحديث للنشر والتوزيع، الأردن، 2004، ص 190.

2- نفس المرجع.

3-خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة 1، دار الثقافة للنشر والتوزيع، الأردن، 2011، ص 249.

4-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر، 2006، ص 125.

وفي حال عدم توفر النسخة الأصلية للدليل الجنائي الإلكتروني أو في حالة تعرضها للتعديل أو التلف يمكن التأكد من سلامة الدليل الإلكتروني باستخدام عمليات حسابية متخصصة تعرف بالخوارزميات أو بالإعتماد على نوع آخر من الأدلة الإلكترونية يطلق عليه " الدليل الرقمي أو الإلكتروني المحايد "، وهو دليل غير مرتبط مباشرة بموضوع الجريمة لكنه يساعد في التحقق من سلامة الدليل الجنائي الإلكتروني.

لذلك ولتفادي أي تعديل أو تلف يصيب الدليل الجنائي الرقمي ينصح المختصون دائما بالحفاظ على النسخة الأصلية واستغلال الميزة التي يتمتع بها هذا الدليل، وهي إمكانية استخراج عدة نسخ مطابقة له دون التأثير على سلامته[1].

ب–تقييم الدليل الجنائي الإلكتروني من حيث السلامة الفنية لإجراءات استخلاصه: أثناء إتباع جملة من الأساليب والإجراءات التقنية للحصول على الأدلة الجنائية الإلكترونية يمكن أن تعتري هذه الإجراءات على أخطاء قد تشكك في سلامة النتائج، لذا يجب في هذه الحالة الإعتماد على إختبارات محددة كوسيلة للتأكد من سلامة الإجراءات المتبعة في الحصول على الدليل االالكتروني[2].

المطلب الثاني: صعوبات استخلاص الدليل الإلكتروني

على الرغم من الجهود المبذولة لمكافحة الجريمة الإلكترونية، وذلك من خلال وضع قواعد موضوعية لمواجهتها وإجراء تعديلات على القواعد الإجرائية لتطوير أساليب المكافحة، إلا أن هناك صعوبات لا تزال تعترض عملية جمع الأدلة الجنائية الإلكترونية، يمكن أن نجمعها في عقبات وصعوبات في استخلاص تتعلق بالدليل الإلكتروني في (الفرع الأول) وصعوبات استخلاصه من طرق جهات التحقيق في (الفرع الثاني).

1- فؤاد أوساسي، المرجع السابق، ص 42

2-نفس المرجع.

الفرع الأول: صعوبات تتعلق بالدليل الإلكتروني في الجريمة الإلكترونية

تعترض الدليل الإلكتروني عدة عقبات في استخلاصه، وتتمثل هذه العقبات فيما يلي:

أولا: الطبيعة غير المرئية للدليل الإلكتروني

دائما ما يكون الدليل الجنائي في الجريمة التقليدية مرئيا وطبيعته مادية، بحيث يكون للقائمين على عملية التحقيق بمعاينة مسرح الجريمة وضبط أي دليل يفيد في كشف ملابستها، ولكن في الجريمة المعلوماتية تقع في بيئة مختلفة تماما عن بيئة الجريمة التقليدية، إذ تكون فيها الأدلة عبارة عن نبضات أو مجالات مغناطيسية أو كهربائية مُشَكِلَةً معلومات وبيانات رقمية في العالم الإفتراضي[1].

فهو دليل غير ملموس، وتتمثل في بيانات غير مرئية لا تفصح عن شخصية معينة عادة، وهذه المشكلة بصفة خاصة بالنسبة لجرائم الإنترنت مثل الجرائم التي ترتكز على البريد الإلكتروني في إرتكابها[2]. ومنه عدم رؤية الدليل الجنائي الإلكتروني يشكل العديد من الصعوبات من خلال جمعه وتحليليه مما يتوجب لدى المحققين الفنيين دراية كافية ومهارات كبيرة في التعامل مع هذا النوع من الأدلة[3].

ثانيا: سهولة تدمير ومحو الدليل الجنائي الإلكتروني

إن تدمير ومحو الأدلة الجنائية الرقمية من بين أكبر الصعوبات التي تعترض من عملية الاستخلاص، نظرا للسهولة التي تتميز بها هذه العملية واستغراقها لوقت قصير جدا[4]. فمرتكبي الجرائم المعلوماتية يتميزون بالذكاء والإتقان الفني للعمل الذي يقومون به، ولذلك فإنهم يسعون دائما لمحو وتدمير أو حتى تعديل أي دليل يؤدي إلى إدانتهم عن طريق التلاعب في أنظمة الحاسب الآلي ومحتوياته[5].

1- حنان عكوش، مسعود خطوي، " خصوصية الدليل الإلكتروني "، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي-الأغواط، الجزائر، المجلد 07، العدد 01، 2023، ص 1006.

2- حنان ميمون، عارف ناصري، المرجع السابق، ص 23.

3-عبد الفتاح بيومي الحجازي، مبادئ الإجراءات الجنائية في جرائم الكومبيوتر والإنترنت، الطبعة 1، دار الفكر الجامعي، مصر، 2006، ص 79.

4-هشام فريد رستم، " أصول التحقيق الجنائي الفني "، مجلة في بحوث القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، المجلد 12، العدد 03، 2004، ص 429.

5-عبد الفتاح بيومي الحجازي، المرجع السابق، ص 89.

ثالثا: إعاقة الوصول إلى الدليل الإلكتروني

يلجأ مرتكبي الجريمة المعلوماتية دائما لإبتكار أحدث الوسائل والأساليب لعرقلة جمع أدلة الإدانة، ومن بين هذه الوسائل استخدام تقنية التشفير[1]، أو فرض تدابير أمنية لمنع وعرقلة عملية التفتيش والإطلاع عن الأدلة وضبطها، وذلك باستخدام كلمات السر أو لجوء مرتكب الجريمة المعلوماتية إلى إخفاء هويته وخاصة عند استخدام شبكة الإنترنت، وذلك باستعمال العديد من البرامج والتطبيقات التي تعمل على طمس هويته في شبكة الإنترنت[2].

رابعا: ضخامة البيانات المتعين فحصها

لعل من أكبر الصعوبات التي تواجه رجال الضبط وسلطات التحقيق في استخلاص الأدلة الجنائية الرقمية، هو الكم الهائل للمعلومات والبيانات المراد فحصها وتحليلها[3].

ففضلا عن ضرورة توفر الخبرة الفنية للمحقق في مجال الحاسب الآلي وملحقاته بتعيين لذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة في جهاز الحاسب الآلي أو في دعائم التخزين الرقمية، لذلك ولمواجهة هذه الصعوبة وتجاوزها وجب الاستعانة بخبراء فنيين في مجال الحاسب الآلي بداعي معرفتهم بمكان وكيفية جمع المعلومات والبيانات التي يمكن أن تفيد التحقيق[4]، وإنما لابد أن تمتلك هذه السلطات أيضا القدرة على فحص الكم الهائل من المعلومات والبيانات المخزنة على أنظمة المعالجة الآلية[5].

1- هشام فريد محمد رستم، المرجع السابق، ص 427.

2-ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 121

3-تيثان ناصر ال تيتان، إثبات الجريمة الإلكترونية في دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، 2021، ص 131.

4- فؤاد أوساسي، المرجع السابق، ص 34.

5-بثينة حبيب تيتي، " معوقات مكافحة الجريمة المعلوماتية "، مجلة العلوم الإنسانية، جامعة الإخوة منتوري-قسنطينة1، الجزائر، العدد 05، ديسمبر 2018، ص 89.

الفرع الثاني: الصعوبات المتعلقة بخصوصية التحقيق في الجرائم الإلكترونية

تتمثل الصعوبات المتعلقة بالتحقيق بصعوبة التحري في كشف غموض الجريمة، وضعف التعاون الدولي في مكافحة الجرائم الإلكترونية.

أولا: صعوبة التحري في كشف غموض الجريمة الإلكترونية

أ-ضخامة البيانات المتعين فحصها: يمثل الكم الهائل من البيانات والمعلومات التي تتطلب فحصا ودراسة دقيقة لاستخلاص أدلة الجريمة منها، إحدى التحديات الجوهرية التي تعيق عملية الإثبات في الجرائم المعلوماتية. إذ أن طباعة كافة المحتويات المخزنة على الوسائط الممغنطة قد تستلزم مئات الآلاف من الصفحات، والتي قد لا تسهم في تقدم التحقيق بأي شكل فعال.

ومن ثم يتعين على الجهات المختصة بالضبط والتحقيق أن تمتلك ليس فقط الخبرة الفنية في مجال الحاسب الآلي، بل وأن تكون قادرة أيضا على معالجة وفحص الكم الكبير من البيانات والمعلومات المخزنة على أنظمة المعالجة الآلية بكفاءة ودقة[1].

ب-لا محدودية شبكة الأنترنت: من الصعوبات التي تواجه سير الإثبات في الجرائم الإلكترونية، هو أن شبكة الإنترنت ليس لها حدود دولية، فهي لا تعترف بتلك القائمة بين الدول، كما أنها ليست مملوكة لأحد، وبالتالي فليس هناك جهاز رقابي عليها ولا سلطة مركزية تتحكم فيها فالإنترنت ظاهرة دولية تنعدم مركزيتها وتتساوى أمامها الدول الكبيرة والصغيرة دون استثناء ودون المساس بسيادة الدول، ما خلق صعوبة كبيرة أمام الجهات التي تقوم بتعقب دليل الإثبات عبر هذه الشبكة.

ونظرا لإنتشار الشبكات على مستوى العالم فإنه يستحيل الحصول على دليل في حالة توزيع مسرح الجريمة بين أكثر من دولة بسبب تعقيد الإجراءات ووجود مشاكل عملية وتشريعية في بعض الدول، مما

يحول دون الحصول على دليل إلكتروني، كما أن سرعة مرور البيانات الإلكترونية عبر الشبكات في أقل من ثانية له تأثير عكسي على دليل الإدانة والبراءة[1].

ج–أساليب التحري التقليدية: إن الأساليب التي تستعمل في الجرائم العادية لا تصلح استعمالها في الجرائم المعلوماتية، لذلك نجد تسارع التشريعات إلى تكييف القوانين الخاصة بالجرائم المعلوماتية واستحداث أساليب ووسائل تتلائم مع خصائص هذا النوع من الجرائم، بالإضافة إلى أن إثبات الجرائم التي تقع على العمليات الإلكترونية باستخدام الوسائل الإلكترونية سيتأثر بطبيعة هذه الجرائم وبالوسائل العلمية التي قد ترتكب بها، مما قد يؤدي إلى عدم إكتشاف العديد من الجرائم في زمن إرتكابها أو عدم الوصول إلى الجناة الذين يرتكبون هذه الجرائم أو تعذر إقامة الدليل اللازم لإثباتها، مما يترتب عليه إلحاق الضرر بالأفراد والمجتمع[2].

د–ضعف التعاون الدولي في مكافحة الجرائم الالكترونية: إن الاختلافات في الأطر الوطنية تمثل تحديات أمام التعاون بين الدول الأعضاء في أوروبا، فإن الإفتقار إلى إطار قانوني مشترك في جميع أنحاء العالم يمثل تحديات كبيرة للتعاون الدولي بشكل عام، هذا ما يمثل مشكلة خاصة في حالة الهجمات الإلكترونية واسعة النطاق التي تمتد عبر قارات متعددة. وينظر إلى المساعدة القانونية المتبادلة على أنها بطيئة وغير فعالة، مع عدم تأمين الأدلة في كثير من الأحيان في الوقت المناسب لضمان نجاح قضية جنائية[3].

1- حنان ميمون، عارف ناصري، المرجع السابق، ص ص: 26 و27.

2- نفس المرجع، ص 27.

3-عدي محمد علي الشوايكة، " معوقات مكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الإختصاص"، المجلة العربية للنشر العلمي، الأردن، العدد 43، 2002، ص 337.

الفرع الثالث: الصعوبات التشريعية في الجرائم الإلكترونية

يُعد القصور التشريعي في مجال استخلاص الأدلة الجنائية الإلكترونية من بين أكبر الصعوبات التي تعترض الخبراء والفنيين المختصين في مكافحة الجرائم المعلوماتية، وهو ما جعل الدول تعمل على تحديث منظومتها القانونية من خلال تعديل قوانينها الإجرائية[1].

وقد كانت الجزائر من بين الدول التي استحدثت آليات قانونية تسهل عملية جمع الأدلة الجنائية الإلكترونية، وذلك من خلال ما أتت به ضمن القانون رقم 09-04 المؤرخ في 05 أوت 2009، والمتضمن للقواعد الخاصة للوقاية من جرائم المتعلقة بتكنولوجيا الإعلام والإتصال ومكافحتها. والذي أتى بإجراءات وأساليب تقنية، تمثل في مراقبة الاتصالات الالكترونية، وتفتيش المنظومة المعلوماتية، وحجز المعطيات المعلوماتية. زيادة عن ذلك أيضا قام المشرع الجزائري باستحداث الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، و ذلك بهدف تنسيق و مساعدة السلطات القضائية في التحريات بما في ذلك تجميع المعلومات و انجاز الخبرات.

أما المشرع الفرنسي فقد كان السباق في تعديل قوانينه لمواجهة القصور التشريعي في مجال استخلاص الأدلة الجنائية الالكترونية، بحيث قام بتعديل قانون الإجراءات الجزائية بموجب القانون رقم 239/ 2003 والمؤرخ في 18 مارس 2003، وأتى بعديد من القواعد القانونية التي تسهل من عملية جمع الأدلة الجنائية الإلكترونية، من بينها ما نصت عليه المادة 17 من نفس القانون، بحيث أجازت لضباط الشرطة القضائية أو تحت مسؤوليتهم أعوان الشرطة القضائية الدخول إلى الأنظمة المعلوماتية وتفتيشها وحجز كل ما يفيد في الجريمة[2].

إلا أن المشرع الجزائري ورغم سنه للقانون رقم 09-04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتهما، إلا أنه يبقى قاصرا في مجال الأدلة الجنائية الإلكترونية، نظرا لما يشهده

1- فؤاد أوساسي، المرجع السابق، ص 37.

2- نفس المرجع .

العالم من تسارع في التطور التكنولوجي الحاصل، وكما أن هذا القانون لم تمسه أي تعديلات منذ تكريسه، على قصد الأقل مواكبة التطورات التكنولوجية وعصرنة المنظومة التشريعية.

خلاصة الفصل

من خلال ما تم تناوله في هذا الفصل نستنتج أن الدليل الإلكتروني هو عبارة عن مجموعة من المعلومات التي يستقبلها العقل ويعترف بها المنطق، ويتم الحصول عليها من خلال إجراءات قانونية وعلمية، يمكن الاستعانة بها في أي مرحلة من مراحل التحقيق أو المحاكمة، ويجب على القاضي عند الإعتماد على الأدلة الإلكترونية الالتزام بالشروط التي وضعها المشرع حيث تعد هذه الشروط بمثابة ضابط أمان يقي من إنحراف القاضي عند التعامل مع هذه الأدلة للإثبات.

خاتمة

نستخلص من خلال ما سبق دراسته، أن موضوع التحقيق في الجرائم الإلكترونية وإثباتها في ظل التشريع الجزائري يُطرح كمجال معقد تتخلله العديد من الصعوبات والإشكاليات، و التي تشكل عائقا أمام تطوير أدوات كشف وضبط هذا النوع من الجرائم، و تعود أبرز هذه التحديات إلى قصور النصوص الإجرائية التقليدية، التي لم تصمم أصلا لمواجهة جرائم ترتبط بالتكنولوجيا الحديثة، من هذا المنطلق بادر المشرع الجزائري إلى إصدار القانون رقم 09- 04 المتضمن الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما، الذي يعد أول نص إجرائي خاص بتكنولوجيا الإعلام والاتصال وجاء استجابة للتطورات التقنية المتسارعة، كما تضمن هذا القانون استحداث آليات جديدة للتحري كالتسرب الإلكتروني والمراقبة الإلكترونية .

ورغم هذه الخطوات لا تزال الجهات المختصة في البحث والتحقيق تواجه إشكالات كبيرة، خاصة فيما يتعلق بالقيمة القانونية للأدلة الإلكترونية ومدى قبولها أمام القضاء الجزائي، إذ يتعين أن يجوز الدليل الإلكتروني على مشروعية تامة وأن يكون حجة معتبرة لإثبات الوقائع.

ونظرا لخطورة الجرائم الإلكترونية وصعوبة التحقيق فيها وكذلك إثباتها بسبب تعددها وصعوبة حصرها في منطقة معينة، نرى بضرورة تقديم بعض **النتائج** التي توصلنا إليها والمستمدة من التشريعات المقارنة للدول و لنصوص الدولية العالمية والإقليمية، وهي:

- إن القوانين الحالية خاصة منها قانون الإجراءات الجزائية المعدل والمتمم يعتبر قانونا قاصرا بالنظر إلى حداثة الجريمة الإلكترونية .
- صعوبة تكوين قناعة القاضي بأدلة الإثبات في الجريمة الإلكترونية نظرا لنقص التكوين ونقص المختصين في هذا المجال.
- على الرغم من الجهود المبذولة من طرف الحكومة الجزائرية وعلى وجه الخصوص المشرع في إطار تعزيز تبادل الخبرات بينه وبين التشريعات الأخرى إلا أن التطور السريع لتكنولوجيا الإعلام والاتصال صعب مهمة تأطير الجريمة الإلكترونية.

وبناء على هذه النتائج يمكن اقتراح مجموعة من **التوصيات**، على النحو التالي:

- إصدار قانون مستقل ومتكامل يضم كافة القواعد الموضوعية والإجرائية الخاصة بالجرائم الإلكترونية.
- إبتكار وسائل إثبات حديثة تتلاءم مع طبيعة الجرائم الإلكترونية إلى جانب توسيع صلاحيات المساعدين والمختصين في هذا المجال .
- تعزيز التعاون الدولي في مجال التشريع الأمني عبر استحداث وسائل فعالة للوقاية من الهجمات الإلكترونية وإنشاء وحدات متخصصة على المستويين الدولي والعربي تعنى بالتنسيق الأمني بين الدول لمتابعة ومعاقبة مرتكبي الجرائم الإلكترونية.
- الاستفادة من تجارب الدول المتقدمة في مجال مكافحة الجريمة الالكترونية وتبني آليات وقائية تسبق وقوع الجريمة، خاصة في الجرائم ذات الطابع الخطير كالإرهاب الإلكتروني أو التجسس الإلكتروني.

قائمة المصادر والمراجع

أولا: قائمة المصادر

أ– القرآن الكريم.

ب– المعجم الوجيز، مجمع اللغة العربية، طبعة خاصة بوزارة التربية والتعليم، مصر، 2004.

ج– الدستور الجزائري.

د– القوانين والأوامر.

1- القانون رقم 09-04 المؤرخ في 05 أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد رقم 47، 2009.

2- الأمر 66-155 المؤرخ في 08 جوان 1966، المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 49، 1966 المعدل والمتمم.

3-الأمر رقم 66-156 المؤرخ في 8 جوان 1966 المتضمن قانون العقوبات، الجريدة الرسمية للجمهورية الجزائرية، العدد رقم 49، 1966، المعدل والمتمم.

هـ.المراسيم

- المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015، المتعلق بتشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتها، الجريدة الرسمية، العدد رقم 53، 2015.

ثانيا: قائمة المراجع

أ–الكتب

1- أحمد خليفة الملط، الجرائم المعلوماتية–دراسة مقارنة، الطبعة 2، دار الفكر الجامعي، الإسكندرية–مصر، 2006.

2- أحمد مختار عمر وآخرون، معجم اللغة العربية المعاصرة، عالم الكتب، جزء1، الطبعة 1، القاهرة- مصر، 2008.

3- ارتياس نذير، الجريمة الإلكترونية وحجة الدليل الرقمي في الإثبات الجنائي، الطبعة 1، المركز المغاربي، شرق أدنى للدراسات الاستراتجية، المملكة المتحدة –بريطانيا، جانفي 2024.

4- أمحمد اقبلي، عبابد العمراني الميلودي، القانون الجنائي الخاص المعمق في الشروح، الطبعة 1، 2020.

5-حنان ريحان مبارك المنحكي، الجرائم المعلوماتية-دراسة مقارنة، الطبعة 1، منشورات الحلبي الحقوقية، بيروت-لبنان، د.س.ن.

6-خالد حياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والإنترنت، الطبعة 1، دار الثقافة للنشر والتوزيع، الأردن، د.س.ن.

7-خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجريمة الإلكترونية، الطبعة 1، دار الفكر الجامعي، الإسكندرية-مصر، 2009.

8-سامي علي حامد عياد، الجريمة المعلوماتية وجرائم الانترنت، دار الفكر الجامعي، الإسكندرية – مصر،2007.

9-شوقي يقشب تمام، الجريمة المعلوماتية دراسة تأصيلية مقارنة، الطبعة 1، مطبعة الرمال، الوادي- الجزائر، 2019.

10-طارق قادري، الجريمة الإلكترونية وحجية الدليل الرقمي في الإثبات الجنائي، الطبعة 1، المملكة المتحدة-بريطانيا، جانفي 2024.

11-علي حسن احمد الفوالبة، التفتيش الجنائي في نظم الحاسوب-دراسة مقارنة، الطبعة 1، عالم الكتب الحديث للنشر والتوزيع، الأردن، د.س.ن.

12-علي عدنان، إجراءات التحري وجمع الأدلة والتحقيق الإبتدائي في الجريمة المعلوماتية-دراسة مقارنة، دار الكتب والوثائق القومية، مصر، 2012.

13-ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، مصر،2006.

14-نصر الدين مبروك، محاضرات في الإثبات الجنائي، النظرية العامة للإثبات الجنائي، الطبعة 2، دار الهدى، الجزائر، د س ن.

15-نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة 2، دار الشفافة، عمان، 2010.

ب-الأطروحات، الرسائل والمذكرات الجامعية

1-الأطروحات الجامعية

-براهيمي جمال، التحقيق الجنائي في الجريمة الإلكترونية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، 2018.

- بن يحي إسماعيل، التحقيق الجنائي في الجرائم الإلكترونية، أطروحة دكتوراه، تخصص القانون الخاص، كلية الحقوق، جامعة أبي بكر بلقايد –تلمسان، الجزائر، 2021/2020.

-حسين ربيعي، آليات البحث والتحقيق في الجرائم المعلوماتية، أطروحة دكتوراه، تخصص قانون العقوبات والعلوم الجنائية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة 1، الجزائر، 2016/2015.

-بوسندة عباس، مشروعية الدليل الإلكتروني في مجال الإثبات الجنائي، أطروحة دكتوراه، تخصص علوم جنائية، جامعة جيلالي اليابس-سيدي بلعباس، الجزائر، 2013.

2-الرسائل والمذكرات الجامعية

- أوساسي فؤاد، دور الدليل الإلكتروني في الإثبات الجنائي، مذكرة ماستر، تخصص قانون جنائي، جامعة زيان عاشور-الجلفة، الجزائر، 2020/2019.

-بلعملي جليلة، مزري صالح، الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، جامعة قاصدي مرباح – ورقلة، الجزائر، 2021/ 2022.

-بن حديفة محمد أمين، وسائل وأساليب التحري في مجال مكافحة الجرائم الإلكترونية، مذكرة ماستر، قانون قضائي، جامعة عبد الحميد بن باديس-مستغانم، الجزائر، 2020/2019.

-بن عنطر سهام، التحقيق الجنائي في الجرائم الإلكترونية، مذكرة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، 2023.

-بن قسمية أيمن صالح، عيسى نور الدين، دور الضبطية القضائية في البحث والتحري في الجرائم الإلكترونية، مذكرة ماستر، تخصص قانون جنائي وعلوم الجنائية، جامعة عمار ثليجي-الأغواط، الجزائر، 2022/2021.

- بوادي حميدة، بن سالم فطيمة، الهيئة الوطنية للجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها، مذكرة ماستر، تخصص إعلام آلي وإنترنت، جامعة البشير الابراهيمي-برج بوعريرج، الجزائر، 2023/2022.

-بوبعاية ابتسام، التحقيق في الجريمة الإلكترونية، مذكرة ماستر، تخصص قانون الإعلام الآلي والانترنت، جامعة محمد البشير الابراهيمي-برج بوعريريج، الجزائر، 2022/2021.

- بوديسة بجاد عبد الرؤوف ، االيات التحري عن الجريمة الالكترونية في القانون الجزائري، مدكرة ماستر في لقانون،تخصص قانون اعلام الي و انترنت، 2022.

-بوشالة رمزي ، التنصت على المكالمات وإلتقاط الصور بين التجريم والإباحة، مذكرة ماستر، تخصص قانون جنائي للأعمال، كلية الحقوق، جامعة العربي بن مهدي-أم البواقي، الجزائر، 2015/2014.

-بوشرة أمين، موسى سهام، إطار القانوني للجريمة الإلكترونية (دراسة مقارنة)، مذكرة ماستر، تخصص قانون علوم جنائية، جامعة عبد الرحمان مبرة-بجاية، 2018/2017.

-تيثان ناصر ال تيتان، إثبات الجريمة الإلكترونية في دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، السعودية، 2021.

- حشمان عمار، الجريمة المعلوماتية في التشريع الجزائري، مذكرة ماستر، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التسيير، جامعة قاصدي مرياح-ورقلة، الجزائر، 2019/2018.

-خداوي مختار، إجراءات البحث والتحري الخاصة في التشريع الجنائي الجزائري، مذكرة ماستر، تخصص القانون الجنائي والعلوم الجنائية، جامعة الطاهر مولاي-سعيدة، الجزائر، 2016/2015.

-سعيداني نعيم، آليات التحري عن الجريمة المعلوماتية في التشريع الجزائري، رسالة ماجستير، تخصص علوم جبائية، جامعة الحاج لخضر-باتنة1، الجزائر، 2013/2012.

- سوير سفيان، جرائم المعلوماتية، رسالة ماجستير، تخصص العلوم الجنائية وعلم الإجرام، كلية الحقوق والعلوم الساسية، جامعة أبو بكر بلقايد-تلمسان، الجزائر، 2011/2010.

- شرف محمد، خرشبن مختار، أساليب التحري والتحقيق الحديث من النظام الاتهامي ونظام البحث والتحري، مذكرة ماستر، تخصص علوم جنائية، جامعة ابن خلدون-تيارت، الجزائر، 2015/2014.

-شرويلي فاطمة، ديدي فضيلة، آليات مكافحة الجريمة الإلكترونية، مذكرة ماستر، تخصص قانون الأعمال، كلية الحقوق والعلوم السياسية، جامعة صالحي أحمد-النعامة، الجزائر، 2023/2022.

- شنين صالح، اعتراضات المراسلات و سجيل أصوات وإلتقاط الصور في قانون إجراءات الجزائية الجزائري، مذكرة ماستر، كلية الحقوق، جامعة عبد الرحمن ميرة-بجاية، الجزائر، د.س.ن.

- صغير يوسف، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير، تخصص القانون الدولي للأعمال، جامعة مولود معمري-تيزي وزو، الجزائر، 2013.

- طباخ هاجر، مقلاتي صبرينة، الأدلة الرقمية ودورها في الإثبات الجنائي، مذكرة ماستر، تخصص إعلام آلي وإنترنت، جامعة محمد البشير الابراهيمي-برج بوعريريج، الجزائر، 2024/2023.

-طرشي نورة، مكافحة الجريمة المعلوماتية، رسالة ماجستير، تخصص القانون الجنائي، كلية الحقوق والعلوم السياسية، جامعة ين يوسف بن خدة-الجزائر 1، الجزائر، 2012/2011.

- قادري سارة، أساليب التحري الخاصة في قانون الاجراءات الجزائية، مذكرة ماستر، تخصص قانون أعمال، جامعة قاصدي مرباح-ورقلة، الجزائر، 2014/2013.

-كوداد عبد الرحمان ، عملية التسرب على ضوء التشريع الجزائري، مذكرة ماستر، تخصص علم الإجرام، كلية الحقوق والعلوم السياسية، جامعة الدكتور مولاي الطاهر-سعيدة، الجزائر، 2017/2016.

-لصامي أمال، جميلة بن طالب، حجية الدليل الإلكتروني في إثبات وحق التشريع الجزائري، مذكرة ماستر، تخصص قانون جنائي، جامعة مولاي الطاهر-سعيدة، الجزائر، 2022/2021.

- مهدي شمس الدين، النظام القانوني للتسرب في قانون الجزائر، مذكرة ماستر، تخصص قانون جنائي، جامعة محمد خيضر-بسكرة، 2014/2013.

- ميمون حنان، ناصري عارف، سلطة القاضي في تقدير الدليل الرقمي، مذكرة ماستر، قانون إعلام آلي، جامعة محمد البشير الابراهيمي-برج بوعريريج، الجزائر، 2023/2022.

-نايدي عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، تخصص قانون إداري، كلية الحقوق والعلوم السياسية، جامعة أحمد دارية -أدرار، الجزائر، 2017/2016.

ج.المقالات

-أسامة حسن محي الدين عبد العال، "حجية الدليل الرقمي في الإثبات الجنائي للجرائم المعلوماتية (دراسة تحليلية مقارنة)"، مجلة البحوث القانونية والاقتصادية، العدد 76، 2021.

- الغامدي فيصل، الأدلة الرقمية وحجيتها في إثبات النظام السعودي، مجلة العربية للنشر العلمي، المجلد 07، العدد 69، 2024.

-بغدادي إيمان، أثر تعديل العقوبات الجزائرية في التصدي للجريمة المعلوماتية، مجلة الأفاق والدراسات، المركز الجامعي إليزي، الجزائر، العدد 04، 2019.

-بلجراف سامية، " سلطة القاضي الجزائي في قبول وتقدير الدليل الرقمي"، مجلة الدراسات القانونية المقارنة، جامعة حسيبة بن بوعلي-الشلف، الجزائر، المجلد 07، العدد 01، 2012.

- بلعابد عبيدة، "الدليل الرقمي بين حتمية الإثبات وحق في خصوصية المعلومات"، مجلة الآفاق العلمية، جامعة أمين العقال الحاج موسى اق خموك- تمنراست، الجزائر، العدد 01، 2019.

- بن الطيب مبارك ، رحموني محمد، " شروط قبول الدليل الرقمي كدليل إثبات في الجريمة الإلكترونية"، مجلة القانون والعلوم السياسية، المركز الجامعي صالحي أحمد-النعامة، الجزائر، المجلد 05، العدد 02، 2019.

- بن المعمري مسعد، الدليل الإلكتروني لإثبات الجريمة الالكترونية، ملحق خاص، العدد 03، جزء 02، أكتوبر 2018.

-بن بادة عبد الحليم، "المراقبة الإلكترونية كإجراء لإستخلاص الدليل الإلكتروني بين الحق في الخصوصية ومشروعية الدليل الإلكتروني"، المجلة الأكادمية للبحث القانوني، جامعة عبد الرحمان ميرة-بجاية، المجلد 10، العدد 43، 2019.

-بن فردية محمد، "الدليل الجنائي الرقمي وحجيته أمام القضاء الجزائي-دراسة مقارنة"، المجلة الأكادمية للباحث القانوني، جامعة عبد الرحمن ميرة-بجاية، الجزائر، المجلد 05، العدد 01، 2014.

-بوزرة سهيلة، "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام ومكافحتها بين سرية المعطيات الإلكترونية ومكافحة الجرائم الإلكترونية "، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري-تيزي وزو، الجزائر، المجلد 17، العدد 02، 2022.

- حبيب تيتي بثينة، " معوقات مكافحة الجريمة المعلوماتية "، مجلة العلوم الإنسانية، جامعة الإخوة منتوري-قسنطينة1، الجزائر، العدد 05، ديسمبر 2018.

- حكيم محمد عثمان، "حجية الدليل الإلكتروني في مجال الإثبات الجنائي وموقف المشرع الليبي "، مجلة الحق، ليبيا، العدد 07، 2014.

-خرشي إلهام، "النظام القانوني للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافحتها"، المجلة القانونية والسياسية، جامعة محمد لمين دباغين-سطيف، الجزائر، المجلد 04، العدد 01، 2022.

-خليفي سمير، " التسرب الإلكتروني: إجراء لمكافحة الجرائم المخذرات عبر الوسائط الإلكترونية في ظل انتشار جائحة كورونا"، مجلة المحلل القانوني، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج-البويرة، الجزائر، المجلد 04، العدد 02، ديسمبر 2020.

- زوزو هدى، "التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائرية"، مجلة الدفاتر السياسية والقانونية، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة-الجزائر، العدد 11، جوان 2014.

-شاين نوال، "الجريمة الإلكترونية في التشريع الجزائري: ماهيتها، موضوعها، خصائصها ومظاهر تحدياتها"، مجلة سوسولوجيا، جامعة الحاج لخضر-باتنة 1، الجزائر ، المجلد 06، العدد 02، 2022.

- ضو خالد، " حجية الدليل الإلكتروني وشروط قبوله والإثبات الجنائي "، مجلة الباحث الأكاديمي في العلوم القانونية و السياسية ،جامعة بن يوسف بن خدة-جامعة الجزائر 1، الجزائر، 2022.

-فراوي كلثوم، " مشروعية الدليل الإلكتروني في الإثبات الجنائي "، مجلة طبنة للدراسات العلمية والاكاديمية، المركز الجامعي سي الحواس-بريكة، الجزائر، المجلد 05، العدد 01، 2022.

-فلاح عبد القادر، آيت عبد المالك نادية، "التحقيق الجنائي في الجرائم الإلكترونية وإثباتها في التشريع الجزائري"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جامعة محمد بوضياف-المسيلة، الجزائر، المجلد 04، العدد 02، 2019.

- فيصل ماطوف العصاف، سليمان العجاني، "ماهية الدليل الرقمي في النظام السعودي-دراسة مقارنة"، مجلة الدولية للدراسات القانونية والسياسية، مركز كيدني للبحث والتطوير، لندن-المملكة المتحدة، 15 أفريل 2023.

-عباسي حفيظة، " سلطة القاضي الجزائي في تقدير الدليل الإلكتروني وفق التشريع الجزائري"، مجلة القانون والعلوم السياسية، جامعة مولاي الطاهر-سعيدة، الجزائر، المجلد 09، العدد 01، 2022.

-عبد الحميد عائشة، "الدليل الرقمي كحجية للإثبات أمام القاضي الجزائري في المعاملات الإلكترونية"، مجلة صوت القانون، جامعة الجيلالي بونعامة - خميس مليانة، الجزائر، المجلد 07، العدد 01، ماي 2020.

- عدي محمد علي الشوايكة، " معوقات مكافحة الجرائم الالكترونية في المجتمع الأردني من وجهة نظر ذوي الإختصاص"، المجلة العربية للنشر العلمي، الأردن، العدد 43، 2002.

- عكوش حنان، خطوي مسعود، " خصوصية الدليل الإلكتروني "، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي-الأغواط، الجزائر، المجلد 07، العدد 01، 2023.

-عمارة فوزي، "إعتراض المراسلات وتسجيل الأصوات والتقاط الصور والتسرب كإجراءات تحقيق قضائي في المواد الجزائية"، مجلة العلوم الإنسانية ،كلية الحقوق، جامعة الإخوة متنوري-قسنطينة1، الجزائر، العدد 33، جوان 2010.

- مجذوب نوال، "آليات الإجرائية للكشف عن الجريمة المعلوماتية"، مجلة البحوث القانونية والاقتصادية، مركز الجامعي-مغنية، الجزائر، المجلد 06، العدد 04، 2023.

- محمد محمد عبد الظاهر موسى، "القيمة الثبوية للدليل الرقمي وضوابط إقناع القاضي الجنائي"، مجلة البحوث القانونية والإقتصادية، جامعة بن يوسف بن خدة-الجزائر1، الجزائر، المجلد 36، العدد 2، يوليو 2006.

-محمودي نور هدى، "حجية الدليل الرقمي في إثبات الجريمة المعلوماتية"، مجلة الباحث للدراسات الأكاديمية، جامعة الحاج لخضر- باتنة1، الجزائر، العدد 11، 2017.

-مزعاء شهيرة، حداد عيسى، " حجية الدليل الإلكتروني أمام القضاء الجزائي"، دائرة البحوث والدراسات القانونية والسياسية، المركز الجامعي مرسلي عبد الله- تيبازة، الجزائر، المجلد 07، العدد 02، 2023.

- مسـعود بن حميد المعمري، " الدليل الإلكتروني لإثبات الجريمة الإلكترونية "، مجلة القانون الكويتية العالمية، أبحاث المؤتمر السنوي الدولي، عدد خاص، الجزء 2، العدد 3، 2018.

-معروف كريم، بن حليمة سعاد، "الإجراء المستحدث في البحث والتحقيق للكشف عن الجرائم التي ترتكب في الفضاء الإلكتروني (دراسة تحليلية وصفية وفق ما جاء به المشرع الجزائري)"، مجلة الدراسات الاستراتجية والعسكرية، المركز الديمقراطي العربي، برلين-ألمانيا، العدد 13، ديسمبر 2021.

-مولاي براهيم عبد الحكيم، الجرائم الإلكترونية، مجلة الحقوق والعلوم الإنسانية، الجزائر، العدد 23، 2015.

-هشام فريد رستم، " أصول التحقيق الجنائي الفني "، مجلة في بحوث القانون والكمبيوتر والإنترنت، جامعة الإمارات العربية المتحدة، المجلد 12، العدد 03، 2004.

د.الملتقيات

-بوخلفة سعاد، مكافحة الجرائم الإلكترونية في التشريع الجزائري، مداخلة مقدمة ضمن أعمال الملتقى الوطني، بعنوان:" الجرائم الإلكترونية في المجتمع الجزائري"، جامعة يحي فارس-المدية، الجزائر، المنعقد بتاريخ 15 مارس 2022.

-بوزينة آمنة امحمدي، إجراءات التحري الخاصة في مكافحة الجرائم المعلوماتية، مداخلة مشارك بها في الملتقى الوطني حول:" آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري"، الجزائر العاصمة، المنعقد بتاريخ 29 مارس 2017.

-خنيفر شفيقة، الجريمة الإلكترونية (الواقع والتحديات)، مداخلة ملقاة في يوم دراسي، حول:" الاجرام الإلكتروني كفاءات ضائعة في عالم التقنية"، جامعة محمد الشريف مساعدية -سوق أهراس، الجزائر، 2022.

-سعداني عبد النور ، بومحراث ليندة، إجراءات البحث والتحري في الجرائم الإلكترونية، مداخلة مقدمة ضمن أعمال الملتقى الوطني بعنوان:" الجرائم الإلكترونية في المجتمع الجزائري "، جامعة يحي فارس- المدية، الجزائر، المنعقد بتاريخ 15 مارس 2022.

5.المواقع الالكترونية

-http//www .noor-book.com.

-http// tele enc .umiv-oeb.bg.

- www Noor – book com https.

فهرس الموضوعات

فهرس الموضوعات

قائمة المختصرات: .....-

مقدمة 2

الفصل الأول: ماهية التحقيق الجنائي في الجريمة الإلكترونية في التشريع الجزائري 7

تمهيد 8

المبحث الأول: مضمون الجريمة الإلكترونية 9

المطلب الأول : مفهوم الجريمة الإلكترونية 9

الفرع الأول: تعريف الجريمة الإلكترونية وأطرافها 9

أولا: التعريف الفقهي للجريمة الإلكترونية.....10

ثانيا: أطراف الجريمة الإلكترونية.....12

الفرع الثاني: خصائص الجريمة الإلكترونية.....16

أولا: الجريمة الإكترونية جريمة عابرة للحدود.....16

ثانيا: صعوبة إثبات الجريمة الإلكترونية.....16

ثالثا: الجريمة الإلكترونية أقل عنفا وجهدا في التنفيذ 16

رابعا: الجريمة الإلكترونية جريمة مستحدثة 17

خامسا: قلة الإبلاغ عن الجرائم الإلكترونية.....17

الفرع الثالث: أركان الجريمة المعلوماتية.....17
أولا: الركن الشرعي للجريمة الإلكترونية 18
ثانيا: الركن المادي للجريمة الإلكترونية 18
ثالثا : الركن المعنوي للجريمة الإلكترونية.....19
المطلب الثاني: تصنيفات الجرائم الإلكترونية في التشريع الجزائري 19
الفرع الأول: الجرائم الواقعة بواسطة النظام المعلوماتي.....20
أولا: الجرائم الإلكترونية الواقعة على الأشخاص بواسطة النظام المعلوماتي 20
ثانيا: الجرائم الواقعة على الأموال بواسطة النظام المعلوماتي 21
ثالثا: الجرائم الإلكترونية الواقعة على الأسرار 21
الفرع الثاني: الجرئم الواقعة على النظام المعلوماتي.....22
أولا: جريمتي الدخول والبقاء غير المشروعان في منظومة المعلومات.....22
ثانيا: جريمة المساس بمنظومة معلوماتية.....23
المبحث الثاني: أساليب البحث والتحري عن الجرائم الإلكترونية في التشريع الجزائري 24
المطلب الأول: الأجهزة المكلفة بالبحث والتحري عن الجرائم الإلكترونية في الجزائر 25
الفرع الأول: البحث والتحري عن الجرائم الإلكترونية في الضبطية القضائية 25
أولا: البحث والتحري عن الجرائم الإلكترونية على مستوى جهاز الشرطة 26

ثانيا: البحث والتحري عن الجرائم الإلكترونية على مستوى الدرك الوطني.....28

الفرع الثاني: مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية 30

أولا: تعريف مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية.....30

ثانيا: إختصاصات مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية 31

ثالثا: تشكيلة مركز الوقاية من جرائم الإعلام والجرائم الإلكترونية 31

المطلب الثاني: إجراءات التحقيق في الجرائم الإلكترونية في الجزائر 33

الفرع الأول: إجراءات التحري المألوفة والتقليدية في الجرائم الإلكترونية في الجزائر 33

أولا: المعاينة في الجرائم الإلكترونية 33

ثالثا: ضبط الأدلة في الجرائم الإلكترونية.....39

رابعا: الخبرة التقنية في مجال الجرائم الإلكترونية 40

الفرع الثاني: إجراءات التحري المستحدثة في الجرائم الماسة بأنظمة المعالجة الآلية للبيانات...41

أولا: التسرب الإلكتروني.....41

ثانيا: المراقبة الإلكترونية.....43

ثالثا: إعتراض المراسلات 45

رابعا: الحفظ وإفشاء الإعلام للمعطيات الإلكترونية 49

خلاصة الفصل الأول.....51

الفصل الثاني: الدليل الإلكتروني كأداة إثبات في الجرائم الالكترونية.....52
تمهيد 53
المبحث الأول: ماهية الدليل الإلكتروني ومشروعيته 54
المطلب الأول: مفهوم الدليل الإلكتروني 54
الفرع الأول: تعريف الدليل الإلكتروني 54
أولا: تعريف مصطلح الدليل 54
ثانيا: تعريف مصطلح الالكتروني.....55
ثالثا: تعريف الدليل الإلكتروني 55
الفرع الثاني: خصائص الدليل الإلكتروني 56
أولا: الدليل الإلكتروني ذو طابع تقني ومتطور 57
ثانيا: الدليل الإلكتروني يصعب التخلص منه 57
ثالثا: الدليل الإلكتروني دليل قابل للنسخ 58
رابعا: الدليل الإلكتروني ذو طبيعة ثنائية 58
المطلب الثاني: مشروعية الدليل الإلكتروني 59
الفرع الأول: مشروعية الدليل الإلكتروني في النظام الحر 59
الفرع الثاني: مشروعية الدليل الإلكتروني في النظام المقيد 60

الفرع الثالث: أنواع الدليل الإلكتروني.....62
أولا: الأدلة المعدة لتكون وسيلة إثبات.....62
ثانيا: الأدلة غير المعدة لتكون وسيلة إثبات.....63
المبحث الثاني: سلطة القاضي الجزائي في تقدير الدليل الإلكتروني 64
المطلب الأول: شروط قبول الدليل الإلكتروني.....65
الفرع الأول: شرط مشروعية الدليل الإلكتروني 65
الفرع الثاني: شرط مناقشة الدليل الإلكتروني.....66
الفرع الثالث: شرط يقينية الدليل الإلكتروني.....68
أولا: مفهوم مبدأ يقينية الدليل الإلكتروني 68
ثانيا: القواعد التي تحكم مبدأ يقينية الأدلة الجنائية الإلكترونية.....69
المطلب الثاني: صعوبات استخلاص الدليل الإلكتروني.....70
الفرع الأول: صعوبات تتعلق بالدليل الإلكتروني في الجريمة الإلكترونية 71
أولا: الطبيعة غير المرئية للدليل الإلكتروني.....71
ثانيا: سهولة تدمير ومحو الدليل الجنائي الإلكتروني.....71
ثالثا: إعاقة الوصول إلى الدليل الإلكتروني 72
رابعا: ضخامة البيانات المتعين فحصها 72

الفرع الثاني: الصعوبات المتعلقة بخصوصية التحقيق في الجرائم الإلكترونية 73
أولا: صعوبة التحري في كشف غموض الجريمة الإلكترونية 73
الفرع الثالث: الصعوبات التشريعية في الجرائم الإلكترونية.....75
خلاصة الفصل.....77
خاتمة 78
قائمة المصادر والمراجع 81
فهرس الموضوعات 93
ملخص.....100
Abstract 102

ملخص

ملخص

تشكل الجرائم الإلكترونية تحديا أمنيا كبيرا يواجه المجتمع الدولي نظرا لتعقديها واستخدامها لتقنيات حديثة ومتطورة من قبل مجرمين يتمتعون بذكاء وخبرة عاليتين، مما يصعب عمليات التحقيق والإثبات، بحيث أن الصورة التقليدية لإجراءات التحقيق التي تقوم بها الجهات المكلفة بالبحث والتحري عن الجريمة لا تتماشى مع طبيعة الجرائم الإلكترونية. ولمواجهة هذا التحدي أدخل المشرع الجزائري تعديلات على قانون الإجراءات الجزائية سنة 2006 الذي جاء بآليات التحري الخاصة للتحقيق في الجرائم الإلكترونية، ثم كرس المشرع الجزائري بموجب القانون رقم 09-04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والإتصال ومكافحتهما، والذي يعد أول قانون إجرائي خاص بمكافحة الجرائم الإلكترونية.

ونهدف من خلال دراستنا هذه، إلى تسليط الضوء على أهم أساليب التحقيق والكشف عن الجرائم الإلكترونية التي أقرها المشرع الجزائري ومدى فعاليتها في ضبط وإثبات هذا النوع من الجرائم.

الكلمات المفتاحية: الجريمة الإلكترونية- التحقيق الجنائي- الإثبات الإلكتروني- الدليل الإلكتروني- التفتيش الإلكتروني.

Abstract

Cybercrimes pose a major security challenge to the international communit due to their complexity and the use of advanced and sophisticated technologies by criminals who possess high intelligence and expertise.Which makes from of investigation and proof difficult so that the traditional from of investigation price duress carried out out dy the authorities in charge of research and investigation of crime is not in line with the nature of cy dercrime.

To face the challenge the Algerian legislator introduced amendments to the code of criminal procedure in 2006 with introduced special investing attire mechanisms to inirestigate cybercrimes them the Algerian legislator enshrined law 09-04 an crimes related to information and communication technologies .what is the first procedural law to combat cybercrime. through this study we aim to shed light on the mast important methods of investigation and detection of cybercrime approved by the Algerian legislator and their effectiveness in detecting and proving that type of crime.

Key words: Cybercrime, Criminal Investigation, Electronic Evidence, Electronic Directory, Electronic Inspection.