جامعة أمحمد بوقرة بومرداس

كلية الحقوق والعلوم السياسية بودواو

شعبة الحقوق

التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية

مذكرة مقدّمة لنيل شهادة الماستر علوم في القانون

تخصص قانون عام

من إعداد الطّالبين:

- شكري خالد
- لراشي أبوبكر

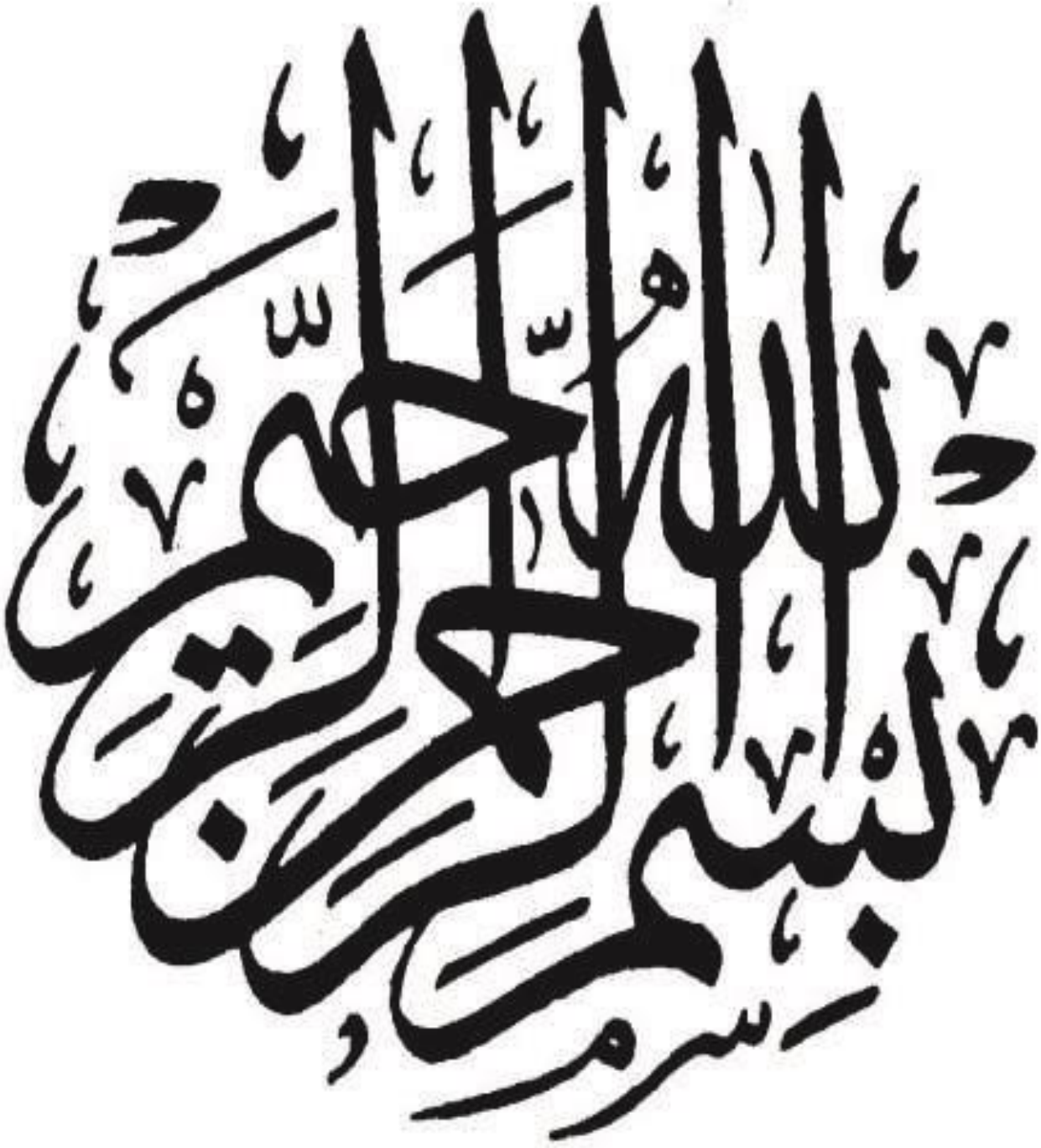
إشراف الدكتورة

العرفي فاطمة الزهراء

لجنة المناقشة

الاسم واللقب	الرتبة	الجامعة	الصفة
بن عياد جليلة	أستاذة محاضرة أ	كلية الحقوق - آمحمد بوقرة بومرداس	رئيسا
العرفي فاطمة الزهراء	أستاذة محاضرة أ	كلية الحقوق - آمحمد بوقرة بومرداس	مشرفا ومقررا
سايحي محمد	أستاذ مساعد أ	كلية الحقوق - آمحمد بوقرة بومرداس	ممتحنا

السنة الجامعية: 2023/2022


بسم الله الرحمن الرحيم

شكرا وتقدير

" . . . وقل ربي أوزعني أن أشكر نعمتك على وعلى والديا وأن أعمل صالحا ترضاه

وأدخلني برحمتك في عبادك الصالحين . " سورة النمل الاية 19

أسجد لله تعالى شكرا وعرفانا لما وفقنا اليه في إتمام هذه المذكرة وأشكر سبحانه وتعالى على ما أسبغه

علي من نعمة ظاهرة وباطنة .

فله الحمد وله الشكر حمدا يليق بجلال وجهه وعظيم سلطانه الذي أنار لنا دربنا وسهل لنا كل صعب ويسره لنا وبعد :

"ولئن شكرتم لأزيدنكم"

أتقدم بالشكر ووافر الامتنان الى الأستاذة عرفي فاطمة التي شرفنا بالإشراف على مذكرة الماستر ،

كما نشكر جزيل الشكر أساتذتنا الكرام والذين لم يبخلوا عنا بالمعلومات طيلة مشوارنا الدراسي كلا باسمهم

كما أتقدم بجزيل الشكر وفائق الاحترام الى كل من ساعدنا من قريب أو بعيد في إنجاز هذه المذكرة

لك الحمد ربي على كثير فضلك و جميل عطائك ووجودك ، الحمد لله ربي ومهما حمدنا فلن نستوفي حمدك والصلاة والسلام على من لا نبي بعده وعلى اله و صحبه الميامين ومن تبعهم بإحسان الى يوم الدين أما بعد :
اولا الحمد لله وفقني لتثمين هذه الخطوة في مسيرتي الدراسية بمذكرتي هذه ثمرة الجهد و النجاح بفصله تعالى ، والتي أدين بها لمن قال فيها عز وجل وقضى ربك الا تعبدوا الا اياه و بالوالدين احسانا

الى من سهرت الليالي وتعبت من أجلي وروتني من نبع حنانها و سقتني عطفها

امي العزيزة اطال الله في عمرها .

الى الغالي الذي تعب و ضحى من أجلي و شجعني على مواصلة درب العلم

ابى العزيز .

الى من كانوا لي سندا بحنانهم ومحبتهم أخواتي وإخوتي .
الى كل من ساعدني ولو بتشجيع في إنجاز مذكرتي زملائي في العمل .

خالد شكري

الحمد لله رب العالمين والصلاة و السلام على خاتم الانبياء والمرسلين اما بعد :

الحمد لله الذي وفقنا لتثمين هذه الخطوة في مسيرتنا الدراسية بمذكرتنا هذه

ثمرة الجهد و النجاح بفضله تعالى مهداة :

الى روح امي الغالية رحمة الله عليها

الى من اشدد بيه ازري و اعتمد عليه في كل كبيرة وصغيرة اخي فريد

الى كل من ساعدني ولو بتشجيع في إنجاز مذكرتي زملائي في العمل .

أبو بكر لراشي

مقدمة

مقدمة

عرف عالمنا المعاصر نقلة نوعية جد متسارعة، في مجال التطور العلمي والتكنولوجي في جميع الميادين خاصة ما تعلق منها بالشبكات الرقمية وسرعة تنقل المعلومات، أو ما يعرف بتكنولوجيات الإعلام و الاتصال، حيث عرفت هذه الأخيرة قفزة و طفرة علمية و تكنولوجية جد متقدمة، حيث بات يعرف عصرنا اليوم بعصر المعلومات، بحيث تلاشت الحدود الجغرافية بين الدول و الشعوب و الأفراد و أصبح العالم مجرد قرية صغيرة، أين اجتاحت هذه التقنيات حياة الأفراد و أصبحت من الضروريات يستحيل الاستغناء عنها، حيث سمحت هذه الأخيرة بربط شبكات اتصال بين الأفراد والدول و جعلتهم في اتصال دائم و مستمر، خاصة بعد ظهور الحواسيب المحمولة و الهواتف الذكية والأقمار الصناعية وشبكات الأنترنت و قوة سرعة تدفقها التي بلغت الجيل الخامس و التي تبلغ سرعتها 01 جيغابايت في الثانية، لتشكل شبكة هائلة لنقل المعلومات حيث يمكن للمستخدم الولوج إليها في أي وقت و في أي مكان باستعمال تقنيات جد حديثة في المعالجة الآلية للمعطيات والبيانات أو نقلها، ما انعكس سلبا و إيجابا على كثير من جوانب الحياة المعاصرة و ما توفره من جهد و وقت و تكلفة، ما جعل حياة الإنسان أكثر بساطة و أكثر سهولة، الشيء الذي أدى إلى تضاعف الطلب على هذا النوع من التكنولوجيا و توسع ميادين استعمالها.

بالرغم من الإيجابيات والمزايا التي سبق ذكرها، بفضل تقنيات وسائل تكنولوجيا المعلومات و الاتصال إلا أنها لا تخلو من جوانب السلبية، حيث تمثل في بعض الحالات تهديدا خطيرا للأمن و الاستقرار، ما أدى إلى بروز نوع جديد من الجرائم المستحدثة لم تكن معروفة من قبل، ما اصطلح على تسميتها " بالجرائم الإلكترونية" أو "الجرائم المعلوماتية، بالتالي تعقدت معها أكثر فأكثر مهمة التحقيق الجنائي على سلطات التحقيق و الضبطية القضائية، حيث تتميز هذه الأخيرة بخصائص تختلف في مفهومها و أركانها و وسائل ارتكابها و ونوعية الجناة عن الجرائم التقليدية، ما يجعلها أكثر خطورة و تعقيد، فظلا على أنها جرائم عابرة للحدود تتم عبر شبكات اتصال لا متناهية بالإضافة إلى السهولة والسرعة في التنفيذ و طمس الأدلة و إخفائها التي يستفيد منها المجرم الإلكتروني في هذا النوع من الجرائم.

وتثير مسالة الإثبات في الجرائم الإلكترونية عوائق و مشاكل عديدة في مجال التحقيق وجمع الأدلة الجنائية، نظرا لمميزات و خصوصيات هذه الجريمة ما يشكل عقبة كبيرة أمام كشفها كما تكمن صعوبة الإثبات في هذا النوع من الجرائم، في تشفير البيانات المخزنة إلكترونيا أو المنقولة عبر الأنترنت في سهولة محو الدليل الإلكتروني ، كما لا يترك مرتكبيها أثار مادية بسبب دقتها و سرعة القيام بها و إمكانية محو أثارها و إخفاء الأدلة عقب وقوع الجريمة مباشرة كما أن ارتكاب هذه الجرائم يتعدى الاختصاص الإقليمي للدول يثير مشكلة الاختصاص المكاني و القانون الواجب التطبيق .

كل ما سبق ذكره من خصوصيات للجرائم الإلكترونية و عوائق التحقيق فيها، دفع المختصون في مجال القانون و الإعلام الآلي و تكنولوجيات الإعلام و الاتصال، يكثفون جهودهم العلمية بالعمل على تطوير المنظومة القانونية و تطوير أساليب الحماية للنظم و البرامج الإلكترونية، و سد الثغرات التي تعتري النصوص الإجرائية للتشريعات التقليدية القائمة، لمواجهة هذه الجريمة باستنباط الدليل الذي يتوافق مع الطبيعة التقنية التي يتميز بها هذا النوع من الجرائم.

أهمية الموضوع

تظهر لنا أهمية هذه الدراسة باعتبار أن مرحلة التحقيق تعتبر من أهم مراحل الدعوى الجنائية، حيث تسمح هذه المرحلة بالحصول على دليل إثبات قوي و متماسك لا يمكن دحضه من أجل ضمان حماية حقوق الضحايا و محاكمة الجاني محاكمة عادلة و توقيع الجزاء المناسب مبنية على مبدأ الشرعية، كما تبرز أهمية الموضوع في التطور السريع و المستمر الذي تتميز به الجريمة الإلكترونية الأمر الذي ألزم المشرع و سلطات التحقيق العمل على تطوير وسائل و أساليب التحقيق، للتصدي لهذه الجريمة التي تمتد إلى جميع القطاعات و الميادين ، فهي جريمة بلا حدود تمس الأشخاص المعنوية و الطبيعية على حد سواء كما أن الخاصية اللامادية للدليل الإلكتروني خلقت صعوبات غير مسبوقة أمام سلطات التحقيق بالتالي كان من المنطقي أن تنصب دراستنا على الجوانب الإجرائية المتعلقة بجمع الدليل الإلكتروني و نتيجة ذلك سوف نركز في بحثنا هذا على السلطات المختصة بالتحقيق في الجريمة الإلكترونية و كذلك على الجانب الإجرائي و ما تقوم به هذه السلطات من إجراءات لجمع دليل الإلكتروني و كذلك الأجهزة المناط بها مهمة التحقيق الجنائي

بالتالي بات من الضروري إعطاء هذا الموضوع الأهمية اللازمة و اتخاذ التدابير و الإجراءات اللازمة لحماية الأفراد و المجتمع و مؤسسات الدولة من هذه الجريمة.

أسباب اختيار الموضوع

يرجع اختيار هذا الموضوع إلى عدة أسباب، الشخصية منها و هي التعرف أكثر على هذا النوع من الجرائم نظرا لحداثتها و تقنية الوسائل المستعملة و التزايد الهائل لعدد القضايا المطروحة في أروقة العدالة و انتشارها بمعدلات قياسية تزامنا مع التطور التكنولوجي المستمر الذي يعرفه هذا المجال بظهور الهواتف الذكية -كما أن طبيعة المهنة التي نمارسها في مجال الضبط القضائي كانت حافزا قويا دفعنا لاختيار هذا الموضوع والتعمق في إجراءات التحقيق و جمع الأدلة و الحصول على الدليل الإلكتروني، و طرق إثبات هذا النوع من الجرائم و ما يميزه من تعقيد و خروج عن المألوف مقارنة بالجريمة التقليدية المادية.

أهداف الدراسة

أما أهداف هذه الدراسة هو تسليط الضوء على هذا النوع من الجرائم المستحدثة التي تزداد انتشارا، مع الانتشار الهائل لتكنولوجيات الإعلام والاتصال بشكل رهيب وتطور شبكة الانترنت وازدياد سرعة تدفقها وكثرة استعمال وسائل التواصل الاجتماعي على غرار الفايسبوك والانستغرام وتويتر...الخ وبالتالي التركيز من خلال بحثنا هذا على التعرف على الجرائم الإلكترونية وخاصة إجراءات التحقيق وجمع الأدلة في هذا المجال.

الدراسات السابقة

و لعل موضوع الجريمة الإلكترونية على العموم و إجراءات التحقيق و جمع الأدلة بالخصوص، لم تستقطب الكثير من الباحثين و الدارسين، وما تم العثور عليه من مراجع و مؤلفات قد تناول جانب من الموضوع دون الجانب الأخر و أهم الدراسات السابقة التي تناولت الموضوع بصفة ملمة تم الاعتماد على المراجع الآتية : حسين طاهري، "الجرائم الإلكترونية" الطبعة الأولى، دار الخلدونية، الجزائر ، 2022 أما فيما يخص الرسائل الجامعية : براهيمي جمال" التحقيق الجنائي في الجرائم الإلكترونية "، مذكرة دكتورة، كلية الحقوق و العلوم السياسية، جامعة مولود معمري، تيزي وزو، 2018/06/27 و بن يحي

إسماعيل" التحقيق الجنائي في الجرائم الإلكترونية "، مذكرة دكتورة، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد ، تلمسان، 2021.

صعوبات الدراسة

تواجه كل دراسة أو بحث من الصعوبات التي اعترضتنا أثناء إعداد هذا العمل المتواضع حيث تتمثل في حداثة هذا الموضوع و نقص المراجع و المؤلفات المتخصصة في هذا المجال و لو أن هناك مجموعة من المراجع و المقالات التي تطرقت إلى الموضوع لكن بشكل جزئي دون تناول كل جوانبه و إنما تمت معالجته بشكل سطحي بالإضافة إلى ارتباط هذا النوع من الجرائم بالحاسب الآلي و الذكاء الاصطناعي و ما يتطلبه من إحاطة بمكونات هذا الأخير و ما بتطلبه من تقنيات تتعلق بهذا النوع من الجرائم و كل ما يحتاجه من جهد فني و قانوني ، بالتالي صعوبة الإلمام بالموضوع والحصول على المعلومات الكافية.

إشكالية الموضوع

أما عن الإشكالية التي يطرحها موضوع دراستنا هذا، فتنصب أساسا حول ما مفهوم الجريمة الإلكترونية ومدى نجاعة إجراءات التحقيق وحجية أدلة الإثبات في مواجهة هذا النوع المتجدد من الجرائم ومواكبتها؟

منهج الدراسة

كما يعتبر الاختيار الصحيح للمنهج من أهم العناصر التي تساعد على انجاز البحوث العلمية بطريقة ناجحة، من خلال دراستنا هذه تم الاعتماد على المنهج الوصفي التحليلي، وصفي من خلال و تعريف الجريمة الإلكترونية و خصائصها و كذا وصف الجهات والسلطات المناط بها مهمة التحقيق و كذلك الإجراءات المتبعة في التحقيق في الجرائم الإلكترونية لاستخلاص الدليل الإلكتروني و الصعوبات التي تعتريها أما بخصوص المنهج التحليلي تم الاعتماد عليه في تحليل و مناقشة آليات التحقيق في الجرائم الإلكترونية و مدى فعاليتها في مواجهة هذه الجريمة.

تقسيم البحث

وللإجابة على الإشكالية المطروحة من خلال دراستنا هذه، ارتأينا تقسيم البحث إلى فصلين بحيث خصصنا الفصل الأول لعرض ماهية التحقيق في الجرائم الإلكترونية بحيث تم تقسيم هذا الفصل بدوره إلى مبحثين أين تناولنا في المبحث الأول إلى مفهوم التحقيق في الجرائم الإلكترونية والمبحث الثاني إلى السلطات المخولة للتحقيق فيها، أما بخصوص الفصل الثاني تم التطرق إلى آليات التحقيق والدليل الرقمي كدليل إثبات في الجرائم الإلكترونية وقد أنهينا البحث بإعداد خاتمة تتضمن أبرز النتائج المتوصل إليها.

الفصل الأوّل:

ماهية التحقيق

في الجرائم الإلكترونية

الفصل الأول: ماهية التحقيق في الجرائم الإلكترونية

لقد شهدت الألفية الأخيرة تطورا مذهلا في المجال الإلكتروني خاصة في يتعلق بالمعاملات الاقتصادية، الإدارية و التجارية، أين نتج عنه تحول العالم من نمط الفضاء المغلق إلى المفتوح على جميع المستويات، بالرغم من امتيازات هذه الثورة الالكترونية فقد صاحبتها انعكاسات سلبية، خاصة بعد ظهور الذكاء الصناعي، أين بدأ التخوف حول الوتيرة التي تتطور معها الجرائم الالكترونية و التي ظهرت و انتشرت بشكل رهيب جرائم تمس بالحياة الشخصية للأفراد و كذا بأمن واستقرار البلدان، عليه سنتطرق في هذا الفصل الى ضبط الإطار المفاهيمي لإجراءات التحقيق في الجريمة الإلكترونية، وذلك من خلال التطرق لمفهوم التحقيق في الجرائم الالكترونية في **(المبحث الأول)** و من ثم للسلطات المختصة بالتحقيق في الجرائم الإلكترونية **(المبحث الثاني)**.

المبحث الأول: مفهوم التحقيق في الجرائم الإلكترونية

إن التطور السريع للجرائم الإلكترونية أمام القاعدة القانونية الجزائية جعل من أحكام قانون الإجراءات الجزائية و قانون العقوبات محدودة و عاجزة على مواكبة التطور الذي تعرفه الجريمة الرقمية، خاصة في مجال التحقيق كونه يعتمد على النصوص الجزائية القائمة، سواء الموضوعية أو الإجرائية لمحاولة ضبط السلوك الإجرامي و تفادي إفلات الجناة من العقاب ولكن في الكثير من الأحيان يكون التحقيق دون جدوى نظرا لخصوصية و طبيعة هذه الجرائم عليه سنتطرق في هذا المبحث لتحديد مفهوم الجريمة الإلكترونية في**(المطلب الأول)**، ثم للتحقيق في الجريمة الإلكترونية في **(المطلب الثاني)**.

المطلب الأول: مفهوم الجريمة الإلكترونية

تتميّز الجريمة الالكترونية بالحداثة واستمرارية التطور السريع للتكنولوجيا والوسائل الإلكترونية التي يتم استعمالها في ارتكاب هذه الجرائم لهذا قد يجد البعض صعوبة في تعريف الجريمة الالكترونية ;بالتالي صعوبةفي مواكبة التطورات التقنية وتحديث المفاهيم من أجل التعامل مع الجرائم الإلكترونية، خاصة أمام تطور القوانين التي تنظمها باستمرار مما يزيد من صعوبة ضبط وتحديد مفهوم دقيق لهذه الجرائم.

وهذا ما سنحاول دراسته في هذا المطلب أين سنتعرض لتعريف الجريمة الإلكترونية في **(الفرع الأول)**، ثم أنواعها في **(الفرع الثاني)** ثم خصائصها في **(الفرع الثالث)** وأخيرا تحديد أركانها في **(الفرع الرابع)**.

الفرع الأول: تعريف الجريمة الإلكترونية

باعتبار أن الجريمة الإلكترونية حديثة، لا زالت لحد الساعة محل بحث و دراسة من طرف القانونيين والعديد من الفقهاء و نظرا لذلك لا نجد تعريف موحد عن هذا النوع من الجرائم كون التعريف القائم عليها الآن قد يصبح بلا جدوى غدا، لصعوبة حصر مجالها في ظل التطور المعلوماتي، ومن أجل ضبط تعريف الجريمة الإلكترونية نتطرق في هذا الفرع لتعريف الذي جاء بها الفقه **(أولا)** ثم للتعريف الذي جاءت به التشريعات **(ثانيا)**.

أولا : تعريف الفقه للجريمة الإلكترونية

تباين رأي الفقه في تعريف الجريمة الإلكترونية و اختلف حتى في تسمية هذا النوع من الجرائم، فتعذر إيجاد فهم مشترك لها وما يستتبع من صعوبة التوصل إلى الحلول المناسبة لمواجهتها[1]، فبالرجوع لتسميات هذا النوع من الجرائم يتبادر إلى الأذهان أنها مختلفة من حيث دلالتها، هناك من يطلق عليها إثم الجرائم الإلكترونية، جرائم الحاسوب الآلي والأنترنت الجرائم المتصلة بالكمبيوتر، و جرائم تكنولوجيا المعلومات، جرائم إساءة استخدام تكنولوجيا المعلومات[2]، الجرائم السبيرانية، الجرائم المعلوماتية والغش المعلوماتي الجرائم الافتراضية أو الانحراف الافتراضي[3]، بالرغم من كل هذا فقد حاول الفقه و لا يزال إجاد تعريف للجرائم الإلكترونية وانقسم في ذلك لثلاث اتجاهات .

1-التعريف الضيق للجريمة الإلكترونية: بدورهم أنصار هذا الاتجاه اختلفوا في تحديد المعيار الذي يتم من خلاله تعريف الجريمة الإلكترونية إلى المعايير التالية:

---

[1] – كوثر مازوني ، **الجريمة المعلوماتية أعمال ندوة وطنية** ، منشورات دار الخلدونية ، ط 1 ، الجزائر ، 2022 ص 7 .

[2] – أمينة بوشعرة – سهام موساوي ، **الإطار القانوني للجريمة الإلكترونية – دراسة مقارنة** ، مذكرة ماستر في الحقوق تخصص القانون الخاص و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة عبد الرحمان ميرة بجاية 2017-2018 ، ص ص 6-7 .

[3] – غنية باطلي ، **الجريمة الإلكترونية – دراسة مقارنة** ، الدار الجزائرية ، الجزائر ، 2016 ، ص 7 .

أ- معيار الوسيلة المستعملة لارتكاب الجريمة: يرى أنصار هذا المعيار أن الحاسوب الآلي هو أساس هذه الجريمة بالنظر للعلاقة ما بين الجاني والضحية، فيرى جانب من الفقه الألماني على أنها: " كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي"[1]، كما قد يكون مسهلا لها بالنظر للعلاقة ما بين الجناة كتسهيل تبادل المعلومات فيما بينهم [2].

ب-معيار توفر المعرفة التقنية: يحصر أصحاب هذا الاتجاه الجريمة الإلكترونية في الحالات التي تتطلب قدرا معتبرا من المعرفة التقنية وإلا اعتبرت جرائم عادية تتكفل بها النصوص التقليدية للقوانين العقابية [3]، فأصحاب هذا الرأي لا يعتمدون على الحاسب الآلي لارتكاب هذا النوع من الجرائم وإنما إلى الشخص الجالس أمامه فنجد من بين التعاريف، تعريف دافيد تومسون "David Tompson" الجريمة الإلكترونية هي الجريمة المرتكبة من طرف فاعل له معرفة في تقنية المعلومات [4].

ج- معيار موضوع الجريمة: أنصار هذا المعيار يرون أن تعريف الجريمة الإلكترونية لا يكون على أساس الوسيلة المستعملة ولا الفاعل وإنما الأمر متعلق بموضوع الجريمة فعرفها على هذا الأساس الفقيه روزبلات " Ros Blat " على أنها نشاط غير مشروع موجه لنسخ أو تغيير أو الوصول إلى المعلومات المخزنة داحل الحاسب الآلي[5].

1-التعريف الواسع لجريمة الإلكترونية: إنتقد أصحاب هذا الرأي الاتجاه الأول في تعريفهم للجريمة الإلكترونية كون أنها جاءت قاصرة على الإحاطة إما بموضوع الجريمة أو الوسيلة المستخدمة لارتكابها أو الفاعل، ومن ثم قام أصحاب هذا الرأي بتضييق نطاق الجريمة الإلكترونية

---

[1] - حسين خليل مطر ، **إجراءات التحقيق و جمع الأدلة في الجرائم الإلكترونية** ، المؤتمر العلمي الثالث لكلية القانون تحت شعار " الإصلاح التشريعي طريق نحو الحكومة الرشيدة و مكافحة الفساد" المنعقد بـ 25 و 26 أفريل 2018 ، الصادر بمجلة الكوفة للعلوم القانونية و السياسية ، جامعة الكوفة ، العراق ، 2018 ، ص 397 .

[2] - غنية باطلي ، **الجريمة الإلكترونية** – دراسة مقارنة ، الدار الجزائرية ، الجزائر ، 2016، ص 15 .

[3] - يوسف جفال ، **التحقيق في الجريمة الإلكترونية** ، مذكرة ماستر تخصص قانون جنائي ، كلية الحقوق و العلوم السياسية جامعة محمد بوضياف ، المسيلة ، 2016-2017 ، ص 9 .

[4] -Mohamed Chawki ,**Essai sur la notion de cybercriminalité**, IEHEI, juillet 2006, p27.

[5] - Mohamed Salah Mehdaoui - Fatiha Khelifi, **Procedural mechanisms for proving digital crime**, Journal of legal and economic research, university of Aflou, V5, N3, November 2022, p272 .

مما جعل الرأي الثاني يقوم عند تعريفه لها بتوسيع مفهومها لتفادي القصور الذي واجه أصحاب الرأي الأول فيعاب على الرأي الأول:

- الجريمة الإلكترونية تقع على أشياء غير مادية من برامج ومعطيات أما الحاسب الآلي في حد ذاته لا يختلف عن الأموال الأخرى ومن ثم تقع عليه في هذه الحالة تطبيق أحكام الجرائم التقليدية و يستوي الأمر إذا كان له دور رئيسي أو ثانوي في الجريمة فلا تكون أبدا الوسيلة المستعملة في الجريمة تدخل في تكوينها ولا في تعريفها .
- كذلك لا يمكننا اعتماد معيار توفر المعرفة بتقنية المعلوماتية في الجريمة الإلكترونية كون أنه في الكثير من الأحيان لا يتوفر في الفاعل كإرسال رسالة تحمل فيروسا، لهذا ذهب أنصار هذا الرأي إلى توسيع تعريف مفهوم الجريمة الإلكترونية ونذكر منهم الفقيهان" Credo "و" Micel " على أنها تشمل استخدام الحاسب كأداة لارتكاب الجريمة بالإضافة الحالات المتعلقة بالولوج غير المصرح به لحاسوب المجني عليه أو بياناته وتمتد لتشمل الاعتداءات المادية سواء تلك المتعلقة بالحاسوب أو مستلزماته وكذا استخدام غير المشروع لبطاقات الائتمان، تزييف المكونات المادية والمعنوية للحاسوب[1].

وعليه يمتد التعريف الواسع ليشمل[2]:

- الحالات التي يكون فيها المال المعلوماتي مناسبة لارتكاب الجريمة.
- الحالات التي يكون فيها المال المعلوماتي أداة لارتكاب الجريمة.
- الحالات التي يكون فيها المال المعلوماتي موضوع للجريمة.

أنتقد كذلك هذا الاتجاه انه لا يمكن الاعتماد على الوسيلة أو المناسبة التي حدث فيها الاعتداء من أجل تعريف الجريمة الإلكترونية وإنما يقتضي البحث عن الفعل الأساسي المكون فليس مجرد استخدام الحاسب معيار لذلك وبناء للاتجاهين الضيق والموسع ظهر اتجاه ثالث اتجاه يعتمد على معيار المصلحة المحمية.

1-التعريف الجامع (معيار المصلحة المحمية): عند تعريف منظمة التعاون والتنمية الاقتصادية للجريمة الإلكترونية أضافت الجانب المعنوي الأخلاقي، فالجريمة الإلكترونية تشمل أي سلوك غير مشروع أو يتعارض مع قواعد السلوك أو غير مرخص والذي يخص المعالجة

[1] – يوسف جفال ، مرجع سابق ، ص 11 .

[2] – غنية باطلي ، مرجع سابق ، ص 20 .

الآلية للمعطيات و/أو نقل المعطيات[1]، غير أن الخبراء إعتبروا أن هذا التعريف غير عملي و يفضلون الطريقة الأنجلوساكسونية أي طريقة الجرد والقائمة التي يضعون فيها الأعمال غير المشروعة والتي تدخل في نطاق الجريمة الإلكترونية، كما أن التشريعات في الكثير من الأحيان تحدد المصالح المهمة في المجتمع لتقوم بحمايتها عن طريق تجريم الأفعال تهددها بالخطر ومحل الاعتداء هو المحل القانوني للجريمة وهو الذي يميز الجريمة عن غيرها [2].

ثانيا: تعريف المشرع الجزائري للجريمة الإلكترونية: اختلفت التشريعات في تعريف الجريمة الإلكترونية نتيجة لتطور التكنولوجي السريع والمتواصل الذي ظهر بموجبه عدة أنماط من جرائم مستنبطة منها وكذا باختلاف البيئة الذي تطور فيها مما يجعل تعريف الجريمة الإلكترونية غير مستقر ومتنوع [3].

أما المشرع الجزائري فمثله مثل أغلبية التشريعات المقارنة لم يقم بإعطاء تعريف قانوني لهذه الجرائم في قانون العقوبات واكتفى بالنص على العقاب المقرر لمثل هذه الجرائم، كما أنه اصطلح عليها بـ " **الجرائم الماسة بنظام المعالجة الآلية للمعطيات** ".

فنظام المعالجة الآلية للمعطيات شرط أولي لضرورة قيام الجريمة فإذا تخلف هذا الشرط لا مجال لهذه الجرائم، ويعتبر هذا النظام تعبير فني لا يمكن لرجل القانون إدراكه بسهولة فهو خارج اختصاص كما أنه يعتبر تعبير للتطورات السريعة والمتلاحقة في مجال الحاسبات الآليات لهذا نجد المشرع الجزائري وحتى الفرنسي عزفوا عن وضع تعريف لهذا النوع من الجرائم وترك الأمر للفقه والقضاء [4].

وقد نص المشرع الجزائري على هذه الجرائم بالقسم السابع مكرر(1) تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات من قانون العقوبات الجزائري[5] من المواد 394 مكرر إلى 394

---

[1] – Brigitte Pereira , **La lutte contre la cybercriminalité – de l'abondance de la norme à sa perfectibilité** , Revue internationale de droit économique , 2016 , p3 .

[2] – غنية باطلي ، مرجع سابق ، ص 21 .

[3] – عائشة بن قارة مصطفى ، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري و القانون المقارن ، دار الجامعة الجديدة ، الإسكندرية ، 2010 ، ص ص 31–31 .

[4] – يوسف جفال ، مرجع سابق ، ص 12 .

[5] – القانون رقم 06–22 المؤرخ في 20 ديسمبر 2006 ، م م ، للأمر رقم 66–155 المؤرخ في 8 يونيو 1966 **و المتضمن قانون الإجراءات الجزائية** ، ج ر ، ع 84 ، الصادرة بتاريخ 24 ديسمبر 2006 .

مكرر 7، يمكننا استقراء أن المشرع الجزائري اعتمد على عدة معايير من أجل ضبط تعريف الجريمة الإلكترونية، فاعتمد على معيار وسيلة الجريمة (نظام الاتصال الإلكتروني) وكذا معيار موضوع الجريمة (المساس بأنظمة المعالجة الآلية للمعطيات) وأخيرا معيار قانون الواجب التطبيق على الأفعال ألا وهو الركن الشرعي لهذه الجرائم المنصوص عليها بقانون العقوبات الجزائري، إضافة إلى إقرار المشرع لمعيار رابع في تحديده لمفهوم الجرائم الإلكترونية و هو أن ترتكب عن طريق منظومة معلوماتية أو نظام الاتصالات الإلكترونية إذ نصت المادة 2 الفقرة 1-أ من القانون(09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها : يقصد في مفهوم هذا القانون بما يأتي:

– الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[1].

الفرع الثاني: صور الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية متنوعة ومن الصعوبة القيام بحصرها فهي تشمل أي أمر غير مشروع بدءا من عدم تسليم الخدمات مرورا بإقتحام الكمبيوتر وصولا إلى انتهاك حقوق الملكية الفكرية والتجسس الاقتصادي وغيرها فالقائمة مفتوحة لتشمل كل ما يمكن تصوره بما يمكن ارتكابه على شبكة الأنترنيت من إنحرافات وتوجد عدة تصنيفات للجرائم الإلكترونية [2].

وبالرجوع للمشرع الجزائري فنجد على العموم أن الجرائم الإلكترونية تنقسم لثلاث صور[3]:

1- الجرائم ضد الأفراد (جرائم الانترنيت الشخصية)، كسرقة الهوية.

2- الجرائم ضد الملكية كوضع فيروسات من أجل تدمير برامج مملوكة لشركات.

3-الجرائم ضد الحكومات كمهاجمة المواقع الرسمية لها.

---

[1] – القانون رقم 09-04 المؤرخ في 5 غشت 2009 ، **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها** ، ج ر ، ع 47 ، الصادرة بتاريخ 16 غشت 2009 .

[2] – كهينة سلام ، **الجريمة المعلوماتية و المجرم المعلوماتي : مفهوم جديد للإجرام في البيئة الرقمية ، مجلة الندوة الوطنية** بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 ص 353

[3] – مختارية بوزيدي ، **ماهية الجريمة الإلكترونية** ، مداخلة في الملتقى الوطني بعنوان آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، مركز جيل البحث العلمي ، المنعقد يوم 29 مارس 2017 بالجزائر العاصمة، ص 11 .

وعلى العموم نذكر بعض الجرائم التي نص عليها المشرع الجزائري بقانون العقوبات الجزائري كما يلي[1]:

– جريمة الدخول الغير المشروع في المنظومة المعلوماتية، طبقا لأحكام المادة 394 مكرر من ق ع ج، وعليه مجرد اختراق الجهاز يعد انتهاكا.

– جريمة الدخول والبقاء في المنظومة المعلوماتية طبقا لأحكام المادة394 مكرر من ق ع ج

– جريمة إدخال معطيات في نظام المعالجة الآلية أو إزالتها بطرق تدليسية طبقا لأحكام المادة 394 مكرر 1 من ق ع ج .

– جرائم نشر المعطيات المخزنة أو المعالجة أو مراسلة بواسطة منظومة معلوماتية وحيازتها والإتجار بها طبقا لأحكام المادة 394 مكرر 2 من ق ع ج.

– جرائم تمس الأمن الوطني ومؤسسات الدولة، طبقا لأحكام المادة 394 مكرر3 من ق ع ج.

– جرائم المنصوص عليها سابقا صادرة عن شخص معنوي مع تشديد العقوبة بمضاعفة الحد الأقصى من العقوبة بـ 5 مرات عن تلك المقررة للشخص الطبيعي طبقا لأحكام المادة 394 مكرر 4 من ق ع ج.

– جريمة تكوين مجموعة أشرار بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية طبقا لأحكام المادة 394 مكرر 5 من ق ع ج.

الفرع الثالث: خصائص الجريمة الإلكترونية

أهم الخصائص التي تتميّز بها الجرائم الإلكترونية هي :

– هي جريمة عابرة للحدود الوطنية: وهذا نتيجة لربط عدد هائل من الحواسيب عبر العالم بهذه الشبكة بحيث يمكن أن يكون الجاني في دولة والمجني عليه في دولة أخرى مما قد يثير مسألة تنازع الاختصاص بين الدول [2].

[1] الأمر رقم66–155 المؤرخ في 8 جويلية 1966، يتضمن قانون العقوبات المعدل والمتمم بالقانون 20–06 المؤرخ في 28 أفريل2020، ج ر عدد 25 الصادرة بتاريخ 29 أفريل 2020 .

[2] – محمود رعد سعدون، حسن جلوب كاظم ، **الجرائم الإلكترونية** ، مجلة الدراسات المالية و المصرفية، الأكاديمية العربية للعلوم المالية و المصرفية ، ع 3 ، العراق ، سبتمبر 2015 ، ص 34 .

– الجريمة الإلكترونية صعبة الاكتشاف والإثبات: فهي لا تترك أثرا خارجيا فهي عبارة عن بيانات وأرقام تتغير أو تمحى من السجلات المخزونة في ذاكرة الحاسوب، كما يمكن للجاني تدمير دليل إدانته في أقل من ثانية واحدة مما يجعل هذه الجريمة صعبة الاكتشاف[1].

– الجريمة الإلكترونية سريعة التنفيذ: ففي غالبة الأحيان يكون الركن المادي لها مجرد ضغط على مفتاح معين في الجهاز وتنفيذ الجريمة عن بعد دون اشتراط التواجد في مسرح الجريمة لذلك فهي تشكل عنصر إغراء للمجرمين[2].

– الجرائم الإلكترونية تتطلب خبرة وتحكما في تكنولوجيا المعلوماتية عند متابعتها كون لها طابع تقني لذلك وجب أن يكون المحقق متخصص في جريمة المعلوماتية حتى لا يتسبب في إتلاف الدليل الإلكتروني[3].

– دافع ارتكاب الجريمة المعلوماتي: فقد يكون الدافع مخالفة النظام العام والخروج عن القوانين، كما قد يكون مادي يراد منه كسب مبالغ مالية، إهانة، تشهير وكل هذا دون الاحتكاك المباشر بالمجني عليه[4].

– قلة الإبلاغ عن الجريمة المعلوماتية: وحتى في حالة الإبلاغ نجد المجني عليه لا يتعاون مع جهات التحقيق خوفا مما قد يترتب عليه من دعاية مضرّة وضياع ثقة المساهمين مثلا إذا كان المجني عليه بنكا أو مؤسسة مالية[5].

الفرع الرابع: أركان الجريمة الإلكترونية

يجدر بنا التساؤل حول أركان قيام الجريمة الإلكترونية بالنظر لطبيعتها الخاصة لتوفر وعليه سنتطرق في هذا الفرع لدراسة الركن المفترض **(أولا)**، ثم الركن الشرعي **(ثانيا)**، الركن المادي **(ثالثا)** وأخيرا نتطرق للركن المعنوي **(رابعا)**.

---

[1] أمينة عبيشات ، **الجرائم الإلكترونية بين المواثيق الدولية و التشريعات الوطنية** ، المجلة الجزائرية للحقوق و العلوم السياسية ، جامعة تيسيمسيلت ، مج 6 ، ع1 ، جوان 2021 ، ص 4 .

[2] أمينة عبيشات ، مرجع نفسه ، ص 5 .

[3] خالد أمين بن نعوم ، **إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري** ، مذكرة ماستر تخصص قانون قضائي ، كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم ، 2018–2019 ، ص 21 .

[4] خالد أمين بن نعوم، مرجع نفسه ، ص 22 .

[5] أمينة بوشعرة – سهام موساوي ، مرجع سابق ، ص 18 .

أولا – الركن المفترض: نقصد بالركن المفترض في الجرائم الإلكترونية هي نظام المعالجة الآلية للمعطيات و الذي يعد الشرط الأولي و البديهي الذي يجب توفر لاعتبار الجريمة إلكترونية و التي قد تتحول لجريمة تقليدية في حالة إنتفاء هذا الركن و من ثم توفر هذا الشرط يسمح بالانتقال إلى المرحلة التالية من أجل البحث عن قيام الجريمة لإلكترونية فهو عنصر لازم[1]، و بالرجوع للمشرع الجزائري وذلك بموجب القانون 09-04 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها[2] وذلك بنص المادة 2 الفقرة ب التي تنص: **"**يقصد في مفهوم هذا القانون بالجرائم المتصلة بتكنولوجيا الإعلام و الاتصال : هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات و أي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية"[3]، غير أن هذا التعريف ورد واسع و غير دقيق في مفهومه ذلك انه لا يتضمن على كامل العناصر المكونة للجريمة الإلكترونية دالا فقط على البعض منها كوسيلة الجريمة ألا وهي نظام الاتصالات الإلكتروني[4].

كما نصت نفس المادة 2 في فقرتها ب على تعريف المنظومة المعلوماتية كما يلي: «أي نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة يقوم واحد منها أو أكثر بمعالجة آلية للمعطيات تنفيذا لبرنامج معين"[5]، ومن ثم ليقوم نظام المعالجة الآلية للمعطيات وجب توفر عنصرين، الأول مادي ومعنوي تربط بينها نتيجة علاقات توحدها لأجل تحقيق هدف

---

[1] – فريال العاقل، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة ماستر في القانون العام، تخصص القانون الجنائي، كلية الحقوق و العلوم السياسية، جامعة أكلي محند اولحاج، البويرة، ص 27.

[2] – القانون رقم 09-04، المرجع السابق.

[3] – القانون رقم 09-04، مرجع نفسه.

[4] – عبد الصديق شيخ ، **الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها** ، مجلة معالم للدراسات القانونية و السياسية ، المركز الجامعي تيندوف ، مج 4 ، ع 1 ، جوان 2020 ، ص 193 .

[5] – المادة 2-ب من القانون 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، مرجع سابق.

محدد، وقد جاءت هذه العناصر على سبيل المثال لا الحصر لمواكبة التطور التقني في هذا المجال، أما العنصر الثاني هو ضرورة إخضاع هذا النظام لحماية فنية[1].

ثانيا- الركن الشرعي: لا يمكننا الحديث عن قيام أي جريمة إذا كانت مخالفة لقواعد القانون الذي يكون أساسه تطابق السلوك والنص القانوني الذي يجرمه سواء كان النشاط فعلا أو امتناع[2]، فلا جريمة ولا عقوبة إلا بنص، ولهذا الركن عنصرين، مطابقة الفعل لنص التجريم وألا يخضع الفعل المرتكب لسبب من أسباب الإباحة، ونجد المشرع الجزائري استحدث القسم السابع مكرر بعنوان المساس بالأنظمة المعالجة الآلية للمعطيات من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الأموال.

ثالثا- الركن المادي: ليكتمل الركن المادي للجريمة الإلكترونية يجب أن تتوفر عناصره على النحو التالي:

- **السلوك الإجرامي:** يعد السلوك الإجرامي الأمر الذي يصدر من الفاعل ويخشى المشرع منه ضررا على الأشخاص فما لم يصدر من الفاعل نشاط في صورة من صوره لا يتدخل المشرع بالعقاب وهي أعمال خارجية تختلف باختلاف الجرائم[3].
- **النتيجة الإجرامية:** هي الأثر الذي يترتب على السلوك الإجرامي والمقرر حمايتها.
- **العلاقة السببية:** و هي الصلة ما بين السلوك الإجرامي والنتيجة الإجرامية، بحيث تثبت بأن السلوك الإجرامي الواقع هو الذي أدى إلى حدوث تلك النتيجة الضارة[4]، على أنه يمكن لبعض صور هذه الجرائم أن يتحقق الركن المادي دون تحقق النتيجة وهو ما يطلق عليه بالجرائم الشكلية تكتفي بعنصر واحد الذي هو النشاط لقيام ركنها المادي، وفي هذه الحالة نكون أمام جريمة قائمة بحد ذاتها دون الحاجة للبحث في النتيجة المتحققة أو العلاقة السببية حتى وإن كان وجودها من

---

[1] - عائشة واشك ، **أصناف الجريمة الإلكترونية في التشريع الجزائري** ، مذكرة ماستر في القانون ، تخصص قانون جنائي و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، 2015-2016 ، ص 15 .

[2]- علي حسين الخلف، عبد القادر الشاوي ، **المبادئ العامة في قانون العقوبات** ، توزيع المكتبة القانونية ، بغداد د س ن ، ص 152 .

[3] - محمود محمود مصطفى ، **شرح قانون العقوبات القسم العام** ، مطابع دار الكتاب العربي ، مصر ، ط5 1960-1961 ، ص 193 .

[4] - علي حسين الخلف، عبد القادر الشاوي، مرجع السابق . ص 141.

طبيعة مادية فليس له أثر قانوني[1]، كإنشاء موقع للتشهير بشخص معين دون طرح هذا الموقع على الشبكة لكن بالرغم من ذلك فلا مناص من معاقبة الفاعل ومن ثم فيتخذ الركن المادي في الجرائم الإلكترونية عدة صور سنتطرق لها [2].

رابعا- الركن المعنوي: لا يكفي لقيام الجرائم الإلكترونية ارتكاب سلوك إجرامي ينص و يعاقب عليه القانون بل يجب أن يصدر هذا الفعل عن إرادة الجاني و تسمى العلاقة التي تربط العمل المادي بالفاعل " الركن المعنوي"، أخذ المشرع الجزائري وفقا للقواعد العامة على النية في الإتيان بالسلوك الإجرامي، سواء فيما تعلق بقيام الجريمة أو قمعها فالإنسان يسأل عن الجريمة إذا أمكن إسناد الفعل إليه وأنه مخطأ[3]، فيتكون الركن المعنوي للجريمة الإلكترونية من عنصريها العلم (إدراك الفاعل) و الإرادة ومن ثم اتجاه السلوك الإجرامي لتحقيق النتيجة[4].

المطلب الثاني: التحقيق في الجريمة الإلكترونية

التحقيق هو ذلك الإجراء الذي تتخذه سلطة البحث و التحري وجمع الأدلة، المتمثلة في أعضاء الضبط القضائي، وسلطة التحقيق المتمثلة في قاضي التحقيق والمحقق بشأن الجريمة المرتكبة لمعرفة حقيقتها، وذلك تمهيداً لإحالة أو عدم إحالة الدعوى الجزائية الناشئة عنها إلى المحكمة، بحسب ما نص عليه القانون، ومن أجل ضبط مفهومه نتطرق في هذا المطلب لدراسة تعريف التحقيق في الجريمة الإلكترونية في **(الفرع الأول)**، ثم خصائص التحقيق في الجرائم الإلكترونية في **(الفرع الثاني)** ، ثم التمييز بين التحقيق الجنائي الإلكتروني و التقليدي في **(الفرع الثالث)** وأخيرا ضمانات التحقيق في الجرائم الإلكترونية **(الفرع الرابع)**.

الفرع الأول: تعريف التحقيق في الجريمة الإلكترونية

للتحقيق أهمية كبيرة في إثبات وقوع الجريمة و إقامة الدليل على مرتكبيها بأدلة الإثبات على اختلاف أنواعها، إذ يعتبر نشاط قانوني يتعلق بإجراءات ضبط الجرائم و البحث عن مرتكبيها و جمع الاستدلالات التي يتطلبها التحقيق، و هو إجراء يتخذ بعد وقوع الجريمة و يسبق مرحلة المحاكمة و عليه فالتحقيق يهدف إلى تمهيد الطريق أمام القضاء الحكم باتخاذ جميع

---

[1] خالد ممدوح إبراهيم ، **أمن الجريمة الإلكترونية** ، الدار الجامعية للطباعة و النشر ، الإسكندرية ، 2008 ص 25.

[2] كهينة سلام ، **مرجع سابق** ، ص 344 .

[3] فخري عبد الرزاق صلبي الحديثي ، **شرح قانون العقوبات القسم العام** ، الناشر العاتك ، القاهرة ، ص 273 .

[4] كهينة سلام ، مرجع سابق ، ص 344 .

الإجراءات الضرورية للكشف عن الحقيقة و هذا ما أكدته نص المادة 1/68 من ق إج ج، وقد تعددت التعريفات حوله إلا أنها لا تخرج عن مدلولها كونها تعتبر مجموعة من الإجراءات القضائية التي تمارسها سلطات التحقيق بالشكل الذي يتم تحديده قانونا بغية التنقيب عن الأدلة وتجميعها و من ثم تقديرها لمعرفة إن كانت كافية من أجل إحالة المتهم للمحاكمة أو الأمر بألا وجه للمتابعة[1].

وعليه لقد أدى ظهور الجرائم الإلكترونية الى ظهور التحقيق الجنائي للجرائم الإلكترونية فهو "عمل قانوني يقوم به مأمور الضبط القضائي المختص لضبط الجريمة الإلكترونية من فاعل لها ودليل إلكتروني لتقديمهم إلى سلطات التحقيق القضائي المتخصصة في هذا النوع من الجرائم لإقامة العدل، كما يعرف على أنه: "الإجراءات التي يقوم بها مأموري الضبط القضائي أو المحققين عبر العالم الافتراضي لضبط الجريمة الإلكترونية والتثبت من أدلتها ومعرفة فاعلها تمهيدا لإحالتهم للمحاكمة "[2].

الفرع الثاني: التمييز بين التحقيق في الجريمة الإلكترونية والتقليدية

من خلال تعريف الجريمة الإلكترونية وكذا تعريف التحقيق الإلكتروني فنجد أن هنالك تميز واختلاف فيما بينهما، فيما يخص الطبيعة ونطاق كلا الجريمتين ومن بين أوجه التمييز نذكر[3]:

– إن امتياز الجرائم الإلكترونية بالتطور بوتيرة عالية من السرعة يجعلها في كل مرة عرضة للتعديل القانوني لمواكبة مكافحتها على عكس الجرائم التقليدية التي هي ثابتة الأركان لا تتغير.

– التحقيق في الجرائم الإلكترونية يتميّز بتطور المفاهيم التي يتم استخدامها في هذه المرحلة كاستخدام مصطلح الولوج بدلا من التفتيش وكذا النسخ بدلا من الضبط.

– للتحقيق الإلكتروني ذاتية خاصة ومستقلة مستمدة من خصاصها المتميّزة.

– في التحقيق الإلكتروني نكون أمام متهم من نوع خاص، يتميّز بنسبة معتبرة من الذكاء والخداع فضلا عن قدراته الفنية والتقنية لجهاز الحاسوب.

---

[1] – خالد علي نزال الشعار ، **التحقيق الجنائي في الجرائم الإلكترونية** ، أطروحة دكتوراه في الحقوق ، كلية الحقوق جامعة المنصورة ، 2020 ، ص 4 .

[2] – خالد علي نزال الشعار مرجع نفسه ، ص 5 .

[3] – خالد علي نزال الشعار مرجع نفسه، ص ص 6-7 .

– اختلاف شكل الدليل في الجرائم الإلكترونية يجعل من المحقق التقليدي يجد صعوبة في فهم حدود هذه الجريمة الإجرامية وما تخلفه من آثار غير مرئية.

الفرع الثالث خصائص: التحقيق في الجريمة الإلكترونية

نظرا لخصوصية الجرائم الإلكترونية ينجر عنه أيضا خصوصية التحقيقي خاصة أمام عدم كفاية أساليب التحري و التحقيق الكلاسيكية نتطرق في هذا الفرع لإبراز خصائص التحقيق **(أولا)** ، و المحقق المعلوماتي **(ثانيا)**.

أولا– خصائص التحقيق في الجرائم الإلكترونية: هي متعددة ونذكر منها[1]:

– الجرائم الإلكترونية لا تترك أية آثار في مسرح الجريمة .

– إمكانية إتلاف الدليل بسهولة من طرف المجرم في وقت قياسي، و بالمقابل إمكانية الحصوص على الدليل المعلوماتي وعمل نسخة منه في ظرف قياسي.

– اعتماد التحقيق الإلكتروني على وسائل تقنية والبرامج الكفيلة بكشف هذا النوع من الجرائم.

– التحقيق في الجرائم الإلكترونية يكون مرهون بالمعرفة القانونية و الفنية للمحقق المعلوماتي وضرورة احترامه لضوابط إجراءات التفتيش والضبط وسلامة إجراءات الحصول على الأدلة.

– تشكيل فريق مختص في التحقيق الجنائي المعلوماتي و كذا خبراء فنيين.

أولا: خصائص المحقق المعلوماتي في الجرائم الإلكترونية: يعتبر المحقق الجنائي في الجرائم الإلكترونية، المكلف بالبحث عن الحقيقة في الجرائم الإلكترونية للكشف و حل الغموض الذي كان يشوب ملابسات الجريمة و ينقسم المحققون في هذه الجرائم إلى نوعين، الفئة الأولى هي الفئة الخبيرة فنيا أو من النخبة المتخصصة في مجال الحاسوب و يتم الاستعانة بهم في جميع مراحل الضبط و الفئة الثانية تمثل الكفاءة المهنية و المتخصصون في التحقيق الجنائي كون أن استجواب المتهمين يعتمد على مهارات و قواعد و قدرات لا تتوافر في الفئة الأولى[2].

و تتمثل الخصائص التي يجب أن يمتاز بها المحقق المعلوماتي:

– خصائص فنية، فيجب أن يكون على علم ودراية لأجهزة الحاسوب و غيرها.

---

[1] – بدرة والي ، **المواجهة الإجرائية لجرائم المعلوماتية** ، مذكرة الماستر تخصص قانون جنائي ، كلية الحقوق و العلوم القانونية ، جامعة محمد بوضياف ، المسيلة ، 2018–2019 ، ص ص 24–25.

[2] – علي حسين محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب و الانترنت ،عالم الكتب الحديقة ، الطبعة الأولى ، 2004 ص02.

– تأهيل وتدريب المحقق المعلوماتي.

الفرع الرابع: ضمانات التحقيق في الجريمة الإلكترونية

تختلف ضمانات التحقيق حسب الصور التي يمكن للمحقق المعلوماتي اتخاذها وهذا من أجل ضمان حماية حرية الأفراد المكرسة دستوريا، و التي تتقرر للفاعل عبر كافة مراحل المتابعة، و هي لا تختلف عن الضمانات المقررة له في الجرائم التقليدية خاصة أنه أهم هذه الضمانات هي ضمانات المشتبه فيه عند التوقيف للنظر باعتبارها أخطر إجراء يمكن للمحققين الإلكترونيين اتخاذه و التي تمس بحرية الفرد باعتباره يتضمن نوع من القسر، بناء على ذلك سنتطرق في هذ الفرع لتبيان هذه الضمانات عند التوقيف للنظر نظرا لأهمية و خطورة الإجراء **(أولا)**، ثم للضمانات المقررة في الجرائم المستحدثة و التي تتضمن إجراءات يمكن للمحقق اتخاذها غير أنه وجب ضبط ضمانات من أجل عدم التعسف في اتخاذها **(ثانيا)**.

أولا– ضمانات التوقيف للنظر: ويتضمن التوقيف للنظر عدة ضمانات تتمثل فيما يلي:

–الحقوق المبدئية اللازمة للموقوف للنظر، أي الحقوق اللصيقة بشخص الإنسان وهي:

– الحق في الغذاء و النظافة البدنية [1].

– الحق في الراحة من خلال تنظيم فترات الاستماع مع مراعاة ظروف التوقيف وكذا الشخص محل التوقيف [2].

– الحق في السلامة الجسدية وكرامة الإنسانية وهذا ما أكدته مواثيق حقوق الإنسان والقوانين الجنائية بما في ذلك المؤسس الدستوري بنص المادة 39 من دستور 2020 تضمن الدولة عدم انتهاك حرمة الإنسان[3] ومن بين الضمانات المقررة في هذا الإطار:

---

[1] – قرار وزاري مشترك بين وزارة الداخلية والمالية مؤرخ في 2011/6/12 **يحدد كيفيات التكفل بمصاريف التغذية و النظافة البدنية للأشخاص الموقوفين تحت النظر داخل مقرات الأمن الوطني،** ج ر ،ع 36 ،الصادرة في 2011/6/29.

[2] – دليلة ليطوش ، **الحماية القانونية للفرد الموقوف للنظر** ، مذكرة لنيل شهادة الماجستير في القانون العام، فرع قانون العقوبات و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة الإخوة منتوري ، قسنطينة ، 2008–2009 ، ص79 .

[3] – تنص المادة 39 من المرسوم الرئاسي رقم 20–442 مؤرخ في 30 ديسمبر 2020 **يتعلق بإصدار التعديل الدستوري، المصادق عليه في استفتاء أوّل نوفمبر 2020 ، في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية** ، ج ر ع 82 الصادرة بتاريخ 30 ديسمبر 2020:" تضمن الدولة عدم إنتهاك حرمة الإنسان، يحظر أي عنف بدني أو معنوي، أو أي مساس بالكرامة و يعاقب القانون على التعذيب ، و على المعاملات القاسية ، و اللاإنسانية أو المهينة و الإتجار بالبشر ".

– الحق في عدم الاعتداء على الكيان المادي والمعنوي للموقوف للنظر، إذ أقر للموقوف للنظر هذه الحماية في الإعلانات والمواثيق العالمية والاتفاقيات الدولية وكذا التشريعات الوطنية وتم المناداة على معاملته على أنه بريء حتى تثبت إدانته[1] وهذا عن طريق حظر كل أشكال وأنواع التعذيب من جهة وكذا وضعه بأماكن لائقة طبقا لأحكام المادة 52 الفقرتين 4 و5 من قانون الإجراءات الجزائية[2].

– الحق في الفحص الطبي و الذي يعد كضمان لعدم تجاوز ضابط الشرطة القضائية أو المحققين لحدود صلاحيتهم[3].

– الحق في تبليغ الموقوف بحقوقه طبقا لأحكام المادة 51 مكرر من ق إ ج ج [4].

– الحق في الالتزام بالصمت، بالرغم من أن المشرع الجزائري لم ينص على هذا الحق[5].

– الحق في الاتصال بعائلته وزيارتها له وهو حق مركس دستوريا بنص المادة 45 الفقرة 2 من دستور 2020[6].

---

[1] – علي محمد جبران آل هادي ، **ضمانات المتهم في مرحلة التحقيق طبقا لنظام الإجراءات الجزائية السعودي الجديد – دراسة تأصيلية تطبيقية** ، مذكرة ماجستير في العدالة الجنائية، تخصص تشريع جنائي إسلامي ، كلية الدراسات العليا ، جامعة نايف العربية للعلوم الأمنية ، 2004 ، ص 263 .

[2] – إذ تنص المادة 52 الفقرة 4 و 5 من الأمر 15–02 المؤرخ في 23 يوليو 2015 م م للأمر رقم 66–155 المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية، ج ر، ع 40 الصادرة بتاريخ 23 يوليو 2015،على ما يلي : " لا يتم التوقيف للنظر إلا في أماكن معلومة مسبقا من طرف النيابة العامة ومخصصة لهذا الغرض تضمن إحترام كرامة الإنسان".

تبلغ أماكن التوقيف للنظر لوكيل الجمهورية المختص إقليميا ، الذي يمكنه أن يزورها في أي وقت " .

[3] – عبد الله أوهايبية، **شرح قانون الإجراءات الجزائية الجزائري**، دار هومة، ط 2، الجزائر، 2018، ص 398 .

[4] – تنص المادة 51 مكرر من ق إ ج ج : " كل شخص أوقف للنظر يخبره ضابط الشرطة القضائية بالحقوق المذكورة في المادة 51 مكرر 1 أدناه و يمكنه عند الإقتضاء ، الإستعانة بمترجم و يشار إلى ذلك في محضر الإستجواب " .

[5] – تنص المادة 100 من ق إ ج ج : " " يتحقق قاضي التحقيق حين المثول المتهم لديه لأول مرة من هويته ويحيطه علما صراحة بكل واقعة من الوقائع المنسوبة إليه و ينبهه بأنه حر في عدم الإدلاء باي إقرار و ينوه عن ذلك في المحضر فإذا أراد المتهم أن يدلي بأقوال تلقاها قاضي التحقيق منه على الفور ... " .

[6] – تنص المادة 45 الفقرة 2 من دستور 2020 : " يملك الشخص الذي يوقف للنّظر حقّ الإتّصال فورا بأسرته" .

ثانيا-الضمانات المقررة في الجرائم المستحدثة بموجب قانون 15-02 ونفرق بين حالتين:

1- الضمانات المقررة عند اعتراض المراسلات و تسجيل الأصوات والتقاط الصور: و قد حدد المشرع الجزائري كيفية اللجوء لهذه التدابير بموجب نص المادة 65 مكرر 5 من القانون أعلاه مع إحاطته ببعض الضمانات القانونية[1]، و التي تتمثل في[2]:

- ترخيص السلطة القضائية و مراقبتها.
- ضرورة الاعتراض لإظهار الحقيقة.
- مراعاة الجرائم التي يجوز فيها الاعتراض والتي ذكرت على سبيل الحصر بالمادة 65 مكرر 5 من ق إ ج.
- مراعاة مدة الإجراء وهي 4 أشهر قابلة للتجديد وفقا للسلطة التقديرية للجهة المصدرة للإذن طبقا المادة 65 مكرر 7 الفقرة 2 من ق إ ج.
- مراعاة السر المهني عند الاعتراض المنصوص عليه بالمادة 45 من ق إ ج.
- تحرير محضر حول عملية الاعتراض.

1- التسرب: نص عليه المشرع الجزائري بالمادة 65 مكرر 11 من ق إ ج: "عندما تقتضي ضرورات التحري أو التحقيق في إحدى الجرائم المذكورة في المادة 65 مكرر 5 أعلاه يجوز لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة بمباشرة عملية التسرب ضمن الشروط المبيّنة في المواد أدناه"، و يكون ذلك بقيام ضابط أو عون شرطة بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنه فاعل معهم أو شريك [3]، مع إحاطته ببعض الضمانات القانونية و التي تتمثل في:

- صدور إذن قضائي بالتسرب[4].
- احترام المدة المقررة للتسرب[5].

---

[1] - كمال ديب ، مكافحة الجريمة المعلوماتية في التشريع الجزائري ، **الجريمة المعلوماتية و المجرم المعلوماتي : مفهوم جديد للإجرام في البيئة الرقمية** ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 ، ص 412 .

[2] - كمال ديب ، مرجع نفسه ، ص 412-413 .

[3] - المادة 65 مكرر 12 من ق إ ج .

[4] - المادة 65 مكرر 11 من ق إ ج .

[5] - المادة 65 مكرر 15 من ق إ ج .

تسبيب عملية التسرب تحت طائلة البطلان.

– محل التسرب: وهي أن تنصب على أحد الجرائم المنصوص عليها في المادة 65 مكرر 5 من ق إ ج والتي منها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

المبحث الثاني: السلطات المختصة بالتحقيق في الجرائم الإلكترونية

إن الاعتماد على الإجراءات أو أجهزة التحقيق التقليدية لمكافحة الجرائم التي ترتكب في البيئة الرقمية يكون عائقا أمام القائمين على البحث وإثبات الجرائم الإلكترونية والتحقيق فيها وعليه وبناء لما تقدم نقوم بدراسة في هذا المطلب، لمفهوم جهاز التحقيق في الجرائم الإلكترونية في **(المطلب الأول)**، ثم نبيّن أجهزة التحقيق المختصة في الجرائم الإلكترونية في **(المطلب الثاني)**.

المطلب الأول: مفهوم جهاز التحقيق في الجرائم الإلكترونية

ونقصد بجهاز التحقيق في الجريمة الإلكترونية الوظائف المتخصصة إلكترونيا وقانونيا والتي بموجبها يصدر قرار إداري، وتشغل نوعين من الأفراد الضباط وضباط الصف والمدنيين وتحكم علاقاتهم الوظيفية التسلسل النظامي للرتب العسكرية، وقانون الخدمة المدنية للمدنيين وقواعد الأمن ويستخدمون التقنية الإلكترونية وضبطها والتي يكون محلها التقنية الالكترونية الرقمية ونظامها وبرامجها وشبكاتها [1]، و هذا ما سنحاول دراسته في هذا المطلب أين سنتعرض لأقسام جهاز التحقيق في الجرائم الإلكترونية في **(الفرع الأول)**، وأخيرا صعوبات التحقيق في الجرائم الإلكترونية في **(الفرع الثاني)**.

الفرع الأول: أقسام جهاز التحقيق في الجرائم الإلكترونية

إن الجرائم الإلكترونية تتعدد وتصنيفاتها إلى جرائم الاعتداء على الأشخاص جرائم الاعتداء على الأموال، انتهاك حقوق الملكية الفكرية كالاعتداء على مواقع وصفحات الشبكة العنكبوتية، انتهاك الحقوق المادية للمؤلف كحق النسخ، جريمة الإتلاف المعلوماتي باستخدام مثلا فيروس[2].

أولا–أجهزة الأمن العام: وتختص بالتحقيق في جرائم الاعتداء على النفس والمال ونذكر منها:

أ– **الجرائم الواقعة على الأشخاص** وهي:

---

[1] – محمد بوعمرة – سيدعلي بنينال ، **جهاز التحقيق في الجريمة إلكترونية في التشريع الجزائري** ، مذكرة ماستر في العلوم القانونية كلية الحقوق و العلوم السياسية ، جامعة آكلي محند أولحاج ، البويرة ، 2019–2020 ، ص 24 .

[2] – حسين طاهري ، **الجرائم الإلكترونية** ، دار الخلدونية ، ط1 ، 2022 ، ص ص 19–71 .

- الاعتداء على حرمة الحياة الخاصة من خلال:

- جريمة الإخلال بالآداب العامة وجريمة التجسس بين الأفراد، جريمة القذف والتشهير.

ب- الجرائم الواقعة على الأموال: بظهور شبكة أنترنيت تطورت العديد من المجالات وأصبحت المعاملات التجارية تستحوذ على الشبكة من بيع وشراء ومن ثم تطور وسائل الدفع والوفاء والسحب وكذا ظهور حافظات النقود الإلكترونية التي تعد نوع من أنواع البطاقات الذكية وهي عبارة عن احتياط مالي يتم تخزينه في معالج "Micro Processor" [1].

ومن بين أهم جرائم الأموال نذكر: جريمة غسيل الأموال إلكترونيا وجريمة السرقة الإلكترونية، جريمة الاحتيال والنصب، الاستيلاء على بيانات البطاقة الائتمانية.

ثانيا - أجهزة التحقيق في الجرائم المخلة بأمن الدولة و نجد:

- أجهزة مختصة في التحقيق في الجرائم المضرة بأمن الدولة من جهة الداخل وتتولاها أجهزة متخصصة مثل مباحث أمن الدولة في مصر وفرنسا.

- أجهزة مختصة في التحقيق في الجرائم المضرة بأمن الدولة من جهة الخارج وتتولاها أجهزة متخصصة مثل المخابرات العامة في مصر.

و من بين الجرائم الماسة بأمن الدولة:

- جرائم الإرهاب والجريمة المنظمة اللذان أخذا بعدا آخرا بدخولهما للبيئة الإلكترونية.

- التجسس ، و الذي يعد حرب معلومات من خلال القيام بجميع الإجراءات التقنية بهدف الوصول واستغلال البيانات المخزنة في الحاسب، تغييرها تدميرها[2].

الفرع الثاني: صعوبات التحقيق في الجريمة الإلكترونية

حداثة الجريمة الإلكترونية و طبيعتها المستمرّة في التطور والنمو السريع، جعل من هذه الخصائص عقبات تقف أمام جهاز التحقيق من أجل الكشف عن الحقيقة، و هذا سواء من ناحية الوصول إلى الصورة الكاملة للواقعة إن كانت فعلا تشكل جريمة أم لا ومن ثم اتخاذ الإجراء الذي يراه مناسبا لذلك، فقد تكون هناك صعوبات في اكتشاف الجريمة في حد ذاتها التي لا تكتشف

---

[1] - عادل يوسف الشكري ، **الحماية الجنائية لبطاقات الدفع الإليكتروني – راسة مقارنة** ، مجلة مركز دراسات الكوفة العراق ، مج1 ، ع 11 ، 2008 ، ص ص 92-93 .

[2] - حسين طاهري ، مرجع سابق ، ص 24 .

إلا بمحض الصدفة **(أولا)** أو صعوبات من أجل إثباتها نتيجة لسهولة محو أثر هذه الجريمة **(ثانيا)** وأخيرا قد تكون هذه صعوبات تعود لجهاز التحقيق بحد ذاته **(ثالثا)**.

أولا- صعوبة اكتشاف الجريمة: تختلف صعوبات اكتشاف الجريمة الإلكترونية حسب الحالات التالية:

1- صعوبات اكتشاف الجريمة الإلكترونية بسبب الجاني: المجرم الإلكتروني هو شخص طبيعي يعيش وسط المجتمع يمارس وظائفه الاجتماعية ويتمتع بكافة حقوقه ويكون لديه دراية بميدان الإعلام الآلي أو هاوي أو مشتغل للحاسوب يتمتّع بقدر كبير من الذكاء[1]، يعمل لحسابه الخاص لكن في الغالب يقوم بذلك لأحد الأشخاص الطبيعية أو المعنوية كشركة مثلا من أجل السطو على أحد الأنظمة المعلوماتية أو الإضرار بالغير[2]، و تختلف العوامل التي تدفع الجاني الإلكتروني لارتكاب هذه الجرائم ، فهناك من يقسمها لدوافع شخصية (مادية و ذهنية)، و دوافع خارجية[3] فقد تكون بدافع التحدي و التسلية، أو من أجل السعي وراء الربح و الإغراء المادي أو بدافع إيديولوجي، أو بدافع الانتقام و الثأر[4].

وعليه يختلف الجاني الإلكتروني عن الجاني التقليدي مما يجعل اكتشاف الجريمة أمر صعب لعدة أسباب:

ب- وهذا نظرا للسمات المشتركة بين الجناة الإلكترونيين عكس الجناة العاديين فهم يتميّزون بما يلي:

- ✓ **الذكاء**، لهذا نجد البعض يطلق على الجرائم الإلكترونية بإجرام المتخصصين[5].

---

[1] - حسين طاهري ، مرجع سابق ، ص 32 .

[2] - غنية باطلي ، مرجع سابق ، ص 34-35 .

[3] - نور الدين حيرش ، مداخلة بعنوان " **ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في القانون الجزائري** " ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 ص 69 .

[4] - نور الدين حيرش ، مرجع نفسه ، ص 36-38 .

[5] - غنية باطلي ، مرجع سابق ، ص 35 .

✓ **الخبرة و المهارة** لتنفيذ الجريمة الإلكترونية على أنه لا يشترط في ذلك درجة عالية منها كون أن أنجح المجرمين تكنولوجيا معلومات الحديثة لم يتلقوا هذه المهارات لا عن طريق التعليم ولا عن طريق الخبرة المكتسبة في هذا المجال[1].

✓ **الجناة الإلكترونيين عائدين للإجرام:** عادة ما يكون ذلك من أجل الرغبة في سد الثغرات التي أدت إلى التعرف عليهم، كما أنه يميل في الكثير من الأحيان إلى التقليد خاصة عندما يكون في وسط الجماعة[2].

✓ **التكييف الاجتماعي:** كون أن الاختلاف بين المجرم التقليدي والإلكتروني كون أن هذا الأخير يحي في الوسط الاجتماعي ولا يضع نفسه في حالة عداء مع المجتمع [3].

ت- وكذا نظرا لما قد تتميّز به جماعة الجناة في الجرائم الإلكترونية عن الفرد وهي:

✓ التطور في السلوك الاجتماعي عن طريق الاشتراك في ارتكاب الجريمة الإلكترونية[4].

- إضافة إلى وجود صعوبات في اكتشاف الجريمة حسب أنماط المجرم الإلكتروني أو نوعه فقد يكون "Hacker" أو "Cracker" المترفون المهووسون[5] أو "Fraudeur" المخادعون أو "Phreaking" لصوص نظم المعلومات أو قراصنة الهاتف، أو المتطرفون ذوو المثل العليا العاملون في الجريمة المنظمة أو مخربي الأنظمة المعلوماتية[6].

1- صعوبات اكتشاف الجريمة الإلكترونية بسبب المجني عليه: قد يكون الضحية في الجرائم الإلكترونية شخص طبيعي، كما قد يكون شخص معنوي هذا ما يمكن تحديده في المجني عليهم ذلك أنه وعلى عكس الجناة الذين يمكن حصر نطاقهم كون أن الضحايا لا يعلمون أي شيء عن الأفعال المجرمة التي يتعرضون لها إلا بعد أن تقع فعلا ولربما يكون قد مسح كل أثر عنها[7].

---

[1] - علي رضوان ، مداخلة بعنوان " **الإطار المفاهيمي للجريمة المعلوماتية مفهومها و سمات مرتكبيها و أكانها** " ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 ، ص 105 .

[2] - صونية نادية مواسة ، مداخلة بعنوان " **خصوصية الجريمة المعلوماتية** " ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 ، ص 194 .

[3] - علي رضوان ، مرجع سابق، ص 107 .

[4] - صونية نادية مواسة ، مرجع سابق ، ص 195 .

[5] - عبد الوهاب ملياني ، **أمن المعلومات في البيئة الأعمال الإلكترونية** ، أطروحة دكتوراه في القانون العام ، كلية الحقوق و العلوم السياسية ، جامعة أبي بكر بلقايد ، تلمسان ، 2016-2017 ، ص ص 71-72 .

[6] - غنية باطلي ، مرجع سابق ، ص 37-41 .

[7] - نهلا عبد القادر المومني ، **الجرائم المعلوماتية** ، ط2 ، دار الثقافة للنشر و التوزيع ، عمان ، 2010 ، ص55.

ثانيا – صعوبات إثبات الجريمة الإلكترونية: ترجع صعوبة إثبات الجريمة الإلكترونية إلى خصائصها ذلك أن تتم في بيئة غير تقليدية واقعة خارج إطار الواقع المادي الملموس لذلك[1] فهي جريمة بدون أثر مما يجعل الأمر يزداد تعقيدا لدى سلطات الأمن و أجهزة التحقيق و الملاحقة مما يجعل من الدليل الإلكتروني صعب الوصول إليه، مما يجعل من الجريمة صعبة الوصول إليها[2].

ثالثا – صعوبات الخاصة بنقص خبرة سلطات الاستدلال والتحقيق: من بين صعوبات التحقيق في الجرائم الإلكترونية نقص الخبرة لدى رجال الضبط القضائي أو أجهزة الأمن بصفة عامة ولدى أجهزة العدالة الجنائية ممثلة في غرفة الاتهام والتحقيق الجنائي فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجرائم المعلوماتية وكيفية التعامل معها[3].

المطلب الثاني: أجهزة التحقيق في الجرائم الإلكترونية

من أجل تقصي أثر الجريمة الإلكترونية من طرف أجهزة تتولى عملية التحقيق، بعدما تبدأ الإجراءات الجزائية بمرحلة البحث و التحري أو مرحلة الاستدلالات التي تتولاها كأصل عام الضبطية أو الشرطة القضائية[4]، إستدعى الأمر لاستحداث وحدات خاصة من أجل محاربة هذا النوع من الجرائم، عليه سنتطرق في هذا المطلب لدراسة أجهزة التحقيق في الجرائم الإلكترونية و المتمثلة في الهيئات والأجهزة المختصة في البحث والتحري في الجرائم الإلكترونية في **(الفرع الأول)**، ثم الهيئات القضائية الجزائية المتخصصة في **(الفرع الثاني)** وأخيرا المنظومة الوطنية لأمن الأنظمة المعلوماتية في **(الفرع الثالث).**

الفرع الأول: الهيئات والأجهزة المختصة في البحث و التحري في الجريمة الإلكترونية و تتمثل هذه الأجهزة في الضبطية القضائية و التي سنتطرق لها **(أولا)**، ثم الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحته **(ثانيا)**.

---

[1] – نهلا عبد القادر ،المرجع نفسه ، ص 36 .

[2] – فتيحة حواس ، **جرائم الوسط الرقمي** ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 ، ص 39 .

[3] – فتيحة حواس ، مرجع نفسه ، ص 37 .

[4] – جيلالي بغدادي ، **التحقيق – دراسة مقارنة** ، الديوان الوطني للأشغال التربوية ، ط1 ، 1999 ، ص 15 .

أولا- الضبطية القضائية: تعتبر الضبطية القضائية صاحبة الاختصاص الأصيل في الكشف والتحري عن الجرائم بصفة عامة، كما منحها المشرع أساليب جديدة للتحري أطلق عليها " أساليب التحري الخاصة" وهي المتعلقة بالجرائم المساس بأنظمة المعالجة الآلية للمعطيات والتي تتم في أول خطوة من أجل الكشف عن الجرائم الإلكترونية المبلغة لهم[1].

1- على مستوى جهاز الشرطة: نظرا لتوفر إطارات جامعية مؤهلة و الاعتماد على ميكانيزمات جيدة تواكب التطورات الحاصلة في مجال الجريمة قامت المديرية العامة للأمن الوطني بتدشين المخبر المركزي للشرطة العلمية الكائن مقره بشاطونوف الجزائر العاصمة في 22 جويلية 1999، إضافة لذلك مخبرين جهويين لوهران قسنطينة مجهزة بأحدث التقنيات و تحتوي على عدة فروع منها خلية الإعلام الآلي و كذا فرق متخصصة مهمتها الكشف عن الجرائم الإلكترونية [2]، أما المخبرين المتواجدين في قسنطينة و وهران فيظم مخبر خاص مهمته التحقيق في الجريمة الإلكترونية اسمه " دائرة الأدلة الرقمية و الآثار التكنولوجية" و يضم 3 أقسام [3]:

- قسم استغلال الرقمية الناتجة عن الحواسيب و الشبكات .
- قسم استغلال الأدلة الناتجة عن الهواتف النقالة .
- قسم تحليل الأصوات .

2-على مستوى جهاز الدرك الوطني: يعمل جهاز الدرك الوطني على مكافحة الجريمة الإلكترونية بواسطة المعهد الوطني للأدلة الجنائية و علم الإجرام الكائن مقره ببوشاوي التابع لقيادة الدرك العامة قسم الإعلام و الإلكترونيك المختص بالتحقيق و الكشف عن الجرائم الإلكترونية، و هذا من أجل تسهيل مهمة البحث و المعاينة و التفتيش في أنظمة الحواسيب و من أجل هذا الغرض تم وضع مصالح الشرطة القضائية التابعة للدرك الوطني في خدمة هذه

---

[1] – أمنة بوزينة أمحمدي ، **إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية** ، مداخلة في ملتقى وطني بعنوان " آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري" ، مركز جيل البحث العلمي بالجزائر العاصمة ، المنعقد يوم 29 مارس 2017 ، ص 66.

[2] – قدور حسين فاتحة ، **دور الشرطة العلمية و التقنية في الكشف عن الجريمة** ، مذكرة ماستر تخصص القانون الخاص ، كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس مستغانم ، 2020 ، ص 12 ..

[3] – عبد القادر فلاح – نادية أيت عبد المالك ، **التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري** ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، جامعة المسيلة ، مج 4 ، ع 02 ، جانفي 2020 ص ص 1695 – 1696 .

الأهداف[1]، و قد أنشأ هذا المعهد بموجب المرسوم الرئاسي رقم 04-432 المؤرخ في 29-12-2004[2] و تم تنظيم مصالحه و الأقسام و المخابر بموجب قرار وزاري مشترك مؤرخ في 14-04-2007 .[3]

كما ينظر جهاز الدرك الوطني في الكشف عن الجرائم الإلكترونية بواسطة مديرية الأمن العمومي والاستغلال والمصلحة المركزية للتحريات الجنائية صاحبة الاختصاص الوطني مهمتها الأساسية التصدي للجريمة الإلكترونية[4].

ثانيا- الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته:

لقد نصت المادة 13 من القانون رقم 09-04 المؤرخ في 5 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، على إنشاء "الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحته" أما عن تنظيم تشكيلة الهيئة و طبقا لأحكام المادة 13 في فقرتها الثانية، فقد صدر المرسوم الرئاسي رقم 15-261 في 08 أكتوبر 2015 و الذي تضمن في فصوله تحدي التشكيلة و التنظيم و كيفيات سيرها[5]، و تعتبر هذه الهيئة سلطة إدارية مستقلة تتمتع بالشخصية المعنوية و الاستقلال المالي توضع لدى الوزير المكلف بالعدل[6].

يقع مقرها بالجزائر العاصمة[7].

---

[1] – حسين ربيعي ، **آليات البحث و التحقيق في الجرائم المعلوماتية** ، أطروحة دكتوراه العلوم في الحقوق ، تخصص قانون العقوبات و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة باتنة 1 ، 2015-2016 ، ص ص 182-183 .

[2] – المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004 **يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي** ، ج ر ، ع 84 الصادرة بتاريخ 29 ديسمبر 2004 .

[3] – قرار وزاري مشترك مؤرخ في 14 أبريل 2007 ، **المتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبث في علم التحقيق الجنائي** ، ج ر ، ع 36 ، الصادرة بتاريخ 3 يونيو 2007 .

[4] – عبد القادر فلاح – نادية أيت عبد المالك ، مرجع سابق ، ص 1696 .

[5] – المرسوم الرئاسي رقم 15-261 ، مرجع سابق .

[6] – المادة 2 من المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 ، **المحدد لتشكيلة و تنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها** ، ج ر ، ع 53 ، الصادرة بتاريخ 8 أكتوبر 2015.

[7] – المادة 3 من المرسوم الرئاسي رقم 15-261 ، مرجع سابق .

1- مهام الهيئة: وتقوم بالمهام التالية تحت رقابة السلطة القضائية وهذا ما أكدته نص المادة 4 في فقرتها الأول من المرسوم الرئاسي 15-261:

أ- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحته.

ب – مساعدة السلطات القضائية و مصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيا الإعلام و الاتصال بما في ذلك تجميع المعلومات و إنجاز الخبرات القضائية.

ج- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و تحديد مكان تواجدهم"[1].

كما نصت المادة 4 من المرسوم الرئاسي 15-261 على مهام أخرى للهيئة وهي:

– اقتراح عناصر الاستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال ومكافحتها.

– ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة، تحت سلطة القاضي المختص وباستثناء أي هيئات وطنية أخرى.

– تجميع و تسجيل و حفظ المعطيات الرقمية و تحديد مصدرها و مسارها من أجل استعمالها في الإجراءات القضائية.

– السهر على تنفيذ طلبات المساعدة الصادرة عن البلدان الأجنبية وتطوير تبادل المعلومات والتعاون على المستوى الدولي في مجال اختصاصها.

– تطوير التعاون مع المؤسسات و الهيئات الوطنية المعنية المتصلة بتكنولوجيا الإعلام و الاتصال.

– المساهمة في تكوين المحققين المتخصصين في مجال التحريات التقنية المتصلة بتكنولوجيا الإعلام و الاتصال.

---

[1] – المادة 14 من القانون رقم 09-04 المؤرخ في 5 غشت 2009 ، **المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الإعلام و الاتصال و مكافحتها** ، ج ر ، ع 47 ، الصادرة بتاريخ 16 غشت 2009 ، .

المساهمة في تحديث المعايير القانونية في مجال اختصاصها".

2- تشكيلة الهيئة: تتكون اللجنة من هيئة إدارية و هيئة تقنية كما يلي:

أ- **الهيئة الإدارية:** وتتكوّن من اللجنة المديرة يترأسها الوزير المكلف بالعدل المديرية العامة ويترأسها المدير العام والذي يعين بموجب مرسوم رئاسي[1].

ب-الهيئة التقنية: و تتكوّن من عدة مديريات و هي:

- مديرية المراقبة الوقائية و اليقظة الإلكترونية[2].
- مديرية التنسيق التقني[3].

الفرع الثاني: الهيئات القضائية الجزائية المتخصصة

يقصد بها الأقطاب الجزائية المتخصصة و ليست بجهات قضائية خاصة، ظهرت فكرة الأقطاب المتخصصة لأول مرة في قانون التنظيم القضائي، بإنشائها سواء في الجانب الجزائي أو المدني، و تم إنشاء الأقطاب الجزائية بموجب القانون 04-14 المؤرخ في 1 نوفمبر 2004 المعدل و المتمم للأمر 66-155 و المتضمن قانون الإجراءات الجزائية، و التي تعتبر هيئات قضائية جزائية، يشمل اختصاصها الإقليمي كل محاكم مجالس قضاء الوطن، اختصاصها غير مانع بمعنى تبقى الجرائم المختصة بها من اختصاص الماكم العادية التي يكون لها الاختصاص المحلي عليها و تستمر في النظر فيها لحين تفعيل إجراءات إحالتها إلى القطب الجزائي الوطني المختص[4].

و قد جاء تعديل قانون الإجراءات الجزائية سنة 2004، بتمديد اختصاص المحلي لوكيل الجمهورية و قاضي التحقيق و المحكمة، عن طريق التنظيم إلى دوائر اختصاص محاكم أخرى و هذا في أنواع محددة على سبيل الحصر طبقا لأحكام المواد 37 ، 40 و329 منه، حيث نصت المادة 37 في فقرتها الثانية: "يجز تمديد الاختصاص المحلي لوكيل الجمهورية إلى دائرة اختصاص محاكم أخرى عن طريق التنظيم في جرائم المخدرات و الجريمة المنظمة عبر الحدود

---

[1] - حسين ربيعي ، مرجع سابق ، ص 173 .

[2] - طبقا لأحكام المادة 18 من المرسوم الرئاسي 15-261 ، مرجع سابق .

[3] - حسين ربيعي ، مرجع سابق ، ص 175 .

[4] - ريم لغواطي ، **مدى فعالية الأقطاب الجزائية المتخصصة في مكافحة الجريمة** ، مذكرة ماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة زيان عاشور الجلفة ، 2019-2020 ، ص 25

الوطنية و **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** ..." و الذي مدد بناء عليه الاختصاص بصدور المرسوم رقم 06-348 المؤرخ في 05-10-2006[1] المعدل و المتمم بالمرسوم التنفيذي رقم 16-267 المؤرخ في 17-10-2016 [2] المتعلق بتمديد الاختصاص حيث طبقا للمواد 2 ، 3 ، 4 و 5 منه نصت على اختصاص أربع جهات مدّ إليها الاختصاص و هي:

- ✓ محكمة سيدي امحمد الجزائر العاصمة و يمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : الجزائر، الشلف، الأغواط، البليدة، تيزي وزو، الجلفة، المدية، المسيلة، بومرداس البويرة، وعين الدفلة.
- ✓ محكمة قسنطينة و يمتد اختصاصها الإقليمي إلى المجالس القضائية التالية: قسنطينة، أم البواقي، باتنة، بجاية، تبسة، جيجل، سطيف سكيكدة، عنابة، قالمة، برج بوعريريج الطارف، خنشلة، سوق أهراس وميلة.
- ✓ محكمة ورقلة و يمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : ورقلة، أدرار تمنراست، إليزي، بسكرة، الوادي، وغرداية.
- ✓ محكمة وهران و يمتد اختصاصها الإقليمي إلى المجالس القضائية التالية : وهران، بشار تلمسان، تيارت، تندوف، سعيدة، سيدي بلعباس، مستغانم، معسكر، البيّض، تيسمسيلت النعامة، عين تيموشنت، وغليزان.

فمن أجل محاربة الجرائم الإلكترونية، فقد توجه المشرع لإنشاء قضاء متخصص في هذه الجرائم من خلال إنشاء جهات قضائية ذات اختصاص إقليمي، كما رأيناه أعلاه و من أجل توسيع من مفهوم هذه الجرائم إلى كل الجرائم التي لها صلة بتكنولوجيا الإعلام و الاتصال القديمة و الحديثة، و كل تقنية تظهر مستقبلا و ذلك بموجب الأمر رقم 21-11 المؤرخ في 25-08-

[1] – المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 **المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق** ، ج ر ، ع 63 ، الصادرة بتاريخ 8 أكتوبر 2006 .

[2] – المرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 ، يعدل و يتمم المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 ، **و المتضمن تمديد الإختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق** ، ج ر، ع 62 ، الصارة بتاريخ 23 أكتوبر 2016 .

2021[1]، الذي استحدث القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

و بناء على ذلك فإن قواعد المتابعة الجزائية أمام القطب الجزائي لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال تتميّز عن الجرائم التقليدية نظرا لخصوصية الجرائم الإلكترونية من حيث الاختصاص أو سواء من حيث إجراءات توصل القطب بالملف.

أولا- من حيث الاختصاص: يختص القطب الجزائي بمعالجة الجرائم المتصلة بتكنولوجيا الإعلام والاتصال طبقا لنص المادة 211 مكرر 22 من الأمر 21-11، فيختص و يمارس قاضي التحقيق على مستوى القطب المستحدث طبقا لأحكام المادة 211 مكرر 23 من الأمر أعلاه صلاحياته في كامل التراب الوطني، وفقا لنمطين و هما:

1-الإختصاص الحصري للقطب دون سواه في هذا النوع من الجرائم، سواء فيما تعلق بالجرائم المحددة قانونا و الجرائم المرتبطة بها و المنصوص عليها على سبيل الحصر بالمادة 211 مكرر 24 التي تنص: "مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال وقاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال المذكورة أدناه وكذا الجرائم المرتبطة بها:

- الجرائم التي تمس بأمن الدولة أو بالدفاع الوطني.
- الجرائم نشر وترويج أخبار كاذبة بين الجمهور من شأنها المساس بالأمن أو السكينة العامة أو استقرا المجتمع.
- جرائم نشر وترويج أنباء مغرضة تمس بالنظام والأمن العموميين ذات الطابع المنظم أو العابر للحدود الوطنية.
- جرائم المساس بأنظمة المعالجة الآلية للمعطيات المتعلقة بالإدارات والمؤسسات العمومية.
- جرائم الاتجار بالأشخاص أو بالأعضاء البشرية أو تهريب المهاجرين .
- جرائم التمييز وخطاب الكراهية".

[1] - الأمر رقم 21-11 المؤرخ في 25-08-2021 ، يتمم الأمر 66-155 المؤرخ في 8 يونيو 1966 و **المتضمن قانون الإجراءات الجزائية** ، ج ر ، ع 65 ، الصادرة بتاريخ 26 أوت 2021 .

أو بالنسبة للجرائم الأكثر تعقيدا و الجرائم المرتبطة بها طبقا لأحكام المادة 211 مكرر 25 التي تنص:

" مع مراعاة أحكام الفقرة 2 من المادة 211 مكرر 22 أعلاه، يختص وكيل الجمهورية لدى القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وكذا قاضي التحقيق ورئيس ذات القطب، حصريا بالمتابعة والتحقيق والحكم في الجرائم المتصلة بتكنولوجيات الإعلام والاتصال الأكثر تعقيدا والجرائم المرتبطة بها.

الفرع الثالث: المنظومة الوطنية لأمن الأنظمة المعلوماتية

لقد استحدث المشرع الجزائري المنظومة الوطنية لأمن الأنظمة المعلوماتية بموجب المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020[1]، و التي تعد الإطار التنظيمي لإعداد الإستراتيجية الوطنية لأمن الأنظمة المعلوماتية و تنسيق تنفيذها، و توضع لدى وزارة الدفاع الوطني[2]، طبقا لأحكام المادة 3 من المرسوم 20-05 أعلاه تتضمن المنظومة الوطنية لأمن الأنظمة المعلوماتية، مجلس وطني لأمن الأنظمة المعلوماتية و وكالة الأمن الأنظمة المعلوماتية نتطرق لهما تباعا.

1- المجلس الوطني لأمن الأنظمة المعلوماتية

أ- يتشكل المجلس طبقا لأحكام المادة 5 من المرسوم الرئاسي 20-05 من:[3]

- وزير الدفاع رئيسا.
- ممثل عن رئاسة الجمهورية.
- ممثل عن الوزير الأول.
- الوزير المكلف بالشؤون الخارجية.
- الوزير المكلف بالداخلية.
- الوزير المكلف بالعدل.
- الوزير المكلف بالمالية.

[1] - المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 ، **المتعلق بوضع منظومة وطنية لأمن لأنظمة المعلوماتية** ، ج ر ، ع 4 ، الصادرة بتاريخ 26 جانفي 2020 .

[2] - المادة 2 من المرسوم الرئاسي رقم 20-05 ، مرجع نفسه .

[3] المادة 5من المرسوم الرئاسي رقم 20-05 ، مرجع نفسه .

- الوزير المكلف بالطاقة.
- الوزير المكلف بالاتصالات.
- بالتعليم العالي.
- المدير العام لوكالة الأنظمة المعلوماتي بصفة استشارية.

على أنه يمكن للمجلس في كل الحالات الاستعانة بأي شخص أو مؤسسة من شأنه تنويره في أعماله.

ب- **مهام المجلس:** لقد حددت المادة 4 من المرسوم الرئاسي رقم 20-05 مهامه كالآتي:[1]

- البت في عناصر الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المقترحة من قبل الوكالة وتحديدها.
- دراسة مخطط عمل الوكالة وتقرير نشاطاتها والموافقة عليهما.
- دراسة التقارير المتعلقة بتنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية والموافقة عليها.
- الموافقة على اتفاقات التعاون والاعتراف المتبادل مع الهيئات الأجنبية في مجال أمن الأنظمة المعلوماتية.
- الموافقة على سياسية التصديق الإلكتروني للسلطة الوطنية للتصديق الإلكتروني.
- الموافقة على تصنيف الأنظمة المعلوماتية.
- اقتراح ملائمة الإطار الهيكلي أو التنظيمي الخاص بأمن الأنظمة المعلوماتية عند الحاجة.
- يبدي المجلس رأيا مطابقا في أي مشروع نص تشريعي أو تنظيمي ذي صلة بأمن الأنظمة المعلوماتية.

2- وكالة أمن الأنظمة المعلوماتية:

تعتبر الوكالة طبقا لأحكام المادة 17 من المرسوم الرئاسي 20-05 أعلاه مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلالية المالية مقرها الجزائر[2].

أ- مهام الوكالة لقد حددت المادة 18 من المرسوم الرئاسي رقم 20-05 ونذكر من مهامها كالآتي:

[1] المادة 4 من المرسوم الرئاسي رقم 20-05 ، مرجع نفسه .

[2] - المادة 17 من المرسوم الرئاسي رقم 20-05 ، مرجع نفسه.

– تحضير عناصر الاستراتيجية الوطنية في مجال أمن الأنظمة المعلوماتية وعرضها على المجلس.

– تنسيق تنفيذ الاستراتيجية الوطنية لأمن الأنظمة المعلوماتية المحددة من قبل المجلس.

– إقتراح كيفيات اعتماد مزودي خدمات التدقيق في مجال أمن الأنظمة المعلوماتية.

– إجراءات تحقيقات رقمية في حالة الهجمات أو الحوادث السبيرانية التي تستهدف المؤسسات الوطنية.

– السهر على جميع وتحليل وتقييم المعطيات المتصلة بمجال أمن الأنظمة المعلوماتية لاستخلاص المعلومات الملائمة التي تسمح بتأمين منشآت المؤسسات الوطنية.

– متابعة عمليات التدقيق لأمن الأنظمة المعلوماتية.

– ضمان اليقظة التكنولوجية في مجال أمن الأنظمة المعلوماتية.

– إعداد وتحيين خارطة للأنظمة المعلوماتية المصنفة.

– إجراء تحقيقات رقمية في حالة الهجمات أو الحوادث السبيرانية التي تستهدف المؤسسات الوطنية.

كما يتولى إدارة الوكالة لجنة توجيه وتزود بلجنة علمية، كما يكلف بتسييرها مدير عام وتتوفر على مركز وطني عملياتي الأمن الأنظمة ومديرات ومصالح تقنية وإدارية موضوعة تحت سلطته[1].

[1] – فتيحة حزام ، **حماية الأنظمة الرقمية بين الآليات التقنية و أجهزة الحماية – قراءة في أحكام المرسوم الرئاسي 20-05** ، مجلة الحقوق والعلوم الإنسانية ، جامعة زيان عاشور الجلفة ، مج 13 ، ع 3 ، أكتوبر 2020 ، ص 183.

خلاصة الفصل الأول

لقدت تطرقنا في هذا الفصل لدراسة ماهية التحقيق في الجرائم الإلكترونية من أجل ضبط مفهومها من الناحية القانونية، و عليه بيّنا في هذا الفصل بعض النقاط الأساسية و المهمة و التي تسمح لنا بإحاطة موضوع التحقيق في هذا النوع من الجرائم، حيث أثير جدل فقهي كبير حول تعريف الجريمة الإلكترونية، فهناك من وسع من نطاق هذه الجرائم و هناك من الفقهاء من ضيق منه، كما أن أهم ركن تقوم عليه هذه الجريمة هو الركن المفترض المتمثل في وجود وسيط إلكتروني مثل جهاز الكمبيوتر، ما يجعل هذه الجريمة تتميز بعدة خصائص من أهمها أنها جريمة عابرة للحدود، كما أن مسرح ارتكابها هو بيئة افتراضية و القيام بها لا يحتاج إلى وقت أو جهد كبير.

تطرق المشرع الجزائري إلى الجريمة الإلكترونية بموجب قانون العقوبات، قانون الإجراءات الجزائية، بالإضافة إلى قانون الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، نظرا لما يحتاجه هذا النوع من الجرائم من إجراءات للتحقيق تتماشى مع طبيعة وخصوصية هذا النوع من الجرائم، كما يتطلب التحقيق في هذا النوع من الجرائم إلى أجهزة تحقيق جد مؤهلة وتتمتع بمهارات وخبرات فنية عالية، لمواجهة هذا النمط المتجدد من الجرائم ومواكبة التطور السريع والمستمر الذي تتميز به هذه الأخيرة.

الفصل الثاني

إجراءات التحقيق وأدلة الإثبات

في الجرائم الإلكترونية

الفصل الثاني: إجراءات التحقيق وأدلة الإثبات في الجرائم الإلكترونية

لقد أثارت الجريمة الالكترونية عقبات أمام سلطات التحقيق و القانون الجزائي والإجرائي، باعتبار أن نصوص هذا القانون قد أعدت لتنظيم الإجراءات المتعلقة بالجرائم التقليدية المادية القائمة، فهل هي كفيلة بضمان استخلاص الدليل الإلكتروني الجنائي و ما طبيعة هذا الدليل، و ما هي خصائصه، و مدى حجية هذا الأخير في الإثبات الجنائي أمام القضاء، و دوره في مساعدة سلطات التحقيق في الوصول إلى الحقيقة و أمام هذه التساؤلات تم تقسيم هذا الفصل إلى مبحثين، أين سيتم التطرق في **(المبحث الأول)** إلى إجراءات التحقيق التقليدية المألوفة المعتمدة في البحث والتحري في الجرائم التقليدية، و الإجراءات المستحدثة من طرف المشرع لمواكبة التطور السريع للجريمة الالكترونية، أما بخصوص**(المبحث الثاني)** سنتطرق إلى الطبيعة القانونية للدليل الالكتروني و خصائصه و مميزاته، و في الأخير حجية هذا الأخير في الإثبات الجنائي.

المبحث الأول: آليات التحقيق في الجرائم الإلكترونية

سنتطرق من خلال هذا المبحث إلى مدى نجاعة إجراءات التحقيق التقليدية في مكافحة الجرائم الالكترونية، أم أن التطور المتسارع الذي تعرفه هذه الأخيرة يجعل من إجراءات التحقيق التقليدية غير مجدية في مواجهة هذا النمط الإجرامي المتجدد، ما يلزم المشرع بالتدخل و استحداث إجراءات تحقيق جديدة و فعالة، تناسب و تواكب التطور السريع الذي تتميز به الجرائم الالكترونية، عليه سنتناول من خلال هذا المبحث دراسة الإجراءات التقليدية أو المألوفة للتحقيق في الجرائم الإلكترونية و مدى نجاعتها في **(المطلب الأول)** من ثم سنتطرق الى إجراءات التحقيق المستحدثة في **(المطلب الثاني)**.

المطلب الأول: الإجراءات التقليدية أو المألوفة للتحقيق في الجرائم الإلكترونية

بعد وقوع الجريمة، تقوم سلطات التحقيق بجملة من الإجراءات المحددة قانونا للكشف عن الحقيقة و استخلاص الأدلة الجنائية، لفك ملابسات و خيوط الجريمة، قبل مرحلة المحاكمة أو ما يعرف بإجراءات التحقيق التقليدية، هذا ما سنتناوله من خلال هذا المطلب بشيء من التفصيل، و الذي بدوره قسمناه إلى خمسة فروع.

الفرع الأول: تلقي الشكاوى و البلاغات

يعتبر هذا الإجراء من أهم إجراءات التحقيق و تحريك الدعوى العمومية، بحيث يعتبر إخطار لسلطات التحقيق عن وقوع الجريمة، بالتالي الإسراع في البحث و التحري و كذا جمع الأدلة، غير أن مشكلة إحجام المجني عليه و إعراضه عن التبليغ عن الجريمة الإلكترونية يعود إلى اعتبارات كثيرة ، والتي قد تكون في بعض الأحيان شخصية متعلقة بالشرف و الاعتبار[1]، ما يصعب عملية الحصول على الأدلة و بالتالي إفلات الجاني من العقاب و سنتطرق من خلال هذا الفرع إلى تلقي الشكاوى و البلاغات بالطرق التقليدية و تلقي الشكاوى و البلاغات عن طريق الأنترنت.

أولا : تلقي الشكاوى و البلاغات بالطرق التقليدية

يعتبر هذا الإجراء إخطار لسلطات التحقيق بأن جريمة ما ارتكبت، أو أنها سترتكب لاحقا بالتالي، على هذه الأجهزة التحرك لمواجهة الجريمة بالانتقال إلى مكان حدوثها و المحافظة على مسرح الجريمة و الأدلة، و تسجيل أقوال الشهود و جمع كل الاستدلالات التي تفيد التحقيق ..الخ، عليه و من خلال المادة 17 من قانون الإجراءات الجزائية، لم يحدد القانون طريقة الشكاوى من طرف الأشخاص المتضررين من الجريمة فقد تكون شفهية أو كتابية، كما يمكن تقديم الشكوى من المتضرر نفسه أو من طرف محاميه [2]، أما البلاغات فتعني ما يرد من أخبار عن الجريمة إلى علم ضابط الشرطة القضائية سواءا كان ذلك شفاهة أو عن طريق الكتابة فعلى الضبطية القضائية تلقي هذه الشكاوى و البلاغات و إرسالها إلى النيابة العامة فورا طبق لنص المادة 18 من قانون الإجراءات الجزائية[3].

ثانيا – تلقي الشكاوى و البلاغات عن طريق الانترنت:

إن تلقي الشكاوى و البلاغات عن طريق الانترنت أهمية بالغة في مكافحة الجريمة الإلكترونية، نظرا للطبيعة الخاصة التي تتميز بها هذه الأخيرة، حيث توفر لسلطات التحقيق السرعة اللازمة لمباشرة إجراءات البحث و التحري، ما يمكنهم من الكشف المبكر عنها

[1] – يزيد بوحليط، **الجرائم الالكترونية و الوقاية منها في القانون الجزائري**، دار الجامعة الجديدة، الإسكندرية،2019 ص 221 .

[2] –محمد حزيط، **مذكرات في قانون الإجراءات الجزائية**، دار هومه للطباعة و النشر و التوزيع الجزائر،2007،ص59.

[3] – انظر المادة 18 من ق إ ج ج.

وعن مرتكبيها، فتلقي البلاغات عبر الانترنت هو نفسه في العالم المادي حيث تتوفر نماذج للبلاغات غبر الانترنت في عدة مواقع إلكترونية[1].

إن المشرع الجزائري لم يحدد وسيلة لتقديم الشكاوى و البالغات مما يفتح المجال القيام بهذا الإجراء بأي وسيلة ومنها استعمال تقنية الاتصال المتمثلة في شبكة الانترنت و الهاتف الخلوي، على غرار ما استحدثته قيادة الدرك الوطني بإنشاء و إطلاق خدمة عمومية عبر 58 ولاية باستعمال تكنولوجيا الإعلام و الاتصال ، حيث يمكن من خلال هذا التطبيق إيداع الشكاوى و البلاغات المسبقة و تأكيدها بعد ذلك في غضون 30 يوم ما يسمح لأجهزة الضبطية القضائية من ربح الوقت و السرعة في بدء إجراءات التحقيق و البحث و التحري للكشف عن الجريمة قبل أن يتمكن المجرم الالكتروني من تدمير و إزالة الدليل الالكتروني[2].

الفرع الثاني: المعاينة في العالم الافتراضي

حتى تتمكن سلطات التحقيق من استخلاص الدليل الالكتروني عن طريق الآثار التي أحدثها المجرم بمسرح الجريمة، على هذه الأخيرة التنقل و بسرعة من أجل معاينة مسرح الجريمة و جمع الاستدلالات والآثار، هذا ما سنتطرق إليه من خلال هذا الفرع.

أولا- مفهوم المعاينة: هي إجراء يتنقل بمقتضاه المحقق إلى مسرح الجريمة ليعاين و يشاهد و يفحص بنفسه مكانا أو أي شيء له علاقة بالجريمة، لإثبات حالة و ضبط كل ما يلزم لكشف الحقيقة، و يتطلب هذا الإجراء سرعة الانتقال إلى مسرح الجريمة لإثبات حالة و ضبط الأشياء التي لها أية علاقة بالجريمة و تفيد التحقيق و تكشف الحقيقة، فالمعاينة هي إجراء من إجراءات التحقيق التي يجوز لجهات التحقيق اللجوء إليها من تلقاء نفسها كل ما رأت في ذلك ضرورة للوصول إلى الحقيقة أو بناءا على طلب الخصوم، فتجرى المعاينة بحضور أطراف الدعوى غير أنه يجوز للمحقق القيام بها في غيابهم نظرا لما تقتضيه من سرعة الانتقال إلى محل الجريمة قبل ضياع أو تعديل للأدلة[3].

---

[1] – عمر محمد أبو بكر بن يونس،**الجرائم الناشئة عن استخدام الانترنت**، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، القاهرة، مص،2009، ص830.

[2] – يزيد بوحليط، المرجع السابق، ص 225 .

[3] – ابراهيمي جمال، الرجع السابق، ص57 .

و تتم المعاينة في الجريمة الالكترونية بمعاينة الآثار و البصمات الالكترونية التي يتركها مستخدم الشبكة المعلوماتية أو الانترنت و تشمل الرسائل المرسلة والتي يستقبلها و كل الاتصالات التي تمت من خلال الكمبيوتر و الشبكة العالمية[1].

ثانيا – الانتقال لمعاينة مسرح الجريمة الإلكترونية: مسرح الجريمة الإلكترونية عبارة عن بيئة غير مادية، فهي عبارة عن بيانات رقمية تمتد إلى مكونات الحاسب الآلي و شبكات الأنترنت، فجهات التحقيق في الجرائم الالكترونية تجد نفسها أمام مسرحين للجريمة فالمسرح الأول هو المكان الذي تتواجد به المكونات المادية للحاسب الآلي و كل الأجهزة المعلوماتية و العتاد المتصل بالتقنيات الحديثة و التي استعان بها المجرم في تنفيذ جريمته، أما المسرح الثاني فهو البيئة الالكترونية و العالم الافتراضي الذي ارتكبت بداخله الجريمة [2]، فالانتقال هنا يكون من خلال الاتصال جهاز الإعلام الآلي أو مكوناته أو الاتصال بشبكات الانترنت من طرف مختصين تحت إشراف سلطات التحقيق، كما قد يتم ذلك من مقر مزودي خدمة الانترنت و تواجه المعاينة مشكلة الامتداد المكاني الذي تمت فيه الجريمة الإلكترونية، بحث قد يستعمل الجاني عدة حواسيب لاقتراف الجريمة و هذه الأخيرة قد تتواجد في مكان واحد و قد تتواجد في عدة أمكنة و بصفة متفرقة، و قد يتواجد أيضا بعضها أو كلها خارج إقليم الدولة[3].

ثالثا– أهمية المعاينة في الجرائم الإلكترونية: يهدف إجراء المعاينة إلى الكشف عن العناصر المادية و الآثار التي تتعلق بالجريمة و تفيد في التحري لبلوغ الحقيقة، و بالنظر إلى الطبيعة الخاصة للجرائم الإلكترونية التي نادرا ما تخلف أثار مادية خلفها تعود إلى الجاني، فان أهمية المعاينة في الجرائم الالكترونية تبدوا ضئيلة و زيادة على ذلك فان تردد الأشخاص على مسرح الجريمة في الفترة الممتدة بين وقت اقتراف الجريمة و وقت العلم بارتكابها و التبليغ عنها قد يؤدي إلى زوال أثار الدليل هذا من دون نسيان إمكانية عبث الجاني بالدليل بعد ارتكابه للجريمة[4].

---

[1] – خالد ممدوح، **فن التحقيق الجنائي في الجرائم الالكترونية**، دار الفكر لجامعي، 2009، ص136.

[2] – بن يحي إسماعيل، **التحقيق الجنائي في الجرائم الالكترونية**، أطروحة لنيل شهادة الدكتوراه علوم، في القانون الخاص، كلية الحقوق، و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان،2022، ص 176.

[3] – هضام محمد فريد رستم، **الجوانب الإجرائية للجرائم المعلوماتية**، مكتبة الآلات الحديثة، أسيوط،1994 ، ص57.

[4] – بن يحي إسماعيل، مرجع سابق ،ص 177.

رابعا- إجراءات المعاينة لمسرح الجريمة الإلكترونية: تتبع سلطات التحقيق لمعاينة مسرح الجريمة الإلكترونية الخطوات الآتية:

1- إبعاد الأشخاص الغير مرخص لهم بالتواجد في مسرح الجريمة و المساس بأي من الأجهزة الإلكترونية.

2- التريث في نقل أي مادة معلوماتية إلى حين التأكد من عدم وجود أي عامل قد يؤدي إلى إتلافها كالمجالات المغناطيسية مثلا.

3- القيام بتصوير شاشة الحاسوب[1].

خامسا - نطاق المعاينة الإلكترونية: يعتمد المحقق الجنائي لإجراء المعاينة الإلكترونية على مجموعة من المصادر في البيئة الإلكترونية التي ارتكبت فيها الجريمة الإلكترونية و المتمثلة عادة في مكونات جهاز الحاسوب الخاصة بالجاني و المجني عليه و ملحقاتها و كذلك أنظمة الاتصال بالأنترنت.

1-معاينة مكونات الحاسب: تعتبر الحواسيب مصدرا غنيا بالأدلة الرقمية خاصة الحواسيب الشخصية، التي يمكن اعتبارها أرشيف لسلوك الأفراد و نشاطاتهم و رغباتهم لذلك إن عملية فحص هذه الحواسيب تمثل نقطة البداية في الكشف عن خفايا الجريمة الإلكترونية باعتبارها وسيلة لتنفيذ الجريمة أو محل وقوعها، و المعروف أن الحاسب الآلي يقوم في تركيبه على ثلاثة عناصر أساسية هي القطع الصلبة " hard ware " و القطع المرنة أو البرمجيات" soft ware" و كذلك المعطيات أو البيانات أو المعلومات " données informatique " و هو العنصر الذي يتوزع بين القطع الصلبة و البرمجيات [2] و تعتمد طريقة الفحص على طريقتين أساسيتين الأولى هي الفحص الذاتي من خلال قيام الحاسب ذاته بفحص مكونات وتقديم تقرير كاملا إلى صاحب الفحص و هذه العملية تتطلب تقنيات و مهارات فنية عالية أما الطريقة الثانية و هي الفحص بواسطة حاسب آخر و أجهزة تقنية عالية للبحث في جزئيات الحاسب.

---

[1] - نبيلة هبة هروال، **الجوانب الإجرائية للجريمة المعلوماتية**،دار الفكر الجامعي، الإسكندرية 2007، ص ص 219-220.

[2] - عمر محمد أبو بكر بن يونس ، مرجع سابق، ص1009.

1- **معالجة أنظمة الاتصال بشبكة الانترنت:** أحيانا لا تكفي معاينة مكونات الحاسب الآلي لاستخلاص الدليل الالكتروني إنما يتطلب من المحقق فحص أنظمة اتصال الحاسب بشبكة الانترنت كذلك، و هي تلك الإجراءات أو التطبيقات المتبعة حال استخدام وسيلة للاتصال بالأنترنت أو ما يعرف ببروتكول الأنترنت و النظام الأمني للشبكات و كذلك فحص الخادم" le serveur "[1].

الفرع الثالث: ضبط الأدلة في الجرائم الإلكترونية

يعتبر هذا الإجراء النتيجة الطبيعية و الحتمية لعملية التفتيش، و يقصد به وضع اليد على الأدلة و كل الآثار و الأشياء المتعلقة بالجريمة، و التي تفيد مجريات التحقيق و تظهر الحقيقة و فك ملابسات و خيوط الجريمة، ليتم وضعها في أحراز مختومة لتقديمها كأدلة الجهات القضائية كدليل إثبات[2] و تحصيل الأدلة الالكترونية قد يرتبط بعناصر مادية كجهاز الحاسوب الآلي وملحقاته و أقراصه الصلبة، و هذه التجهيزات لا يطرح ضبطها أي إشكال قانوني كونها مادية فتخضع إلى إجراءات الضبط و التحريز التقليدية و قد يرتبط الدليل بالمكونات المعنوية للحاسب كمختلف البرامج و البيانات المعالجة آليا و المراسلات و الاتصالات الإلكترونية التي يتم تبادلها عبر شبكة الانترنت و البريد الالكتروني[3].

خولت المادة 19 من الاتفاقية الأوربية لمكافحة جرائم المعلومات لسنة 2001 لسلطات التحقيق طريقتين لضبط البيانات المعلوماتية و الأدلة الرقمية و ذلك في فقرتها الأولى و الثانية فالأولى تتم عن طريق نسخ و تحميل البيانات و المعطيات محل البحث على دعامة تخزين مادية مثل : الأقراص الممغنطة، بطاقات الذاكرة ، فلاش ديسك ..الخ و تكون هذه الأخيرة قابلة للضبط و وضعها في أحراز مختومة حسب ما هو محدد في قواعد تحريز الأدلة التقليدية المنصوص عليها في قوانين الإجراءات الجزائية أما الطريقة

[1] – براهيمي جمال، مرجع سابق، ص 64.

[2] – خالد عياد الحلبي، **إجراءات التحري و التحقيق في جرائم الحاسوب الانترنت**، دار الثقافة للنشر و التوزيع عمان،2011، ص170.

[3] – براهيمي جمال، مرجع سابق، ص47.

الثانية فتتضمن تدابير جديدة مستحدثة خصيصا لضبط الأدلة الجنائية الرقمية و التي تكون باستعمال تدابير الفنية كتقنيات التشفير و الترميز[1].

تبنى المشرع الجزائري من خلال القانون رقم: (09-04) المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها المؤرخ في: 2009/08/05 إجراءات حديثة خاصة بضبط و تحريز المعطيات و البيانات المعلوماتية و غيرها من الأدلة الرقمية بما يتناسب و طبيعتها اللامادية تحت عنوان "حجز المعطيات المعلوماتية"[2]، من خلال المادة 06 و 07 و 08 من القانون السالف الذكر[3].

الفرع الرابع: التفتيش الإلكتروني

يعد تفتيش نظام الحاســـوب من أخطر المراحل باعتباره إجراء يمس بالحق في الخصوصية وحرمة المساكن حيث قيده المشرع بجملة من الشروط و الضمانات.

أولا – تعريف التفتيش: يقصد به "هو إجراء من إجراءات التحقيق التي تهدف إلى ضبط أدلة الجريمة محل التحقيق وكل ما يفيد في كشـف الحقيقة إذ يمس حق المتهم في سـرية حياته الخاصة ويتمثل مجال هذه السرية إما في شخص المتهم أو في المكان الذي يعمل به أو يقيم فيه و فقا لإجراءات قانونية" [4]، ويعرف تفتيش نظام الحاســوب والإنترانت بأنه " البحث في مســتودع ســر المتهم عن أشــياء مادية أو معنوية تفيد في كشــف الحقيقة ونسبها إليه" [5].

ثانيا- كيفية التفتيش الإلكتروني: تتكون نظم الحاســـوب من مكونات مادية وأخرى معنوية كما أنه تربطه بغيره من الحواسيب شبكات اتصال بعدية.

1- تفتيش المكونات المادية للحاسب الآلي: إن الولوج إلى مكونات المادية للحاسـوب الآلي من أجل البحث عن أدلة مادية التي تكشف عن حقيقة الجريمة الإلكترونية و

[1] – براهيمي جمال، مرجع سابق، ص48.

[2] – المرجع نفسه، ص52.

[3] - انظر المادة،06 و 07 من قانون (09-04) المؤرخ في : 2009/08/05، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها، المرجع السابق.

[4] – أمير فرح يوسف، **القبض و التفتيش**، ط1، مكتبة الوفاء القانونية، مصر2013، ص73.

[5] – على حسن محمد الطوالبة، مرجع السابق، ص 12.

مرتكبيها، تخضـــع لإجراءات التفتيش المألوفة لأن حكم التفتيش في هذه الكيانات المادية يتوقف أســـاســـا على طبيعة المكان الموجود فيه، فإذا كانت موجودة في مكان خاص كمسكن المتهم أو احد ملحقاته كان له حكمه بحيث لا يجوز تفتيشها إلا في الحالات التي يجوز فيها تفتيش المســـاكن و ملحقاتها، مع الأخذ باعتبار إذا كانت مكونات الكمبيوتر المراد تفتيشه منعزلة عن أجهزة الكمبيوتر، أم انها تتصل بأجهزة كومبيوتر أخر في مكان أخر كمسكن الغير مسكن، وإذا كانت المكونات المادية للحاسوب متواجدة في أماكن عامة كالحدائق العامة والطرقات وأماكن عامة بالتخصـــيص كمقاهي الأنترنت فإجراء تفتيشها يكون وفقا للأصول الخاصة لتلك الأماكن[1].

2- التفتيش في المكونات المنطقية للحاســـوب ومدى صـــلاحيتها: تعرف على أنها مجموعة من البرامج و الأســـاليب والقواعد والأوامر المتعلقة بتشـــغيل وحدة المعالجة البيانات، بحيث ثار جدل تشريعي وفقهي حول شأن مدى جواز تفتيش المكونات المعنوية أو المنطقية للحاسب تمهيدا لضبط الأدلة الإلكترونية، و التفتيش يعتبر وسيلة للبحث و ضبط الأثار المتعلقة بالجريمة و تقديمها للمحكمة كدليل الإدانة، مما أثار جدل حول إمكانية البحث عن أدلة الجريمة الإلكترونية في نظم وبرامج الحاسب نوعا من التفتيش كون البيانات الإلكترونية و البرامج نجدها تفتقد المظهر المادي المحســـوس في المحيط الخارجي و نظرا إلى غياب الطبيعة المادية للمعلومات و البيانات وهذا الأمر يجعلها تتعارض مع هدفها الذي ينصب فيه هو البحث عن الأدلة المادية[2].

ثالثا- التفتيش في شبكات الحاسوب (التفتيش عن بعد): إن الشبكة المعلوماتية يقصد بها اتصال جهازين أو أكثر من أجهزة الحاسب الألي اتصالا سلكيا أو لاسلكيا وتكون هذه الأجهزة مرتبطة ببعضها البعض في موقع واحد فيطلق عليها بالشبكة المحلية، أو إذا كانت موزعة على عدة أماكن متفرقة يتم ربطها عن طريق خطوط الهاتف فيطلق عليها بالشبكة الأنترنت[3]، وهنا يكون الموقع الفعلي للبيانات داخل اختصاص قضائي أخر وفي بلد أخر مما تثار مشكلة الاختصاص القضائي، وأثر تفتيش الأنظمة المتصلة بالنظام

---

[1]- ابراهيمي جمال، مرجع السابق، ص 16.

[2]- احمد ضياء الدين محمد خليل، **مشروعية الدليل في المواد الجنائية**، رسالة لنيل الدكتوراه في القانون، كلية حقوق جامعة عين الشمس، القاهرة، ص 374.

[1]- براهيمي جمال ، مرجع السابق ، ص 21 .

المأذون تفتيشه إذا وجدت في دوائر اختصاص مختلفة، مما تتصور هنا حالتين مختلفين هما:

الحالة الأولى: اتصال حاسب المتهم بحاسب ألي أخر أو منظومة معلوماتية متواجدة في موقع أخر داخل إقليم الدولة نفسها:

إن هذه الفرضية تتحقق عندما يقوم المتهم بتحويل عبر الأنترنت معلومات أو بيانات متعلقة بجريمة إلكترونية من حاسوبه إلى حاسوب أخر أو إلى منظومة معلوماتية ملك للغير وتخزينه فيها، وفي هذه الحالة تقع على سلطات التحقيق تجاوز الاختصاص المكاني والاعتداء على حرمة خصوصية غيره، لهذا السبب عمدت بعض التشريعات الإجرائية إلى تنظيم هذه المشكلة بنص صريح حول إمكانية امتداد التفتيش ليشمل أجهزة الحاسب أو أية منظومة معلوماتية مرتبطة بحاسوب المتهم الجاري تفتيشه من أجل إثبات الجريمة دون التقييد بالحصول على إذن مسبق من السلطات القضائية المختصة بخصوص هذا الامتداد[1].

الحالة الثانية: اتصال حاسب المتهم بحاسب أخر أو منظومة معلوماتية متواجدة في إقليم دولة أجنبية: من بين المشاكل التي تواجهها سلطات التحقيق في جمع الأدلة الإلكترونية عند قيام مرتكبي الجريمة بتخزين بياناتهم في أنظمة تقنية خارج الدولة مستخدمي في تلك شبكة الاتصال البعدية بهدف عرقلة التحقيق و سير العدالة ونتيجة لذلك فإن امتداد التفتيش على الأنظمة حتى ولو كانت متواجدة خارج الإقليم، القانون الفرنسي يجيز هذا الفعل من خلال المادة 1/57 من القانون الإجراءات الجزائية لضابط الشرطة القضائية أن يقوم بتفتيش الأنظمة المعلوماتية المتصلة المتواجدة خارج الإقليم الوطني[2].

رابعا- شروط التفتيش الالكتروني: يعتبر التفتيش من الإجراءات التي تمس بالحرية الشخصية للأفراد وبحرمة حياتهم الخاصة و نجد معظم التشريعات تقيده بشروط وتنقسم هذه الشروط التفتيش إلى قسمين شروط موضوعية وشروط شكلية.

---

[1]- طرشي نورة، **مكافحة الجريمة المعلوماتية**، مذكرة لنيل شهادة الماجيستر في قانون، فرع القانون الجنائي، كلية الحقوق، جامعة الجزائر 1، 2011، ص110.

[2]- عائشة بن قارة مصطفى ، مرجع السابق ،ص 59.

1- الشروط الموضوعية للتفتيش: ويقصد بها تلك الضوابط التي لابد من توفرها ليكون تفتيش صحيح ونلخص هذه الشروط في السبب والسلطة المختصة بالتفتيش ومحل التفتيش.

أ-**سبب التفتيش:** إن السبب الأساسي والمبرر للتفتيش هو الحصول على دليل مادي يفيد جهات التحقيق من اجل الحصول على الحقيقة، ويتحقق بوقوع جريمة ما أو جناية أو جنحة يتم بموجبها توجيه اتهام شخص المراد تفتيشه بناء على أدلة أو براهين أو توفر قرائن قوية تفيد في كشف الحقيقة لدى المتهم أو في مسكنه و هو ما ينطبق على الجريمة الإلكترونية إلا بتوفر العناصر التالية:

- وقوع جريمة الإلكترونية تحمل وصف الجناية أو جنحة.

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

ب- محل التفتيش: وهي تخص نظم الحاسوب بكل مكوناته المادية والمعنوية بالإضافة إلى شبكات الاتصال الخاصة به و الأشخاص الذين يستعملون الحاسوب محل التفتيش.

01- مكونات مادية من وحدة الإدخال ووحدة الذاكرة الرئيسية ووحدة الحاسوب والمنطق و وحدة الإخراج و التخزين الثانوية.

02-مكونات معنوية تتمثل في برامج النظام و الكيانات المنطقية التطبيقية أو برامج التطبيقات طبقا للاحتياجات العميل، بحيث كل هذه المكونات تستوجب عدة أشخاص لديهم الخبرة ومهارة في تقنية نظم المعلوماتية [2].

ج-السلطة المختصة بالتفتيش: لكي يكون التفتيش في الجرائم الإلكترونية صحيح لابد أن يتم من طرف سلطات التحقيق الأصلية، وهذا مع مراعاة الاختصاص المحلي للجريمة وكاستثناء يجوز تفويض هذا الأمر إلى أحد أعضاء الضبطية القضائية، وفق للشروط المنصوص عليها في القانون، ويكون التفتيش بالحصول على إذن مسبق صادر عن هيئة مختصة، ليكون لضابط الشرطة القضائية الحق في التفتيش كل الأجهزة

[1]- عائشة بن قارة مصطفى، مرجع السابق، ص 62.

[2] بكري يوسف بكري، مرجع السابق، ص 80-81

الالكترونية ومختلف لواحقها الموجودة في المسكن، وكذا الملفات والبيانات التي تتواجد في تلك الأجهزة وحجتهم أن الأجهزة الالكترونية تحمل سعة تخزين هائلة من الملفات والمعلومات، لذلك لا يمكن إصدار إذن بالتفتيش على حساب عدد الملفات التي تحتويها وهي تعمل على تمديد التفتيش عن بعد على جناح السرعة إلى أية منظومة معلوماتية أخرى مرتبطة بها بموجب إذن واحد[1].

د-تحرير محضر التفتيش: التفتيش يشترط أن يحرر محضر التفتيش الذي يدون فيه كل الخطوات والإجراءات المتخذة أثناء عملية التفتيش، بحيث محضر التفتيش لا يتقيد بشكل وشروط خاصة بل يكتفي بالكتابة باللغة الرسمية، تاريخ تحريره، توقيع محرره والشرط الأساسي الذي يجب التقييد به هو الاستعانة بكاتب يتم اصطحابه لتحرير المحضر وتدوين مجريات التفتيش، وهذا حسب نص المادة 02/68 من قانون إجراءات الجزائية الجزائري، و محضر التفتيش في مجال الجريمة الالكترونية لا يختلف عن غيره من المحاضر التقليدية، سوى أن يكون المحضر محاط بتقنية المعلوماتية الرقمية في الجرائم الإلكترونية وكذا الاستعانة بأهل الخبرة والاختصاص من أجل المساعدة في الصيانة السليمة لمسودة محضر التفتيش[2].

هـ-الشروط الشكلية للتفتيش الالكتروني: يجب احترامها من أجل ضمان صحة إجراءات التفتيش وهي ثلاثة شروط ندرسها كتالي:

أ- وقت إجراء التفتيش: لابد من تحديد الميعاد الزمني او الفترة الزمنية التي يتم فيها التفتيش وذلك صونا لحرية الأفراد وحرمة مسكنهم، لقد اختلفت التشريعات حول تحديد وقت معين لإجراء التفتيش مثل المشرع المصري والعراقي نجده لم يحدد الوقت الزمني للتفتيش والمشرع القطري أجاز التفتيش نهارا وليلا كحالة استثنائية أي إلا إذا كانت الجريمة متلبس بها، أما المشرع الفرنسي حدد وقت التفتيش بين السادسة صباحا والتاسعة ليلا و المشرع الجزائري حدد وقت إجراء التفتيش بين الخامسة صباحا و الثامنة ليلا حسب المادة 47 من قانون الإجراءات الجزائية [3]، وكاستثناء أجاز فيها الخروج عن

---

[1]- ابراهيمي جمال، مرجع السابق، ص 39.

[2]- يحي بن اسماعيل ، مرجع السابق ، ص 207.

[3]- يحي بن إسماعيل، مرجع سابق، ص 209.

الميقات ليصـــبح إجراء التفتيش في أية وقت ليلا و نهارا هذا عندما يتعلق بالجرائم منصـــوص عليها في المواد 342الى غاية 348 من قانون العقوبات، وهذا راجع لتفطن المشرع لطبيعة هذه الجرائم كون أدلة إثبات غير مرئية و سهلة إتلاف[1].

ب-إجراء التفتيش يكون بحضـــور المتهم أو من ينوب عنه: لا يكون التفتيش إلا بحضور المتهم أو من يقوم مقامه أو من ينوب عنه كونه شرط ضروري يفرضه القانون لصـحة إجراء التفتيش أو شـاهدين من غير المعنيين بالتحقيق [2]، بينما المشـرع الجزائري يقضـي لإجراء التفتيش بحضـور المشتبه به أو من يمثله ولم يشترط حضـور الشـهود إلا في حالة تعذر حضور هؤلاء حسب المادة 01/45 من قانون الإجراءات الجزائية.

الفرع الخامس: الخبرة التقنية في المجال الإلكتروني

إن التطور المذهل الذي تعرفه الجريمة الإلكترونية اليوم، جعل الاستعانة بأهل الخبرة أمر ضروريا حتى تتمكن سلطات التحقيق مواصلة البحث و التحري من أجل اكتشاف الحقيقة و معرفة ملابسات و خيوط الجريمة، يتطلب الاستعانة بالخبراء نظرا لحداثتها و التقنية العالية التي تتطلبها في مجال الإعلام الآلي و الرقمنة.

أولا- تعريف الخبرة التقنية: يقصد بالخبرة لغة العلم بالشيء و معرفته على حقيقته[3]، أما اصطلاحا يقصد بها البعض، البصيرة والمعرفة، فالخبرة القضائية هي إجراء يهدف الاستعانة بالقدرات الفنية أو العلمية لشخص الخبير و التي لا تتوفر لدى رجال القضاء و المحققين لاستخلاص دليل يفيد في معرفة الحقيقة بشان جريمة وقعت أو نسبتها إلى المتهم أو تسمح بتحديد ملامح شخصيته الإجرامية [4] ويعرفها البعض الأخر بالاستشارة الفنية التي ستعين القاضي أو المحقق و مساعدته في تكوين عقيدته في المسائل التي يحتاج تقديرها إلى معرفة و دراية علمية خاصة لا تتوفر لدى القاضي أو المحقق[5].

---

[1]- براهيمي جمال، مرجع سابق، ص ص 41-42.

[2]- براهيمي جمال، مرجع نفسه، ص 43.

[3] - انظر ابن منظور، لسان العرب، الطبعة الثالثة، الجزء الرابع دار إحياء التراث العربي، بيروت لبنان،1999 ص12.

[4] - احمد شوقي الشلقاني، **مبادئ الإجراءات الجزائية في التشريع الجزائري** ،الجزء الثاني، ديوان المطبوعات الجامعية الجزائر، 1999،ص259.

[5] - عمار عباس الحسيني، **التحقيق الجنائي و الوسائل الحديثة في كشف الجريمة**، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان،2015، ص184.

ثانيا –أهمية الخبرة القضائية: إن الواقع العملي و حاجة سلطات التحقيق إلى الخبراء الفنيين، خاصة في مجال مكافحة الجريمة الإلكترونية و نظرا لخصوصيتها و طبيعتها الغير مادية و البيئة الافتراضية التي يتم بداخلها ارتكاب الجريمة يفرض على سلطات التحقيق الاستعانة و ندب خبراء في مجال المعلوماتية و التقنيات الحديثة للوصول إلى الحقيقة[1].

ثالثا– إجراءات الخبرة في مجال الجريمة الإلكترونية: تنظمن الخبرة عدة إجراءات يقوم بها الخبير و سنذكر من خلال هذه النقطة إلى أبرز الخطوات و المراحل التي تمر بها إجراءات الخبرة و تتمثل فيما يلي:

– مرحلة ما قبل التشغيل و الفحص يتم من خلالها إحصاء و جرد المكونات التي تم ضبطها.

– مرحلة التشغيل و الفحص يتم من خلالها نسخ البيانات الموجودة و إظهار التي تم إخفائها و استرجاع ما تم محوه.

– مرحلة تحديد الارتباط بين الدليل المادي و الدليل الإلكتروني.

– مرحلة تدوين النتائج التي تم التوصل إليها الخبير لإعداد تقرير الخبرة بخصوص المهام التي أسندت إليه عند تسخيره و تكليفه بالمهمة[2].

الخبير المعلوماتي و أثناء إجراء الخبرة التي أسندت إليه في مجال الجريمة الإلكترونية قد يستعين بعدة برمجيات كتلك التي تسمح له بنسخ البيانات الموجودة بالحاسب الآلي للمتهم الإلكتروني أو الضحية أو الشبكة المعلوماتية، فهناك عدة أدوات تساهم في عمل الخبير مثل برنامج معالجة الملفات "x tree pro gold" و برنامج "lap link" للنسخ و برامح الاتصال مثل "lantastic"[3].

---

[1] – بن يحي إسماعيل، المرجع السابق، ص216.

[2] – بن يحي إسماعيل، مرجع نفسه، ص16.

[3] – ممدوح عبد الحليم عبد المطلب، **البحث و التحقيق الجنائي الرقمي جرائم الكمبيوتر و الانترنت**، دار الكتب القانونية، 2006، ص62.

رابعا- الضوابط القانونية و الفنية للخبرة الإلكترونية: تخضع الخبرة الإلكترونية باعتبارها إجراء من إجراءات التحقيق إلى جملة من الضوابط القانونية و الفنية، هذا ما سنتم التطرق إليه كالاتي:

1-الجوانب القانونية للخبرة الإلكترونية: نظرا للأهمية التي تلعبها الخبرة الإلكترونية في مجال الإثبات الجنائي حرصت معظم التشريعات على تنظيمها و إحاطتها بمجموعة من الضوابط لكي تكون لديها حجية أمام القضاء.

أ- **اختيار الخبير من جل الخبراء:** هي جداول تعدها المجالس القضائية بعد استطلاع رأي النيابة العامة، لكن يجوز استثناءا لسلطات التحقيق أن تختار بقرار مسبب خبراء خارج الجدول في حالة عدم توفر الخبرة المطلوبة[1].

ب - **أداء اليمين القانونية :** اتفقت كل تشريعات العالم على ضرورة أداء اليمين القانونية من طرف الخبراء المنتدبين و إلا كان عملهم باطلا هذا ما حدده المشرع الجزائري من خلال المادة 145 من قانون الإجراءات الجزائية[2].

2- الجوانب الفنية للخبرة الإلكترونية: من اللازم على الخبير اعتماد تقنيات و مهارات علمية و الاستعانة بوسائل تكنولوجية متطورة، حيث وضعت بعض الدول التقنيات الأساسية التي على الخبير الإلكتروني إتباعها لجمع الأدلة الرقمية و فحصها كتحديد الوسائل العلمية اللازمة لإنجاز الخبرة العلمية ليعتمد عليها الخبير في شرح و تحليل ملابسات الجريمة[3] و استخلاص الدليل الإلكتروني، كالاعتماد على أدوات فنية تستخدم في بنية النظام المعلوماتي مثلا بروتوكول الانترنت (IP) أو ما يسمى بالعنوان الالكتروني، حيث يمكن للخبير الالكتروني إتباع المسار التراسل لمعرفة الجهاز المستعمل في ارتكاب الجريمة و تحديد موقعه و منه التعرف على الجاني[4]، كما يعتمد الخبراء أيضا على أنظمة أخرى على غرار أنظمة البروكسي(proxy) الذي يضمن توفير خدمات الذاكرة الجاهزة، و يشتغل هذا النظام كوسيط بين شبكة الأنترنت و مستخدميها و كذلك برنامج (trace route) الذي يحدد بدقة

---

[1] - انظر المادة 144 من قانون الإجراءات الجزائية الجزائري.

[2] - انظر المادة 145 من قانون الإجراءات الجزائية الجزائري.

[3] - براهيمي جمال ، الرجع السابق، ص78.

[4] - سليمان بن مهجع العنزي، **وسائل التحقيق في جرائم نظم المعلومات**، رسالة لنيل درجة ماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض،2003، ص 98.

الأجهزة الإلكترونية التي اشتركت في نقل البيانات على الأنترنت كما يمكن لهذا البرنامج أن يستدعي و يحيط بالملفات التي تم الولوج إليها و كافة عمليات الاختراق و العبور التي تم من خلالها الإعداد للجريمة[1].

المطلب الثاني: الإجراءات الخاصة أو المستحدثة للتحقيق في الجرائم الإلكترونية

بعد تطرقنا إلى الطرق التقليدية لإجراءات التحقيق في الجرائم الإلكترونية لاستخلاص الدليل الإلكتروني في المطلب الأول، اتضح لنا أن سلطات التحقيق أصبحت عاجزة على مواجهة هذا النوع من الجرائم، و قصور الإجراءات التقليدية أمام التطور التكنولوجي الشيء ما ألزم المشرع الجنائي في العديد من الدول بالعمل على إيجاد أساليب و طرق بإمكانها دعم سلطات التحقيق، ذلك باستحداث إجراءات جديدة بإمكانها مواكبة التطور الذي تعرفه الجريمة الإلكترونية، هذا ما سنتناوله من خلال هذا المطلب بشيء من التفصيل بتقسيمه بدوره إلى خمسة فروع.

الفرع الأول: التسرب الإلكتروني

يعد التسرب من بين أهم إجراءات التحقيق الجديدة والمستحدثة و سنتناول من خلال هذا الفرع تعريف التسرب و شروطه و كيفية الاستعانة به في مجال الجرائم الالكترونية.

أولا- تعريف التسرب و صوره:

1- تعريف التسرب: تناول المشرع الجزائري موضوع التسرب من خلال المواد 65 مكرر 11 إلى 65 مكرر 18 من قانون الإجراءات الجزائية، حيث عرفه في المادة 65 مكرر 12، على انه يقصد بالتسرب قيام ضباط أو أعوان الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه فيهم في ارتكابهم جناية بإيهامهم أنه فاعل معهم أو شريك أو خاف، كما أكد المشرع الجزائري في المادة 65 مكرر 11 من قانون الإجراءات الجزائية على شرعية اللجوء إلى إجراء التسرب في الجرائم المنصوص عليها في المادة 65 مكرر 05[2]، و من بين هذه الجرائم جريمة

[1] - ممدوح عبد الحليم عبد المطلب ، المرجع السابق، ص ص15-16.

[2] - القانون (06-22) المؤرخ في 2006/12/20،الصادر في الجريدة الرسمية العدد 84 المؤرخ في:2006/12/24 المعدل و المتمم بالامر رقم(66-15) المؤرخة في 1966/06/08 المتضمن قانون الإجراءات الجزائية.

المساس بأنظمة المعالجة الآلية للمعطيات و بناءا على هذا التعريف يظهر لنا أن التسرب عملية جد معقدة، حيث أن المشرع الجزائري أعفى العون أو ضابط الشرطة القضائية المتسرب من المسؤولية الجزائية على كل الأفعال الغير مشروعة التي يقوم بها طوال العملية بالتالي المشاركة في تشكيل الخلية الإجرامية[1].

كما أحاط المتسرب بعدة ضمانات لحمايته و حماية أسرته أثناء القيام بعملية التسرب حيث نصت المادة 65 مكرر 16 من قانون الإجراءات الجزائية "..لا يجوز إظهار الهوية الحقيقية لضابط أو عون الشرطة القضائية المتسرب بل تتم تحت هوية مستعارة طيلة مراحل القيام بهذا الإجراء .."[2].

2- صور التسرب:

يتم الترب كإجراء من الإجراءات المستحدثة لجمع الأدلة في ثلاثة صور بحث يتخذ أعوان و ضباط الشرطة القضائية في عملية التسرب ثلاثة أشكال حسب نص المادة 65 مكرر12 و هي إما أن يكون فاعل أصلي أو شريك أو خاف.

أ- **المتسرب كفاعل أصلي:** يكون المتسرب في هذه الحالة دور مباشر في القيام بالعمل الإجرامي لجريمة محل عملية التسرب، بغرض إيهام المجرمين بحيث يكون فاعلا ماديا ذلك بالقيام بالأفعال المنصوص عليها في المادة 65 مكرر14 و هي اقتناء و حيازة او نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها، أو استعمال أو وضع تحت تصرف مرتكبي الجريمة الوسائل ذات الطابع القانوني و المالي وكذلك وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال[3].

ب-**المتسرب كشريك:** يكون المتسرب في هذه الحالة دور غير مباشر في القيام بالعمل الإجرامي للجريمة محل عملية التسرب يعتبر شريكا في الجريمة و يساعد الفاعلين على ارتكاب الأفعال التحضيرية أو المسهلة لارتكاب الجريمة مع علمه بذلك أي علمه بالسلوك

---

[1] – القانون (06-22) الؤرخ في 2006/12/20 المتضمن قانون الإجراءات الجزائية، مرجع نفسه.

[2] – انظر المادة 56 مكرر 14 من قانون الإجراءات الجزائية الجزائري، مرجع نفسه.

[3] – نصت المادة 65 مكرر 16على عقوبة تصل 20 سنة حبسا و غرامة 1 مليون دينار على من كشف هوية المتسرب أو احد أفراد أسرته حسب الضرر الذي يسببه الكشف .

الإجرامي فيعتبر شريكا طبقا لأحكام المادة 42 و43 من قانون العقوبات بالتالي فالمتسرب يأخذ أحكام الشريك إذا ارتكب الأفعال المنصوص عليها في المادة 65 مكرر 14 من قانون الإجراءات الجزائية[1].

ج – **المتسرب كخاف:** يقوم المتسرب في هذه الحالة بإيهام المجرمين بأنه واحد منهم للإيقاع بهم، ذلة من خلال إخفائه للعائدات الإجرامية التي يكون مصدرها الجريمة بشكل كلي أو جزئي و هذه الجرائم تم النص عليها في المادة 65 مكرر 05 من قانون الإجراءات الجزائية.

ثانيا– شروط مباشرة عملية التسرب: باعتبار أن عملية التسرب إجراء أو أسلوب من أساليب التحري الخاصة التي تمس بالحريات الخاصة للأفراد و خصوصيتهم فقام المشرع الجزائري بتقييدها بجملة من الشروط نظرا للخطورة التي يشكلها هذا الإجراء على حرمة الحياة الخاصة و هي كالاتي:

1– الشروط والضوابط الإجرائية: فتتمثل في الإذن القضائي و كل ما يجب أن يتضمنه من شروط و أحكام فلا يمكن لضباط و أعوان الشرطة القضائية القيام بعملية التسرب من دون إذن مسبق من طرف الجهات القضائية المختصة، فيقوم بإصدار هذا الإذن السيد وكيل الجمهورية ذلك قبل افتتاح التحقيق أو قاضي التحقيق بعد افتتاح التحقيق على أن تتم العملية تحت الرقابة المباشرة للسلطة الصادرة للإذن لتفادي وقوع أي تجاوزات حفاظا على الحريات الفردية للأشخاص، كما يجب أن يكزن الإذن مكتوبا و إلا كان إجراء التسرب باطلا لأن الأصل في العمل الإجرائي الكتابة حسب ما نصت عليه المادة 65 مكرر15 من قانون الإجراءات الجزائية "..يجب أن يكون الإذن مكتوبا تحت طائلة البطلان.."[2].

و يشترط أيضا أن يتضمن الإذن جملة من البيانات تقوم عليها صحة الإجراء كتحديد نوع الجريمة محل التسرب، اسم ضابط الشرطة القضائية الذي تتم العملية تحت مسؤوليته كذلك تحديد المدة المطلوبة لهذه العملية، و التي لا يجب أن تتجاوز الأربعة04 أشهر قابلة

[1] انظر المادة 65 مكرر 14 من قانون الإجراءات الجزائية الجزائري.

[2] – تنص المادة 65 مكرر 11 من قانون الإجراءات الجزائية على انه "..يجوز لوكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته حسب الحالة مباشرة عملية التسرب.."

للتجديد حسب متطلبات و مقتضيات التحقيق حيث يجوز في أي وقت للسلطة مصدرة الإذن حسب الحالة أن توقف هذا الإذن حتى قبل انقضاء الآجال المحددة[1].

2-**الشروط و الضوابط الموضوعية:** حدد المشرع الجزائري ضوابط و شروط موضوعية يمكن اختصارها في عنصرين هامين:

ا- **التسبيب** : تضمنته المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري و يتمثل في الدوافع و المبررات و الحجج التي تم التأسيس عليها طلب سلطات التحقيق للجهات القضائية لمنحها الإذن للقيام بعملية التسرب فعلى ضابط الشرطة القضائية ان يحدد الأسباب ضمن طلب الإذن[2].

ب- **تحديد نوع الجريمة محل عملية التسرب:** حيث لا يجب أن تخرج عن الجرائم التي حددتها المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري على سبيل الحصر فيظهر لنا من خلال هذه المادة أن الجرائم التي خصها المشرع بإجراء عملية التسرب هي جرائم خطيرة جدا نظرا لسرعة انتشارها و امتداد تداعياتها خارج الحدود الوطنية فهي تقوم على التخطيط و تسخير كل الوسائل لمحو أثار الجريمة و طمس معالمها[3].

الفرع الثاني: اعتراض المراسلات و المراقبة الإلكترونية

أقر المشرع الجزائري على إجراء اعتراض المراسلات و تسجيل الأصوات و التقاط الصور للتحقيق في الجرائم الإلكترونية، ذلك بموجب قانون (06-22) المؤرخ في 2006/09/20 المتضمن قانون الإجراءات الجزائية المعدل و المتمم ثم قام بتعزيز هذا الإجراء بقانون (09-04) المؤرخ في 2009/05/05، حيث حذا المشرع الجزائري حذو التشريعات الأوربية التي أوصت من خلال الاتفاقية الأوربية حول الجرائم الإلكترونية لعام

---

[1]- انظر المادة 65 مكرر 15 من قانون الإجراءات الجزائية الجزائري.

[2]- علاوة هوام، **التسرب كآلية للكشف عن الجرائم في القانون الجزائري**، مجلة الفقه و القانون، كلية الحقوق و العلوم السياسية، جامعة الجاج لخضر بباتنة:2012، ص 03.

[3] - زورو هدى، **التسرب كأسلوب من أساليب التحري في قانون الإجراءات الجزائية الجزائري**، مجلة دفاتر السياسة و القانون، العدد 11،كلية الحقوق و العلوم السياسية، جامعة محمد خيضر، بسكرة،1014،ص 121.

2001 بتبني إجراء اعتراض المراسلات و المراقبة الإلكترونية للاتصالات في تشريعاتها الداخلية ضمن إجراءات البحث و الحقيق في الجرائم الإلكترونية[1].

أولا – تعريف اعتراض المراسلات و المراقبة الإلكترونية: عرف المشرع الجزائري عملية اعتراض المراسلات من خلال المادة 65 مكرر 05 من قانون الإجراءات الجزائية الجزائري كالاتي: "..اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية أو اللاسلكية و هذه المراسلات هي عبارة عن بيانات قابلة للإنتاج، و التوزيع و التخزين و الاستقبال و العرض.."، فيظهر من خلال هذا التعريف أن المشرع الجزائري حدد المراسلات التي يمكن أن تكون محلا للاعتراض و هي المراسلات التي تتم بواسطة وسائل الاتصال السلكية واللاسلكية من دون أن يحدد طبيعة هذه المراسلات[2]، أي الوسائل المكتوبة بغض النظر عن شكلها أو الدعامة التي تنصب عليها أو الوسيلة المستعملة في إرسالها، كما أن القانون (09-04) عرف الاتصالات الالكترونية في المادة 02 بأنها أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو معلومات مختلفة بواسطة أي وسيلة إلكترونية، و بغض النظر عن المراسلات فان عملية الاعتراض و المراقبة تتم بواسطة ترتيبات تقنية سرية يتم وضعها دون موافقة المعنيين لغرض التصنت و التقاط و تثبيت و بث و تسجيل البيانات المرسلة أو المحادثات التي أجراها المشتبه فيه بصيغة خاصة أو سرية في أماكن عامة أو خاصة ومن ثم استعمالها كدليل لمواجهة المتهم[3].

من خلال الاطلاع على المادة 04 من قانون (09-04) يظهر لنا أن المشرع الجزائري أعطى تسريحا إلى سلطات التحقيق لاستعمال عملية مراقبة الاتصالات الإلكترونية كإجراء وقائي استباقي حيث أن مجرد احتمال وقوع أو اكتشاف جريمة متصلة بتكنولوجيا الإعلام و الإتصال و يحتمل أن تشكل خطرا على أمن الدولة كالأفعال الموصوفة بجرائم

---

[1] – براهيمي جمال، **التحقيق الجنائي في الجرائم الالكترونية**، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق جامعة مولود معمري، تيزي وزو، 2018، ص88.

[2] Benoir abdelhakim , les techniques spécial d'enquêtes et d investigations , article publier sur : www.memoireonline,2000-2013, pp 2-3.

[3] – ربيحة زيدان ، **الجريمة المعلوماتية في التشريع الجزائري و الدولي**، دار الهدى ، الجزائر،2011،ص 157.

الإرهاب و التخريب و جرائم الإعتداء على المنظومة المعلوماتية على نحو بهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة.

ثانيا- القيود و الضوابط التي تنظم عملية إعتراض و مراقبة المراسلات: تتم هذه العملية دون علم الأشخاص المشتبه فيهم، حيث أثبتت نجاعتها من الناحية العملية في الكشف المسبق و الوقاية من الكثير من الجرائم الإلكترونية، إلا انه يبقى إستثناء و إجراء يمس بحرية الأفراد و حياتهم الشخصية التي يكفلها الدستور[1]، فاللجوء إلى هذا الإجراء تفرضه المصلحة العامة بالتالي أحاطه المشرع بمجموعة من القيود القانونية التي تضمن عدم التعسف السلطات المحققة و تتمثل فيما يلي:

1-الحصول على إذن السلطات القضائية المختصة: قيد المشرع هذه العملية بشرط الحصول على الإذن المسبق من الجهات القضائية، و يكون هذا الإذن مكتوبا و مسببا و يمنح هذا الإذن عادة من طرف السيد وكيل الجمهورية أثناء مرحلة التحقيق و استثناءا يمنح من طرف النائب العام لمجلس قضاء الجزائر إذا تعلق الأمر بالوقاية من أفعال إرهابية أو التخريب أو الجرائم الماسة بأمن الدولة، أو قاضي التحقيق في مرحلة التحقيق القضائي[2] فالسلطة القضائية هي المختصة بإصدار هذا الإذن و يعتبر هذا ضمانة لازمة لمشروعية هذه العملية و حتى يكون هذا الإذن صحيحا يجب أن يتضمن مجموعة من العناصر الأساسية و تتمثل في ما يلي:

- **نوع الجريمة التي تبرر هذا الإجراء:** يجب أن يكون ضمن الجرائم المحددة التي يجوز فيها اللجوء إلى عملية الإعتراض و المراقبة الإلكترونية[3].

- **التعريف بالعملية:** أي تحديد المراسلات و الإتصالات المراد اعتراضها و تسجيلها و الأماكن المقصودة، إلى جانب تحديد المدة التي تستغرقها التدابير التقنية اللازمة في عملية الإعتراض و التي يجب أن لا تتجاوز 04 أشهر قابلة للتجديد حسب تقدير السلطة القضائية مصدرة الإذن و مقتضيات التحقيق و التحري، و لا يكفي الحصول على إذن بالشروط المذكورة أعلاه للشروع في عملية إعتراض المراسلات و المراقبة بل يجب أن تنفذ هذه

[1] – انظر المادة 02/46 من الدستور الجزائري لسنة 2016، التي تنص على "..سرية المراسلات و الاتصالات الخاصة بكل أشكالها مضمونة..".

[2] – انظر الفقرتين 6 و 7 من المادة 04 من القانون (09-04)، مرجع سابق .

[3] – انظر المادة 65 مكرر 05 من قانون الإجراءات الجزائية و المادة 04من قانون(09-04) .

العملية تحت الرقابة المباشرة للسلطات التي أذنت بها ذلك بان يقوم ضابط الشرطة القضائية بإحاطتها علما بكل الخطوات و تطورات العملية بشكل دوري و مستمر و تدوين ساعة بداية و نهاية هذه العملية على محاضر مرقمة[1].

ثانيا- تسبيب اللجوء إلى إجراء إعتراض أو مراقبة المراسلات الإلكترونية: و هو المبرر الشرعي و الضرورة التي إستدعت اللجوء إلى هذا الإجراء و الضرورة تتحقق عند استحالة الوصول إلى نتيجة تهم مجريات التحقيق و التحري دون اللجوء إلى هذه العملية لإظهار الحقيقة و الكشف عن الجريمة و الجناة مسبقا و لوكيل الجمهورية أو قاضي التحقيق تقدير جدوى و جدية و دواعي القيام بهذا الإجراء.

ثالثا- تحديد الجرائم محل الإعتراض: إن اللجوء إلى عملية الإعتراض و مراقبة المراسلات الإلكترونية يتوقف عند نوع محدد من الجرائم و هي كالأتي :

- الجرائم المذكورة على سبيل الحصر في نص المادة 65 مكرر05 من قانون الإجراءات الجزائية الجزائري و تتمثل في جرائم المخدرات، الجريمة المنظمة العابرة للحدود الوطنية جرائم تبييض الأموال و الإرهاب، الجرائم المتعلقة بالتشريع الخاص بالصرف، جرائم الفساد، و الجرائم الماسة بالمعالجة الآلية للمعطيات[2].
- الجرائم المنصوص عليها في المادة 04 الفقرات: ا، ب، ج، دمن القانون (09-04) و تتمثل في الأفعال الموصوفة بجرائم الإرهاب و التخريب و الاعتداء على المنظومة المعلوماتية الماسة بأمن الدولة و تلك التي تهدد النظام العام و الدفاع الوطني أو مؤسسات الدولة أو الإقتصاد الوطني[3]، ويظهر أن المشرع فتح المجال لجميع جرائم القانون العام لتكون محلا للمراقبة الإلكترونية.

رابعا- سرية الإجراء وكتمان السر المهني: يجب أن تتم عملية الإعتراض و المراقبة الإلكترونية في سرية تامة دون علم أو رضا المشتبه فيه أو صاحب الأماكن مع الإحتفاظ بالسر المهني[4]، ولم يحدد المشرع الجزائري كيفية وضع الأدلة المحصلة من إعتراض

---

[1] – براهيمي جمال، المرجع السابق،ص95.

[2] – انظر المادة 65 مكرر من قانون الإجراءات الجزائية.

[3] – انظر المادة 04/45 من قانون الإجراءات الجزائية الجزائري.

[4] – انظر المادة 04/45 من قنون الإجراءات الجزائية الجزائري.

المراسلات في أحراز مختومة علما انه تعتبر أدلة إثبات رقمية أصلية وجب حفظها بطريقة خاصة و ضعها في أحراز مختومة تضمن عدم التلاعب و العبث بها بالحذف و الإضافة و ضمها إلى ملف الإجراءات مع المحاضر.

الفرع الثالث: الحفظ و الإفشاء العاجلان للمعطيات المتعلقة بالسير

يعتبر من بين الإجراءات الحديثة التي كرسها المشرع لجمع الدليل الإلكتروني، في مجال مكافحة الجريمة الإلكترونية و تمت الإشارة إلى هذا الإجراء لأول مرة في لائحة الجمعية العامة لمنضمة الأمم المتحدة رقم : (65-63) المؤرخة في 2001/01/22 المتعلقة بمكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، حيث نصت المادة 01 على ضرورة سماح الدول الأعضاء المختصة بالإستدلال بأمر مزودي خدمات الإتصال بالقيام بالحفظ السريع للمعطيات الإلكترونية، المتعلقة بالتحقيقات الجنائية وتضمنت اتفاقية بودابست لمكافحة الجرائم الإلكترونية لعام 2001 إجرائي الحفظ و الإفشاء على البيانات المخزنة في نضم المعلوماتية، التي تراها ضرورية من أجل السماح للسلطات المختصة بان تأمر بالحفظ و الإفشاء العجلان على كل المعطيات المعلوماتية المخزنة[1]، هذا ما سنتطرق إليه من خلال هذا الفرع.

أولا- الحفظ العاجل لمعطيات السير: سنتناول من خلال هذا العنصر مفهوم الحفظ العاجل لمعطيات السير و ضمانات المتهم من خلال هذه العملية.

1-**مفهوم الحفظ العاجل لمعطيات السير:** هو قيام مزودي خدمات الإتصال بتجميع المعطيات المعلوماتية التي تسمح بالتعرف على مستعملي الخدمة و حفظها و حيازتها في أرشيف و وضعها في ترتيب معين و الإحتفاظ بها قصد تمكين جهات الإستدلال من الإستفادة منها و إستعمالها لأغراض التحقيق مستقبلا فهي من مهام مقدمي الخدمات و تخص معطيات المرور فقط أو كما يسميها البعض حركة السير[2].

وسمحت المادة 01/10 من قانون (09-04) بتسجيل المعطيات المتعلقة بمحتوى الإتصالات بشرط أن يكون في حينه و هو إجراء تسخير من طرف السلطات القضائية

[1] – انظر المادة 16 و 17 من اتفاقية بودابست لمكافحة الجرائم الالكترونية لسنة 2001 .

[2] – بوكر رشيدة ، **جرائم الاعتداء على أنظمة المعالجة الآلية في التشريع الجزائري و المقارن**، ط1، منشورات الحلبي الحقوقية، بيروت،2012، ص 448.

لمقدمي الخدمات المعنيين لجمع و تسجيل المعطيات المتعلقة بمحتوى إتصالات أيا كانت محادثات هاتفية أو مكالمات فيديو عبر مواقع الأنترنت أو مراسلات كتابية على شكل (SMS .MMS)[1].

حددت المادة11 من قانون (09-04) معطيات المرور التي يجب على مقدمي الخدمات التحفظ عليها بطلب من السلطات القضائية لأغراض التحقيق و تتمثل في:

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة.
- المعطيات المتعلقة بالتجهيزات الطرفية المستعملة للاتصال (كالرقم التسلسلي لأجهزة الإتصال و نوعه).
- الخصائص التقنية و كذلك تاريخ و وقت و مدة الإتصال .
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها .
- المعطيات التي تسمح بالتعرف على المرسل و المرسل إليه (كأرقام الهاتف، عناوين بروتوكول الأنترنت، و تحديد مكانهم)[2].

إلا انه عندما ترتبط معطيات المرور بأكثر من مقدم خدمات فالحفاظ العاجل لهذه المعطيات يشملهم جميعا ليتم جمع هذه الأجزاء و ضمها إلى بعضها البعض و إختبارها[3].

2- ضمانات المشتبه فيهم أثناء حفظ معطيات السير: باعتبار أن الحق في الخصوصية يكرسه الدستور لكل الأفراد فقيد المشرع اللجوء إلى حفظ معطيات السير بجملة من الشروط توضع على عاتق مقدمي الخدمات و هي كالأتي:

أ-احترام المدة المقررة لعملية الحفظ: حددتها اتفاقية بودابست بـ 90 يوم كحد أقصى تبدأ من تاريخ التسجيل و هي قابلة للتجديد حسب تقديرات السلطات المختصة[4]، أما المشرع الجزائري حدد مدة الحفظ بسنة واحدة إبتداءا من تاريخ التسجيل حسب المادة 11 من قانون

---

[1] - احمد مسعود مريم، **آليات مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال في ضوء القانون (09-04)**، مذكرة لنيل شهادة ماجستير في القانون الجنائي، كلية قاصدي مرباح، جامعة ورقلة،2013 ، ص101.

[2] - انظر المادة 11 من قانون (09-04).

[3] - هلالي عبد الإله احمد ، **حجية المخرجات الكمبيوترية في المواد الجنائية**، دار النهضة العربية، القاهرة،2003، ص208.

[4] - انظر المدة 16 من اتفاقية بودابست ، لمكافحة الجريمة المعلوماتية، المنعقدة في بودابست في 23 نوفمبر 2001

(09-04) و نفس المدة اقرها المشرع الفرنسي من خلال المادة (32-3-1L) من قانون البريد و الإتصالات الإلكترونية المعدلة بالمادة 20 من القانون رقم (2003-239) المؤرخ في 18 مارس 2003 المتعلق بالأمن الداخلي[1].

ب-الالتزام بكتمان سرية عملية التحفظ و المعلومات المتعلقة بها: على مقدمي الخدمات الإلتزام بالحفاظ على سرية كل الإجراءات و التدبير التي تفرضها هذه العملية طيلة المدة المحددة لها و الغرض من ذلك هو ضمان حماية الحق في الخصوصية و تجنب القيام بتغييرات في البيانات بمحوها من طرف أشخاص آخرين[2].

ثانيا-الإفشاء العاجل لمعطيات السير: هي الإلتزامات التي تقع على عاتق مقدمي الخدمات الأنترنت لمساعدة السلطات المكلفة بالبحث و التحقيق في الجرائم الالكترونية حيث تعتبر هذه العملية عملية مكملة لإجراء الحفظ العجل للمعطيات كما أوضحت اتفاقية بودابست بنصها في المادة 17 بأنه "..على كل طرف إتخاذ الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية من أجل:

أ-التأكد من أن الحفظ العاجل لهذه المعطيات المتعلقة بالمرور في تطبيق المادة (16) متوفر.

ب-ضمان الإفشاء السريع (divulgation rapide) للسلطة المختصة، أو الشخص المعين من قبلها، عن كمية معطيات المرور الكافية التي تسمح بتحديد هوية مقدمي الخدمات و المسار الذي تم الاتصال من خلاله[3].

من خلال تحليل هذا النص فانه ينشىء إلتزامين على عاتق مقدمي خدمات الأنترنت فالإلتزام الأول يتمثل في الحفاظ العجل للمعطيات المرور المشار إليه في المادة 16 ثم يليه التزام أخر يكمله و هو الإفشاء العاجل للسلطات المختصة بالتحقيق عن بعض هذه المعطيات التي تساعد على إستخلاص الدليل الإلكتروني

الفرع الرابع: إنتاج المعطيات المعلوماتية

[1] - براهيمي جمال،المرجع السابق، ص105.

[2] - انظر المادة 16 فقرة 03 من اتفاقية بودابست، المرجع السابق.

[3] - براهيمي جمال، المرجع السابق، ص107.

هو إجراء يفرضه القانون على مقدمي خدمات الأنترنت بحث تقوم هذه الأخيرة بتزويد سلطات التحقيق بالمعطيات و البيانات المعلوماتية المتعلقة بالمشتركين و خدماتهم، بما تتطلب إجراءات التحقيق بحيث تطرقت إتفاقية بودابست إلى هذا الإجراء من خلال المادة 18 تحت عنوان "الأمر بإنتاج معطيات المعلومات" (njonction de produire) بحيث ألزمت الدول الأطراف بتبني الإجراءات اللازمة أو التي تراها ضرورية لتأهيل السلطات المختصة بأن تأمر:

- كل شخص على أرضة بإرسال معطيات معلوماتية معينة في حوزته أو تحت سيطرته و الخزنة في نظامه المعلوماتي أو في دعامة تخزين معلوماتية.
- كل مزود خدمات الذي يقدم خدماته على أرض ذلك الطرف من اجل إرسال المعطيات المتعلقة بالمشتركين و خدماتهم التي في حوزته أو تحت سيطرته[1].

فالدول الأطراف في هذه الاتفاقية ملزمة على تكييف قوانينها الداخلية و تبني الإجراءات و التدابير اللازمة للتحقيق في الجرائم الإلكترونية تكون أقل انتهاكا لحقوق الأفراد و خصوصيتهم بهدف الحصول على معلومات ضرورية لفائدة لتحقيق و هو الحيازة المادية للمعطيات و البيانات المعنية داخل حدود الدولة الطرف في الإتفاقية أو البيانات التي تكون في الحيازة المادية للشخص لكن بمقدوره السيطرة عليها من خلال مرورها داخل حدوده[2]، المعطيات المطلوب تقديمها يشترط أن تكون متصلة بالمشتركين و خدماتهم، فقد يكون الشخص الذي يدفع مقابل الخدمة، أو العميل الذي يدفع مقدما نظير الخدمات التي يستعملها، كما قد يكون الشخص الذي يستعمل الخدمات مجانا الذي يستخدم الحساب المشترك[3].

و يقصد بالعلاقات المتعلقة بالمشتركين و خدماتهم كل البيانات المتعلقة باستخدام الخدمة و مستخدميها فالصنف الأول: المتعلق بإستخدام الخدمة فتتمثل في معلومات عدى بيانات المرور و المحتوى التي تسمح بالتعرف على نوع خدمة الإتصال و الجوانب الفنية

---

[1] – انظر المادة 18 من اتفاقية بودابست ، الخاصة بمكافحة الجرائم المعلوماتية، المرجع السابق.

[2] – هلالي عبد الاله احمد،**الجوانب الجوانب موضوعية و الإجرائية للجرائم المعلوماتية**، دار النهضة العربية القاهرة،2003، ص 216.

[3] – فايز محمد راجح غلاب ، **الجرائم المعلوماتية في القانون الجزائري و اليمني** ، رسالة لنيل شهادة الدكتوراه في القانون،فرع القانون الجنائي و العلوم الجنائية كلية الحقوق ، جامعة الجزائر 1، 2011، ص 431.

المتصلة بها، كرقم الهاتف، عنوان موقع الويب، عنوان البريد الإلكتروني، و كذلك معدات الإتصال المستخدمة من طرف المشترك و الفترة التي إشترك فيها الفرد في الخدمة[1].

أما الصنف الثاني و المتعلق بالمستخدمين و المشتركين حددته المادة 18 فقرة 03 و يشمل كل المعلومات بإستثناء بيانات المرور أو المحتوى من خلالها يتم تحديد هوية المستخدمين عنوانه البريدي، رقم هاتفه، رقم الولوج و البيانات المتعلقة بدفع الفاتورة و المبلغ المدفوع و كل المعلومات التي تتعلق بموقع تجهيزات الإتصال، المتوفرة على أساس عقد أو باتفاق تقديم خدمة التي تفيد البحث و التحقيق[2].

الفرع الخامس: تجميع معطيات المرور في وقتها الفعلي

يقصد بهذا الإجراء قيام مقدم خدمات الأنترنت و ذلك بناءا على طلب سلطات التحقيق، بتسجيل بيانات أو معلومات إتصال معين في فترة الإنتاج و نسخ صورة منها ثم تجميعها لحظة التنقل عبر الإتصال[3]، و تتم عملية تجميع البيانات بصفة غير مادية في شكل ذبذبات صوتية أو إلكترونية دون أن يؤثر ذلك على تنقلها أو حركتها أو يعيق وصولها إلى المرسل إليه، إن إجراء التجميع في الوقت الفعلي يخص معطيات المرور دون سواها من المعطيات و بيانات المرور تكون غالبا غير متاحة و ليست صالحة للإستعمال وقت حدوث الإتصال، لأن الشخص المشتبه فيه المتدخل بطريقة غير قانونية قد يعدل مسار إتصاله في كل لحظة من أجل طمي أثاره وهنا يظهر دور إجراء التجميع في الوقت الفعلي للبيانات المتعلقة بالمرور في الكشف عن مصادر الإتصال و مساره بين الضحية و الجاني، ما يسمح إجراء مقارنات بين ساعة و مصدر و مآل إتصالات المشتبه به و ساعة و تاريخ التدخلات الغير قانونية في منظومة الضحايا، وهوية الضحايا الآخرين أو بيان روابط مع شركاء آخرين[4].

[1] – هلالي عبد الاله احمد، المرجع السابق، ص221.

[2] – انظر المادة 18 من اتفاقية بودابست، المرجع السابق.

[3] – هلالي عبد الإله احمد، المرجع السابق، ص 248.

[4] – براهيمي جمال، المرجع السابق، ص113.

و تطرقت إتفاقية بودابست إلى إجراء جمع معطيات المرور في وقتها الفعلي كإجراء جديد مفيد ومهم جدا في التحقيق و التحري عن الجرائم الالكترونية و طلبت من الدول الأعضاء بالأخذ به و التقيد بالالتزامات الآتية[1]:

1- تبني الإجراءات التشريعية أو أي إجراءات أخرى يرى أي طرف أنها ضرورية من أجل تخويل سلطاته المختصة بالتحقيق سلطة ، إجبار مقدمي الخدمات في إطار قدراته الفنية على أن يجمع و يسجل عن طريق تطبيق وسائل فنية موجودة على أرضه.

2- عندما لا يكون في مقدور أي طرف تبني المبادئ المذكورة في الفقرة 01 بند " أ " بسبب القواعد الخاصة لنظامه القانوني الداخلي، فإنه لا بد من ذلك تبني الإجراءات التشريعية أو أي إجراءات أخرى يرى أنها ضرورية لتطبيق طرق فنية موجودة على هذه الأرض[2].

3- فهذه المادة تتحدث عن الاتصالات بصيغة الجمع مما يؤكد ضرورة جمع بيانات المرور الخاصة بع اتصالات، لكي يتم تحديد مصدر هذه الإتصالات و منتهاها و يجب أن تقتصر عملية الجمع و التسجيل على بيانات المرور المقيدة في كشف الأنشطة الإجرامية[3]، و يقع الإلتزام و تسجيل بيانات المرور على عاتق السلطات المختصة في الدول الطرف و لها أن تقوم بذلك بنفسها باستخدام وسائل فنية موجودة على أرضها أو عن طريق إجبار مقدمي الخدمات على جمع أو تسجيل بيانات المرور في حدود الإمكانيات المتاحة لديها و يكون الإتصال على أرض الدولة الطرف بمفهوم المادة 20 المشار إليها أعلاه إذا كان أحد المتصلين يتواجد على هذه الأرض[4].

المبحث الثاني: الطبيعة القانونية للدليل الإلكتروني و حجيته في الإثبات الجنائي

يعتبر الدليل الإلكتروني الوسيلة الأساسية و الرئيسية في الإثبات الجنائي في الجرائم الرقمية، وللكشف عليها نحتاج إلى أدلة ذات طبيعة خاصة تختلف عن الأدلة التقليدية

[1] – انظر نص المادة (01) من اتفاقية بودابست الخاصة بمكافحة الجرائم المعلوماتية، المرجع السابق.

[2] – انظر المادة 20 من اتفاقية بودابست لسنة 2001، المرجع السابق.

[3] – فايز محمد راجح غلاب، المرجع السابق، ص 435.

[4] – هلالي عبد الاله احمد، المرجع السابق، ص248.

المادية، ومن خلال هذا المبحث سوف نتطرق إلى مفهوم الدليل الإلكتروني في **(المطلب الأول)**، ثم نتناول حجية الدليل الإلكتروني في الإثبات الجنائي في **(المطلب الثاني)** .

المطلب الأول: مفهوم الدليل الإلكتروني

إن مفهوم الدليل الإلكتروني يشمل عدة عناصر أساسية يجب تبيانها، حتى يتبين لنا هذا المفهوم بشكل جيد و واضح، لذلك سنتناول في هذا المطلب تعريف الدليل الإلكتروني في **(الفرع الأول)** خصائصه في **(الفرع الثاني)**، وأخيرا سنتطرق لتصنيفات الدليل الإلكتروني في **(الفرع الثالث)** .

الفرع الأول: تعريف الدليل الإلكتروني

إن فقهاء القانون الجنائي لم يتفقوا حول تعريف موحد للدليل الإلكتروني وهذا بسبب التطورات التي تطرأ على البيئة التقنية التي ينشأ فيها مما تجعله من الأدلة المتطورة بطبيعتها فقد عرفه البعض على انه " ذلك الدليل المأخوذ من أجهزة الحاسب الآلي ويكون في شكل ذبذبات رقمية ونبضات مغناطيسية أو كهربائية يمكن جمعها أو تحليلها باستخدام برامج وتطبيقات تكنولوجي خاصة ويتم تقديمها في شكل دليل علمي يمكن الاعتماد عليه أمام القضاء الجنائي" [1].

وعرف ايضا " أن الدليل الإلكتروني يستخلص من البرامج المعلوماتية الموجودة في الحاسوب و معدات وأدوات الحاسوب الآلي ، بشرط يستخرج بطريقة قانونية بهدف تحليلها وتقديمها للقضاء في شكلها النهائي نصوص مكتوبة أو صور أو أشكال أو أصوات لإثبات وقوع الجريمة ولتقرير البراءة أو الإدانة فيها"[2].

كما عرفته المنظمة الدولية لأدلة الحاسوب LOCE لأول مرة في مارس 2000 بقولها: "المعلومات المخزنة المتنقلة في شكل ثنائي والتي يمكن الاعتماد عليها أمام المحكمة

[1] – براهمي جمال، مرجع السابق، ص 121.

[2] عبد الناصر محمد محمود غرغليود/ عبيد سيف سعيد المسماري، ورقة بحث مقدمة للمؤتمر العربي الأول للعلوم الأدلة الجنائية والطب الشرعي – الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية –دراسة تطبيقية مقارة الرياض2007–ص13.

وفي سنة 2001 عرفته على انه المعلومات ذات القيمة المحتملة و المخزنة و المنقولة في صورة رقمية"[1].

و التعريف أكثر شمولا للدليل الإلكتروني هو "كل معلومات مخزنة في نظم المعالجة الآلية وملحقاتها أو المتنقلة عبرها بواسطة شبكة الإتصالات في شكل المجالات الإلكترونية أو ذات ذبذبات كهربائية أو نبضات مغناطيسية يتم إستخلاصها وجمعها وتحليلها وفق الإجراءات قانونية وعملية وترجمتها في شكل مجريات يقبلها العقل والمنطق ويعتمدها العلم ، ويمكن استخدامها في أية مراحل من مراحل التحقيق والمحاكمة لإثبات الجريمة وتقرير البراءة أو الإدانة"[2].

الفرع الثاني: خصائص الدليل الإلكتروني

و نظرا لطبيعة هذه البيئة الإلكترونية الحديثة و العالم الإفتراضـــي التي يتواجد فيها الدليل الإلكتروني نجده يتميز ويتصف بالخصائص التالية:

أولا- الدليل الإلكتروني دليل علمي: إن الدليل الإلكتروني يتصـــف بأنه علمي ومكوناته عبارة عن بيانات ومعلومات ومعطيات إلكترونية غير ملموسة لا تدرك بالحواس العادية يتم إدراكها بالإستعانة بأجهزة ومعدات وأدوات الحاسبات الآلية و إستخدام نظم برامجية حاسوبية[3]، وعليه فإن ما يسري على الدليل العلمي يسري على الدليل الإلكتروني فإذا كان الدليل العلمي يخضـــع لقاعدة لزوم تجاوبه مع الحقيقة الكاملة وهذا طبقا للقاعدة التي تنص على أن القانون مســـعاه العدالة أما العلم فمســـعاه الحقيقة بمعنى أن الدليل الإكتروني يتماشى مع العلم الإلكتروني وإذا خرج عن ما توصل إليه فقد معناه[4].

ثانيا- الدليل الإلكتروني دليل تقني: أي ينشأ ويبقى داخل البيئة التقنية المتمثلة في الأجهزة الرقمية الإلكترونية وفي داخل الشـــبكات بحيث يولد و يعيش بداخلها لا يمكننا رصده و لا إستنباطه خارج البيئة التقنية.

---

[1] احمد مسعود مريم، آليات جرائم تكنولوجيا الإعلام والاتصال في ضوء القانون 0304 -مذكرة لنيل شهادة الماجيستر قسم حقوق والعلوم السياسية -جامعة قاصدي -مرياح الجزائر-2013 ص 02.

[2] براهيمي جمال، مرجع السابق، ص 123.

[3] عائشة بن قارة مصطفى، مرجع السابق، ص 34.

[4] براهمي جمال، مرجع السابق، ص124.

ثالثا – الدليل الإلكتروني يصعب التخلص منه: تعد هذه الخاصية من أهم خصائص الدليل الإلكتروني، فيمكن إسترجاع الأدلة بعد محوها و إصلاحها بعد إتلافها وإظهارها بعد إخفائها مما يصعب التخلص منها [1] وذلك عن طريق العديد من البرامج الخاصة مثل DATA-RECOVER BOXأو RECOVER LOST وظيفتها استعادة البيانات صورا أو رسوما أو كتابات[2].

رابعا- الدليل الإلكتروني قابل للنسخ : تسمح هذه الخاصية باستخراج نسخ مطابقة الأصل للدليل الإلكتروني ولديها نفس القيمة والحجية الثبوتية وهذا الشيء الذي لا يتوفر في الدليل التقليدي مما يشكل ضمانة فعليا للحفاظ على الدليل ضد الضياع أو التلف عن طريق عمل استخراج نسخ طبق الأصل من الدليل[3].

خامسا- الدليل الإلكتروني متطور بطبيعته: إن الدليل الإلكتروني نجده متطور بطبيعته ويواكب مجال ثورة المعلوماتية، بحيث بيئة الدليل الإلكتروني من بيئة الجريمة الإلكترونية التي تقع في العالم الإفتراضي الذي لا حدود فيه، وتنعكس الطبيعة المتطورة للدليل الإلكتروني على الأدوات التقنية والطرق التي تستخدم في جمع الأدلة الإلكترونية بحيث تستعمل برامج متطورة ومتعددة الخدمات لمختلف العرض[4].

الفرع الثالث: تصنيفات الدليل الإلكتروني

إن الدليل الإلكتروني يختلف عن غيره من الأدلة و نجده يتميز بالتنوع فلا يأتي في صورة واحدة بل لديه العديد من الصور والأشكال وفي هذا الصدد نجد نوعين من التقسيمات للأدلة الإلكترونية تتمثل في تقسيمات الفقهية والتشريعية:

أولا- التقسيمات الفقهية للدليل الإلكتروني:

[1] شهرزاد حداد، مرجع السابق، ص15.

[2] يزيد بوحليط، الجرائم الالكترونية والوقاية منها في القانون الجزائري في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات –قانون العقوبات –قانون الإجراءات الجزائية قوانين خاصة – دار الجامعة الجديدة – طبعة 2019– ص285.

[3] بن يحي إسماعيل – مرجع السابق– ص 143.

[4] يزيد بوحليط – مرجع السابق– ص 285.

فقهاء القانون الجنائي لم يتطرقوا إلى دراسة الدليل الإلكتروني بشكل واسع كون الدليل حديث من جهة وتطوره المستمر من جهة أخرى ، بحيث قسمه الفقهاء الجنائي إلى أربعة أقسام:

01- الأدلة الإلكترونية المتعلقة بجهاز الكمبيوتر وشبكاته:

تعرف بأنها سلوك إنساني يشكل فعل غير مشروع على أجهزة الكمبيوتر سواء وقع على المكونات المادية له أو المكونات المعنوية أو حتى على القواعد البيانات الرئيسية ومثال على ذالك : تخريب مكونات الكومبيوتر كالطابعة [1].

02- الأدلة الإلكترونية المتعلقة بالشبكة العالمية للمعلومات: وتعرف على أنها سلوك إنساني يشكل فعل غير مشروع قانونا يقع على أي نص أو وثيقة موجودة بالشبكة مثل سرقة أرقام بطاقة الإئتمان قرصنة المعلومات وهذا النوع من الجريمة تتطلب الاتصال المباشر بالانترنت[2].

03- الأدلة الإلكترونية المتعلقة بالانترنت: وهي فعل غير مشروع قانونا يقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات مثل جرائم الدخول غير المشروع لمواقع يمنع الدخول إليها.

04 - الأدلة الإلكترونية المتعلقة ببروتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات: وهي تتعلق بالجرائم التي ترتكب باستخدام الكمبيوتر ولا يعتبر إستعمال الكمبيوتر أو الشبكة العالمية للمعلومات أو الانترنت في هذه الجرائم من طبيعة الفعل الإجرامي بل تستعمل كوسيلة مساعدة لإرتكاب الجريمة مثل نقل المخدرات من مكان إلى أخر أو غسيل الأموال و جهاز الكمبيوتر يقوم في هذه الحالة بحفظ الآثار الإلكترونية التي يمكن أن تستخدم للإرشاد عن الفاعل[3].

ثانيا- التقسيمات التشريعية والقضائية للدليل الالكتروني: ظهرت عدة تشريعات من أجل تقسيم الدليل الإلكتروني وكان تشريع و .م. أ من السابقين لدراسته والتطرق إليه

---

[1] ممدوح عبد الحميد عبد المطلب – البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر الانترنت –دار الكتب القانونية –مصر2006–ص 88.

[2] عائشة بن قارة مصطفى – مرجع السابق– ص72.

[3] عائشة بن قارة مصطفى– مرجع السابق– ص 72.

لهذا ستكون كنموذج لدراستنا مع أبرز التقسيمات المعتمدة سواء كان الأمر على مستوى التشريع أو القضاء واهم التقسيمات وزارة العدل الأمريكية للدليل الإلكتروني لسنة 2002 تم تقسيمه إلى ثلاث مجموعات:

01 -السجلات المحفوظة في الحاسوب: هي مجموعة من الوثائق مكتوبة ومحفوظة والمقصود هنا بالكتابة الإلكترونية أنها كل حروف أو أرقام أو رموز أو علامات أخرى، تثبت على دعامة الكترونية أو رقمية أو ضوئية أو أية وسيلة مشابهة وتعطي دلالة قابلة للإدراك[1]، بحيث عرف البريد الإلكتروني على أنه طريقة تسمح بتبادل الرسائل المكتوبة بين الأجهزة المتصلة بشبكة المعلومات[2]، وأن فكرة البريد الإلكتروني تقوم على أساس تبادل الرسائل الإلكترونية والملفات والصور عن طريق إرسالها من المرسل إلى مجموعة أشخاص أو اقل باستعمال البريد الإلكتروني الذي يعتبر صندوق تتواجد به كل الرسائل المرسلة إلى صاحب البريد والتي سبق له إرسالها والملفات وغيرها من الأمور التي يحتوى عليها البريد الإلكتروني [3].

02- السجلات المحفوظة جزئيا في الحاسوب: تنشأ هذه السجلات بواسطة جهاز الحاسوب، فهي تعتبر مخرجات برامج الحاسوب بالإضافة لسجلات الهاتف وكذا فواتير أجهزة LOG FILES معنى ذلك انه لم يتم لمسها من قبل الأشخاص[4].

03- السجلات المحفوظة للإدخال أو المنشأة بواسطة الحاسوب: و من بين الأمثلة عن ذالك البيانات التي تتم بإدخالها إلى جهاز الحاسب وتتم معالجتها من خلال برامج خاصة[5]، وأمثلة أخرى عنها أوراق العمل المالية التي تحتوى على مدخلات تم تحويلها إلى برامج أوراق عمل مثل EXCEL ثم تمت معالجتها بإجراء العمليات الحسابية بحيث أخذ القضاء الأمريكي بهذا التقسيم وقبلت بالسجلات الحاسوب التي تكون في شكل نصوص[6].

---

[1] محمد حسين منصور – **الإثبات التقليدي و الالكتروني** –دار الفكر الجامعي– مصر–2006– ص272.

[2]خالد ممدوح إبراهيم – **التقاضي الالكتروني** – دار الفكر الجامي مصر–2008– ص101–102.

[3] مناني فراح – **أدلة الإثبات الحديثة في القانون** –دار الهدى للطباعة والنشر–الجزائر– ص59.

[4]براهيمي جمال –مرجع السابق–130.

[5]احمد يوسف الطحطاوي،الأدلة الالكترونية ودورها في الإثبات الجنائي، دار النهضة العربية–القاهرة– 2015 ص21.

[6]عائشة بن قارة مصطفى – مرجع السابق – ص77.

ثالثا – تقســـيمات أخرى للدليل الإلكتروني: الدليل الإلكتروني متنوع من حيث هيئته و شــكله إلى أدلة مكتوبة وأدلة العرض المرئي وأخرى صــوتية وســمعية و إلى أشــرطة مغناطيسية وأقراص مغناطيسية والتي سوف نتناولها كالتالي:

01- **أدلة الإلكترونية مكتوبة:** ونجدها تضـم كل المحفوظات والنصـوص التي تكتب من طرف المســـتخدم عن طريق الأجهزة الإلكترونية الرقمية مثل المراســـلات عبر البريد الإلكتروني أو الهاتف النقال والتي تم إدخالها أو الناتجة عن معالجة البيانات في وحدة المعالجة المركزية أو مختلف ملفات برامج معالجة الكلمات[1].

02-أدلة إلكترونية مرئية: و التي نجدها تجســـد الحقائق المرئية حول الجريمة والتي تظهر في صـور مرئية ثابتة على شكل ورقي وكذالك رقمي بإستعمال الشاشـة المرئية أو في شــكل تســجيلات فيديو أو أفلام مصــورة [2] بحيث إن الصــور الرقمية هي في الواقع تكنولوجيا بديلة أو أكثر تطورا من الصور الفوتوغرافية [3].

03- **أدلة إلكترونية سـمعية أو صـوتية:** تشـمل التسـجيلات الصـوتية التي يتم ضـبطها وتخزينها بواسـطة الوسـائل الإلكترونية مثل المحادثات الصـوتية على غرف الدردشـة عبر الانترنت أو مختلف تطبيقات مواقع التواصل الاجتماعي وكذا المكالمات الهاتفية.

04- الأشرطة المغناطيسية: وهي عبارة عن شريط بلاستيكي مغطى بمادة قابلة للمغنطة يكون ملفوف على بكرة ويسـتعمل هذا الأخير في تخزين البرامج أو الملفات أو المعلومات التي يحتويها تكون منظمة على شكل وحدات خاصة.

05 – الأقراص المغناطيسية: و تعد من أفضل وسائل التخزين تستخدم للتخزين المباشر أو العشوائي وذلك راجع لقدرة استيعابها العالي ، تتميز بخاصية مهمة وهي إمكانية القراءة

[1] هلالي عبد اللاه احمد، حجية المخرجات الكمبيوتر في المواد الجنائية، دار النهضة العربية القاهرة 2003، ص27.

[2] هلالي عبد اللاه مرجع نفسة –ص 20-23.

[3] ممدوح عبد الحميد عبد المطلب، أدلة الصور الرقمية في الجرائم الكمبيوتر، مركز الشرطة دبي 2005،ص 09.

أو التسـجيل وكذا تغيير و تعديل أي ملف دون حاجة إلى إنشـاء ملف جديد، وهناك عدة أنواع نذكر منها : القرص المرن – القرص الصلب – المصغرات الفيلمية[1].

المطلب الثاني: حجية الدليل الإلكتروني في الإثبات الجنائي

إن الدليل الإلكتروني يتمتع بحجية إثبات أي القوة الإستدلالية في إكتشاف الحقائق في الجريمة الإلكترونية، ومع تطور العلم والعلوم أصبح الدليل الإلكتروني أفضل دليل إثبات وهذا ما نعرضه في مطلبنا هذا، من خلال دراسة أساس قبول الدليل الإلأكتروني على ضوء أنظمة الإثبات في **(الفرع الأول)** أو بشهر إفلاسها الذي لا يكون إلا بموجب حكم قضائي **(الفرع الثاني)** أو فصل أحد الشركاء المعيق لنشاط الشركة **(الفرع الثالث)**.

الفرع الأول: أساس قبول الدليل الإلكتروني على ضوء أنظمة الإثبات

تختلف طريقة الاعتراف بالدليل الإلكتروني وقبوله كدليل إثبات من دولة إلى أخرى بحسب طبيعة نضام الإثبات السائد فيها، وتنقسم هذه الأنظمة إلى ثلاثة أولها النظام اللاتيني – نظام انجلوسكسوني– نظام مختلط التي سوف نتطرق إليها كالأتي:

أولا– النظام اللاتيني: يطلق عليه بنظام الإثبات الحر، يسود في هذا النظام مبدأ حرية الإثبات لا يحدد فيه المشرع طرق معينة أو محددة للإثبات ولا حجيتها أمام القضاء، بل يترك الحرية للقاضي في تأسيس حكمه وفقا لإقتناعه الشخصي أمام أدلة موجودة ودون أن يفرض عليه دليل معين، وان القاضي الجنائي هو الذي يختار من بين الأدلة ما يراه مناسبا ومفيد للوصول إلى الحقيقة[2].

هذا النظام يرتكز على مبدأين أساسين ومختلفين هما: الأول يتمثل في الدور الايجابي للقاضي في الإثبات وقبول وتقدير الدليل الإلكتروني[3].

بينما الدور السلبي للمشرع في عملية الإثبات التي من خلالها يمتنع مشرع عن تحديد الأدلة التي تصلح للإثبات مسبقا مما يجعل جميع الأدلة مقبولة وفقا لتقدير

[1] سامي جلال فقي حسين، **الأدلة المحصلة من الحاسب وحجتها في الإثبات**، دار كتب القانونية، القاهرة،2011 ص59.

[2] براهيمي جمال –مرجع السابق–ص 141.

[3] عائشة بن قارة مصطفى– مرجع السابق –ص 193–192.

القاضـي وليس المشـرع ، الذي يقتصـر دوره على تحديد الشـروط اللازمة لصـحة الدليل و طريقة تقديمه ضـمانا للحرية الفردية وكفالة حسـن سـير العدالة[1]، من بين التشـريعات التي انتهجت هذا النظام نجد مل من فرنسا – الجزائر– مصر.

ثانيا– النظام الأنجلوســـكســـوني: ويعرف بنظام الإثبات المقيد، وفي هذا النظام يقوم المشرع بتحديد وحصـر الأدلة التي يسـتعين بها ويقبلها القاضـي في عملية الإثبات، فلا يجوز للقاضـــي أن يقوم ببناء الحكم على خلافها ولا خروج عليها ولا يمكنه تقدير الأدلة أو البحث عنها بل يقتصـــر دوره على فحص الدليل للتأكد من مدى مشـــروعيته وتوفره على الشروط التي حددها القانون ، يلتزم القاضي الجنائي أن يؤسس حكمه على أساس هذا الدليل وان لم يكن مقتنعا به[2]، يعتمد هذا النظام على مبدأين أسـاسـين بحيث يمثل الدور الايجابي للمشرع في عملية الإثبات باعتباره هو الذي ينظم قبول الأدلة سوء عن طريق التعيين المسبق للأدلة المقبولة للحكم بالإدانة أو باستبعاد أدلة أخرى كونه هو الذي يحدد القيمة الاقناعية لكل دليل[3]، الدور الثاني هو ســـلبيا للقاضـــي الجنائي في الإثبات بحيث يلزم بما يرسمه له مشرع وهذا ما يفقده سلطته في الحكم بما يتناسب مع الواقع، ويصـــبح القاضـــي كالآلة في طاعته لنصـــوص القانون دون إبراز قناعته الشخصية[4]، ومن بين التشريعات التي أخذت بهذا النظام نجد انجلترا و أمريكيا الجنوبية وجنوب إفريقيا.

ثالثا– النظام المختلط: هو نظام وســـط بين نظام الإثبات المقيد ونظام الإثبات الحر[5] وهذا النظام دمج بين النظامين عن طريق تحديد قائمة أدلة الإثبات و القيمة الثبوتية من طرف المشـرع من جهة، و من جهة أخرى منح للقاضـي الجنائي السـلطة التقديرية في موازنة و قبول الأدلة المطروحة أمامه، كما أن هذا النظام يقوم على تحديد أدلة

---

[1] احمد يوسف الطحطاوي، الأدلة الالكترونية ودورها في الإثبات الجنائي،دار النهضة العربية،القاهرة،2015،ص 195

[2] شيماء عبد الغاني محمد عطالله، الحماية الجنائية للتعاملات الالكترونية،دار الجامعة الجديدة الاسكندرية2007،ص 387.

[3] براهيمي جمال –مرجع السابق– ص138–139.

[4] سامي جلال فقي ، مرجع السابق، ص 82.

[5] عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمنصفات الفنية ودور الشرطة والقانون، دراسة مقارنة منشورات الحلبي، دمشق 2007، ص373.

الإثبات ســـلفا، كما نجده يحدد قيمتها وحجيتها مع إعطاء للقاضـــي حرية في تقدير القضية المعروضة أمامه أي القاضي له دور ايجابي في ظل هذا النظام[1].

واعتبر الفقهاء هذا المذهب أفضـــل من نظام الإثبات المقيد و الحر لأنه يجمع محاسـنهما و يسـتبعد مسـاوئهما فهو يوازن بين تحقيق العدالة و ما يتطلبه من مرونة و حرية في الإثبات و ما يتطلبه استقرار التعامل من تقييد الإثبات في بعض الأحيان[2].

موقف المشـــرع الجزائري من خلال المـادة 212 و307 من قـانون الإجراءات الجزائية بحيث تنص المادة 212: يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذالك وللقاضـــي أن يصـــدر حكمه تبعا لاقتناعه الخاص و لا يصـــوغ للقاضـــي أن يبني قراره إلا على الأدلة المقدمة له في معرض المرافعات"و المادة 307:"..القانون لا يطلب من القضـاة أن يقدموا حسـابا عن الوسـائل التي بها قد وصـلوا إلى تكوين اقتناعهم ولا يرسـم لهم قواعد بها يتعين عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما..".

وهنا من خلال المادتين يتضح أن المشرع الجزائري اعتمد على نظام الإثبات الحر كأصل ونظام الإثبات المقيد كاستثناء[3].

الفرع الثاني: تقدير الدليل الإلكتروني أمام القضاء الجنائي

القاضي الجنائي يتمتع بسلطة واسعة في تقدير أدلة الإثبات، و وضع المشرع على الأدلة الرقمية شروط لا يجوز للقاضـي الانحراف عليها عند ممارسته لها، ولقبول الدليل الالكتروني كحجية للإثبات تبنى عليه الحقيقة في الدعوى الجزائية لا بدا من توفر بعض الشروط هذا ما سنتطرق إليه من خلال هذا الفرع كما سنتناول سلطة القاضـي الجنائي الجزائري في تقدير الدليل الالكتروني:

أولا- شروط اكتساب الدليل الالكتروني حجية في الإثبات:

[1] سامي جلال ففي حسين، المرجع السابق ص 93.

[2] مسعود زبدة، الاقتناع الشخصي للقاضي الجزائي، المؤسسة الوطنية للكتاب ، الجزائر،1989،ص23.

[3] براهيمي جمال، مرجع السابق، ص167.

1- شرط مشروعية الدليل الالكتروني: إن القاضي الجنائي يتمتع بسلطة تقدير الدليل الالكتروني و يشترط لقبوله أن يتحصل عليه بطرق مشروعة وفقا للنزاهة والأمانة وان يستمد قناعته من هذا الأخير لان محل الحرية و السلطة التقديرية التي يتمتع بها القاضي الجنائي هو الأدلة المقبولة [1]، وان الدليل الالكتروني عندما يكون مشروعا ضامنا للحرية الفردية و إذا استخدمت وسائل غير مشروعة في الحصول عليه أبطلت الإجراءات ويكون غير صالح كدليل إدانة في المواد الجنائية[2].

2 - شرط مناقشة الدليل الالكتروني: يجب على القاضي أن يبني حكمه على أدلة طرحت أمامه لمناقشة الدليل في الجلسة وهذا الأمر من أهم قواعد الإجراءات الجنائية حتى تمنح للخصوم فرصة الاطلاع عليه ومناقشته بحيث يترتب على أن يكون الدليل أصل ثابت في أوراق الدعوى أو على شكل بيانات معروضة على الحاسب الآلي أو معلومات مخزنة على الأقراص أو أشرطة ممغنطة أو في شكل مطبوعات فجميعها تكون محل للمناقشة إذا أخذت كدليل إثبات أمام المحكمة[3]، ومناقشة الدليل تمنح الفرصة للخصوم للإطلاع على الدليل الالكتروني و الرد عليه وحتى يتمكن الخصوم في المواجهة هذه الأدلة وهنا يتجسد مبدأ المواجهة وإحاطة المتهم علما بالتهمة المنسوبة إليه و سماح له بالاستعانة بمحامي و منحه الوقت الكافي لتحضير دفاعه وفي أثناء عملية المناقشة يسمح لكل طرف من الخصوم تقديم بعض المستندات و كذلك سؤال الشهود و الخبراء[4].

ويترتب عن ذلك عدم جواز اقتناع القاضي من المعلومات شخصية حصل عليها خارج الجلسة أو في خارج المناقشات التي جرت وإلا نقول أن القاضي هنا جمع في شخصه صفتين متعارضين صفة الشاهد و صفة القاضي مما يبعث الحرج في نفسية

---

[1] عائشة بن قارة مصطفى، مرجع السابق، ص 268.

[2] على محمود على حموده، الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي – المؤتمر العلمي حول الجوانب القانونية و الأمنية و الأمنية للعمليات الالكترونية، منظم المؤتمر أكاديمية شرطة دبي –مركز البحوث والدراسات ع 01، دبي 28 نيسان 2003، ص 23.

[3] سليمان احمد فضل، المواجهة التشريعية و الفنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية، القاهرة، ص 375.

[4] – عائشة بن قارة مصطفى، مرجع السابق، ص271-272.

الخصـوم ويعيقهم عن مناقشـة شـهادته كونه اعتمد على علمه الشـخصـي مما يجعله عرضه للشبهات و ينزع نزاهته[1]، فالقاضي الجنائي لا يمكن أن يبني قناعته على رأي الغير إلا إذا كان من طرف خبراء و فنيين اسـتشـارهم من قبل وفقا للقانون وضـميره كان مرتاح لرأيهم بما يوافق مع الأدلة المقدمة إليه في أوراق الدعوى المعروضة عليه[2].

3 – **شرط يقينية الدليل الالكتروني:** يستلزم للقاضـي على أن يصـدر حكم عن اقتناع يقيني من خلال الأدلة المتوفرة لديه فيعرف اليقين على انه وجود حقيقة يسـتخلصـها القاضـي الجنائي بواسـطة المعرفة الحسـية بعيدا عن الغموض أو احتمال ويكون ذلك من خلال فحص ومعاينة القاضـي لهذه الوسـائل أو الأدلة بالمعرفة الذهنية و اسـتقراء النتائج ليبرهن على جودة الحقيقة[3].

وبمعنى أخر إن درجة اليقين للقاضـي يتم الوصـول إليها عن طريق ما تسـتنتجه وسـائل الإدراك المختلفة للقاضـي من خلال التمعن و التدقيق في مختلف إشكال وقائع الدعوى و الأدلة الالكترونية و هكذا يسـتطيع القاضـي أن يحدد قوتها الاسـتدلالية على صـدق نسـبة جريمة من الجرائم الالكترونية إلى شـخص معين من عدمه[4]، فاليقين شـرط عام في أحكام الإدانة سواء كانت الأدلة التي يستنتج منها تقليدية أو مستحدثة كالدليل الالكتروني وهذا الأخير لابد أن يكون غير قابل للشـك باعتبار أن الشـك يفسـر لصـالح المتهم فيكفي أن يشك القاضي من صحة إسناد التهمة إلى المتهم حتى يقضي بالبراءة[5].

ولكي يستطيع القاضـي بلوغ درجة اليقين و الجزم في اقتناعه بالأدلة و نسبها إلى المتهم يعتمد على نوعين من المعرفة فالمعرفة الأولي هي المعرفة الحسية التي تستنبط من الحواس بعد المعاينة والفحص لهذه المخرجات أما المعرفة الثانية هي المعرفة العقلية

---

[1] نبيل إسماعيل عمر، عدم قضاء القاضي بعلمه الشخصي، مجلة العربية للدراسات الأمنية– المجلد الأول –العدد الأول، رياض، 1989، ص 24.

[2]– على محمود على حموده ، مرجع السابق، ص120.

[3] على محمود على حموده، المرجع نفسه، ص 37.

[4] علاء عبد الباسط خلاف– الحماية الجنائية لوسائل الاتصال الحديثة –دار النهضة لعربية– القاهرة2002،ص 463.

[5] عائشة بن قارة مصطفى، مرجع السابق، ص277.

التي تدرك عن طريق التحليل والاســـتنتاج والاســـتقراء التي يجريها على المخرجات الالكترونية ويربطها مع الملابسات الموجودة بها [1].

يتميز الدليل الالكتروني بالطبيعة التقنية إلا أن هناك قواعد محددة تم وضـــعها من طرف المختصـــين التي تتحكم في يقينيتها ومن أهمها اســـتعمال الوســـائل الفنية ومن طبيعة هذا الدليل تمكن من فحصـــه للتأكد من ســـلامته من العبث و صـــحة الإجراءات المتبعة للحصول عليه واهم الوسائل التقنية تتمثل في:

ا- تقييم الدليل الالكتروني من حيث ســـلامته من العبث: للتأكد أن الدليل الالكتروني لم يبعث في ســـــلامته يجب أن نتبع طرق التالية :بحيث يلعب علم الكمبيوتر دور مهم في تقدير مختلف المعلومات الفنية التي تعمل على فهم مضـمون الدليل الالكتروني ويستعمل هذا النوع من العلوم في الكشف عن التلاعب بالدليل عن طريق فكرة التحليل التناظري الالكتروني التي تكشـف لنا عن مصـداقية الدليل وهي تقنية يتم مقارنة الدليل الالكتروني المقدم للقضاء بالأصل المدرج بالأدلة الرقمية[2].

كما نجد نوع من الأدلة الالكترونية تعرف بالأدلة المحايدة وهو نوع من الأدلة الالكترونية المخزنة في البيئة الافتراضية والتي لا علاقة لها بموضوع الجريمة وهذا دليل يسـاعد على تأكد من سـلامة الدليل الالكتروني من العبث ويجعله يقنيا لا مجال الشـك فيه [3].

تسـتخدم عمليات حسـابية خاصـة بالخوارزميات في حالة عدم الحصـول على النسـخة الأصلية للدليل آو في حالة ما كان هنالك شك أن عبث في دليل وهده التقنية تسمح لنا من التأكد من مصداقية الدليل الالكتروني.

ب - تقييم الدليل الالكتروني من حيث القيمة الفنية:

نسـبة الخطأ الفني في الحصـول على الدليل الإلكتروني ضـئيلة جدا بإعتباره تطبيقا من الدليل العلمي، وهذا لا يعني أنها منعدمة بل يظل الوقوع في الخطأ ممكنا أثناء إستعماله ، ويكون ذلك إما بسبب الخطأ في استخدام الأداة المناسبة لإستخلاص الدليل

---

[1] إيمان محمدة على الجابري، يقين القاضي الجنائي، منشأ ة المعارف الإسكندرية 2005، ص 131.

[2] جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجية الحديثة، دار النهضة العربية، القاهرة2014،ص27.

[3] ابراهيمي جمال، مرجع السابق، ص155.

كخلل في الشـفرة المسـتخدمة أو بسـبب معلومات خاطئة ، ومن أجل تجنب مثل هذه الأخطاء يمكن إتباع بعض الاختيارات و التطبيقات للتأكد من سلامة الإجراءات المتبعة في الحصـول على الدليل الالكتروني من حيث إنتاجها لدليل تتوافر فيه المصـداقية لقبوله كدليل إثبات نلخصها كأتي[1]:

- إخضـاع الأداة المسـتخدمة في الحصـول على الدليل لعدة تجارب بغية التأكد من دقتها في إعطاء النتائج المبتغاة:

في هذه المرحلة يجب إتباع إختبارين أسـاسـين التي يتم من خلالها التأكد من أن الأداة المسـتخدمة عرضـت كل المعطيات المتعلقة بالدليل الالكتروني وفي نفس الوقت لم تضـف إليها أي بيان جديد وهذا ما يعطي للنتائج المقدمة عن طريق هذه الأداة مصـداقية في التدليل على الوقائع وتتمثل في إختبارين هما:

01- **إختبار السـلبيات الزائفة:** أين تخضـع الأداة المسـتخدمة في الحصـول على الدليل يبين مدى قدرتها على عرض كافة البيانات المتعلقة بالدليل دون إغفال أية بيانات مهمة.

02- اختبار الايجابيات الزائفة: أين تخضـع الأداة المسـتخدمة في الحصـول على الدليل الالكتروني لإختبار فني يمكن من التأكد من أن هذه الأداة لا تعرض بيانات إضـافية جديدة [2].

-الإسـتعانة بأدوات ذات قيمة عالية أثبتت التجارب العلمية نجاعتها في تقديم نتائج أفضـل : هناك دراسـات وبحوث علمية متخصـصـة في مجال تقنية المعلومات حددت الأدوات السـليمة التي يجب إتباعها في سـبيل الحصـول على الدليل الالكتروني وفي المقابل بينت الأدوات المشـكوك في كفاءتها وحثت على إجتنابها ، وعليه فإختيار أية أداة من هذه الأدوات من شأنها أن يؤثر على مصداقية المخرجات المستمدة منها[3].

ثانيا- سلطة القاضي الجنائي الجزائري في تقدير الدليل الالكتروني:

المشرع الجزائري أجاز إثبات الجرائم بأي طريقة ما عدى الجرائم التي تتطلب إثباتها بدليل معين، و للقاضـي الجنائي السـلطة التقديرية في تقدير الدليل و بناء اقتناعه، لكن

[1] براهيمي جمال، المرجع السابق، ص156.

[2] طارق محمد الحلبي، المرجع السابق، ص 28.

[3] براهيمي جمال، المرجع السابق، ص 156

هل هذه السلطة التقديرية الممنوحة للقاضي الجنائي الجزائري يتمتع بها أيضا أثناء تقدير الدليل الالكتروني ؟

بالرجوع إلى القانون رقم: (09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها فانه لا تتواجد أية أحكام تتعلق بحجية المخرجات الالكترونية قي الإثبات[1]، فسكوت المشرع هو تفسير لنيته في إخضاع هذه الأدلة مثلها مثل باقي الأدلة الأخرى للقواعد العامة[2].

أما إذا كان الجرم المرتكب جنحة فالقاضي يكون مطالب بتسبيب حكمه بحيث يكون محل رقابة من طرف جهات الطعن، أي حمله على الإفصاح عن مصادر قناعته للنظر فيما إذا كان من شانها أن تؤدي منطقيا إلى ما انتهى إليه، و لا يبين القاضي في حكمه لماذا اقتنع و الكيفية التي استمد منها قناعته و العلة في اقتناعه، لان ذلك يدخل في نطاق السلطة التقديرية المخولة له قانونا[3].

بالتالي قاضي الموضوع في مواد الجنح مطالب باحترام القواعد العامة المنظمة للقوة الثبوتية لكل وسائل الإثبات بما فيها وسائل الإثبات الالكترونية التي تأخذ شكل محاضر معدة بخصوص استجواب، تفتيش، مراقبة الكترونية، اعتراض مراسلات أو تقرير خبرة محرر بمناسبة معاينة أو فحص الأدلة المضبوطة من دعامة الكترونية، أما المحاضر فالمشرع الجزائري اعتبرها كقاعدة عامة مجرد استدلالات ما لم ينص القانون على خلاف ذلك و لا تكون للمحضر أية قوة إثبات إلا إذا كان صحيحا من حيث الشكل، و قد سوى المشرع بين المحاضر المعدة حول الجرائم الالكترونية و تلك المتعلقة بالجرائم التقليدية و ترك تقدير قيمتها الاستدلالية إلى القاضي الجنائي أما تقارير الخبرة فتخضع لمناقشة و تقدير قاضي الموضوع حسب نص المادة 215 من قانون الإجراءات الجزائية على انه "..لا تعتبر..و التقارير المثبتة للجنايات و الجنح إلا مجرد استدلالات.."[4]، بالإضافة إلى نقص المهارة و الثقافة الفنية للقاضي الجنائي الجزائري تلزمه الاستناد في تكوين اقتناعه

---

[1] انظر القانون رقم(09-04) المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، مرجع سابق.

[2] براهيمي جمال، المرجع السابق، ص 177.

[3] براهمي جمال مرجع نفسه، ص178

[4] نظر المادة 215 من قانون الإجراءات الجزائية.

و بدون تردد على الخبرة الفنية و النتائج المتوصـــل إليها في تقرير الخبرة و لا يمكنه استبعادها إلا إذا قدر أن ما تحتويه من أدلة لا يتوافق مع ظروف و ملابسات الجريمة او تتناقض مع الحقيقة و المنطق العلمي[1].

خلاصــة القول موقف المشــرع الجزائري من الإثبات بالأدلة الرقمية هو على العموم موقف التشـــريعات التي أخذت بنظام الإثبات الحر، حيث أجاز الإثبات في المســـائل الجزائية بكافة وســائل الإثبات، و للقاضـــي مطلق الحرية في بناء قناعته من أي بينة أو قرينة يرتاح إليها[2].

الفرع الثالث: دور القيمة العلمية للدليل الإلكتروني و أثرها في اقتناع القاضي

لا يمكن للقاضـــي الجنائي أن يتنازع في القوة الإســتدلالية و القيمة الإثباتية للأدلة الالكترونيـة بمعنى أخر إن الـدليـل الإلكتروني لـه أهميـة بـالغـة في الإثبـات الجنـائي ولذلك لا بدا من التطرق لمعنى الاقتناع القضائي ثم بيان قيمة الدليل في الإثبات[3].

نجد أن الفقهاء إختلفوا في دقته الفنية و بحكم أصـــالته العلمية التي يبلغ معها إلى درجة اليقين له قوته الثبوتية الملزمة للقاضـــي، و حجتهم أن الدليل العلمي هو النتيجة التي تســفر عنها التجارب العلمية لإثبات أو نفي الواقعة التي يثار حولها الشــك و التي غالبا ما يتطلب لفهمها معرفة و دراية خاصـــة لا يملكها القاضـــي بحكم انه قانوني محض[4] و لا يمكنه أن ينازع في قيمته الاسـتدلالية و انه ليس بشـرط أن يكون إقتناع القاضي بالدليل الإلكتروني يقينيا كون القاضي الجزائي لا يملك وسائل إدراك اليقين كحالة ذهنية تلتصـــق بالحقيقة دون أن تختلط بالشـــك الشـــخصـــي أو الجهل أو الغلط في الموضـــوع وهنا نجد أن الإقتناع في نظرهم يقف موقف وســط بين اليقين والاعتقاد بل

[1] براهيمي جمال ، الرجع السابق، ص179.

[2] براهيمي جمال، المرجع نفسه، ص 180.

[3] اشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الالكترونية، دار الجامعة الجديدة، مصر،2015،ص227.

[4] بوكر رشيدة، الجرائم الاعتداء على الأنظمة المعالجة الآلية في التشريع الجزائري و المقارن، الطبعة الأولى،منشورات الحلبي الحقوقية، بيروت، 2012، ص507.

الإقتناع هو إعتقاد قائم على أدلة موضوعية ومبني على الإستقراء و الإستحياء الذي يتوجه به أطراف الخصومة لنيل الاقتناع القاضي[1].

و إن كان الدليل الإلكتروني سليما ولم يعبث فيه وتوفرت فيه كل الشروط يجب على القاضي قبوله والإقتناع به و لا يمكنه التشكيك فيه من حيث القيمة الثبوتية و بحكم طبيعته الفنية يمثل إخبار صادق عن الوقائع و حقيقة علمية ثابتة ما لم يثبت عدم صلة هذا الدليل بالجريمة المراد إثباتها و لا يمكن التغلب على مشكلة التشكيك في مصداقيته من خلال إخضاعه لإختبارات فنية التي تسمح بالتأكد من سلامتها وصحتها أو لوجود خطا في الحصول عليه و القيمة الإقناعية لهذا الدليل و قد جعلوا الطبيعة العلمية للدليل الإلكتروني قيدا حقيقيا لحرية القاضي الجزائي في تقدير الدليل يجبره على الاقتناع به والحكم بمقتضاه و لو لم يكن مقتنع بصحة الوقائع المطروحة أمامه[2].

و هناك من يرى بأن مبدأ حرية القاضي في الإقتناع يجب أن يبسط سلطانه على كل الأدلة دون إستثناء بما فيها الدليل الإلكتروني و ينتمي أنصار هذا الاتجاه إلى الدول التي تبنت نظام الإثبات الحر مثل فرنسا، إيطاليا، مصر و الجزائر[3]، بحيث أن الوسائل العلمية ليست دليلا في حد ذاته إنما هي قرائن تتم دراستها و تحليلها لإستخلاص دلالتها أي مهما يعلوا شان الأدلة العلمية الإلكترونية في مسالة الإثبات الجنائي فانه يجب الإبقاء على سلطة القاضي في تقدير تلك الأدلة و تكوين قناعته منها بكل حرية و تفسير الشك لصالح المتهم و إستبعاد الأدلة التي يتم الحصول عليها بطرق غير مشروعة و يجعل من الحقيقة العلمية حقيقة قضائية[4].

و الرأي الراجح، يجب على القاضي الجنائي أن لا يتقيد بالدليل العلمي و منه بالدليل الإلكتروني، المطروح أمامه لتكوين قناعته و الحكم وجوبا بما أسفرت عليه نتائج

---

[1] طاهري شريفة، تأثير أدلة على الاقتناع الشخصي للقاضي الجنائي، مذكرة لنيل ماجيستر، كلية الحقوق جامعة الجزائر 2003-ص 23.

[2] براهمي جمال، مرجع سابق، ص163- 164.

[3] براهمي جمال، المرجع نفسه، ص164.

[4] علي محمود علي حمودة، الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي، الإمارات العربية المتحدة،2003 ص ص 01-31.

هذه الأدلة، بل لا بد أن يستمد هذا الاقتناع مما له من سلطة في تقدير الأدلة ،مهم بلغت درجتها اليقينية و العلمية، ولي نظمن نجاح مهمة القاضـــي في مناقشـــة الأدلة العلمية و التقنية، يتطلب منه أن يكون مؤهلا فنيا و تقنيا على كيفية التعامل مع هذه الأدلة عند الأخذ بها كدليل إثبات، ذلك بعقد دورات تدريبية مكثفة في مجال تقنية المعلومات[1].

[1] براهمي جمال مرجع السابق، ص 166.

خلاصة الفصل الثاني

من خلال هذا الفصل نستنتج أن إستخلاص الدليل الرقمي في مجال الجرائم الإلكترونية، يتم عن طريق إعتماد سلطات التحقيق، لإجراءات تحقيق تقليدية نفسها التي يتم إستعمالها في الجرائم التقليدية المادية، على غرار تلقي الشكاوى و البالغات بالطرق العادية و الإلكترونية، الإنتقال و المعاينة في البيئة الإفتراضية لمسرح الجريمة الرقمية وتفتيش المنظومات المعلوماتية قصد الوصول إلى إكتشاف أدلة الإلكترونية و ضبطها ليتم إخضاعها للخبرة التقنية بفحصها من طرف خبراء و فنيين بغية إستخلاص الدليل الإلكتروني لمواجهة هذا النوع الإجرامي المتطور، إلا أن الإجراءات التقليدية السالفة الذكر، أثبت الواقع العملي قصورها وعجزها في مسايرة التطور السريع الذي تعرفه الجريمة الإلكترونية، هذا من جهة و من جهة أخرى عدم قدرت إجراءات التحقيق التقليدية مواجهة الجريمة الالكترونية نظرا لتقنية هذه الأخيرة وحداثة التجهيزات والتقنيات المستعملة في إرتكاب الجريمة، وكذلك نوع الجناة الذين يتميزون بتقنيات ومهارات جد متطورة كل هذا ألزم المشرع في مختلف دول العالم بالعمل على تطوير وإستحداث أساليب وإجراءات تحقيق تواكب التطور السريع الذي يعرفه هذا النوع من الجرائم و التكيف مع الطبيعة الخاصة لها و المتمثلة في التسرب الإلكتروني، إعتراض المراسلات و المراقبة الالكترونية، الحفظ و الإفشاء العجلان للمعطيات المتعلقة بالسير، إنتاج المعطيات المعلوماتية، تجميع المعطيات في وقتها الفعلي، ورغم المخاوف الكثيرة التي أبداها رجال القانون و الفقهاء إتجاه هذه الإجراءات المستحدثة و ما ينجر عنها من مساس لحق الخصوصية المكرس دستوريا، إلا أنها أثبتت نجاعتها من الناحية العملية نظرا للتقنيات و المهارات و التكنولوجيات الحديثة التي تعتمد عليها، بالتالي أصبح أمر الإستعانة بها ضرورة ملحة للمواجهة الفعالة و الناجعة لهذا النمط الإجرامي المستحدث، الذي يعرف معدلات قياسية، نتيجة إقتحام المعلوماتية للحياة اليومية للأفراد و أصبح الاستغناء عنها أمر مستحيلا في ظل التطور الرهيب في مجال الإعلام الآلي و تكنولوجيا الإعلام و الإتصال إلى حد توجه بعض الدول إلى إنشاء ما يعرف بالمدن الذكية.

الخاتمة

خاتمة:

من خلال إنجاز هذه المذكرة نستخلص بأن موضوع التحقيق و جمع الأدلة في مجال الجرائم الإلكترونية، هو موضوع مركب، و متشعب، هذا النمط الجديد من الجرائم هو وليد ثورة تقنية المعلومات و الإتصالات التي يعرفها عالمنا المعاصر اليوم و إن سوء إستخدام و إستغلال هذه التكنولوجيا على نحو غير مشروع، أدى إلى ظهور جيل جديد من الجرائم ذات خصائص تقنية و علمية جد متطورة و التي تختلف تماما عن الجرائم التقليدية و تتميز عنها، ناهيك عن الجانب الإجرائي الذي يعتبر مجالا خصبا لدراسة الجريمة الإلكترونية، و حتى نتمكن من حصر موضوع الدراسة والقدرة على التحكم فيه تم التركيز على الجوانب الإجرائية المتعلقة بالتحقيق و جمع الأدلة و الجهات التي أسندت لها مهمة التحقيق لإستخلاص الدليل الإلكتروني و حجيته أمام القضاء.

و بما أن إشكالية الدراسة كانت منصبة حول مدى نجاعة إجراءات التحقيق و حجية أدلة الإثبات في مواجهة الجريمة الإلكترونية، أثبت هذا البحث عجز سلطات التحقيق في ظل إجراءات التحقيق التقليدية المعتمدة و قصورها، في جمع و إستخلاص الدليل الإلكتروني نظرا للتقنية و المهارة الفنية و العلمية التي تتطلبها مواجهة هذا النوع من الجرائم، الشيء الذي ألزم المشرع الجنائي على تحديث التشريعات الجنائية بإستحداث إجراءات جديدة تسمح بإستخلاص الدليل الجنائي في البيئة الإفتراضية، على غرار التسرب الإلكتروني، إعتراض المراسلات و المراقبة الإلكترونية..الخ بشكل يمكنه من تقديم الدعم لكافي لسلطات التحقيق لمواجهة الجرائم الإلكترونية و مواكبة تطورها السريع و المستمر مع ضرورة إستحداث هيئات مختصة بالتحقيق في هذا النوع من الجرائم بتدعيمها بأحدث التكنولوجيات و الوسائل التقنية المتطورة يقوم بتسييرها موارد بشرية تمتع بقدرات عالية من التكوين و الكفاءة و التحكم الدقيق في التقنيات الحديثة، ما يسمح لها التحكم و مواجهة الجريمة الإلكترونية في عالمها الإفتراضي و الرقمي إلى جانب العديد من الإشكالات التي تواجه سلطات التحقيق أهمها القيمة القانونية للأدلة الرقمية و مدى قبولها من طرف القاضي و تتجسد هذه القيمة في مشروعية الدليل و حجيته على الوقائع المراد إثباتها.

من خلال هذه الدراسة تم إستخلاص النتائج الآتية:

1- عجز أجهزة التحقيق في مواجهة الجريمة الإلكترونية بالاعتماد على الإجراءات التقليدية المادية للتحقيق و إفتقارها إلى التكنولوجيات الحديثة و الوسائل التقنية المتطورة لمواكبة التطور السريع و الهائل الذي تعرفه الجرائم الإلكترونية.

2- التحقيق الجنائي في مجال الجرائم الإلكترونية يواجه صعوبات متعلقة بشخص المجرم و صعوبة تحديد هويته الإلكترونية و التعرف على عنوانه الإلكتروني بحيث يمكنه التلاعب به و إخفائه بحيث يتمكن بعض المجرمين من حتى إختراق أجهزة أشخاص آخرين لينفذ أعماله الإجرامية انطلاقا من تلك الأجهزة ما يساعد على تظليل أجهزة التحقيق.

3- سلطات التحقيق تفتقر إلى مهارات التحقيق و تقنيات البحث و التحري لعدم إستفادة العنصر البشري من تكوين ذو مستوى و جودة عالية لمواجهة خصائص و مميزات الجرائم الإلكترونية و الدليل الإلكتروني، بإعتباره دليل غير مادي لا يمكن إدراكه بالحواس و يسهل التلاعب به و تغييره و تدميره، كما قد يكون هذا الدليل مشفر يتطلب الإعتماد على برامج معقدة و كلمات سرية تعقد من مهمة سلطات التحقيق من الوصول إليه.

4- إن سعي سلطات التحقيق إلى للوصول لإستخلاص الدليل الإلكتروني بالإعتماد على الإجراءات الحديثة للتحقيق الجنائي قد يؤدي إلى التعسف و إنتهاك الحق في الخصوصية المحمي دستوريا، ما يشكل انتهاك للشرعية الإجرائية بالتالي بطلان إجراءات التحقيق.

5- الأخذ بالدليل الإلكتروني يخضع لتقدير القاضي الجنائي، بحيث يملك الحق في مناقشة الظروف و الملابسات المحيطة بالدليل و له الحق أن يرفضه إن لم يقتنع بظروف و ملابسات القضية، عكس القيمة العلمية القاطعة التي يتميز بها الدليل الإلكتروني فلا يمكن للقاضي الفصل فيها لأنها مسالة فنية تعود لأهل الإختصاص.

6- يعتبر مبدأ حرية الإثبات الجنائي أساس قبول الدليل الإلكتروني في الإثبات الجنائي عند الدول اللاتينية و الكثير من الدول المتأثرة بها على غرار الجزائر و مصر و الإعتماد على سلطة القاضي التقديرية في تقدير و الأخذ بالأدلة العلمية.

7- إن تقنية و لا محدودية الجرائم الإلكترونية خلق مشكل تنازع الإختصاص على المستوى الدولي و هو من بين صعوبات التحقيق التي تواجه التعاون الدولي في التحقيق و التحري في مجال الجرائم الإلكترونية، فالتحقيق في بعض الحالات يلزم الولوج إلى أنظمة معلوماتية متواجدة خارج الدولة المحققة ما يتطلب تعاون و تنسيق دولي حقيقي و جاد بين الدول فيما بينها.

و لتجاوز العقبات و المشكلات المذكورة آنفا ارتأينا أن نقدم جملة من الحلول و الإقتراحات المستوحاة من مختلف الكتب و المؤلفات و الدراسات المنجزة في هذا المجال و التي تم الإعتماد عليها في إعداد هذا البحث و المتمثلة في الأتي:

- على المستوى المحلي:

1- ضرورة تدعيم الترسانة القانونية لمختلف دول العالم لمكافحة الجريمة الإلكترونية و مواجهة التطور السريع الذي تتميز به هذه الأخيرة، ذلك بسن قوانين موضوعية و إجرائية خاصة بهذا النوع من الإجرام، و العمل على تعديل قوانينها الداخلية بما يجعلها تواكب التطور الرهيب الذي تعرفه هذه الجريمة، في عالم تغزو الرقمنة شتى ميادين الحياة لتفادي القصور التشريعي و تخطي الثغرات القانونية القائمة التي قد تسمح للمجرم الإلكتروني من الإفلات من العقاب كما فعل المشرع الجزائري من خلال سنه للقانون رقم (09-04) المتعلق بالقواعد الخاصة من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال و الاعتماد على التقنيات الحديثة لإستخلاص الدليل الإلكتروني على غرار التسرب، إعتراض المراسلات و المراقبة الإلكترونية.

2- ضرورة تكوين القضاة و ممثلي الهيئات النظامية، و إستحداث وحدات أمنية و أجهزة قضائية متخصصة في مكافحة الجريمة الإلكترونية، و إشراك مهندسين و فنيين و مختصين في مجال الإعلام الآلي و الإستفادة من معارفهم و خبراتهم و إطلاعهم على أخر المستجدات في مجال الرقمنة و التقنيات الخاصة بالعالم الإفتراضي، بالتالي إخضاع سلطات التحقيق إلى دورات تكوينية و تدريبية للإمام الكافي بالجوانب التقنية و الفنية لتحسين و تحديث معارفهم في هذا المجال.

3- التركيز على العمل التوعوي و التحسيسي داخل المجتمع بإشراك المجتمع المدني و العمل على الإستخدام الأمثل للتطبيقات الحديثة و إدراك المواطن للمخاطر الناجمة عن الإستخدام الغير مشروع للأنترنت و ما يترتب عنه من إنعكسات سلبية على المستوى النفسي، الاقتصادي و الإجتماعي..الخ، ذلك من خلال برمجت حملات تحسيسية للتوعية من مخاطر الجرائم الإلكترونية خاصة على مستوى المؤسسات التعليمية و الجامعات بتسطير برنامج من طرف وزارة التربية الوطنية و وزارة التعليم العالي و البحث العلمي و حتى إستحداث مواد علمية متخصصة في مجال الرقمنة و إدماجها في البرنامج الدراسي على مستوى المؤسسات التربوية و الجامعات لحث الفئات الشبانية على الإستعمال الإيجابي

لهذا النوع من التكنولوجيا و إستغلالها في الغرض الذي أعدت من أجله إلا و هو مجال البحث العلمي.

4- إستحداث خطوط و قنوات إتصال خضراء من أجل إشراك المواطن و إتاحتهم الفرصة في المشاركة في مكافحة هذا النوع من الجرائم، وتفعيل و ترسيخ ثقافة الإبلاغ في أسرع وقت ممكن بالتالي الكشف المبكر لها و مواجهتها.

5- تفعيل التعاون بين سلطات التحقيق و مزودي خدمة الأنترنت بشكل يسمح تحصيل المعلومات اللازمة في الوقت المناسب لغرض التحقيق بالتالي إستخلاص الدليل الإلكتروني في أسرع وقت ممكن.

6- على المشرع الجزائري الإهتمام و التركيز على الجانب الإجرائي للجرائم الإلكترونية و العمل على إثرائها، لأنها لم تنل حقها بعد من الدراسة و العناية الكافية من طرف الفقهاء و رجال القانون في الجزائر، رغم الإنتشار المخيف و المتزايد لهذا النوع من الجرائم داخل أوساط المجتمع.

7- على المشرع الجزائري تضييق الخناق على المجرم الإلكتروني الذي يستغل مقاهي الأنترنت و إستعمالها كمنطلق لتنفيذ جرائمه، بحيث تعتبر ملاذا آمنا له للتخفي، و ذلك من خلال إستحداث إجراءات جديدة لاستغلال مقاهي الأنترنت كمسك سجلات و دفاتر خاصة لتسجيل هوية الزبون، و رقم جهاز الحاسوب المستعمل، و تاريخ ووقت و مدة الإستعمال و إشتراط تزويد مقاهي الأنترنت بكميرات مراقبة لتسجيل حركة الزبائن و التعرف على المجرم الإلكتروني في حالة إستعماله لهوية مستعارة و الإحتفاظ بهذه البيانات على الأقل لمدة 06 أشهر قصد الرجوع إليها لمقتضيات التحقيق .

8- تأسيسا محاكم خاصة متخصصة في النظر في القضايا المتعلقة بالجرائم الإلكترونية فالتخصص و التكوين في هذا المجال يجعل من القضاة أكثر تحكم في هذا النوع من القضايا و السرعة في الحسم في الدعاوى المطروحة في أروقة العدالة و ما توفره الأجهزة القضائية من جهد و وقت للحسم في هذا النوع من القضايا التي تتطلب مهارات فنية وعلمية و سرعة كبيرة في التنفيذ لمواجهتها.

9- ضرورة عقد ندوات و ملتقيات وطنية و جهوية من طرف مختصين و رجال القانون بصفة دائمة و مستمرة و البحث في مسالة التحقيق و جمع الأدلة في الجرائم الإلكترونية وما يكشفه من غموض و ما يحيط به من صعاب في ظل الإنتشار الهائل و التطور السريع

الذي يعرفه هذا النوع من الجرائم و البحث في تطوير آليات مكافحتها و إقحام جميع الشركاء على غرار السلطة التشريعية و القضائية و مختلف سلطات التحقيق و الضبطية القضائية بغية تدعيم و تكيثف التعاون فيما بينها و توحيد الجهود لمواكبة التطور الرهيب الذي تعرفه هذه الظاهرة الإجرامية.

- على المستوى الدولي:

1- على المجتمع الدولي تكثيف الجهود و التعاون و التنسيق بين الدول بتوحيد القوانين لمكافحة الجرائم الإلكترونية، ذلك بالعمل على إبرام إتفاقيات دولية على غرار إتفاقية بودابست لسنة 2001 لمكافحة الجريمة المعلوماتية، و الإعتماد على سياسة فعالة و موحدة في مجال التعاون الدولي المتبادل و تكريس إجراءات تحقيق و المتابعة بشكل يسمح بالتدخل و التحقيق بشكل متكامل في إقليم دولة أجنبية دون المساس بسيادة هذه الدولة .

2- الإسراع في الإنضمام إلى مختلف الإتفاقيات الدولية الخاصة بمكافحة الجريمة الإلكترونية، و كل ما من شانه تكثيف الجهود على المستوى الدولي و الإقليمي، كإنشاء الدول الإفريقية أو العربية، لأجهزة و هيئات و منظمات تهتم بالتنسيق الأمني في مجال مكافحة الجريمة الإلكترونية و العمل على تطوير كفاءاتها و خبراتها في هذا المجال .

3- بطئ الإجراءات على المستوى الدولي بسبب الأعراف و الطرق الدبلوماسية المعقدة و الطويلة، خاصة في مجال الإنابات القضائية الدولية و تسليم المجرمين، المقيدين بجملة من الشروط ما يعرقل من جهود سلطات التحقيق و يستفيد منه المجرم الإلكتروني الذي يتميز بالسرعة في تنفيذ جرائمه في العالم الإفتراضي اللامتناهي الحدود.

4- الإستفادة من تجارب الدول المتقدمة في مجال مكافحة الجرائم الإلكترونية و التي تملك تقنيات و خبرات علمية جد متقدمة في هذا المجال، ذلك بتفعيل عمل الإستباقي و إستحداث آليات إجرائية وقائية للوقاية من هذه الظاهرة الإجرامية المستحدثة و المخلفات الذي تتركها على جميع الأصعدة، بحيث تعتبر في بعض الحالات تهديدا مباشرا لأمن الدولة كالجرائم المتعلقة بالإرهاب الإلكتروني و التجسس الإلكتروني.

قائمة المراجع

قائمة المراجع

أولا – باللغة العربية :

I.الكتب :

أ- الكتب العامة

1. احمد شوقي شلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، الجزء الثاني، ديوان المطبوعات الجامعية، الجزائر،1999.
2. جيلالي بغدادي ، التحقيق – دراسة مقارنة ، الديوان الوطني للأشغال التربوية ط1 ، 1999 .
3. عبد الله أوهايبية، شرح قانون الإجراءات الجزائية الجزائري، دار هومة، ط 2 الجزائر، 2018.
4. علي حسين الخلف، عبد القادر الشاوي ، المبادئ العامة في قانون العقوبات توزيع المكتبة القانونية ، بغداد.
5. علي محمد جبران آل هادي، ضمانات المتهم في مرحلة التحقيق طبقا لنظام الإجراءات الجزائية السعودي الجديد –دراسة تأصيلية تطبيقية ، مذكرة ماجستير في العدالة الجنائية، تخصص تشريع جنائي إسلامي ، كلية الدراسات العليا جامعة نايف العربية للعلوم الأمنية ، 2004.
6. عمار عباس الحسيني، التحقيق الجنائي و الوسائل الحديثة في كشف الجريمة الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 1999.
7. فخري عبد الرزاق صلبي الحديثي ، شرح قانون العقوبات القسم العام ، الناشر العاتك ، القاهرة .
8. محمد حزيط، مذكرات في قانون الإجراءات الجزائية الجزائري، دار هومه للطباعة و النشر و التوزيع، الجزائر،2007.
9. محمود محمود مصطفى ، شرح قانون العقوبات القسم العام ، مطابع دار الكتاب العربي ، مصر ، ط5 ، 1960-1961.
10. محمود محمود مصطفى، الإثبات في المواد الجنائية،في القانون المقارن،مطبعة جامعة القاهرة،الطبعة الثانية ، 1977.

ب- الكتب المتخصصة:

1. احمد ضياء الدين محمد خليل – مشروعية الدليل في المواد الجنائية – رسالة لنيل الدكتوراه في القانون – كلية حقوق – جامعة عين الشمس –قاهرة
2. احمد يوسف الطحطاوي – الادلة الالكترونية ودورها في الاثبات الجنائي –دار النهضة العربية–القاهرة–2015–
3. احمد يوسف الطحطاوي – الادلة الالكترونية ودورها في الاثبات الجنائي –دار النهضة العربية–القاهرة– 2015
4. اشرف عبد القادر قنديل – الاثبات الجنائي في الجريمة الالكترونية – دار الجامعة الجديدة مصر 2015
5. امير فرح يوسف – القبض و التفتيش – الطبعة الأولى –مكتبة الوفاء القانونية– مصر 2013
6. ايمان محمدة على الجابري – يقين القاضي الجنائي – منشأ ة المعارف الإسكندرية – 2005
7. بكري يوسف بكري، التفتيش عن معلومات في الوسائل التقنية الحديثة، دار الفكر الجامعي، الإسكندرية، 2010.
8. بوبكر رشيدة، جرائم الاعتداء على الأنظمة الإلية للمعطيات في التشريع الجزائري و المقارن، الطبعة الأولى، منشورات الحلبي، بيروت، 2012.
9. جميل عبد الباقي الصغير – ادلة الاثبات الجنائي والتكنولوجية الجديثة –دار النهضة العربية –القاهرة2014
10. حسام محمد نبيل الشنراقي، الجرائم المعلوماتية، دراسة مقارنة على جرائم الاعتداء على التوقيع الالكتروني، دار الكتب القانونية، القاهرة، 2013.
11. حسين طاهري ، الجرائم الإلكترونية ، دار الخلدونية ، ط1 ، 2022.
12. خالد عياد الحلبي، إجراءات التحري و التحقيق في جرائم الحاسوب و الانترنت دار الثقافة للنشر و التوزيع، عمان، 2011.
13. خالد ممدوح ابراهيم – التقاضي الالكتروني – دار الفكر الجامي –مصر–2008 –
14. خالد ممدوح إبراهيم ، أمن الجريمة الإلكترونية ، الدار الجامعية للطباعة و النشر ، الإسكندرية ، 2008

15. خالد ممدوح، فن التحقيق الجنائي في الجرائم الالكترونية، دار الفكر الجامعي 2009.
16. ربيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري و الدولي، دار الهدى الجزائر، 2011.
17. سامي جلال فقي حسين – الادلة المتحصلة من الحاسب وحجتها في الاثبات – دار كتب القانونية –القاهرة–2011
18. سليمان احمد فضيل – المواجهة التشريعية و الامنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية الانترنت –دار النهضة العربية – القاهرة 2008
19. شيماء عبد الغاني محمد عطالله– الحماية الجنائية للتعاملات الالكترونية–دار الجامعة الجديدة الاسكندرية2007–
20. صونية نادية مواسة، مداخلة بعنوان " خصوصية الجريمة المعلوماتية "، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 منشورات دار الخلدونية ، ط1 ،2022.
21. عفيفي كامل عفيفي – جرائم الكمبيوتر وحقوق المؤلف والمنصفات الفنية ودور الشرطة والقانون – دراسة مقارنة– منشورات الحلبي –دمشق 2007–
22. علاء عبد الباسط خلاف– الحماية الجنائية لوسائل الاتصال الحديثة –دار النهضة العربية– القاهرة2002–
23. علي محمود علي حمودة،الأدلة المحصلة من الوسائل الالكترونية في إطار نظرية الإثبات الجنائي، بحث مقدم إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، دبي، الإمارات العربية المتحدة،2003.
24. غنية باطي ، الجريمة الإلكترونية – دراسة مقارنة ، الدار الجزائرية ، الجزائر ، 2016.
25. فتيحة حواس ، جرائم الوسط الرقمي ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022.
26. كمال ديب ، مكافحة الجريمة المعلوماتية في التشريع الجزائري ، الجريمة المعلوماتية و المجرم المعلوماتي : مفهوم جديد للإجرام في البيئة الرقمية ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022.

27. كوثر مازوني ، الجريمة المعلوماتية أعمال ندوة وطنية ، منشورات دار الخلدونية ، ط 1 ، الجزائر ، 2022.

28. محمد الامين البشري– التحقيق في الجرائم المستحدثة – الطبعة الاولي–دار الحامد – الاردن–2014

29. محمد حسين منصور – الاثبات التقليدي و الالكتروني –دار الفكر الجامعي– مصر– 2006 –

30. مروك نصر الدين – محاضرات في الاثبات الجنائي –جزء 01–الطبعة الثالثة–دار هومة–جزائر 2009–

31. ممدوح عبد الحميد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، القاهرة، 2006.

32. ممدوح عبد الحميد عبد المطلب – أدلة الصور الرقمية في الجرائم غير الكمبيوتر – مركز الشرطة دبي 2005–

33. ممدوح عبد الحميد عبد المطلب – البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر ولانترنات – دار الكتب القانونية – مصر 2006 –

34. مناني فراح – أدلة الاثبات الحديثة في القانون –دار الهدى للطباعة والنشر–الجزائر–

35. نبيل اسماعيل عمر– عدم قضاء القاضي بعلمه الشخصي –مجلة العربية للدرسات الامنية– المجلد الاول –العدد الاول –رياض 1989

36. نبيلة هبة هروال، الجوانب الإجرائية للجرائم المعلوماتية، دار الفكر الجامعي، الإسكندرية، 2007.

37. نهلا عبد القادر المومني ، الجرائم المعلوماتية ، ط2 ، دار الثقافة للنشر و التوزيع ، عمان ، 2010.

38. هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، مكتبة الآلات الحديثة، آسيوط، 1999.

39. هلالي عبد الاله احمد، حجية المخرجات الكمبيوترية في المواد الجنائية، دار النهضة العربية، القاهرة، 2003.

40. يزيد بوحليط، الجرائم الالكترونية و الوقاية منها في القانون الجزائري، دار الجامعة الجديدة، الإسكندرية، 2019.

41. علي حسين محمد الطوالبة ، التفتيش الجنائي على نظم الحاسوب و الانترنت ،عالم الكتب الحديقة ، الطبعة الأولى ، 2004 ص02.

II. الرسائل و المذكرات الجامعية

أ- المذكـــرات الجامعية

1) أطروحة الدكتوراه

1. براهيمي جمال، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه، تخصص قانون، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2018.
2. بن يحي إسماعيل، التحقيق الجنائي في الجرائم الالكترونية، أطروحة لنيل شهادة الدكتوراه، تخصص قانون خاص، كلية الحقوق و العلوم السياسية، جامعة أبو بكر بلقايد، تلمسان، 2021.
3. حسين ربيعي ، آليات البحث و التحقيق في الجرائم المعلوماتية ، أطروحة دكتوراه العلوم في الحقوق ، تخصص قانون العقوبات و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة باتنة 1 ، 2015-2016 ، ص ص 182-183 .
4. خالد علي نزال الشعار ، التحقيق الجنائي في الجرائم الإلكترونية ، أطروحة دكتوراه في الحقوق ، كلية الحقوق ، جامعة المنصورة ، 2020.
5. عبد الوهاب ملياني ، أمن المعلومات في البيئة الأعمال الإلكترونية ، أطروحة دكتوراه في القانون العام ، كلية الحقوق و العلوم السياسية ، جامعة أبي بكر بلقايد ، تلمسان ، 2016-2017.
6. عمر محمد أبو بكر بن يونس، أطروحة لنيل شهادة الدكتوراه في القانون، كلية الحقوق، جامعة عين شمس القاهرة، 2004 .
7. فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري و اليمني، أطروحة لنيل شهادة الدكتوراه في القانون، تخصص قانون جنائي و العلوم الجنائية، كلية الحقوق، جامعة الجزائر 1، 2011.

2) مذكرات الماجستير

1. احمد مسعود مريم، آليات مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال في ضوء القانون (09-04)، رسالة لنيل شهادة الماجستير في القانون الجنائي، كلية قاصدي مرباح، ورقلة، 2013.
2. دليلة ليطوش ، **الحماية القانونية للفرد الموقوف للنظر** ، مذكرة لنيل شهادة الماجستير في القانون العام ، فرع قانون العقوبات و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة الإخوة منتوري ، قسنطينة ، 2008-2009.
3. سليمان بن مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة لنيل شهادة الماجستير في العلوم الشرطية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2003.
4. عائشة بن قارة مصطفى، حجية الدليل الالكتروني في مجال الاثبات الجنائي درسة مقارنة، للحصول على درجة الماجيستر في حقوق ، كلية الحقوق جامعة اسكندرية، 2009 .
5. طاهر شريفة – تأثير ادلة على الاقتناع الشخصي للقاضي الجنائي، مذكرة لنيل ماجيستر – كلية الحقوق جامعة الجزائر 2003-

1. مذكرات الماستر

1. احمد مسعود مريم –اليات جرائم تكنولوجيا الاعلام والاتصال في ضوء القانون 03-04 –مذكرة لنيل شهادة الماجيستر – قسم حقوق والعلوم السياسية –جامعة قاصدي –مرياح الجزائر–2013
2. أمال بدرة والي ، المواجهة الإجرائية لجرائم المعلوماتية ، مذكرة الماستر تخصص قانون جنائي، كلية الحقوق و العلوم القانونية، جامعة محمد بوضياف، المسيلة 2018-2019.
3. أمينة بوشعرة – سهام موساوي ، الإطار القانوني للجريمة الإلكترونية – دراسة مقارنة ، مذكرة ماستر في الحقوق تخصص القانون الخاص و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة عبد الرحمان ميرة ، بجاية 2017-2018.
4. حمري سميرة،عاشور رزيقة ،حجية الدليل الالكتروني في الاثبات الجزائي،مذكرة لنيل شهادة الماستر في القتون الجنائي، كلية الحقوق و العلوم السياسية، جامعة مولود معمري تيزي وزو.

5. خالد أمين بن نعوم ، إجراءات التحقيق في الجريمة المعلوماتية في التشريع الجزائري ، مذكرة ماستر ، تخصص قانون قضائي ، كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس ، مستغانم ، 2018- 2019.
6. ريم لغواطي ، مدى فعالية الأقطاب الجزائية المتخصصة في مكافحة الجريمة مذكرة ماستر في الحقوق تخصص القانون الجنائي و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة زيان عاشور الجلفة ، 2019-2020.
7. طاهر شريفة – تأثير ادلة على الاقتناع الشخصي للقاضي الجنائي – مذكرة لنيل ماجيستر – كلية الحقوق جامعة الجزائر 2003
8. عائشة واشك ، أصناف الجريمة الإلكترونية في التشريع الجزائري ، مذكرة ماستر في القانون ، تخصص قانون جنائي و العلوم الجنائية ، كلية الحقوق و العلوم السياسية ، جامعة مولود معمري ، تيزي وزو ، 2015-2016.
9. عبد الناصر محمد محمود غرغليود/ عبيد سيف سعيد المسماري –ورقة بحث مقدمة للمؤتمر العربي الاول للعلوم الادلة الجنائية والطب الشرعي – الاثبات الجنائي بالادلة الرقمية من الناحيتتين القانونية والفنية –دراسة تطبيقية مقارة –الرياض2007
10. على محمود على حموده – الادلة المتحصلة من الوسائل الالكترونية في اطار نظرية الاثبات الجنائي – المؤتمر العلمي حول الجوانب القانونية و الامنية و الامنية للعمليات الالكترونية – منظم المؤتمر اكاديمية شرطة دبي –مركز البحوث والدراسات ع 01–دبي 28 نيسان 2003
11. قدور حسين فاتحة ، دور الشرطة العلمية و التقنية في الكشف عن الجريمة مذكرة ماستر تخصص القانون الخاص ، كلية الحقوق و العلوم السياسية ، جامعة عبد الحميد بن باديس مستغانم ، 2020.
12. محمد بوعمرة – سيدعلي بنينال ، جهاز التحقيق في الجريمة لإلكترونية في التشريع الجزائري ، مذكرة ماستر في العلوم القانونية كلية الحقوق و العلوم السياسية ، جامعة آكلي محند أولحاج ، البويرة ، 2019-2020.
13. يوسف جفال ، التحقيق في الجريمة الإلكترونية ، مذكرة ماستر تخصص قانون جنائي ، كلية الحقوق و العلوم السياسية ، جامعة محمد بوضياف ، المسيلة ، 2016-2017.

III. <u>النصوص القانونية</u>

1) <u>الأوامر</u>

1. الأمر رقم66-155 المؤرخ في 8 جويلية 1966، يتضمن قانون العقوبات المعدل والمتمم بالقانون 20-06 المؤرخ في 28 أفريل2020، ج ر عدد 25 الصادرة بتاريخ 29 أفريل 2020 .
2. الأمر رقم 66-156 المؤرخ في 8 جويلية 1966، يتضمن قانون الإجراءات الجزائية ، ج ر ، ع 48 الصادرة بتاريخ 10 جوان 1966، مم بموجب القانون 19-10 المؤرخ في 11 ديسمبر2019، ج ر ، ع 78 الصادرة بتاريخ 18 ديسمبر 2019 .
3. الأمر 15-02 المؤرخ في 23 يوليو 2015 م م للأمر رقم 66-155 المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية، ج ر، ع 40 الصادرة بتاريخ 23 يوليو 2015،
4. الأمر رقم 21-11 المؤرخ في 25-08-2021 ، يتمم الأمر 66-155 المؤرخ في 8 يونيو 1966 و المتضمن قانون الإجراءات الجزائية ، ج ر ، ع 65 ، الصادرة بتاريخ 26 أوت 2021 .

2) <u>القوانين</u>

1. القانون رقم 09-04 المؤرخ في 5 غشت 2009 ، **يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها** ، ج ر ، ع 47 ، الصادرة بتاريخ 16 غشت 2009
2. القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 ، م م ، للأمر رقم 66-155 المؤرخ في 8 يونيو 1966 ، **و المتضمن قانون الإجراءات الجزائية** ، ج ر ، ع 84 ، الصادرة بتاريخ 24 ديسمبر 2006 .
3. القانون رقم 06-22 المؤرخ في 29 ذي القعدة 1427، الموافق لـ 20 ديسمبر 2006 الصادر بالجريدة الرسمية العدد 84 المؤرخة في : 24 ديسمبر 2006 يعدل و يتمم الامر 66-155 المؤرخ في 18 صفر 1386 الموافق لـ 0 جوان 1966 المتضمن قانون الإجراءات الجزائية.

4. القانون رقم 18-07 المؤرخ في 29 رمضان 1439 الموافق لـ 10 جوان 2018 الصادر الجريدة الرسمية العدد 34، يتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.
5. القانون رقم 06-01 المؤرخ في 2006/02/20، يتعلق بالوقاية من الفساد ومكافحته، الجريدة الرسمية العدد 14، الصادرة بتاريخ: 2006/03/08 .

3) المراسيم

1. المرسوم الرئاسي رقم 15-261 المؤرخ في 8 أكتوبر 2015 ، المحدد لتشكيلة وتنظيم و كيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، ج ر ، ع 53 ، الصادرة بتاريخ 8 أكتوبر 2015.
2. المرسوم الرئاسي رقم 04-432 المؤرخ في 29 ديسمبر 2004 يتضمن إنشاء المعهد الوطني للبحث في علم التحقيق الجنائي ، ج ر ، ع 84 الصادرة بتاريخ 29 ديسمبر 2004 .
3. المرسوم الرئاسي رقم 14-252 المؤرخ في 8 سبتمبر 2014 ، يتضمن التصديق على لاتفاقية العربية لمكافحة جرائم تقنية المعلومات ، المحررة بالقاهرة بتاريخ 21 ديسمبر 2010 ، ج ر ، ع 57 ، الصادرة بتاريخ 28 سبتمبر 2014 .
4. المرسوم الرئاسي رقم 20-442 مؤرخ في 30 ديسمبر 2020 يتعلق بإصدار التعديل الدستوري ، المصادق عليه في استفتاء أوّل نوفمبر 2020 ، في الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، ج ر ع 82 الصادرة بتاريخ 30 ديسمبر 2020
5. المرسوم الرئاسي رقم 20-05 المؤرخ في 20 جانفي 2020 ، المتعلق بوضع منظومة وطنية لأمن لأنظمة المعلوماتية ، ج ر ، ع 4 ، الصادرة بتاريخ 26 جانفي 2020 .
6. المرسوم التنفيذي رقم 16-267 المؤرخ في 17 أكتوبر 2016 ، يعدل و يتمم المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 ، و المتضمن تمديد الإختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق ، ج ر ، ع 62 ، الصارة بتاريخ 23 أكتوبر 2016
7. المرسوم التنفيذي رقم 06-348 المؤرخ في 5 أكتوبر 2006 المتضمن تمديد الاختصاص المحلي لبعض المحاكم و وكلاء الجمهورية و قضاة التحقيق، ج ر ، ع 63 ، الصادرة بتاريخ 8 أكتوبر 2006 .

4) القرارات

1. قرار وزاري مشترك بين وزارة الداخلية والمالية مؤرخ في 2011/6/12 يحدد كيفيات التكفل بمصاريف التغذية و النظافة البدنية للأشخاص الموقوفين تحت النظر داخل مقرات الأمن الوطني، ج ر ،ع 36 ،الصادرة في 2011/6/29 .
2. قرار وزاري مشترك مؤرخ في 14 أبريل 2007 ، المتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبث في علم التحقيق الجنائي، ج ر، ع 36، الصادرة بتاريخ 3 يونيو 2007.

5) الاتفاقيات الدولية

1. اتفاقية بودابست المتعلقة بمكافحة الجريمة المعلوماتية، المنعقدة ببودابست، في 23 نوفمبر 2001.
2. الاتفاقية الأوربية حول الجريمة الالكترونية لعام 2001.

IV.<u>المجلات و المداخلات</u>

1. أمنة بوزينة أمحمدي ، إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية ، مداخلة في ملتقى وطني بعنوان " آليات مكافحة الجرائم الإلكترونية في التشريع الجزائري" ، مركز جيل البحث العلمي بالجزائر العاصمة، المنعقد يوم 29 مارس 2017 .
2. أمينة عبيشات، الجرائم الإلكترونية بين المواثيق الدولية و التشريعات الوطنية، المجلة الجزائرية للحقوق و العلوم السياسية ، جامعة تيسيمسيلت ، مج 6، ع1 ، جوان 2021 .
3. جمال الدين بوقرة – جمال الدين عنان، القطب الجزائي الوطني لمكافحة الجرائم المتصلة بتكنولوجيا الإعلام والإتصال، مجلة الأستاذ الباحث للدراسات القانونية و السياسية، جامعة المسيلة، مج 7، ع 2، جوان 2022.
4. حسين خليل مطر، إجراءات التحقيق و جمع الأدلة في الجرائم الإلكترونية، المؤتمر العلمي الثالث لكلية القانون تحت شعار " الإصلاح التشريعي طريق نحو الحكومة الرشيدة و مكافحة الفساد" المنعقد بـ 25 و 26 أفريل 2018، الصادر بمجلة الكوفة للعلوم القانونية و السياسية، جامعة الكوفة، العراق ، 2018.
5. حكيمة عز الدين عثماني ، إجراءات التحقيق و التفتيش في الجرائم الماسة بأنظمة الإتصال و المعلوماتية ، مجلة البحوث و الدراسات القانونية و السياسية ، المركز الجامعي تيبازة ، مج 2 ، ع 4 جانفي 2018 .

6. زورو هدى، التسرب كآلية من أساليب التحري في قانون الإجراءات الجزائية الجزائري، مجلة دفاتر السياسة و القانون، العدد 11، كلية الحقوق و العلوم السياسية، جامعة محمد خيظر، بسكرة، 2014.
7. عادل يوسف الشكري ، الحماية الجنائية لبطاقات الدفع الإليكتروني – راسة مقارنة ، مجلة مركز دراسات الكوفة ، العراق ، مج1 ، ع 11 ، 2008 .
8. عبد الصديق شيخ ، الوقاية من الجرائم الإلكترونية في ظل القانون رقم 09-04 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها ، مجلة معالم للدراسات القانونية و السياسية ، المركز الجامعي تيندوف ، مج 4 ، ع 1 ، جوان 2020.
9. عبد القادر فلاح – نادية أيت عبد المالك ، التحقيق الجنائي للجرائم الإلكترونية و إثباتها في التشريع الجزائري ، مجلة الأستاذ الباحث للدراسات القانونية و السياسية ، جامعة المسيلة ، مج 4 ، ع 02 ، جانفي 2020 .
10. علاوة هوام، التسرب كآلية للكشف عن الجرائم في القانون الجزائري، مجلة الفقه و القانون، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر، باتنة، 2012.
11. علي رضوان ، مداخلة بعنوان " الإطار المفاهيمي للجريمة المعلوماتية مفهومها و سمات مرتكبيها و أِكانها " ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 .
12. فتيحة حزام ، حماية الأنظمة الرقمية بين الآليات التقنية و أجهزة الحماية – قراءة في أحكام المرسوم الرئاسي 20-05 ، مجلة الحقوق والعلوم الإنسانية ، جامعة زيان عاشور الجلفة ، مج 13 ، ع 3 ، أكتوبر 2020 .
13. كهينة سلام ، الجريمة المعلوماتية و المجرم المعلوماتي : مفهوم جديد للإجرام في البيئة الرقمية ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 .
14. محمود رعد سعدون – حسن جلوب كاظم ، الجرائم الإلكترونية ، مجلة الدراسات المالية و المصرفية ، الأكاديمية العربية للعلوم المالية و المصرفية ، ع 3 ، العراق ، سبتمبر 2015 .

15. مختارية بوزيدي ، ماهية الجريمة الإلكترونية ، مداخلة في الملتقى الوطني بعنوان آليات مكافحة الجرائم الالكترونية في التشريع الجزائري ، مركز جيل البحث العلمي ، المنعقد يوم 29 مارس 2017 بالجزائر العاصمة .

16. نور الدين حيرش ، مداخلة بعنوان " ماهية الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات في القانون الجزائري " ، مجلة الندوة الوطنية بعنوان الجريمة المعلوماتية ، عدد خاص يوم 12 نوفمبر 2019 ، منشورات دار الخلدونية ، ط1 ،2022 .

ثانيا : المراجع باللغة الأجنبية

I- Thèse de doctorat

1- El chaer nidal , la criminalité informatique devant la justice pénal,thése de doctorat, l'université de Poitiers, 2003

II- REVUES

1. Brigitte Pereira , La lutte contre la cybercriminalité – de l'abondance de la norme à sa perfectibilité , Revue internationale de droit économique , 2016
2. Mohamed Salah Mehdaoui - Fatiha Khelifi , Procedural mechanisms for proving digital crime, Journal of legal and economic research , university of Aflou , V5 , N3 , November 2022
3. Mohamed Chawki ,Essai sur la notion de cybercriminalité , IEHEI , juillet 2006 .

الفهرس