الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي والبحث العلمي

جامعة محمد بوضياف -المسيلة-

كلية الحقوق والعلوم السياسية

قسم الحقوق

ميدان : الحقوق

التخصص: قانون جنائي

مذكرة مكملة لنيل شهادة الماستر أكاديمي

العنوان :

الإثبات في الجريمة الإلكترونية

إعداد الطالبتين:

-لبيبات خولة

- عميرات أميرة

اشراف الدكتور:

داود كمال

لجنـة المناقشـة

الاسم واللقب	الرتبة	الصفة
مقروف محمد	أستاذ محاضر–أ-	رئيسا
د. داود كمال	أستاذ محاضر–أ-	مشرفا ومقررا
برابح السعيد	أستاذ محاضر–أ-	ممتحنا

السنة الجامعية: 2022/2021

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد بوضياف بالمسيلة

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

كلية الحقوق والعلوم السياسية

قسم :.....الحقوق.....

المرجع: القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز البحث

أنا الممضي أدناه،

السيد(ة).....لبيبات حوله.....

الصفة: طالب، أستاذ باحث، باحث دائم.....طالبة.....

الحامل لبطاقة التعريف الوطنية رقم: .....103187323.....

الصادرة بتاريخ .....2017/02/02.....عن دائرة/ بلدية .....العناصر.....

المسجل(ة) بكلية .....الحقوق والعلوم السياسية.....قسم : .....الحقوق.....

والمكلف بانجاز أعمال بحث (مذكرة ماستر، مذكرة ماجيستير، أطروحة دكتوراه) الموسومة بـ :

.....مذكرة ماستر الموسومة بـ الاجرءات الجزائية.....

.....الجريمة الالكترونية.....

.....

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

التاريخ 2022/05/30

إمضاء المعني

الجمهورية الجزائرية الديمقراطية الشعبية
وزارة العدل مجلس قضاء المسيلة
أنا الممضي أسفله لبيبات حوله
أقر بأن رقم التعريف الوطني 103187323
المسلم بتاريخ 2017.02.02
صورة طبق الأصل للأصل

الجمهورية الجزائرية الديمقراطية الشعبية

وزارة التعليم العالي و البحث العلمي

جامعة محمد بوضياف بالمسيلة

جامعة محمد بوضياف - المسيلة
Université Mohamed Boudiaf - M'sila

كلية الحقوق والعلوم السياسية

قسم : الحقوق

المرجع: القرار الوزاري رقم 933 المؤرخ في 28 جويلية 2016 المحدد للقواعد المتعلقة بالوقاية من السرقات العلمية ومكافحتها

تصريح شرفي

خاص بالالتزام بقواعد النزاهة العلمية لانجاز البحث

أنا الممضي أدناه،

السيد(ة) عميراتة أميرة

الصفة: طالب، أستاذ باحث، باحث دائم طالبة

الحامل لبطاقة التعريف الوطنية رقم: 103152792

الصادرة بتاريخ 2017.05.31 عن دائرة/ بلدية بئر قاصد علي

المسجل(ة) بكلية الحقوق والعلوم السياسية قسم : الحقوق

والمكلف بانجاز أعمال بحث (مذكرة ماستر، مذكرة ماجيستير، أطروحة دكتوراه) الموسومة بـ :

مذكرة ماستر الموسومة بـ: الإثبات في الجريمة الإلكترونية

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

التاريخ 2022/05/30

إمضاء المعني

عميراتة أميرة
103152792
بطاقة التعريف رقم
2017.05.31

استمارة معلومات

المعلومات الشخصية:

الاسم: أميرة اللقب: عميران

اسم الأب: الحبيب اسم ولقب الأم: صانع ذهبية .

تاريخ الازدياد: 13 _ 11 _ 1996 مكان الازدياد: بشرفاء سد علي

رقم الهاتف: 06,76,24.90,74

البريد الالكتروني: amiramda610@gmail.com

العنوان الشخصي: حي 30 مسكن العمارة 04, رقم ايباب 30 -

الباكالوريا:

المعدل: 12,38 الشعبة/التخصص: آداب وفلسفة سنة الحصول على شهادة الباكالوريا: 2017

الليسانس:

تخصص الليسانس: قانون خاص الدفعة/ سنة التخرج: 2020 .

الماستر:

تخصص الماستر: قانون جنائي الدفعة/ سنة التخرج: 2022 .

المعدل التراكمي للماستر: (المعدل العام)

الوضعية المهنية:

موظف: ☐ عاطل عن العمل: ☒

في حالة موظف:

وظيف عمومي: قطاع خاص:

المصلحة المستخدمة: اسم المؤسسة / الشركة:

الرتبة في العمل:

الصيغة:

موظف دائم: موظف في إطار عقود: نوع العقد:

امضاء الطالب

استمارة معلومات

المعلومات الشخصية:

الاسم: خولة اللقب: لبيبات

اسم الأب: جمال بسم ولقب الأم: حواهرية فهيمة

تاريخ الازدياد: 1999/10/13 مكان الازدياد: سطيف

رقم الهاتف: 07908886 14

البريد الالكتروني: barakhaoula3@gmail.com

العنوان الشخصي: حي 400 مسكن - العناصر - بوج بوعريريج

الباكالوريا :

المعدل: 12,35 الشعبة/التخصص: آداب وفلسفة سنة الحصول على شهادة الباكالوريا: 2017

الليسانس:

تخصص الليسانس: قانون خاص النفعة/ سنة التخرج: 2020

الماستر:

تخصص الماستر: قانون جنائي الدفعة/ سنة التخرج: 2022

معدل الترتيبي للماستر: (المعدل العام)

الوضعية المهنية:

موظف: ☐ عاطل عن العمل: ☑

في حالة موظف:

وظيف عمومي: قطاع خاص:

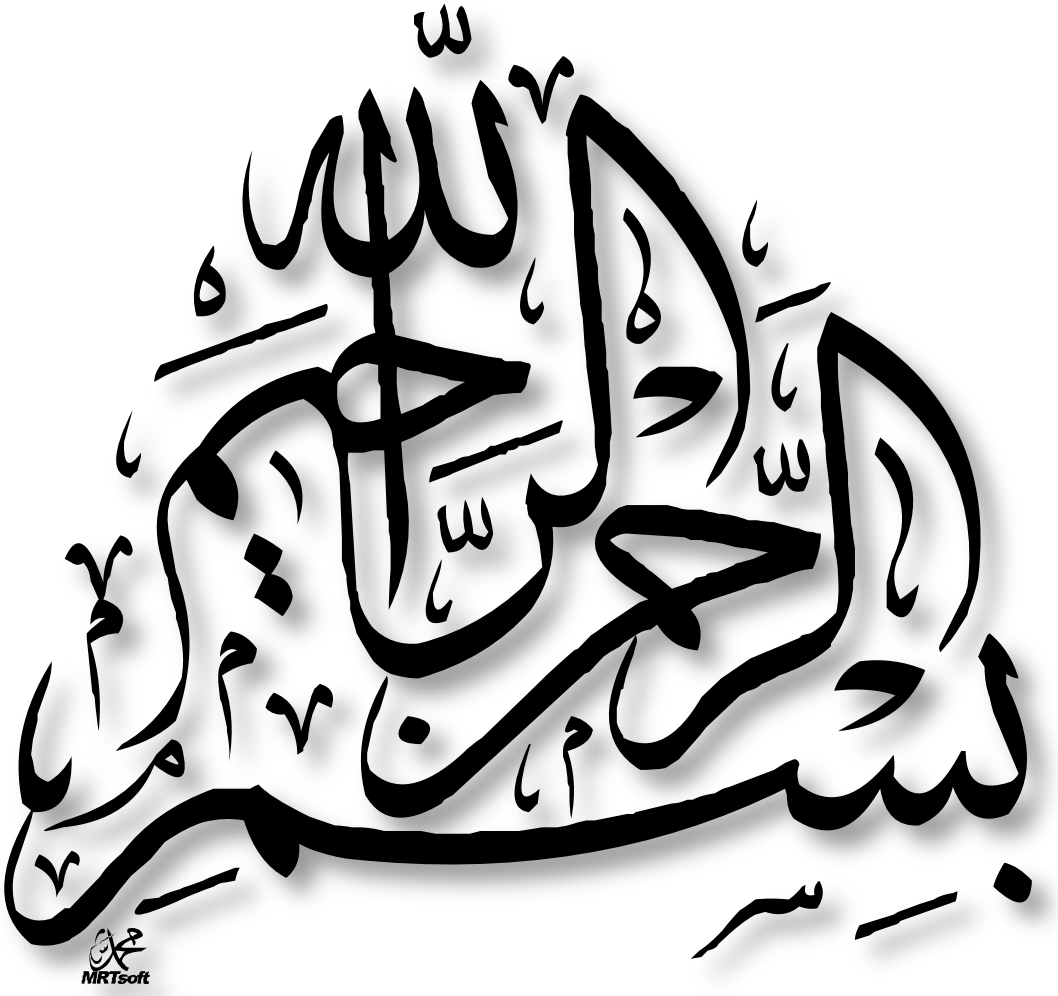
المصلحة المستخدمة: اسم المؤسسة / الشركة:

الرتبة في العمل:

الصيغة:

موظف دائم موظف في إطار عقود: نوع العقد:

امضاء الطالب


بسم الله الرحمن الرحيم
MRTsoft

شكر وعرفان

نتوجه بالحمد والشكر لله تعالى الذي ألهمنا وأعاننا على إتمام بحثنا هذا والذي نأمل أن نكون قد حققنا الغاية المرجوة منه.

كما نخص بالشكر والتقدير والامتنان للأستاذ:

داود كمال

الذي تفضل بالإشراف على هذه الرسالة، والذي أسرنا بسعة أفقه ورحابة صدره وطيب تعامله وتقديم النصح والمشورة طوال فترة إعداد هذه الرسالة.

ولا ننسى أن نشكر كل من قدم لنا يد العون من قريب وبعيد .

الاهداء

الحمد لله والصلاة والسلام علي الحبيب المصطفي وأهله ومن وفى أما بعد:

الحمد لله الذي وفقني لتثمين هذه الخطوة في مسيرتي الدراسية بمذكرتي هذه.

أهدي ثمرة جهدي هذه إلى :

من حصد الأشواك عن دربي ليمهد لي طريق العلم

إلى نبض الفؤاد الذي يدق ليملأ قلبي حبا وقوة

" إلى أمي وأبي "

إلى السند والعضد والساعد " أخي "

إلى من سرنا سويا ونحن نشق الطريق معا نحو النجاح إلى كل أصدقائي وزملائي ومن كانو برفقتي ومصاحبتي أثناء دراستي في الجامعة.

إلى كل من لهم أثر طيب في حياتي، وإلى كل من أحبهم قلبي ونسيهم قلمي

أهديكم تخرجي هذا

شاكرة المولي عز وجل

خولة

الاهداء

إلى الذي علمني رفعة كتبي وأقلامي إلى الذي كان ولا يزال حبه بين الأجساد إلى الذي أرشدني إلى طريقي إلى سندي واتكائي أبي ونور عيني.

إلى التي تعبت وما بالت إلى التي حملت وعانت إلى التي كبرت وما اشتكت إلى أمي الغالية نور حياتي بلسم جروحي .

حفظكما الله وأدام صحتكما وعافيتكما .

إلى مصدر قوتي عند ضعفي إلى الذين آمنو بقدراتي إخوتي وأختي وحيدة دربي.

إلى كل زملائي وزميلاتي وكل من ساعدني من قريب وبعيد.

أميرة

قائمة المختصرات:

ج رج ج: الجريدة الرسمية الجمهورية الجزائرية.

ق ع: قانون عضوي.

ق ع: قانون العقوبات.

ق إ ج ج: قانون الإجراءات الجزائية الجزائري.

د ط: دون طبعة.

د ب ن: دون بلد النشر.

د س ن: دون سنة النشر.

ص: الصفحة.

مقدّمـــة

مقدمة:

تعتبر الجريمة ظاهرة اجتماعية وجدت منذ القدم وتطورت بتطور المجتمع، حيث اتساع نطاقها في العقود الأخيرة من الزمن، لتشمل نوعا آخر متعلق بوسائل الاتصال والمعلومات الذي تجسد أساسا في انتشار أجهزة الحاسب الآلي والتي تطورت بشكل مستمر.

بحيث أصبحت العديد من الدول تعتمد عليها في تسير مرافقها الحيوية كالدفاع والأمن والاقتصاد، كما أن هذه الأخيرة عرفت انتشارا واسعا على المستوي الاجتماعي بحيث أصبح معظم الأفراد يلجؤون إلى استخدام مجموعة من التقنيات الالكترونية في تسيير حياتهم اليومية، كالتواصل وتبادل المعارف عبر شبكة الانترنت في شكل أرقام ورموز الكترونية ويتم ذلك بمجرد كبسة الزر على الحاسب الآلي.

وبفضل هذه القدرة التكنولوجية التي غيرت المجتمعات بشكل جوهري فهي مستمرة في إحداث التغيرات في المجالات الأخرى فبقدر ما حققته هذه التكنولوجيا من فوائد ومزايا هائلة في مجال الرقي والتقدم الإنساني فإنها في الوقت نفسه صاحبتها جملة من الانعكاسات السلبية الخطيرة جراء الاستخدام الغير مشروع لها والانحراف عن الأغراض المتوخاة منها، مما أسفر على ظهور أنماط جديدة من الجرائم لم يكن للإنسان سابق عهد بها أصطلح عليها بالجرائم الالكترونية، فتعد الجرائم الالكترونية من أبرز أنواع الجرائم الجديدة التي يمكن أن تشكل أخطارا جسيمة في ظل العولمة، وفقد أضحت الجريمة الالكترونية أكبر تحدي يواجه رجال القانون والتشريع في العالم أجمع، نظرا لانتشارها في الدول بشكل مفاجئ أو حديث، وأصبحت تشكل خطرا وتهديدا حقيقي لأمن شبكات الإعلام الآلي، بحيث ازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة الانترنت.

إن خطورة هذه الظاهرة الإجرامية المستحدثة، هي أنها سهلة الارتكاب نتيجة للاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، فإن ارتكابها وتنفيذها يستغرق دقائق معلومة بل أحيانا ترتكب في بضع ثواني وأن محو هذه الجريمة وإتلاف أدلة إثباتها غالبا ما يلجأ إليه الجاني عقب ارتكاب الجريمة، فضلا عن مرتكبي هذه الجرائم بالذات يلجؤون إلى تخزين بياناتهم المتعلقة بأنشطتهم الإجرامية في أنظمة الكترونية مع استعمال شفرات ورموز سرية لإخفائها عن الأجهزة المكلفة بالمتابعة .

ولقد كان ظهور الجرائم الالكترونية عاملا حاسما لتدخل المشرع الجزائري في مختلف العديد من الدول بوضع نصوص خاصة، والمشرع الجزائري كغيره من التشريعات المقارنة تصدي لمثل هذه الظواهر ومعاقبة مرتكبيها وفقا لأحكام المادة الأولى من قانون العقوبات الجزائري التي تنص على: "لا جريمة ولا عقوبة ولا تدابير أمن بغير قانون".

ومن أجل مسايرة التشريع لتطورات التكنولوجيا جراء العولمة وأيضا نحتل جزءا من الفضاء الالكتروني، نظم المشرع الجزائري الجريمة الالكترونية ووضع الآليات المختصة بالمتابعة لسد ماكان من فراغ قانوني وللحد منها .

وعلى ضوء ذلك فإن كشف هذا النوع من الجرائم يحتاج إلى طرق الكترونية تتناسب مع طبيعته بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة، تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية، ومن ثم نسبتها إلى فاعليها، وتدعى هذه الوسيلة بالدليل الالكتروني.

وتجدر الإشارة إلى أن تأثير التطور التكنولوجي لا يقف عند مضمون الدليل، إنما يمتد هذا التأثير إلى الإجراءات التي يترتب عليه الحصول على هذا الدليل، ولذلك يجب أن تكون هذه الإجراءات المتطورة ذات طبيعة مشروعة لكي تحافظ على مشروعية الأدلة

المتولدة منها، وبالمقابل من ذلك تعترض عملية استخلاص هذا الدليل إلى جملة من الصعوبات التي تواجه سلطات البحث والتحري للإثبات الجنائي .

أهمية إختيار المضوع :

وتبرز قيمة هذا الموضوع في أن الجريمة الالكترونية تعد من الجرائم الأكثر صعوبة في عملية إثباتها نظرا للطبيعة الخاصة التي تميزها مقارنة بالجرائم التقليدية وكيفية مواجهتها، فالإثبات الجنائي الذي يعتمد على الأدلة الالكترونية يعد من أبرز تطورات العصر الحديث في مجال الإثبات الجنائي في مختلف النظم القانونية، فلم تعد الأنظمة والقواعد التقليدية في إجراءات البحث عن الجريمة والإثبات الجنائي لها تلائم إثبات الجرائم الالكترونية، سواء من الناحية القانونية أم الفنية، مما يستوجب الاعتماد على الدليل الالكتروني الذي يلائم طبيعة هذه الجرائم التي تحتاج إلى نوعية خاصة من أدلة الإثبات.

وتبرز أهمية هذا الموضوع أيضا كونه أن الجرائم الالكترونية من الجرائم المستحدثة والتي هي في تطور مستمر، كما أن أساليب ارتكابها دائمة العمل على مواكبة التطور التكنولوجي الحاصل في ميدان المعلوماتية.

أسباب إختيار الموضوع:

أسباب ذاتية: نظرا لما أحدثته الجريمة الالكترونية من ضجة كبيرة في العالم، وما للموضوع من أهمية بالغة، اخترنا الخوض في هذا الموضوع رغبة منا أن نثري المكتبة القانونية بعمل ولو بسيط .

أسباب موضوعية: إن السبب الرئيسي الذي دفعنا لاختيار موضوع الإثبات في الجريمة الالكترونية كونه من الموضوعات الحديثة التي تعاني من نقص الدراسات كما أنه للتطرق لهذا الموضوع، يتسنى لنا معرفة مدى مواكبة التطور القانوني للتطور التكنولوجي، لأن هذا التطور لم يخلف أثار ايجابية فحسب بل تعدى إلى أبعد من ذلك فقد

استعمل ذلك معظم الأشخاص للقيام بمختلف الجرائم وذلك بالاستعانة بالتقنيات التكنولوجيا الحديثة.

وبناءا على ما سبق كانت إشكالية البحث في التساؤل التالي:

ما هي السبل الكفيلة لإثبات الجريمة الالكترونية ؟

التساؤلات الفرعية:

ما مفهوم الجريمة الالكترونية؟ وماهي خصائصها؟ وماهي أهم تصنيفات التي جاءت بها؟

ماهي ضوابط إثبات الجريمة الالكترونية؟ وما هي معوقات والصعوبات التي تعترض مسألة الإثبات في الجريمة الالكترونية؟

غير أن الهدف الرئيسي من وراء هذه الدراسة هو تسليط الضوء على مفهوم الجريمة الالكترونية من الجانب الفقهي والتشريعي، مع بيان الأدلة العلمية الحديثة والتنبيه على أهمية هذه الأدلة في تحقيق العدالة.

وللإجابة على الإشكالية المطروحة أعلاه ارتئينا إتباع المنهج الوصفي لوصف الجريمة الالكترونية من خلال معرفتها، وكذا المنهج التحليلي من خلال الاعتماد على تحليل القواعد العامة للإجراءات الجنائية.

اقضت طبيعة البحث تقسيمه بعد هذه المقدمة إلى فصلين: أين تطرقنا في الفصل الأول إلى الإطار المفاهيمي للجريمة الالكترونية وتناولنا فيه مبحثين، وكل مبحث يندرج تحته مطلبين.

كما تطرقنا في الفصل الثاني إلى ضوابط الإثبات ومعوقاته في الجريمة الالكترونية ويتضمن أيضا مبحثين، وكل مبحث مقسم إلى مطلبين وفي الأخير ختمنا بحثنا بخاتمة تطرقنا فيها إلى أهم النتائج و التوصيات.

الفصل الأول

الإطار المفاهيمى للجريمة الإلكترونية

الفصل الأول

الإطار المفاهيمى للجريمة الإلكترونية

تعتبر الجريمة الإلكترونية من الجرائم المستحدثة والخطيرة التي لم يكن المجتمع البشري يتوقعها، وذلك لارتباطها بالتطور التكنولوجي الهائل الذي يشهده عالم الكمبيوتر في الآونة الأخيرة وذلك توافقا مع انتقال المجتمعات إلى المجتمع الرقمي أي من الواقع الفعلي (المادي) إلى الواقع الافتراضي، فقد تنامت بسرعة فائقة في ظل الانفتاح العالمي وارتباط الأسواق الدولية ببعضها البعض، فأصبحت هذه الظاهرة الإجرامية تقرع أجراس الخطر لتنبه مجتمعنا عن حجم الخسائر والمخاطر التي تهدد الأفراد في ممتلكاتهم وخصوصياتهم والمؤسسات في كيانها المادي والاقتصادي وحتى المعلومات في أمنها وسيادتها خاصة أنها جرائم ذكية تنشأ في بيئة أإلكترونية (رقمية)، لهذا وجب الإلمام بالجريمة الإلكترونية من حيث مفهومها وخصائصها وتصنيفيها.

وعليه سنقسم الفصل الأول إلى مبحثين: سنتطرق في المبحث الأول إلى ماهية الجريمة الإلكترونية، أما المبحث الثاني سنتطرق إلى تصنيفات الجرائم الإلكترونية.

المبحث الأول: ماهية الجرائم الإلكترونية

لقد عرف رواج الانترنت كوسيلة للاتصالات واستعمالها في جل المعاملات اليومية ظهور سلبيات عديدة، خاصة بعد استغلال الكثير من المجرمين هذا التغير في نمط المعاملات مما أدي إلى ظهور جرائم لم يكن يعرفها القانون من قبل ك الجريمة الإلكترونية بحيث أخذت هذه الظاهرة الإجرامية حيزا كبيرا من الدراسات من أجل تحديد مفهومها، ولهذا قسمنا هذا المبحث إلى مطلبين: سنتطرق إلى مفهوم الجريمة الإلكترونية في (المطلب الأول) ثم خصائص الجريمة الإلكترونية في (المطلب الثاني).

المطلب الأول: مفهوم الجريمة الإلكترونية

نظرا لطبيعة الخاصة للجرائم الإلكترونية، أختلف الفقه في وضع تعريف جامع لها لذلك بذل الفقهاء جهودا ما أجل محاولة وضع تعريف لها حيث ظهر اتجاهان: الاتجاه الأول يعرف بالاتجاه المضيق في تعريفه وهو ما سنتناوله في (الفرع الأول) ويعرف الاتجاه الثاني ب الاتجاه الموسع لها (الفرع الثاني) لنخلص في الأخير إلى تعريف المشرع الجزائري لها في (الفرع الثالث).

الفرع الأول: التعريف الضيق للجريمة الإلكترونية

حاول هذا الاتجاه حصر مفهوم الجريمة الإلكترونية وربطها بعناصر عديدة كالحاسوب أو مستخدمه أو بموضوع الجريمة حيث عرفها الفقيه ماروي (Merwe) على أنها: "الفعل غير مشروع الذي يستخدم في ارتكابه الحاسب الآلي." وهناك من عرفها على أنها: " فعل غير مشروع تكون المعرفة بتقنية المعلومات أساسية لمرتكبه."، وفي تعريف أخر هي: "الأفعال غير القانونية المرتكبة بواسطة العمليات الإلكترونية والتي تمس بالنظام المعلوماتي أو بالمعطيات التي يحتويها ومهما كان الهدف من ذلك"[1].

---

[1] –يزيد بو حليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري (في ضوء الإتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات –قانون الإجراءات الجزائية –قوانين خاصة) دط، دار الجامعة الجديدة للنشر، الإسكندرية، 2019، ص48.

كما عرفت أيضا أنها: "مجموعة الأفعال غير القانونية التي تتم عبر شبكة الانترنت أو تبث عبر محتوياتها"[1].

كما عرفها الفقيه تديمان (Tièdement) بأنها: "كل أشكال السلوك غير المشروع أو الضار بالمجتمع الذي يرتكب باستخدام الحاسب الآلي"[2].

كما عرفها الفقيه روزنبلات (Rosenblatt) بأنها: "نشاط غير مشروع موجه لنسخ أو تغير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو التي تحول عن طريقه "[3].

ويعرفها مكتب تقييم التقنية في الولايات المتحدة الأمريكية من خلال تعريف الحاسب بأنها: "الجرائم التي تلعب فيها البيانات الكومبيوترية والبرامج المعلوماتية دورا رئيسيا "[4].

وعليه يربط أنصار هذا الاتجاه تعريفهم لهذه الجرائم بضرورة وجود الحاسب الذي قد يكون أداة للجريمة أو هدفا لها، ناهيك عن وجود معارف مسبقة بتكنولوجيا الكومبيوتر ليس فقط من المجرم المعلوماتي، وإنما أيضا من القائمين على ملاحقة هذا النوع من الجرائم، وهذا يضيق على نحو كبير من الجريمة الإلكترونية التي هي في اتساع يوما بعد يوم تبعا لتطور تكنولوجيا المعلوماتية[5].

---

(1) –هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أبو بكر بالقايد، تلمسان، 2014/2013، ص2.

(2)–غانم مرضي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها، كيفية التصدي لها قانونا، ط1، دار العلمية الدولية للنشر والتوزيع، عمان، 2016، ص25.

(3)–حسن الطوالبة، الجرائم الإلكترونية، ط1، جامعة العلوم التطبيقية، مملكة البحرين، 2008، ص48.

(4)–أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، 2015، ص93.

(5)–يزيد أبو حليط، المرجع السابق، ص49.

الفرع الثاني: التعريف الموسع للجريمة الإلكترونية

على عكس الاتجاه السابق يذهب فريق من الفقهاء لضرورة التوسيع من مفهوم الجريمة الإلكترونية أو المعلوماتية وعدم حصرها في الحاسوب وحده أو في موضوع الجريمة أو في شخص مستخدمه، وإنما بالتقنية ذاتها المستخدمة في كافة الأجهزة المعلوماتية أو الإلكترونية[1].

فعرفت على أنها: "كل فعل أو امتناع عمدي، ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية يهدف إلى الاعتداء على الأموال أو الأشياء المعنوية "[2].

كما عرفها الأساتذة (Lestanc) و(Vivant) أنها: "مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب."، كما أن الخبير الأمريكي (Parker) تبني مفهوما واسعا للجريمة المعلوماتية على أنها: "كل فعل إجرامي متعمد أيا كانت صلته بالمعلوماتية، ينشأ عنه خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل "[3].

كما عرفتها منظمة التعاون الاقتصادي والتنمية (OCDE) بأنها: "كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية."، كما تعرف أيضا: "تلك الجرائم المرتكبة ضد الأملاك باستعمال التقنية أو المعلوماتية ".

إن هذه التعريفات واسعة تتيح الإحاطة الشاملة قد الإمكان بظاهرة جرائم التقنية، كما أنها تعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، كما أنه يتيح إمكانية التعامل مع التطورات التقنية المستقبلية، ويعرفها آخرون على أنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو

---

[1]–يزيد أبو حليط، المرجع السابق، ص50.

[2]–بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، (دراسة مقارنة)، مذكرة مكملة من مقتضيات نيل شهادة الماستر، كلية الحقوق جامعة محمد خيضر، بسكرة، 2016/2015، ص10.

[3]–نهلا عبد القادر المومني، الجرائم المعلوماتية، ط 1، دار الثقافة للنشر وتوزيع، عمان، 2008، ص49.

بنقلها."، إذ يعتمد هذا التعريف على معيارين: أولهما وصف السلوك، وثانيهما اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها، كما يجمع الفقه الفرنسي بصفة عامة على القول بأن فكرة الغش المعلوماتي (Fraude informatique) التي تعادل جرائم الحاسب الآلي تشمل العديد من الأفعال المتنوعة، حيث عرف كل من الفقيه ميشال (Michel) والفقيه ريدو(Redo) الجريمة المعلوماتية بأنها: "سوء استخدام الحاسب ويشمل الحالات المتعلقة بالولوج غير المصرح به لحاسب المجني عليه أو بياناته، وكذا الاستخدام غير المشروع لبطاقات الائتمان وانتهاك ماكينات الحاسب الآلية بما تتضمنه من شبكات تحويل الحسابات المالية بطرق إلكترونية وتزييف المكونات المادية والمعنوية للحاسب وسرقة الحاسب الآلي في حد ذاته أو أي مكون من مكوناته "[1].

وبذلك تمثل هذه التعاريف المفهوم الموسع للجرائم الإلكترونية، والتي تتم بالحاسوب سواء كان هدفا لها أو وسيلة لارتكابها، أو عن طريق شبكة الإنترنت أو بأي وسيلة إلكترونية أخري تظهر مستقبلا كوسائل الاتصال الحديثة مثل الهاتف النقال وجهاز الفاكس وغيرها[2].

الفرع الثالث: تعريف الجريمة الإلكترونية في التشريع الجزائري

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال وعرفها بموجب أحكام المادة 2 من القانون رقم 09-04 على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، أو أية جريمة أخري ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الإلكترونية "[3].

---

[1] -يزيد أبو حليط، المرجع السابق، ص ص 50 - 51.

[2]- المرجع نفسه، ص51.

[3]-المادة 02من القانون رقم 09-04المؤرخ في 14شعبان عام 1430، الموافق ل 05أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47.

-ويلاحظ من هذا التعريف ما يلي:

أولا: أن المشرع الجزائري اعتمد على معيار الجمع بين عدة معايير لتعريف الجريمة الإلكترونية أولها معيار وسيلة الجريمة وهو نظام الاتصالات الإلكترونية، وثانيها معيار موضوع الجريمة المساس بأنظمة المعالجة الآلية للمعطيات، وثالثها معيار القانون الواجب التطبيق أو الركن الشرعي للجريمة المنصوص عليها في قانون العقوبات.

ثانيا: كما حدد المشرع الجزائري نطاق الجريمة الإلكترونية وذلك عن طريق إقراره بأن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها عليه، وهذا ما يوسع من نطاق مجال الجرائم الإلكترونية في القانون الجزائري[1].

المطلب الثاني: خصائص الجريمة الإلكترونية

تتميز الجريمة الإلكترونية بصفة عامة عن الجريمة التقليدية بجملة من الخصائص والسمات التي تجعلها تنفرد عن غيرها من الجرائم وسوف نحاول أن نبرز أهم هذه الخصائص من خلال تقسيم هذا المطلب إلى 4 فروع مقسمة التالي: سنتناول وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات في (الفرع الأول)، ثم جريمة عابرة للحدود في (الفرع الثاني)، ثم صعوبة اكتشافها وإثباتها في (الفرع الثالث)، ثم أخيرا سرعة التنفيذ وذلك في (الفرع الرابع).

الفرع الأول: وقوع الجريمة في بيئة المعالجة الآلية للبيانات والمعلومات

يشترط لقيام الجريمة المعلوماتية أن يقع التعامل مع بيانات مجمعة ومجهزة للدخول للنظام المعلوماتي، وذلك من أجل معالجتها إلكترونيا، بما يمكن المستخدم من إمكانية تصحيحها أو محوها أو تخزينها واسترجاعها أو طباعتها، وهذه العمليات وثيقة الصلة بارتكاب الجرائم المعلوماتية.

---

[1]- إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد11، سبتمبر، مسيلة، 2018، ص ص 352- 353.

وعلي الرغم من ارتكاب جرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات في الحاسب الآلي (الإدخال-المعالجة –الإخراج)، فإن لكل مرحلة من هذه المراحل نوعية خاصة من الجرائم لا يمكن بالنظر إلى طبيعتها ارتكابها إلا في وقت محدد، ففي مرحلة الإدخال المعلوماتي يمكن إدخال معلومات غير صحيحة، أو عدم إدخال وثائق أساسية، وفي هذه المرحلة وفي مرحلة المعالجة الآلية للبيانات فإنه يمكن إجراء أي تعديلات تحقق الهدف الإجرامي عن طريق التلاعب في برامج الحاسب الآلي، أما في مرحلة المخرجات فقد يقع التلاعب في النتائج التي يخرجها الحاسوب بشأن بيانات صحيحة أدخل فيه وعالجها بطريقة صحيحة.

من المفيد الإشارة أن بعض التشريعات وسعت تعريف المعدات المستخدمة في مجال المعالجة الآلية إلى تلك التي تقوم بالتخزين أو نقل وتلقي بيانات الحاسوب أو المعلومات، ومن الشائع وصف بيانات الحاسوب مثلا: كتمثيل للحقائق والمعلومات التي يمكن قراءتها ومعالجتها أو تخزينها بواسطة الحاسوب[1].

توضح بعض الاتجاهات أن هذا يشمل جهاز الحاسوب والبعض الأخر لم يحدد موقفه لكن من المرجح في الممارسة العلمية أن تتضمن تلك البيانات والمعلومات على وسائط التخزين المادية (مثل الأقراص الصلبة وبطاقات الفلاش للتخزين)، وكذا البيانات والمعلومات المخزنة في نظام بث المعلومات سواء السلكية أو البصرية أو تردد الراديو[2].

الفرع الثاني: جريمة عابرة للحدود

بعد ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة فالمقدرة التي تتمتع بها الحواسيب وشبكاتها في نقل كميات

---

[1] -يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، ط1، مطبعة الرمال، الوادي(الجزائر)، جانفي2019، ص ص 26- 27.

[2] – يعيش تمام شوقي، نفسه، ص ص 27 – 28.

كبيرة من المعلومات وتبادلها بين أنظمة يفصل بينها ألاف الأميال[1]، بمعني أن مسرح الجريمة المعلوماتية لم يعد محليا بل أصبح عالميا إذ إن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد وهو ما يعني عدم التواجد المادي للمجرم المعلوماتي في مكان الجريمة ومن ثم تتباعد المسافات بين الفعل الذي تم من خلال جهاز كمبيوتر الفاعل وبين المعلومات محل الاعتداء، فقد يوجد الجاني في بلد ما ويستطيع الدخول إلى ذاكرة الحاسب الآلي الموجود في بلد أخر وهو بهذا السلوك قد يضر شخص أخر موجود في بلد ثالث[2].

وعليه تعد جرائم المعلومات شكلا جديد من الجرائم العابرة للحدود الوطنية أو الإقليمية أو القارية، وقد خلفت هاته الخاصية الكثير من الإشكالات القانونية في مسألة الاختصاص القضائي[3]، هل هي الدولة التي وقع فيها النشاط الإجرامي أم التي أضيرت مصالحها نتيجة هذا التلاعب، بالإضافة إلى إشكالية مدي فعالية القوانين القائمة في التعامل مع الجريمة المعلوماتية، وبصفة خاصة مسألة جمع الأدلة وقبولها، إذ تتباين مواقف الدول فيما يتعلق بقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية، وغيرها من المشاكل التي يمكن أن تثيرها الجرائم العابرة للوطنية بشكل عام.

لذلك فقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة الجريمة المعلوماتية والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم لمختلف الدول.

---

[1]– يوسف صغير، الجريمة المرتكبة عبر الانترنت، مذكرة لنيل شهادة الماجستير في القانون الخاص، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2013، ص 16.

[2]–نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2013/2012، ص 31.

[3]–يعيش تمام شوقي، المرجع السابق، ص 29.

ومن أجل ذلك فقد تعالت الأصوات الداعية إلى التعاون الدولي المكثف من أجل التصدي لها بحزم، وأن يشمل هذا التعاون تبادل المعلومات وتسليم المجرمين وضمان أن الأدلة التي يتم جمعها في دولة تقبل في محاكم دولة أخري[1].

الفرع الثالث: صعوبة اكتشافها وإثباتها

تتميز الجريمة الالكترونية بصعوبة اكتشافها وإثباتها، وإذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث يبدو من الواضح أن عدد الحالات التي تم فيها اكتشاف هذه الجرائم قليلة إذا قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء صعوبة في اكتشاف الجريمة الالكترونية وإثباتها إلى عدة عوامل منها[2]:

أولا: أن الجريمة الالكترونية لا تترك أثار مادية، فهي جريمة تقع في بيئة الكترونية يتم فيها نقل المعلومات وتداولها بالنبضات الالكترونية ولا توجد مستندات ورقية، فهذه الجريمة عبارة عن أرقام تتغير في السجلات فالجريمة الالكترونية لا تترك شهودا يمكن استجوابهم ولا أدلة يمكن فحصها.

ثانيا: صعوبة الاحتفاظ بدليل الجريمة الالكترونية، إذ يستطيع المجرم في أقل من ثانية أن يمحو أو يحرف أو يغير المعلومات الموجودة في الكمبيوتر[3].

ثالثا: تحتاج الجريمة الالكترونية لاكتشافها إلى خبرة فنية، حيث تتطلب جريمة الكمبيوتر إلمام ومعلومات واسعة سواء لارتكابها أو التحقيق فيها، كما أن رجال الضبطية القضائية يجدون صعوبة للتعامل مع الدليل الالكتروني، فقد يتسبب المحقق دون قصد في إتلاف الدليل الالكتروني أو تدميره كما في حالة محو البيانات الموجودة على الأسطوانة

---

(1) –محمد بوعمرة، سيد على بنيال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة تخرج لنيل شهادة الماستر، كلية الحقوق، جامعة أكلي محند أولحاج، البويرة، 2020/2019، ص ص 8 – 9.

(2) –ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة ماجستير، كلية الدراسات العليا قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012، ص24.

(3) – حسين فريجة، الجرائم الالكترونية والانترنت، مجلة المعلوماتية، العدد36، أكتوبر، 2011، ص 3.

الصلبة أو قد لا يقوم بمصادرة جهاز الكمبيوتر المستخدم في ارتكاب الجريمة أو الطابعة أو الماسح الضوئي، لذلك أصبح من الضروري في وقتنا إجراء دورات تدريبية لرجال الضبطية القضائية ورجال القضاء والخبراء والفنين للتعاون فيما بينهم وصولا إلى أحسن الطرق لمكافحة الجريمة الالكترونية.

رابعا: تعتمد الجريمة الالكترونية على الخداع والذكاء في التعرف على مرتكبيها، إن الذي يساعد على عدم التعرف على مرتكبي الجرائم الالكترونية هو إحجام البنوك والشركات ومؤسسات الأعمال عن الإبلاغ عما يرتكب من جرائم تجنبا للإساءة إلى سمعتها وهز ثقة العملاء بها، وإخفاء أسلوب ارتكاب الجريمة خوفا من قيام الأخريين بتقليد هذا الأسلوب، وهو ما يدفع المجني عليه إلى الإحجام عن إبلاغ السلطات المختصة بها، كما أن الجريمة المعلوماتية تعتمد على الذكاء وهي جريمة فردية تعتمد على مهارات عالية وإلمام بتكنولوجيا النظم المعلوماتية [1].

الفرع الرابع: السرعة في التنفيذ

لا تتطلب جرائم الانترنت عنفا لتنفيذها أو مجهودا كبيرا، فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل أو الاختطاف، أو في صورة الخلع أو الكسر وتقليد المفاتيح كما هو الحال في جريمة السرقة[2].

تتميز جرائم الانترنت بأنها جرائم هادئة بطبيعتها لا تحتاج إلى العنف بل كب ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوي تقني يوظف في ارتكاب الأفعال غير المشروعة، وتحتاج كذلك إلى وجود شبكة المعلومات الدولية (الانترنت) مع وجود مجرم يوظف خبرته أو قدرته على التعامل

---

[1] –حسين فريجة، المرجع السابق، ص3.

[2] –يوسف صغير، المرجع السابق، ص 16.

مع الشبكة للقيام بجرائم مختلفة كالتجسس أو اختراق خصوصيات الغير أو الغرير بالقاصرين, فمن هذا المنطلق تعد الجريمة المرتكبة عبر الانترنت من الجرائم النظيفة فلا أثار فيها لأية عنف أو دماء، وإنما مجرد أرقام وبيانات يتم تغيرها من السجلات المخزونة في ذاكرة الحاسبات الآلية وليس لها أثر خارجي مادي [1].

[1] -يوسف صغير، المرجع السابق، ص 16.

المبحث الثاني: تصنيف الجرائم الالكترونية

تصنف الجريمة التقليدية من حيث خطورته إلى جناية وجنحة ومخالفة، ومن حيث طبيعتها تصنف إلى جريمة عادية وجريمة سياسية، جريمة عسكرية، على خلاف الجريمة الالكترونية التي تعددت تصنيفاتها وذلك لكونها من الجرائم المستحدثة، حيث عرفت اختلافا حول تقسيماتها نظرا للاختلاف في تسميتها، ولعل ما يميز هذه الجريمة عن غيرها من الجرائم كونها تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج....الخ).

والجرائم الالكترونية لا حصر لها ولذلك لا يمكننا أن نجملها بكل أصنافها فهي متشعبة وذلك راجع إلى سرعة تطورها فهناك من صنفها برجوع إلى وسيلة ارتكاب الجريمة أو على أساس محل الجريمة وعلي هذا الأساس قسمنا هذا المبحث إلى مطلبين: سنتطرق إلى الجرائم الواقعة بواسطة النظام المعلوماتية في (المطلب الأول)، ثم الجرائم الواقعة على النظام المعلوماتية والبرامج الالكترونية في (المطلب الثاني).

المطلب الأول: الجرائم الواقعة بواسطة النظام المعلوماتية

يعد النظام المعلوماتية الوسيلة الأساسية لارتكاب هذا النوع من الجرائم ووسيلة لتسهيل النتيجة الإجرامية ومضاعفة لجسامتها وهي أنواع منها الجريمة الواقعة على الأشخاص (الفرع الأول)، ومنها ما هو واقع على الأموال (الفرع الثاني)، والجريمة الأخيرة الواقعة على أمن الدولة (الفرع الثالث)، وهذا ما سنوضحه في النقاط التالية:

الفرع الأول: الجرائم الواقعة على الأشخاص

إن للحياة الشخصية خصوصية وحرمة لا يجوز لأي شخص أن يقتحمها، حيث أن الهدف الأول والاسمي من وضع القوانين هو حماية سلامة الأشخاص من مختلف الانتهاكات التي قد يتعرضون لها سواء في أبدانهم كالقتل أو الجرح أو الضرب أو إعطاء مواد ضارة، كما يمارس بعضها على الجنين في رحم أمه كجريمة الإجهاض ومنها ما يمس عرض الإنسان وحياءه كالاغتصاب[1].

أما فيما يتعلق بالجريمة الالكترونية (المعلوماتية) فهناك العديد من الأفعال تدخل في نطاق هذا النوع من الجرائم والتي تستهدف الأشخاص في حياتهم وتشويه سمعتهم وكذلك التحريض عن القتل عبر الانترنت والتهديد والتحرش والمضايقة عبر وسائل الاتصال والملاحقة عبر وسائل تقنية وأنشطة اختلاس النظر والاطلاع على البيانات الشخصية [2].

وهذا ما سنتطرق إليه في النقاط التالية:

أولا: جرائم القذف والسب

عرف المشرع جريمة القذف في المادة 296من قانون العقوبات الجزائري وعرف السب في المادة 297من نفس القانون كما أن هذه المواد لم تشر إلى الوسيلة الالكترونية لنشر ذلك الإدعاء أو الإسناد[3].

---

[1]– محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص)، ط16، دار النهضة العربية القاهرة، مصر، 1989، ص 317.

[2]– لينا محمد الأسدي، مدي فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، دط، دار حامد، د ب ن، د س ن، ص35.

[3]– تنص المادة 296من قانون العقوبات الجزائري "يعد قذفا كل إدعاء بواقعة من شأنها المساس بشرف واعتبار الأشخاص أو الهيئة المدعي عليها به أو إسنادها إليهم أو إلى تلك الهيئة ويعاقب على نشر هذا الإدعاء أو ذلك الإسناد مباشرة أو بطريق إعادة النشر حتى ولو تم ذلك على وجه التشكيك أو إذا قصد به شخص أو هيئة دون ذكر الاسم ولكن كان من الممكن تحديدهما من عبارات الحديث أو الصياح أو التهديد أو الكتابة أو المنشورات أو اللافتات أو الإعلانات موضوع الجريمة "، وتنص المادة 297من نفس القانون على "يعد سبا كل تعبير مشين أو عبارة تتضمن تحقيرا أو قدحا لا ينطوي على إسناد أية واقعة ".

تعتبر جريمة القذف والسب من أكثر الجرائم شيوعا عبر شبكة الانترنت حيث توجد هناك مواقع متخصصة تعمل على إبراز سلبيات الشخص المستهدف وإفشاء أسراره[1]، من أجل تشويه شرفه وسمعته.

وتعتبر شبكة الانترنت مسرحا غير محدود لارتكاب تلك الجرائم، وتتم وجاهيا عبر خطوط الاتصال المباشر أو يكون كتابيا، وذلك عبر المبادلات الالكترونية (بريد الكتروني، صفحات الويب، غرف المحادثة)[2].

وهنا لابد من القول أن الجاني في مثل هذه الجرائم غالبا ما يستعمل البرامج التي تساعده على إخفاء هويته أثناء القيام بمثل هذه الأفعال عند إرسال البريد أو تصفح المواقع، الهدف من ذلك هو الخوف من تعرضهم للمساءلة القانونية أو الخجل من التصرفات الغير لائقة التي يقومون بها [3].

وفي المادة 144 مكرر والمادة 146 من قانون العقوبات نجد أن القذف والسب الموجه لرئيس الجمهورية أو الهيئات سواء قضائية أو أمنية أو أي هيئة أخري قد تكون بأية آلية لبث الصورة أو الصوت أو بأي وسيلة الكترونية أو معلوماتية أو إعلامية أخري.

ثانيا: جرائم الاعتداء على حرمة الحياة الخاصة

تعد فكرة الحياة الخاصة مسألة دقيقة جدا، وذلك لأنها تحكمها معايير المجتمع وعاداته وتقاليده.

---

[1]– حكيمة شريد، مايسة ربيع، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2016، ص 22.

[2]– عبد الرحمن بن عبد الله السند، الأحكام الفقهية لتعاملات الالكترونية الحاسب الألي وشبكة المعلومات (الانترنت)، ط1، دار الوراق لطباعة والنشر والتوزيع، بيروت، 2004، ص312

[3]– لينا محمد لأسدي، المرجع السابق، ص 37.

وعلى هذا فإن جريمة الاعتداء على حرمة الحياة الخاصة في مجال المعلوماتية هي كل اعتداء على البيانات الاسمية عبر الانترنت وذلك عن طريق التمركز في موقع معين داخل شبكة الانترنت والعمل على تسجيل وحفظ البيانات المتبادلة فيما بين الأنظمة المعلوماتية [1].

ثالثا: جريمة التهديد

وهي التي يتم من خلالها إرسال بعض الصور أو الكتابات غلي الشخص المراد تهديده أو ابتزازه بغية حمله على القيام بفعل معين أو منعه من القيام به[2]، ويتم إرسال مثل هذه الكتابات إلى البريد الالكتروني أو في وسائل الحوارات الآنية المختلفة على شبكة الانترنت مثل الفايسبوك والواتساب....الخ

رابعا: انتحال الشخصية

تعني هذه الجريمة استخدام شخصية شخص أخر للاستفادة من سمعته أو ماله أو صلاحياته، وتتخذ جريمة انتحال الشخصية عبر الانترنت أحد الأسلوبين: إما انتحال شخصية الفرد أو انتحال شخصية المواقع، من أجل تحقيق أغراض ومصالح غالبا ما تكون الاستفادة منها بشكل مادي بطريقة ذكية تجعل من الصعب اكتشاف الفاعل[3].

الفرع الثاني: الجرائم الواقعة على الأموال

إذا كان قانون العقوبات الجزائري شأنه شأن كل القوانين العقوبات الأخرى قد جرم الاعتداء على الأموال في صورها التقليدية كالسرقة والنصب، خيانة الأمانة، واختلاس الأموال العامة، فقد كان ذلك في ظل عصر لا يعرف سوي النقود الورقية أو المعدنية وما يحل محلها من الصكوك والأوراق المالية كالسفتجة والشيك...إلخ.

---

[1]– يرمش مراد، خصوصية الجريمة الالكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر1، 2021/2020، ص 72.

[2]– لينا محمد الأسدي، المرجع السابق، ص45.

[3]– حكيمة شريد، مايسة ربيع، المرجع السابق، ص 23.

ونظرا لتطور التقني والتكنولوجي في الوسائل المستخدمة في الاعتداءات عبر الانترنت، أصبحت معظم المعاملات التجارية تتم من خلالها مثل البيع والشراء، مما انجر عنه تطور وسائل الدفع والوفاء وأصبحت جزء لا يتجزأ من هذه المعاملات، في خصم هذا التداول المالي عبر الانترنت، حيث انتهز بعض المجرمين الفرصة من أجل السطو عليها، فابتكرت عدة طرق من أجل ذلك كالسرقة والتحويل الالكتروني الغير المشروع للأموال والغسيل المعلوماتي[1]، وهناك عدة جرائم تندرج تحتها لعل أهمها:

أولا: جريمة غسيل الأموال عبر الانترنت

إن جريمة غسيل الأموال هي من الجرائم المعاصرة وتعتبر من أخطر جرائم عصر الاقتصاد الرقمي[2]، فالسبب الذي أدي إلى ارتكاب مثل هذه الجريمة (غسيل الأموال)عبر هذه الوسائل المستحدثة، هي السرعة وإغفال التوقيع وانعدام الحواجز الحدودية بين الدول، كما أن البطاقات الذكية والتي تشابه بطاقات البنوك التي تستخدم في مكان الصرف الآلية، تساعد على تحويل الأموال بواسطة المودم أو الانترنت مع ضمان تشفير وأمان العملية[3].

وهذا ما جعل عملية غسل الأموال عبر الوسائل التقنية خاصة عبر شبكة الويب العالمية، تتم بسرعة ودون أن تترك أي أثار في الغالب[4].

ثانيا: جريمة الإتلاف المعلوماتي

الإتلاف هو تخريب الشيء محل الجريمة وذلك بإتلافه أو التقليل من قيمته مما يجعله غير صالح للاستعمال أو تعطيله [5].

---

(1) –إسمهان بوضياف، المرجع السابق، ص 358.

(2) –خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، د ط، دار الفكر الجامعي، الإسكندرية، 2018، ص 452.

(3) – لينا محمد الأسدي، المرجع السابق، ص 51.

(4) –عبد الفتاح بيومي حجازي، جريمة غسيل الأموال بين الوسائط الالكترونية، د ط، دار الفكر الجامعي، الإسكندرية، 2007، ص 17.

(5) –خالد ممدوح إبراهيم، المرجع السابق، ص 416.

وجريمة إتلاف المعلومات تتخذ إما صورة إجراء تعديلات غير مشروعة لها أو تدميرها أو الإدخال غير مشروع للمعلومات داخل أنظمة الحاسبات الآلية وهذا الجاني يكون على دراية وعلم بأن الأموال التي يتعدي عليها ب الإتلاف ملك للغير وأن فعله من شأنه أن يتلف الشيء أو يجعله معطل أو يجعله غير صالح للاستعمال أو ينقص من قيمته[1].

ثالثا: التلاعب بالبطاقة المالية

لقد ظهرت أولي هذا النوع من الاحتيال بالتقاط الأرقام السرية لبطاقات الائتمان وبطاقات الوفاء المختلفة من أجهزة الصرف الآلي للنقود إلى أن ظهرت الصرافة الآلية، أما جرائم الاعتداء على هذه البطاقات فتتمثل في استخدامها من قبل غير صاحب الحق بعد سرقتها أو بعد سرقة الأرقام السرية الخاصة بها وهو ما يتم عن طريق اختراق بعض المواقع التجارية التي يمكن أن تسجل عليها أرقام هذه البطاقات وفي هذا النوع من الاعتداءات لا نجد صعوبة في تطبيق نصوص جرائم السرقة والنصب عليها سواء تم ذلك عن طريق سرقة البطاقة نفسها، أو عن طريق سرقة الرقم السري واستخدامه استخدام غير مشروع.[2]

رابعا: جريمة الاحتيال الالكتروني

الاحتيال المعلوماتي أو الغش المعلوماتي هي كل فعل أو مجموعة من الأفعال غير المشروعة والمعتمدة التي ترتكب بهدف الخداع أو التحريف للحصول على شي ذي قيمة ويكون نظام الحاسوب لازما لارتكابها أو إخفائها[3].

---

[1] – خالد ممدوح إبراهيم، المرجع السابق، ص420.

[2] – عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، مذكرة لنيل الماجستير، جامعة الشرق الأوسط، الأردن، 2014، ص 2.

[3] –بشري عواطة، حجية الدليل الالكتروني في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق، جامعة 08 ماي 1945، قالمة، 2018/2017، ص 21.

وقد يسعي البعض إلى استغلال المعلومات للحصول على كسب مادي غير مشروع، من خلال الدخول إلى معطيات الحاسوب والتلاعب بها وتحويل الأموال إلى حسابه الخاص مما يسبب الضرر للأخرين[1].

فجرائم الاحتيال تنصب على معطيات الحاسوب المخزنة فيه من أجل الحصول على الأموال أو الخدمات، حيث تتم بالتلاعب وفق الدلالة التقنية الواسعة بمعطيات الحاسوب المخزنة أو نظام المعالجة الآلية [2].

الفرع الثالث: الجرائم الواقعة على أمن الدولة

إن التقدم الهائل في الوسائل الالكترونية واستخدام الانترنت وانتشارها الواسع سمحت لبعض الجماعات المتطرفة بنشر وبث معتقداتهم وأفكارهم، بل تعدي الأمر إلى ممارسات تهدد أمن الدولة خاصة المتمثلة في الإرهاب والجريمة المنظمة، اللذان أخذا طريق أخر لاستخدام النظام المعلوماتي حيث سمحت لهم بارتكاب جرائم في غاية الخطورة بحق المجتمعات والدول، بل الأخطر من هذا سمح للكثير من الدول معرفة أسرار الدولة كأسرارها العسكرية والاقتصادية لممارسة ما يسمي بالتجسس[3]، وسنطرح بعض الجرائم التي تمس بأمن الدولة في النقاط التالية:

أولا: الإرهاب

تعد جريمة الإرهاب من الجرائم البالغة الخطورة التي تواجه العالم بأسره، فهو يرتبط بعوامل اجتماعية وثقافية وسياسية وتكنولوجية، حيث أصبحت هذه الأخيرة أحد العوامل الإستراتيجية التي تمكن التنظيمات الإرهابية وأنصارها من استخدام الانترنت

---

[1] – خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، د ط، دار الثقافة للنشر والتوزيع، الشرق الأوسط، الأردن، 2011، ص99.

[2] –المرجع نفسه، ص 101.

[3] –إسمهان بوضياف، المرجع السابق، ص358.

استخداما متزايدا في مجموعة واسعة ومتنوعة الأغراض، تشمل التجنيد والتمويل، والدعاية والتحريض على ارتكاب أعمال إرهابية[1].

حيث أصبح الإرهاب يستخدم الانترنت كثيرا لبث دعايتهم، وعادة ما تتخذ الدعاية شكل اتصالات عبر وسائط متعددة تحمل تعاليم إيديولوجية وإرشادات عملية، أو تقدم شروع للأنشطة الإرهابية أو تسوق المبررات لها أو تشجع على القيام بها، ومن بين ما يمكن أن تتضمنه هذه الاتصالات والرسائل الافتراضية والعروض الإيضاحية والمجلات والأطروحات، وملفات صوتية ومرئية، وألعاب الفيديو التي تصممها التنظيمات الإرهابية أو يصممها المتعاطفون معها[2].

ثانيا: جريمة التجسس

تعتبر جريمة التجسس من أذكي الجرائم وأدهاها مقارنة بتلك الواقعة على أمن الدولة الخارجي، وازدادت ظاهرة التجسس خطورة في العصر الحالي نظرا لتزايد الوسائل وتطورها، فالتجسس هو الإطلاع على المعلومات الخاصة بالغير المؤمنة وليس مسموحا لغير المخولين بالإطلاع عليها[3].

فالفاعل يسعي إلى كشف الأسرار أو معناها أو جهتها أو صاحبها أو قيمتها المهم أن تتمتع تلك المعلومات بخاصية الإخفاء.

فالتجسس المعلوماتي لا يشمل مجال واحد بل هو متعدد المجالات وأوجه النشطات المختلفة، حيث يمكننا القول عنه أنه أصبح يشمل الجوانب الصناعية والتجارية للمؤسسات الاقتصادية كما يشمل الجوانب المتعلقة بالجانب العسكري والأمني للدولة[4].

---

(1) – مكتب الامم المتحدة المعني بالمخدرات والجريمة UNODC بفيينا، استخدام الانترنت في أغراض ارهابية، الامم المتحدة نيويورك، 2013، ص 3.

(2) –المرجع نفسه، ص3

(3) –محمد عبد الرحيم، سلطان العلماء، جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، المجلد3، ط3، كلية الشريعة والقانون، جامعة الإمارت العربية المتحدة، 2004، ص880.

(4) –نهلا عبد القادر المومني، المرجع السابق، ص 209.

كما تمارس العديد من الدول التجسس المعلوماتي حيث تمارس من قبل دولة على دولة أخري، أو من قبل دولة على مواطنيها، أو من قبل شركة على شركة منافسة.

ثالثا: الجريمة المنظمة

تعرف الجريمة المنظمة بأنها تعبير عن المجتمع الإجرامي يعمل خارج إطار الشعب والحكومة ويضم بين طياته ألاف المجرمين الذين يعملون وفقا لنظام بالغ الدقة والتعقيد يفوق النظم التي تتبعها أكثر المؤسسات تطورا وتقدما، كما يخضع أفرادها لقواعد قانونية سنوها لأنفسهم وترفض أحكام بالغة القسوة على من يخرج من نظام الجماعة ويلتزمون في أداء أنشطتهم الإجرامية بخطط دقيقة مدروسة حيث يجنون من وراءها أموال طائلة.

فالجريمة المنظمة وبسبب تقدم وسائل الاتصال والتكنولوجيا، أصبحت غير محددة لا بقيود الزمان ولا بقيود المكان، بل أصبح انتشارها على نطاق واسع وكبير وأصبحت لا تحدها الحدود الجغرافية[1].

المطلب الثاني: الجرائم الواقعة على النظام المعلوماتية والبرامج الالكترونية

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام المعلوماتية هناك نوع أخر من الجرائم المعلوماتية يمس النظام المعلوماتية ويستهدف إما المكونات المادية للنظام المعلوماتية أو المكونات المنطقية أو المعلومات المدرجة بالنظام المعلوماتية[2].

وهذا ما سنتطرق إليه بشي من التفصيل في النقاط التالية:

الفرع الأول: الجرائم الواقعة على المكونات المادية للنظام المعلوماتية

يقصد بالمكونات المادية للنظام المعلوماتية الأجهزة والمعدات الملحقة به والتي تستخدم في تشغيله كالأسطوانات والشرائط والكابلات...الخ، ونتيجة للطبيعة المادية لهذه المكونات ف الاعتداء عليها يكون عن طريق جرائم عادية وتقليدية، كأن تكون محلا

---

(1) – نهلا عبد القادر المومني، المرجع السابق، ص 87.

(2) –إسمهان بوضياف، المرجع السابق، ص 358.

للسرقة أو خيانة الأمانة أو الإتلاف العمدي كإحراقها أو ضرب الآلات بشيء ثقيل أو حاد أو العبث بمفاتيح التشغيل أو خربشة الشريط وإفساد أسطوانات التشغيل مغناطيسيا بتعريضها إلى أي مجال مغناطيس متلف، ويترتب على هذا الإتلاف خسائر كبيرة[1].

الفرع الثاني: استغلال نظم المعلومات كمحور أساسي في الجريمة الالكترونية

تستلزم هذه الطائفة من الجرائم المعلوماتية معرفة فنية عالية في مجال البرمجة، حيث يتمثل هذا الأسلوب في تدمير البرامج من خلال التسلل إلى المواقع وبث الفيروسات أو البرامج المخربة التي تمحو البيانات وتعرقل سير العمل، وتؤدي إلى خسائر اقتصادية فادحة، ولعل أهمها الاختراق واستعمال البرامج الخبيثة (فيروس Virus)، والجرائم الواقعة على برامج التشغيل[2].

أولا: الاختراق

يتحقق هذا بولوج شخص غير مخول له الدخول إلى نظام الكومبيوتر والقيام بأنشطة غير مصرح له بها كتعديل البرمجيات التطبيقية وسرقة البيانات السرية أو تدمير الملفات أو البرمجيات أو النظام أو لمجرد الاستخدام الغير مشروع، ويتحقق الاقتحام بشكل تقليدي من خلال أنشطة (الاختراق والتخفي)، ويراد به تظاهر الشخص المخترق بأنه شخص أخر مصرح له بالدخول، أو من خلال استغلال نقاط ضعف في النظام إجراءات السيطرة والحماية أو من خلال المعلومات التي يجمعها الشخص المخترق من مصادر مادية ومعنوية، كالتنقيب في قمامة المنشأة للحصول على كلمة السر أو معلومات عن النظام[3]، حيث تنص المادة 394 مكرر من ق ع "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1)

---

(1) –إسمهان بوضياف، المرجع السابق، ص 358.

(2) –بن طالب ليندا، الدليل الالكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتورا، كلية الحقوق، جامعة مولود معمري، ، تيزي وزو، 2019، ص24.

(3) –خالد عياد الحلبي، المرجع السابق، ص51.

وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من المنظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة أذا ترتب على ذلك حذف أو تغير لمعطيات المنظومة.

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام الاشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين(2) والغرامة من 50.000 دج إلى 150.000 دج "[1].

ومن أهم أساليب الاختراق ما يلي:

1-الاختراق عن طريق استعمال نظام التشغيل: لأن نظم التشغيل مليئة ب الثغرات، فإنه يتم استغلالها في عملية الاختراق ولكن الأهم هو القيام بذلك عن طريق البروتوكولات التي يستخدمها النظام للتعامل مع شبكة الانترنت أو الشبكات الداخلية بأنواعها[2].

2-الاختراق باستخدام البرامج: لابد لقيام الاختراق بهذه الطريقة من وجود برنامجين، أحدهما بجهاز الضحية ويسمى بالبرنامج الخادم server لأنه بمثابة الخادم الذي يتأثر ب أوامر المخترع وينفذ المهام الموكلة إليه داخل جهاز الضحية، وثانيهما برنامج يوجد بجهاز المخترق ويسمى ببرنامج المستفيد العميل client، وأشهر مثال على هذه البرامج وأخطرها هو برنامج حصان طروادة[3].

3- المسح والنسخ: هو أسلوب يستخدم فيه برنامج الماسح وهو برنامج احتمالات يقوم على فكرة تغير وتركيب أو تبديل احتمالات المعلومة، ويستخدم تحديثا بشأن

---

[1] -المادة 394 مكرر من الأمر رقم 156/66 المؤرخ في 18 صفر عام 1386، الموافق ل 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، ج ر، العدد 37.

[2] -محمد خليفة، الحماية الجنائية لمعطيات الحاسب الألي، د ط، دار الجامعة الجديدة للنشر، الإسكندرية، 2007، ص 42.

[3] -المرجع نفسه، ص42.

احتمالات كلمة السر أو رقم الهاتف الموزع أو نحو ذلك، ومن جديد فإن هذا الأسلوب تقني يعتمد واسطة تقنية هي برنامج الماسح بدلا من اعتماد على التخمين البشري[1].

ثانيا: البرامج الخبيثة (Les virus)

تعد الفيروسات بمثابة المرض المعدي الذي يصيب المعطيات فيقضي عليها أو يشوهها فتذهب في كلتا الحالتين بفائدتها، وفيروس الحاسب الآلي يشبه إلى حد كبير الفيروس الذي يصيب الإنسان لقدرته على الانتقال من حاسب إلى أخر فهو برنامج مثل أي برنامج أخر موجود على جهاز الحاسب الآلي يصمم بشكل يجعل منه قادر على نسخ نفسه إلى نسخ كثيرة والانتشار من نظام لأخر عبر شبكات الاتصال والقدرة على الاختفاء داخل برنامج سليم بحيث يصعب اكتشافه، كما انه قد يكون مصمما لتدمير برامج أخري أو تغير معلومات ثم يقوم بتدمير نفسه ذاتيا دون أن يترك أي أثر يدل عليه، فبمجرد فتح البرنامج الحامل للفيروس أو الرسائل البريدية المرسل معها الفيروس يصاب الجهاز به ومن ثم يبدأ الفيروس بالعمل وفقا للأسلوب الذي صمم لأجله[2]، والفيروسات أنواع لعل أهمها:

1-فيروس الحب: يتمثل هذا الفيروس في شكل رسالة أو صورة مثيرة للإغراء، ترسل إلى البريد الالكتروني للمستخدم لحثه على فتحها وتكون ملحقة برسالة عادية، ويتنكر الفيروس في شكل رسالة بريدية آمنة وبمجرد فتح الرسالة، يقوم الفيروس بنسخ نفسه مرات عديدة، مما يضاعف قدرته على الانتشار لحذف الملفات أو إخفائها ويستبدلها بنسخ منه، ويقوم أيضا بإرسال رسالة بريد الكتروني لكافة العناوين الالكترونية الموجودة في سجل العناوين الالكترونية[3].

---

(1) – محمد خليفة، المرجع السابق، ص 44.

(2) – بن طالب ليندا، المرجع السابق، ص ص 25-26.

(3) –محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، د ط، دار النهضة العربية، د ب ن، 1994، ص 145.

2-دودة الانترنت: هي فيروس تنتقل عبر شبكة الانترنت، ويعتمد على استخدام برنامج Outlook express بشكل أساسي للقيام بعملية الانتشار وإصابة أكبر عدد ممكن من الأجهزة، ويقوم مصممه بزرعه داخل رسالة بريد إلكتروني، ويرسلها إلى عدد كبير من مستخدمي الشبكة وبمجرد قيامهم بفتحها يبدأ الفيروس في الحصول على دفتر العناوين Address book الخاص بكل واحد منهم ثم إرسال هذه الرسالة للعديد من أصدقائهم فيفتحونها دون أدني شك لمعرفتهم للمرسل فيقع ضحية هذا الفيروس، وهذا ما أدي إلى انتشاره بنسبة كبيرة في العالم[1].

الفرع الثالث: جرائم الاعتداء على المعلومات المدرجة بالنظام المعلوماتية

للمعلومة المعالجة آليا أهمية كبيرة باعتبارها أساس عمل النظام المعلوماتية ولما لها من قيمة اقتصادية، وبهذا تعد هدفا للجرائم المعلوماتية من خلال التلاعب فيها أو إتلافها أو حذفها أو تغييرها[2].

أولا: إتلاف المعلومات

إن مكونات الحاسوب سواء مادية أو معنوية يمكن أن تتعرض لجريمة الإتلاف التي تعني تخريب وتغير المعلومات والبيانات المخزنة على الحاسوب ومحوها وتعديلها بهدف الاستفادة منها أو مجرد تخريبها، والهدف من تدمير نظم المعلومات هو إتلاف أو محو تعليمات البرامج أو البيانات ذاتها، ولا يهدف إلى مجرد الحصول على منفعة الحاسوب أيا كان شكلها ولكن يريد ببساطة إحداث ضرر بنظام المعلوماتية وإعاقته على أداء وظائفه.

ويتخذ الإتلاف عدة صور فقد يتم عن طريق طرق الإتلاف العادية كالحريق أو السرقة أو عن طريق استبدال أو محو المعلومات، ويشكل استبدال المعلومات نوع من جرائم الغش أو التزوير المعلومات وأما محو المعلومات فهو أسهل طرق الإتلاف كونه

---

[1]-عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتورا، كلية الحقوق، جامعة ابوبكر بلقايد، تلمسان، 2018/2017، ص 123.

[2] -إسمهان بوضياف، المرجع السابق، ص 360.

من خصائص الجرائم الالكترونية، وقدرة الجاني على محو أثار الجريمة في فترة وجيزة جدا لا تتعدي الضغط على زر بسيط في لوحة المفاتيح عن طريق الفأرة[1].

ثانيا: التلاعب بمعطيات الحاسوب

إن التلاعب بمعطيات الحاسوب، يعني التلاعب بالبرامج والبيانات والمعلومات المخزنة فيه بقصد الإستلاء على المال دون وجد حق وهو أخطر طرق الاحتيال لصعوبة اكتشافه وللأضرار الجسيمة التي يسببها للأخرين.

والتلاعب بالبيانات والمعلومات يعني تغير مضمونها أو تعديلها أو تحريفها أو وضع بيانات خاطئة وغير صحيحة أو التوصل إلى منع إدخال بيانات جديدة، وهذه من صور الغش المعلوماتى الذي يهدف إلى الحصول على الأموال بطرق غير مشروعة[2].

أما فيما يتعلق بالبرامج فهي تعني إدخال أوامر الحاسوب من أجل الاستيلاء على أموال الآخرين بطريقة الغش والتحايل، حيث يقوم المحتال وغالبا ما يكون موظفا في البنك بفتح حساب خاص بيه وتحويل مبالغ من حسابات الآخرين لحسابه[3].

الفرع الرابع: الجرائم الواقعة على البرامج الالكترونية

وتنقسم هذه الجرائم إلى جرائم واقعة على البرامج التطبيقية وبرامج التشغيل وسنتطرق لهاتين الصورتين:

أولا: الجرائم المعلوماتية الواقعة على البرامج التطبيقية

يقوم الجاني في هذه الصورة بتحديد البرنامج أولا ثم التلاعب فيه لتحقيق أكبر قدر من الاستفادة المادية.

---

(1) – خالد عياد الحلبي، المرجع السابق، ص 68.

(2) –المرجع نفسه، ص 106.

(3) – المرجع نفسه، ص 106.

1-تعديل البرنامج: الهدف الرئيسي من تعديل هذه البرامج يتمثل في اختلاس النقود وتكثر هذه البرامج في مجال الحسابات[1].

و من أمثلة ذلك قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقيد المصاريف الزائدة في الحساب الخاص به أطلق عليه اسم Zzwick وحصل على إثر ذلك على مئات الدولارات كل شهر[2].

2-التلاعب في البرنامج: يأخذ التلاعب في البرنامج عدة أشكال فقد يتم عن طريق استعمال القنبلة المنطقية، أو عن طريق قيام أحد المبرمجين بزرع برنامج فرعي غير مسموح به بالبرنامج الأصلي يسمح له بالدخول الغير مشروع في العناصر الضرورية لأي نظام معلوماتي[3].

ثانيا: الجرائم المعلوماتية الواقعة على برامج التشغيل

وهي البرامج المسؤولة عن عمل النظام المعلوماتي من حيث قيامها بتنظيم وضبط ترتيب التعليمات الخاصة بالنظام، ويتحقق هذا النوع من الجرائم المعلوماتية في شكلين:

1-المصيدة: تتمثل في إعداد برنامج به أخطاء وعيوب عمدا، لا يكتشف بعضها عند استخدام البرنامج، إذ يترك المبرمج ممرات خيالية وفواصل وتفرعات في البرنامج حتى يستطيع فيما بعد تنفيذ التعديلات الضرورية بإدخال تفرعات إضافية أو إحداث مخارج وسيطة للولوج داخل نظام معلوماتية، وبهذه التقنية يمكن للمبرمج استخدام البرنامج في أي وقت وفق أهوائه [4].

---

[1] -أحمد خليفة الملط، الجرائم المعلوماتية، ط2، دار الفكر الجامعي، الإسكندرية، 2006، ص 174.

[2] – إسمهان بوضياف، المرجع السابق، ص 360.

[3] – أحمد خليفة الملط، المرجع السابق، ص 545.

[4] – محمد سامي الشوا، المرجع السابق، ص 82.

2-تصميم برنامج وهمي: وتقوم هذه الصورة من خلال قيام المبرمج بوضع برنامج يصعب اكتشافه مخصص خصيصا لارتكاب الجريمة ومراقبة تنفيذها، ومن أمثلة ذلك قيام إحدى شركات التأمين الأمريكية في مدينة لوس انجلوس بواسطة مبرمجيها تصميم برنامج وهمي يقوم بتصنيع وثائق تأمين الأشخاص وهمين بلغ عددهم 46.000 بهدف تقاضي هذه الشركة من اتحاد شركات التأمين عمولات من نظيراتها [1].

[1] -إسمهان بوضياف، المرجع السابق، ص 360.

الفصل الثاني

ضوابط ومعوقات الإثبات في الجريمة الالكترونية

الفصل الثاني

ضوابط ومعوقات الإثبات في الجريمة الالكترونية

الإثبات هو اقامة الدليل على وقوع الجريمة ونسبتها إلى المتهم وذلك وفق طرق مشروعة ومحددة قانونا، والاثبات في مجال الجرائم الالكترونية ينطبق عليه المفهوم العام للإثبات، وتبعا لذلك فهو يواجه العديد من الاشكاليات بغية استخلاصه نظرا للخصوصيات المتعلقة بطبيعة الجريمة باعتبارها غير مرئية ويسهل نحو آثارها ويصعب الوصول إلى أدلة ادانتها، والسمات المتعلقة بخصوصية التحقيق في هذه الجرائم نظرا لصعوبة التحري في كشف غموضها .

كما ان الطرق التقليدية في استخلاص الادلة والضوابط يصاحبها العديد من المشكلات العملية، ويكشف التحليل العميق لهذه الطرق أن هناك بعض الخطوات يمكن الغاؤها باستعمال نظام قائم على تكنولوجيا، حيث اصبحت عاجزة لمواجهة الكثير من الافعال التي تهدد مصالح اجتماعية واقتصادية ارتبطت بظهور الحاسب الآلي والذي نتج عنها ظهور تسمية اخرى جديدة للدليل تعرف بالدليل الرقمي أو الالكتروني .

وعليه وجب تحديث الاساليب الاجرائية المتبعة بجمع الادلة في الجرائم الالكترونية أو تبني وسائل جديدة، وهذا ما قام به المشرع الجزائري إضافة إلى الوسائل التقليدية في الجرائم الالكترونية.

كما ان استخدام هذه الوسائل في استخلاص الادلة الالكترونية تعترضه عدة عقبات منها ما يتعلق بخصوصية الدليل الالكترونية ومنها ما يتعلق بخصوصية التحقيق وهذا ما سنتناوله في هذا الفصل الذي ينقسم إلى مبحثين: المبحث الأول تحت عنوان ضوابط الإثبات في الدليل الالكتروني أما المبحث الثاني تحت عنوان معوقات الإثبات في الجريمة الالكترونية.

المبحث الأول: ضوابط الإثبات في الدليل الالكتروني

ان ظهور أشكال مستحدثة من الجرائم المعلوماتية ادى بطبيعة الحال إلى ظهور ادلة مستحدثة وفي اثبات الجاني تختلف عن الادلة التقليدية وتعرف بالدليل الالكتروني[1]، وهذا الاخير هو كل دليل مأخوذ من جهاز الكمبيوتر محل الجريمة أو يكون في شكل بيانات وملفات مخزنة بداخله وقد يكون عبارة عن ملفات ناجمة عن اتصالات بين الجاني والمجني عليه من خلال مواقع الانترنت، وهو ما يساعد القاضي على توضيح موقفه من القضية ومنها إصدار حكم آليات في القضية المعروضة امامه . [2]

وعلى هذا الاساس قسمنا هذا المبحث إلى مطلبين سنتطرق إلى الأدلة الرقمية(المطلوب الأول) ثم إلى الأدلة الاجرائية المستخدمة في جميع الأدلة الرقمية (الالكترونية).

المطلب الأول: الأدلة الرقمية

يحتاج إثبات الجرائم الإلكترونية إلى دليل رقمي، كوسيلة لإثبات ارتكاب جريمة الاحتراق والتعدي على البيانات والمعلومات، سواء بسرقتها أو اتلافها أو تزويرها، أو سرقة المنظومة الالكترونية الخاصة بفرد معين أو منظمة معينة لصالح الفرد أو الغير.

والدليل الرقمي (العلمي، الالكتروني) يقتصر على اجراء تجارب علمية وعملية على جهاز الحاسب الآلي التي استخدم في الاختراق أو التعدي، لتعزير دليل سبق تقديمه سواء بالنفي أو الإثبات الواقعة التي ثار الشك بشأنها.[3]

---

[1]- ثنيان ناصر آل ثنيان، المرجع السابق، ص 70

[2]- عبير بعقيقي، فيصل نسيغة، الاثبات في الجرائم المعلوماتية على ضوء القانون 0409، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، المجلد09، العدد02، جوان2018، ص37.

[3]- عبد الفتاح البيومي حجازي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والأنترنت، د.ط، دار الكتب القانونية، مصر، د.س.ن، ص49

ومن خلال هذا، يمكن توضيح الادوات العلمية لضبط إثبات الجريمة في النقاط التالية:

الفرع الأول: برامج الحاسب الآلي

برنامج الحاسب الآلي هو مجموعة من الاوامر والارشادات والإيعازات التي تحدد لجهاز الحاسوب العمليات التي يقوم بتنفيذها بتسلسل وخطوات محددة، وتحمل هذه العمليات على Medai معين يمكن قراءته عن طريق الآلة .[1]

من خلال عمليات التحري الإلكتروني يمكن استخدام برامج استرجاع المعلومات من الأقراص التالفة، وبرامج كسر كلمة المرور، وبرامج الضغط، وفك الضغط، وبرامج البحث عن الملفات العادية والمخفية، وبرامج تشغيل الحاسب، وبرامج نسخ البيانات بالإضافة إلى برامج منع الكتابة على القرص الصلب التي تستخدم بعد ارتكاب الجريمة لحماية مسرحها (وهو مسرح افتراضي يختلف عن غيره من الجرائم لكونه يتميز بوجود الأدلة الالكترونية ذات الطبيعة الغير المرئية)، وكذلك برامج استرجاع الملفات المحذوفة التي تلجأ المجرم إلى حذفها للتخلص من الدليل الالكتروني، وذلك بهدف جميع الاستدلالات إلكترونيا.

وتظهر فاعليتها عند إتباع الإجراءات العلمية والفنية للتحري، حيث تمنع من تغيير المواد والبرامج المستخدمة في الاختراق والتعدي وارتكاب الجرائم.[2]

---

[1]- رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، ط1، منشورات الحلبي الحقوقية، الجزائر، 2012، ص68، أنظر كذلك فاروق الحفناوي، موسوعة قانون الكومبيوتر ونظم المعلومات، قانون البرمجيات دراسة متعمقة في الاحكام القانونية برمجيات الكومبيوتر، الكتاب الأول، دار الكتاب الحديث، القاهرة، 2003، ص 79

[2]- ثنيان ناصر آلة ثنيان، المرجع السابق، ص 76.

الفرع الثاني: فحص ومراقبة الشبكات

وهي البرامج التي نستخدم في فحص البروتوكول IP/TCP، حيث يعد هذا البروتوكول [1] من اكثر البروتوكولات المستخدمة في شبكة الانترنت لأنه يعتبر جزء أساسي منه، والمسؤول عن تراسل حزم البيانات عبره وتوجيهها إلى اهدافها، فهو يوجد بكل جهاز مرتبط بالأنترنت، ويتكون من أربعة أجزاء، فيشير الجزء الأول من اليسار إلى منطقة الجغرافية، والجزء الثاني لمزود الخدمة وثالث لمجموعة الحاسبات الالية المترابطة، واما جزء الرابع يحدد الحاسب الآلي الذي تم اتصال منه . [2]

يعمل عنوان IP بشكل متزامن مع بروتوكول آخر وهو بروتوكول التحكم بالنقل TCP , والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية، يقوم بروتوكولTP بعنونة كل حزمة مع إضافة معلومات اخرى إليها، ومنه فيتم استخدام عنوان TPمن خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إلى امكانية مراقبة المستخدم من طرف مزود خدمة الانترنت وتقديم المعلومات التي تفيد في التحقيق، بناء على ان لكل جهاز حساب إلى يتصل بالأنترنت عنوان TPخاص به . [3]

وهذه البرامج تقوم بفحص هذه البروتوكولات لمعرفة المشكلات المتعلقة بالشبكات والعمليات التي تعرضت لها،، وترجع فاعليتها إلى قدرتها الفائقة في الدخول على الشبكات وللمس برامج السرقة والتلصص، وكذلك الفيروسات التي تستخدم في عمليات الاختراق والتعدي والتزوير وتحديد مصدرها بدقة .

---

[1]- أنظر البروتوكولات هي مجموعة من القواعد التي تستخدمها أجهزة الكومبيوتر للاتصال مع بعضها البعض عبر شبكة . والبروتوكول هو وجود اتفاقية أو ضوابط التي تمكن من الاتصال، ونقل البيانات بين نقاط النهاية الحوسبة في أبسط أشكالها عن .http: //ejabat.google.com

[2]- طاهري عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة مسيلة، 2014 / 2015، ص 15

[3]- ممدوح عبد الحميد عبد المطلب، بحث والتحقيق جنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006، ص 101 .

الفرع الثالث: برامج فك الشفرات

من اهم فوائد التشفير أنه يقي من كشف التصنت على حزم المعلومات الخاصة بالمنظمات، والتصنت يعني نسخ حزم المعلومات عند انتقالها عبر الشبكة، حيث يمكن من الناحية التقنية مراقبة أداء الشبكة من خلال حزم البيانات المتدفقة عبر الشبكة، مما ييسر وصول المخترقين

لهذه الحزم، ولكن تمكن منع التنصت باستخدام وسائل التشفير المناسبة ؛ لان عدم معرفة الشفرة معناه الحصول على بيانات ومعلومات مبهمة وغير مفهومة [1]، الا أن هناك برامج يمكنها فك الشفرات، وبصفة خاصة البرامج والمواقع التي تقوم بعمليات الاختراق والتعدي والتزوير وهذه البرامج تحتوي على مليارات الشفرات، وتقوم باستغلال الحاسب الآلي في تجربة هذه الشفرات في ثواني محدودة حتى تقوم بفتح الموقع المشفر، ومن ثم متابعته ومعرفة ماذا كان قد استخدم في عملية الاختراق والتعدي وارتكاب الجرائم الإلكترونية .

وتتميز ما إذا كان قد استخدم في عملية اختراق والتعدي وارتكاب الجرائم الإلكترونية، وتتميز هذه البرامج المشورة التي استخدمت في الاختراق والتزوير والتعدي معرفة مصدرها . [2]

الفرع الرابع: استخدام برامج التتبع وكشف الاختراق وبرامج اكتشاف الثغرات

ان طبيعة عمل هذه البرامج تمكن في التعرف على محاولات الاختراق وكشف كافة المعلومات المتعلقة بمن قام بها، وايضا اشعار الجهة المتضررة من هذه العملية، ومن بين هذه البرامج , Hack Tracer vl.2 فعندما يرصد اي محاولة القرصنة أو اختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول امام المخترق، ثم يبدا في عملية انتفاء اثره

---

[1]- ثنيان ناصر آل ثنيان، المرجع السابق، ص 78

[2]- محمود عبد الحميد عبد المطلب، جرائم استخدام حاسب الآلي وشبكة المعلومات العالمية الجريمة عبر الانترنت، د.ط، مكتبة دار الحقوق، الشارقة، 2001، ص220 .

حتى يصل إلى الجهاز الذي حدث العملية من خلاله، ويستغرق هذا البرنامج مجموعة شاملة من بيانات المخترق من حيث عنوان TP الخاص به، وتاريخ حدوث الاختراق باليوم والساعة، وفي الاخير المعلومات الخاصة لمزود الخدمة [1]

وبرامج اكتشاف الثغرات توجد على شبكة الانترنت وهذه البرامج تساعد المستخدم على القيام بأعمال مهمة كالاتصال، وزيادة سرعة الانترنت ولكن المشكلة في امكانية ترك المخترقين لثقوب بهذه البرامج يستعطون من خلالها النفاذ إلى نظام واختراقه من خلال البحث عن هذه البرامج ودخول من خلالها إلى نظم المعلومات وسيطرة عليه وارتكاب الجرائم الإلكترونية، ويمكن اكتشاف الثقوب الموجودة على البرامج باستخدام جدران الحماية والبرمجيات التي تساعد في معرفة مصدر الاختراق .[2]

المطلب الثاني: القواعد الاجرائية

ان تطور التقني الذي لحق المعالجة الالية، فضلا عن الطبيعة الخاصة للدليل الرقمي، ادى إلى تغيير الكثير من المفاهيم السائدة حول اجراءات وطرق الوصول اليها، وهو الامر الذي فرض معه ضرورة إعادة تقسيم مناهج بعض الإجراءات المتبعة في استخلاص الدليل الالكتروني، والتي ثبتت عدم كفايتها نظرا الميزات التي تتسم بها، الامر الذي فرض معه ضرورة استحداث قواعد اجرائية اخرى تتلاءم مع طبيعة البيئة التقنية، تستند هاته الاخيرة على طرق ومناهج بحث متخصصة ومتطورة.[3]

فتطور الإثبات ووسائله أمر في غاية الأهمية لمواجهة هذا النوع الجديد من الجرائم، وهذا الامر الذي سوف نعالجه من حيث بحث القواعد الاجرائية الحديثة في الوصول إلى الدليل الالكتروني وهذا ما سنتطرق اليه في النقاط التالية:

---

[1]- سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، اكاديمية نايف العربية العلوم الامنية، كلية الدراسات العليا، السعودية 2003، ص 100.

[2]- ثنيان ناصر آل ثنيان، المرجع السابق، ص 78 .

[3]- رشيدة بوكر، المرجع السابق، ص393.

الفرع الأول: القواعد الاجرائية التقليدية لاستخلاص الدليل الالكتروني

تشترك الجريمة المعلوماتية مع باقي الجرائم في بعض الإجراءات التقليدية لجمع الدليل التي حافظت على وجودها رغم التطور الذي عرفته الجريمة في عصر التكنولوجيا، فهذه الإجراءات لاتزال صالحة للقيام بدورها في جميع الدليل وإثبات كل الجرائم بمختلف أنواعها ومنها الجريمة الإلكترونية، وأهم هذه الإجراءات كما بينها القانون هي إجراءات مادية شخصية وهذا ما سنتطرق اليه في النقاط التالية:

سنتناول ثلاث اجراءات ذات طبيعة مادية تتم بنتائج مادية ملموسة، وسوف نبين في التالي دور كل إجراء في استنباط الدليل الإلكتروني: [1]

1- المعاينة: تعتبر المعاينة إجراء من إجراءات التحقيق تتطلب سرعة الانتقال إلى محل الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته وضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها.[2]

ويمكن أن تقوم بها سلطة التحقيق بنفسها أو تندب ضباط الشرطة القضائية للقيام بها. كما يمكن المحكمة أن تقوم بإجراءات المعاينة إذا رأت.[3]

عند العلم بوقوع الجريمة فات أول خطورة يقوم بها امور ضبط القضائي هو الانتقال إلى مسرح الجريمة، لان هذا الأخير حجز الزاوية في التحقيق الجنائي ومكمن الآثار والأدلة المادية، وينبغي التعامل في الإطار مع مسرح الجريمة المعلوماتية على أنه مسرحان هما:

---

[1]- أشرف عبد القادر قنديل، المرجع السابق ، ص135.

[2]- انظر المادة 79 من الامر رقم 66155 المؤرخ في صفر عام 1386 الموافق 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، جريدة الرسمية الجمهورية الجزائرية، عدد48 بتاريخ 11 جوان1966، المعدل والمتمم.

[3]- عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق، جامعة الإسكندرية، 2006، ص84.

- **المسرح التقليدي:** يقع خارج بيئة الحاسوب والانترنت، ويتكون بشكل رئيسي من المكونات المادية المحسوسة المكان الذي وقعت فيه الجريمة، وهو أقرب إلى مسرح الجريمة التقليدية ويترك فيها الجاني عدة آثار كالبصمات وبعض متعلقاته الشخصية أو وسائط تخزين رقمية.[1]

- **المسرح الافتراضي:** ويقع داخل البيئة المعلوماتية، لأنه يتكون من البيانات الرقمية التي تتواجد داخل الحاسوب وشبكة الانترنت في ذاكرة الأقراص الصالة الموجودة بداخله.[2]

ومن الإجراءات التي يتعين اتباعها عند إجراء المعاينة ما يلي:

1. القيام بتصوير جهاز الحاسب الآلي الذي ترتكب عن طريق الجرائم .[3]
2. العناية البالغة بملاحظة الطريقة التي تم بها إعداد النظام، وبوجه خاص السجلات الالكترونية التي تزود بها لمعرفة موقع الاتصال.

عدم التسرع في نقل اي مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقن من عدم وجود أي مجالات مغناطيسية في المحيط الخارجي حتى لا يحدث اي اتلاف البيانات المخزنة.[4]

2_التفتيش في البيئة الإلكترونية: يمكن تعريف التفتيش بصفة عامة أنه إجراء من الإجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهم

---

[1]- أشرف عبد القادر قنديل، المرجع السابق، ص138.

[2]- المرجع نفسه، ص138.

[3]- ممدوح عبد الحميد عبد المطلب، المرجع السابق، ص 115

[4]- اشرف عبد القادر قنديل، المرجع السابق، ص139.

الإجراءات التحقيق في كشف الحقيقة لأنه غالبا ما يسافر عن أداة مادية تؤيد نسبة الجريمة إلى المتهم.[1]

ولا يمكن أن يقوم به سوى النيابة العامة وقاضي التحقيق، الغرض منه هو البحث عن أدلة إثبات، الجريمة المرتكبة محل التفتيش قد يكون مسكنا أو شخصا متعلقا بالمتهم أو غير المتهم .[2]

يقصد بالشخص كمحل لتفتيش الوسائل الالكترونية، قد يكون من مستغلي أو مستخدمي الإجهزة الإلكترونية أو خبراء البرامج، سواء كانت برامج نظام أو برامج تطبيقات، أو من اي اشخاص اخرين يكون بحوزتهم اجهزة أو معدات معلوماتية أو اجهزة حاسب إلى محمولة أو هواتف متصلة بجهاز مودم أو مستندات .[3]

3ـ الضبط: إن النتيجة الطبيعة التي ينتهي إليها التفتيش هي ضبط الادلة المتحصل عليها أثناء تفتيش المنظومة المعلوماتية، وضبط يعني وضع اليد على أي شئ يتصل بالجريمة المعلوماتية للكشف عن مرتكبيها. [4]

اما الضبط المعلوماتي فهو ينطبق على مكونات المادية والمعنوية للنظام المعلوماتي، كما انه تعتليه عدة صعوبات بسبب ضخامة البيانات واجب فحصها من محقق المعلوماتي قدرة المجرم المعلوماتي على اخفاء ومحو أثار جريمته، وفي مقابل عاجز السلطات تحقيق عن كسر كلمات السر أو شفرات المرور، وضع المشرع الجزائري في قانون 09-04 المتعلقة بتكنولوجيات الاعلام والاتصال ومكافحتها طريقتين: اول تكون عن طريق نسخ المعطيات محل البحث وثاني باستخدام التقنيات المناسبة .

---

[1]-اشرف عبد القادر قنديل، المرجع السابق، ص140.

[2]- عبد الفتاح البيومي الحجازي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والأنترنت، المرجع السابق، ص377

[3]- بن طالب ليندة، المرجع السابق، ص 49 .

[4]- خالد عياد الحلبي، المرجع السابق، ص168 .

ثانيا: الإجراءات الشخصية

سنتطرق لمجموعة من الإجراءات الطبيعية ذات طبيعة الشخصية لأنه غالبا ما يتوسط فيها الشخص بين القيام بالإجراء والحصول على الدليل

1 – الشهادة:

الشهادة بصفة عامة هي إثبات حقيقة واقعة معينة، علم بها الشاهد من خلال ما شاهده أو سمعه أو ادركه بحواسه الأخرى عن تلك الواقعة بطريقة مباشرة وشهادة على هذا الاساس تعد وسيلة إثبات اساسية في مسائل الجزائية . [1]

يطلق عليه اسم الشاهد المعلوماتي لأنه هو الشخص الفني صاحب الخبرة والمتخصص في تقنية وعلوم الحاسب الآلي والذي يكون لديه معلومات جوهرية لازمة لدخول لنظام المعالجة الالية للبيانات فلذلك تجد ان شاهد المعلوماتي ينحصر في عدة طوائف تتمثل في مشاغلة الحاسب الآلي، خبراء البرامج، المحللون مهندسو الصيانة والاتصالات، مديرو النظام .

وللشاهد التزامات لابد التقيد بها مثل: طبعا ملفات البيانات المخزنة في ذاكرة الحاسوب الآلي على ان يقوم بطبها وتسليمها إلى سلطان التحقيق والافصاح عن كلمات المرور السرية وكشف عن الشفرات المدونة بها الاوامر الخاصة بتنفيذ البرامج المختلفة . [2]

2 ــ الخبرة:

لابد ان يكون الخير صاحب مقدرة وامكانية العلمية والفنية في مسألة الخبرة ويستطيع القيام بدوره وللقيام بهذا الاخير عليه ان يبين المكان المحتمل الدولة الإثبات

---

[1]– ابراهيم الغمار، السهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1989، ص 30

[2]– بن زرت أسيا، اثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2019، ص 26

وشكلها وهيئتها واثار الاقتصادية والمالية المترتبة على التحقيق في جريمة المعلوماتية وكيفية عزل نظام المعلوماتي عند الحاجة دون اتلاف الادلة أو الأجهزة أو تدميرها . [1]

الفرع الثاني: الادلة الاجرائية الحديثة للوصول للدليل الالكتروني

تبين من الإجراءات التقليدية انها صعبة الاتباع للحصول على الدليل الإلكتروني، فكان من الضروري على التشريعات المختلفة خلق ادلة أو اجراءات حديثة تتماشى مع طبيعة الخاصة للدليل الالكتروني وهذا عن طريق الاعتماد على تكنولوجيا المعلومات .

والمشرع الجزائري كغيره من التشريعات قام بإرسال جملة من مقومات التشريعية لمكافحة الجريمة المعلوماتية من خلال ما جاء به في القانون 06-22 المؤرخ في 20-12-2006 المعدل والمتمم للقانون الإجراءات الجزائية الامر (66-155) من خلال إجراءي التسرب واعتراض المراسلات السلكية واللاسلكية وكذلك بموجب إصدار قانون إجراء خاص به القانون 09-04 المتضمن للقواعد الخاصة بالوقاية من جرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، وثاني باستخدام إجراء المراقبة التكنولوجية وسنتطرق إلى كل هذه الإجراءات المتحدثة في مجال المعلوماتية . [2]

أولا: التسرب

هو الإجراء المستحدث التي تنص عليه المواد من 64 مكرر 11 إلى مكرر 18 من ق إ ج ج عرفتها المادة 65م مكرر 12 من ق إ ج ج، بانه قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضباط الشرطة القضائية المكلف بتنسيق العملية بمراقبة الأشخاص المشتبه بارتكابهم جناية أو جنحة بإيهامهم أنه فاعل أو شريك لهم . [3]

وتكون عملية التسرب في الجريمة الالكترونية بدخول ضابط أو عون شرطة إلى العالم الافتراضي وذلك عن طريق اشتراكه في محادثات معرفة الدردشة، أو اختراق

---

[1]-بن زرت أسيا، المرجع السابق، ص 27

[2]- عبير بعقيقي، فيصل نسيغة، المرجع السابق، ص41

[3]- بن طالب ليندة، المرجع السابق، ص 87

مواقع معينة مستخدما في ذلك أسماء أو صفات وهيئات مستعار وهمية سعيا منه للاستفادة منهم في كيفية اقتحام الهاكر الموقع، أو القيام بحلقات اتصال مع المشتبه فيهم عن طريق البريد الالكتروني .

ووكيل الجمهورية هو من يقوم بمراقبة التسرب أو قاضي التحقيق وفقا لنص المادة 65 مكرر 11 ق إ ج ج ويمكن لهما الامر يوقف التسرب في أي مرحلة وذلك من اجل تامين متسلسل من الشبكة الإجرامية .

ثانيا: المراقبة الالكترونية

تناول المشرع الجزائري هذا الإجراء من المادة 04 من القانون رقم 09-04 المتعلق بالقواعد الخاصة بالرقابة من الجرائم المتصلة بتكنولوجيا لإعلام والاتصال ومكافحتها بعنوان مراقبة الاتصالات الالكترونية.[1]

والمشرع لم يعرف بإجراء المراقبة الالكترونية بل ترك امر تعريفها للفقه ومنه تعرف بانها: " عمل انني اساسي له نظام معلومات الكتروني، ويقوم فيه المراقِب بمراقبة المراقَب بواسطة الاجهزة الالكترونية أو عبر شبكة الانترنت، لتحقيق فرض محدد وافراغ النتيجة في الملف الإلكتروني، وتحديد التقارير بالنتيجة.[2]

والمراقبة الالكترونية وسيلة من وسائل جمع البيانات والمعلومات عن المشتبه فيه، بحيث يقوم بها مراقب الكتروني يتمثل في ضابط من ضباط الشرطة القضائية ذي كفاءة تقنية عالية وباستخدام تقنيات وبرامج الكترونية فيها، وبالتالي ومن خلال القانون رقم 09-04 الذي سبق ذكره، نجد ان المشرع لم يعتبر هذا الإجراء طريقة من طرق

---

[1]- عبير بعقيقي، فيصل نسيغة، المرجع السابق، ص41.

[2]- مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت (دراسة مقارنة بين المراقبة الامنية التقليدية والالكترونية)، دار الكتب القانونية، مصر، 2005، ص192.

الحصول على الدليل الرقمي فقط بل ادرجه ايضا ضمن التدابير الوقائية من الجريمة المعلوماتية .[1]

ويمكن استنتاج شروط واليات المراقبة الالكترونية في التشريع الجزائري من خلال نص المادة 65 مكرر 5 الق إ ج ج: وهي ان يتم تنفيذ هذه العملية تحت سلطة الفضاء وبإذن منه، وهو ما نصت عليه المادة 4 من الق إ ج ج 09-04 المذكور، بحيث لا يجوز إجراء عمليات المقاربة الا بإذن مكتوب من السلطة القضائية المختصة .[2]

ثالثا: اعتراض المراسلات السلكية واللاسلكية

نستشف من نص المادة (65 مكرر 5) [3] من ق إ ج ج ان المقصود باعتراض المراسلات اعتراض أو تسجيل أو نسخ المراسلات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية وهاته المراسلات عبارة عن بيانات قابلة للإنتاج، والتوزيع، والتخزين، الاستقبال والعرض . [4]

وهي ايضا عملية مراقبة سوية المراسلات السلكية واللاسلكية في اطار البحث والتحري عن الجريمة وجمع الادلة أو المعلومات حول الأشخاص المشتبه فيهم في ارتكابهم أو في مشاركتهم في ارتكاب الجريمة

بالرغم من ان عملية اعتراض المراسلات تشكل انتهاكا لحرمة حياة الخاصة للأفراد، واعتداء على سرية مراسلاتهم والتي كفلها في دستور 2020 المعدل بموجب القانون رقم 16-01 وذلك من خلال المادة 46 فقيرة 2 التي نصت « سرية المراسلات

---

[1]- اوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، 20120/2019، ص21 22 .

[2]- طاهري عبد المطلب، المرجع السابق، ص 24 .

[3]- أجازت الفقرة الأولى من المادة (65 مكرر 5) من ق اج ج لوكيل الجمهورية ان بإذن بـــ « اعتراض المراسلات التي تتم عن طريق وسائل الاتصال السلكية واللاسلكية » .

[4]- رشيدة بوكر، المرجع السابق، ص 441 .

والاتصالات الخاصة بكل اشكالها مضمونة » .[1] الا ان المشرع الجزائري قد وضع شروط قانونية تنص على منع التعسف في استعمالها وكذلك حماية الحرية الفردية وتتمثل هذه الشروط في الحصول على اذن من وكيل الجمهورية أو من قاضي التحقيق اذا تم فتح تحقيق فضائي [2]

زيادة على ذلك يجب ان يكون الإذن مكتوب لمدة اقصاها أربعة أشهر قابلة للتجديد، وايضا وجوب تضمنه على كل العناصر التي تسمح بالتعرف على الاتصالات المطلوبة التقاطها والاماكن المقصودة .[3]

ويعتبر البريد الالكتروني اهم وسيلة تنفيذ في مجال التراسل الالكتروني ومن ثم فات عملية الاعتراض تنصب عليه والتي تمثل مصدرا غنيا الادلة الرقمية للإثبات الجرائم الإلكترونية.

وكل رسالة الكترونية يظهر فيها معلومات عامة ولكن هذه المعلومات ليست كافية لمعرفة المرسل، لأنه يمكن لهذا الاخير إرسال رسالة بأسماء وهمية، كما ان هناك وسائل تسمح للمرسل بإرسال رسالته دون ان يظهر فيها بريده الالكتروني، لذلك لابد من الحصول على المزيد من المعلومات التي يمكن العصور عليها في حاشية وسائل البريد (Email Leader) وهي أو خطوة للبدء في التحري عن المرسل الرسالة الالكترونية.[4]

---

[1]- انظر المادة 46 / 2 من الدستور الجزائري، المؤرخ في 8 ديسمبر 1966، المعدل بالقانون رقم 1601 المؤرخ في 26 جمادى الأول عام 1437 المواقف ل 6 مارس 2016، المتضمن التعديل الدستوري، العديد 14 .

[2]- انظر المادة 65 مكرر 5 من الامر 66155 المؤرخ في 18 صفر 1386هـ المواقف ل 8 يونيو سنة 1966 م، المتضمن قانون الإجراءات الجزائية الجزائري ج .ر .ج .ج، عدد 48 صادر بتاريخ 11 جوان 1966، المعدل والمتمم.

[3]- انظر المادة 65 مكرر 7، المتضمن ق . إ . ج . ج، السابق الذكر

[4]- مدربل كريم، الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة الماستر، كلية الحقوق، جامعة اكلي محند اولحاج، البويرة، 2019، ص 43 .

المبحث الثاني: معوقات إثبات الجريمة الالكترونية

مما لا شك فيه أن الصعوبات والمعوقات التي تعترض سبل مكافحة وإثبات الجريمة الالكترونية متعددة، وكلها تنبع من كون هذه الجرائم تتسم بطابع خاص ولا تترك أثار مادية يمكن إدراكها بالحواس، على عكس الجرائم التقليدية، الأمر الذي أضحي يشكل تحديا كبيرا يمكنه المساس بغالبية فئات المجتمع نظرا للأضرار التي تترتب عليها، سواء من الناحية التقنية أو القانونية لاكتشاف هذه الجريمة وإثباتها مما يؤدي إلى صعوبة ملاحقة المجرمين من طرف الأجهزة المعنية بمكافحتها، ووضع اليد على الدليل لاثبات جرائمهم .

وعليه سنتطرق في هذا المبحث إلى جملة من المعوقات والصعوبات التي تقف عائق أمام مكافحة وإثبات الجريمة الالكترونية منها ما هو متعلق بخصوصية الأدلة الرقمية ومنها ما هو متعلق بجهات التحقيق، وعليه سنقسم هذا المبحث إلى مطلبين، معوقات خاصة بالدليل الجنائي الرقمي (المطلب الأول)، معوقات خاصة بجهات التحقيق (المطلب الثاني).

المطلب الأول: معوقات خاصة بالدليل الجنائي الرقمي

لقد ساهمت تقنية المعلومات في مجال العولمة والاتصال وتدخل الألة كعنصر مهم في مختلف مجالات الحياة في تراكم مذهل في المعرفة، وحصيلة هائلة في المعلومات تعجز الوسائل البشرية عن ملاحقتها وفهرستها واستخلاصها ومعالجتها، كما أدت إلى تخطي نطاق ارتكاب الجريمة من الواقع المادي إلى الافتراضي، لهذا بات من اللازم الاستعانة بالتقنيات الحديثة التي أسفرت عن التطور العلمي في مجال التكنولوجيا ويتعلق الأمر بالدليل الرقمي من أجل مكافحتها، بحيث يلعب هذا الأخير دور أساسي وفعال في مجال الإثبات الجنائي فقد أثبت فعاليته في التصدي للجرائم ومكافحتها، فعن طريقه يمكن إدانة المتهم أو إعلان براءاته، فبرغم من مزايا هذا النوع من الأدلة الجنائية والجهود

المبذولة في مكافحة الجريمة عن طريقه تعترض عملية استخلاصه إلى مجموعة من الصعوبات والمعوقات، وسنتطرق لها في هذا المطلب من خلال تقسيمه إلى 4فروع .

سنتناول غياب دليل مرئي في (الفرع الأول)، الطبيعة الديناميكية لدليل الرقمي في (الفرع الثاني)، ثم سهولة محوه أو تدميره في (الفرع الثالث)، ثم أخيرا صعوبة الوصول إلى الدليل في (الفرع الرابع).

الفرع الأول: غياب دليل مرئي

دائما ما يكون الدليل الجنائي في الجريمة التقليدية مرئيا ذو طبيعة مادية، بحيث يمكن للقائمين على عملية التحقيق بمعاينة مسرح الجريمة وضبط أي دليل يفيد في الكشف عن ملابساتها[1]، من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الضرب، وكذلك المادة السامة التي تستعمل في القتل أو المحرر ذاته الذي تم تزويره، أو النقود التي زيفت وأدوات تزيفيها، ولكن في الجرائم التي تقع على العمليات الالكترونية المختلفة خاصة التي تقع عبر شبكة الانترنت، كالتي تقع على عمليات التجارة الالكترونية، أو على العمليات الالكترونية للأعمال المصرفية، أو على أعمال الحكومة الالكترونية يكون محلها جوانب معنوية تتعلق بالمعالجة الآلية للبيانات، فإذا وقفت جرائم معينة على هذه الجوانب المعنوية، كجرائم السرقة أو الاختلاس أو الإستلاء أو الغش أو التزوير أو الإتلاف فإنه قد يصعب إقامة الدليل بالنسبة لها بسبب الطبيعة المعنوية للمحل الذي وقفت عليه الجريمة.

يوجد شك في أن إثبات الأمور المادية، التي تترك أثار ملحوظة يكون سهلا ميسورا، بعكس إثبات الأمور المعنوية فإنه يكون في منتهي الصعوبة بالنظر إلى أنه لا يترك وراءه أي أثار قد تدل عليه أو تكشف عنه، بحسبان أن أغلب المعلومات والبيانات التي تتداول عبر الحاسبات الآلية والتي من خلالها تتم العمليات الالكترونية تكون في هيئة رموز ونبضات مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو

[1]- طاهري عبد المطلب، المرجع السابق، ص 38.

إدراكها إلا من خلال هذه الحاسبات الآلية فالجرائم التي ترتكب على العمليات الالكترونية التي تعتمد في موضوعها على التشفير والاكواد السرية والنبضات والأرقام والتخزين الالكتروني يصعب أن تخلف وراءها أثار مرئية قد تكشف عنها أو يستدل من خلالها على الجناة[1].

تعد الطبيعة الغير مرئية للأدلة المتحصل عليها من الوسائل الالكترونية تلقي بضلالها على الجهات التي تتعامل مع الجرائم التي تقع عبر الانترنت حيث يعتبر كشف وتجميع من هذا النوع لإثبات وقوع الجريمة والتعرف على مرتكبيها أحد أبرز المشكلات التي يمكن أن تواجه جهات التحري والملاحقة كضباط الشرطة[2].

الفرع الثاني: الطبيعة الديناميكية للدليل الرقمي

فالأدلة الرقمية أدلة ليست أقل من مادية من الأدلة المادية فحسب بل تصل إلى درجة التخيلية في حجمها وشكلها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة إذ تنتقل عبر شبكات الاتصال بسرعة فائقة، بمعني إمكانية تخزين المعلمات Le stockage des données في الخارج –علي خادم server – بواسطة شبكة الاتصال عن بعد، وهو ما قد يثير مشكلات عديدة قد تعوق اتخاذ الإجراءات اللازمة لضبط الأدلة التقنية والبحث عنها، لأنه يستلزم القيام بها خارج حدود الدولة في نطاق دولة أخري حيث ارتكبت الجريمة أو جزء منها، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية، لما ينطوي عليه من مساس بسيادة هذه الدولة، وهذه المشكلة تظهر بصورية جلية حين اتخاذ إجراءات التفتيش لضبط هذه الجرائم عندما يكون نظام المعالجة الآلية متصلا بنظم أخري خارج الدولة، ويكون تفتيش هذه النظم ضروريا لإماطة اللثام عما تشمله من جرائم.

---

[1]- يوسف صغير، المرجع السابق، ص ص 124-125.

[2]- عبد الرحمن محمد بحر، معوقات التحقيق في جرائم الانترنت دراسة مسحية على ضباط الشرطة في البحرين، رسالة مقدمة إلى معهد الدراسات العليا استكمالا لمتطلبات الحصول على درجة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا قسم العلوم الشرطية، الرياض، 1999، ص 27.

وهو ما يفرض الحاجة إلى الحصول على إذن الدولة التي يتم إجراء البحث في مجالها الإقليمي أو إبرام اتفاقيات ومعاهدات دولية ثنائية أو متعددة الأطراف في مجال التعاون الدولي التي تستهدف من وراء ذلك التقريب بين القوانين الجزائية الوطنية من أجل جمع هذا النوع من الأدلة العابرة للحدود[1].

وتعد معاهدة المجلس الأوروبي حول جرائم تقنية المعلومات الموقعة في 2001/11/23، والتي أيدتها الولايات المتحدة بقوة هي أول خطوة رئيسية في هذا الاتجاه ويمكن اعتبارها بداية لعمل وضع القواعد والمعايير التي يتوقع من البلدان المعنية أن تتبعها في نهاية الأمر في جهودها.

خصصت اتفاقية بودابست الباب الثالث منها لدراسة التعاون الدولي cooperation ومن خلاله نصت المادة 23 على ضرورة تعاون الأطراف فيما بينها وفقا لأحكام هذا الفصل، ومن خلال تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المسائل الجزائية والترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بالنسبة للقوانين المحلية، إلى أقصي مدي ممكن، بغرض التحقيقات والإجراءات الجزائية المتعلقة بالجرائم ذات الصلة بالنظم الحاسوبية، والبيانات المعلوماتية، أو لجمع الأدلة ذات الشكل الإلكتروني لمثل هذه الجرائم.

وفي هذا الصدد نجد أن المشرع الجزائري قد خصص الفصل السادس من القانون رقم (09-04) لسنة 2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها "للتعاون والمساعدة القضائية الدولية"، وما يستتبع ذلك من ضرورة أن تطلب الجزائر الدعم من الدول التي سبقتنا في هذا المجال على غرار اتفاق التعاون الذي وقعته الجزائر بتاريخ 25 أكتوبر 2003 مع فرنسا لمحاربة الإجرام المنظم، وبالخصوص الإجرام التقني والمتضمن التعاون الأمني والدعم التقني للشرطة الجزائرية

[1]- رشيدة بو كر، المرجع السابق، ص ص 456-457.

لمحاربة المجرمين الإلكترونين إذ يجب إذا اقتضت الضرورة وضع قانون يسهل هذا التعاون بين الجزائر والدول الأخرى[1].

الفرع الثالث: سهولة محوه أو تدميره

إن تدمير ومحو الأدلة الجنائية الرقمية من بين أكبر الصعوبات التي تعترض عمليات الإثبات في الجرائم الالكترونية، نظرا للسهولة التي تتميز بها هذه العملية واستغراقها لوقت قصير جدا[2]، فالجاني يمكنه أن يمحو الأدلة التي تكون قائمة ضده أو تدميرها في فترة زمنية يسيرة بحيث لا تتمكن السلطات من كشف الجريمة إذ ما علمت بها وفي هذه الحالة التي قد تعلم بها فإنه يستهدف بالمحو السريع عدم استطاعة هذه السلطات إقامة الدليل ضده وبالتالي تنصله من مسؤولية هذا الفعل وإرجاعه إلى خطأ في نظام الحاسبة الإلكترونية أو الشبكة أو في الأجهزة، ومن أمثلة ذلك قيام مهربي الأسلحة في النمسا.

بإدخال تعديلات على الأوامر العادية لنظام تشغيل جهاز الحاسبة، الالكترونية الذي يستخدمه في تخزين عناوين عملائه والمتعاملين معه بحيث يترتب على إدخال أمر النسخ أو الطباعة إلى هذه الحاسبة من خلال لوحة مفاتيحه محو وتدمير كافة البيانات كاملة[3].

وعلي ذلك نري أنه يمكن الحفاظ على الأدلة ومن ثم ضمان أن الإجراءات التقليدية لجمع الدليل التقني كالتفتيش والضبط لا تزال فعالة في بيئة تكنولوجية تتميز بالتلاشي أو التبخر، وذلك فضلا عن البرمجيات التي يمكن بمقتضاها استرداد كافة الملفات التي تم إلغائها أو إزالتها، إتباع نظام إلزام مزودي الخدمات بالتحفظ على المعطيات المخزنة لديهم حيث أنه إذ لم تتوافر الأدلة على الاتصال وعن عناوين الأشخاص المشتركين في

---

[1]- رشيدة بوكر، المرجع السابق، ص ص 457458.

[2]- هشام محمد فريد رستم، "أصول التحقيق الجنائي الفني"، في بحوث مؤتمر القانون والكمبيوتر والانترنت، المجلد الثاني، ط3، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، 2004، ص 429.

[3]- الطيبي البركة، إشكالية الإثبات في الجرائم الالكترونية، مجلة آفاق علمية، المجلد 11، العدد01، ادرار، 2019، ص 271

الجريمة فإنها تكون عرضة للاختفاء، وهذا ما نصت عليه اتفاقية بودابست في المادة 16 من ضرورة السماح لكل طرف لسلطاته المختصة أن تأمر أو تفرض بطريقة أخري مزود الخدمة التحفظ على المعطيات المعلوماتية المخزنة بما في ذلك المعطيات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي[1].

إن التحفظ على المعطيات يعتبر إجراء أولي أو تمهيدي الهدف منه هو الاحتفاظ بالمعطيات قبل فقدانها، وهي المبررات التي حددتها المذكرة التفسيرية لاتفاقية بودابست، والتي تدعو إلى اتخاذ مثل هذا الإجراء وذلك كما يلي:

1-غالبا ما يتم ارتكاب جرائم الاعتداء على نظم المعالجة الآلية عن طريق نقل الاتصالات عبر نظم الحاسوب، حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة مثل الفيروسات، فتحديد مصدر هذه الاتصالات يمكن أن تساعد في تحديد هوية مرتكبي الجريمة.

2-تأمين الدليل التقني من الضياع، حيث يتم نسخ دليل على نشاط جنائي من قبل مزودي الخدمات، مثل المراسلة الالكترونية التي تم إرسالها أو استقبالها، ومن ثم يمكن الكشف عن دليل جنائي للجرائم المرتكبة[2].

يلاحظ مما سبق أن إجراء التحفظ على المعطيات المخزنة يعد لبعض الدول العربية كسوريا سلطة قانونية جديدة فهو أداة تحقيق مستحدثة في إطار مكافحة جرائم تقنية المعلومات[3]، في حين نجد المشرع الجزائري قد نص في القانون رقم(09-04) لسنة

---

[1]- رشيدة بوكر، المرجع السابق، ص 459.

[2]- المرجع نفسه، ص ص 459460.

[3]- المرجع نفسه، ص 460.

2009 بشأن الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها على إجراء الحفظ وذلك في المادة (10) منه[1].

الفرع الرابع: صعوبة الوصول إلى الدليل

إن النتائج العلمية الدقيقة للأجهزة المعملية لم تعد مجال تشكيك من محامي الدفاع بل طرق تجميعها وحفظها وتقديم الأدلة العلمية للمحكمة هي التي أصبحت محل تشكيك من جانب المتهم، والأصل أن الوصول إلى هذه الأدلة يتم عن طريق الشكاوي التي يتم تقديمها من طرف المجني عليهم، لكن الأمر بالغ التعقيد في الجرائم الالكترونية بالنسبة لجهات التحقيق التي لم تصل إلى تلك المعرفة والخبرة التي تملكها اتجاه التحقيق في الجرائم التقليدية لأن الأمر يتطلب إحاطة كاملة بالتكنولوجيا الحديثة ومعرفة واسعة بالعقبات التي تصعب من الوصول إلى الدليل الالكتروني والمتمثلة في[2]:

أولا: إحاطته بوسائل الحماية الفنية

يصعب الوصول إلى الدليل لإحاطته بوسائل الحماية الفنية كاستخدام كلمات السر حول مواقعهم أو ترميزها أو تشفيرها لإعاقة المحاولات الرامية إلى الوصول إليها والاطلاع عليها واستنساخها[3]، بحيث تكون البيانات المخزنة الكترونيا أو المنقولة عبر شبكات الاتصال محاطة بجدار من الحماية الفنية لإعاقة محاولة الوصول الغير مشروع إليها، كذلك يمكن للمجرم المعلوماتي أن يزيد من صعوبة عملية التفتيش التي قد

---

(1)- تنص المادة (10) من قانون04/09 من القانون السالف لذكر على "في إطار تطبيق أحكام هذا القانون، يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوي الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 أدناه، تحت تصرف السلطات المذكورة.

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

(2)- الطيبي البركة، المرجع السابق، ص ص 272-273.

(3)- على عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة) ماجستير قانون، كلية الحقوق، جامعة الموصل، المكتب الجامعي الحديث، الإسكندرية، 2012، ص 80.

تباشر للحصول على الأدلة التي تدينه عن طريق مجموعة من التدابير الأمنية كاستخدام كلمة السر للوصول إليها أو دس تعليمات خفية بينها أو ترميزها لإعاقة أو منع الإطلاع عليها أو ضبطها، لذا فإن استخدام تقنيات التشفير لهذا الغرض يعد أحد العقبات الكبرى التي تعوق رقابة البيانات المخزنة أو المنقولة عبر حدود الدولة والتي تقلل من قدرة جهات التحري والتحقيق والملاحقة على الإطلاع عليها الأمر الذي يجعل حماية حرمة البيانات الشخصية المخزنة في مراكز الحاسبات والشبكات أو المتعلقة بالأسرار التجارية العادية والالكترونية أو بتدابير الأمن والدفاع أمر بالغ الصعوبة[1].

ثانيا: سلوكات الجاني

يتعمد الجاني تشفير الملفات أو البيانات الالكترونية التي تتضمن محتوى غير مشروع بهدف منع الغير من الإطلاع عليها واكتشافها كما هو الحال في حالة نقل البيانات المتعلقة بجرائم غسيل الأموال عبر الانترنت بعد تشفيرها، ويحرص بعد ارتكابه لجريمته على محو أثارها التي تدل على وقوعها وذلك عن طريق استعمال تقنيات معدة لهذا الغرض مع الأخذ بعين الاعتبار سهولة وسرعة إمكانية محو وتعديل البيانات الالكترونية التي يمكن القيام بها في أزمان قياسية تقاس باللحظات والثواني، لذلك تشكل عملية تشفير البيانات المخزنة الكترونيا أو المنقولة عبر الشبكات المعلوماتية عقبة كبيرة أمام إثبات الأدلة الرقمية[2].

ثالثا: الامتناع عن التبليغ

إن المجني عليه أيضا يعوق من الوصول إلى الدليل بحيث يمتنع في الغالب عن التبليغ على الجرائم الالكترونية، وقد يسعي إلى التعتيم على المحققين وتضليلهم حتى لا

---

[1]- الديربي عبد العال، محمد صادق إسماعيل، الجرائم الاكترونية (دراسة قانونية قضائية مقارنةط1)، المركز القومي للإصدارات القانونية، القاهرة، 2012، ص 330.

[2]- جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، المجلد2016، العدد12، كلية القانون، جامعة ذي قار، العراق، 30 جوان 2016، ص 08.

يكتشفوا هذه الجرائم [1]، وتبقي مستترة ولا تصل إلى علم السلطات المعنية بالصورة العادية كما هو الحال في الجريمة التقليدية وذلك لصعوبة، اكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقفت مجنيا عليها هذه الجرائم أو لأن هذه الجهات تحاول درأ الأثر السلبي للإبلاغ عما وقع لها[2]، لهذا لا نعجب إذا وجدنا أن أكثر تلك الجرائم لم تكتشف إلا بمحض الصدفة وهناك ما يشير إلى أن هذه الجرائم لم تكتشف منها إلا ما بنسبة واحد فقط بالمئة وما تم الإبلاغ عنه إلى السلطات المختصة لم يتعدى 15 بالمئة وحتى ما طرح أمام القضاء من هذه الجرائم فإن أدلة الإدانة لم تكن كافية إلا في حدود الخمس 5/1[3].

المطلب الثاني: معوقات خاصة بجهات التحقيق

يعتبر التحقيق الرقمي عبارة عن مجموعة من الأساليب المتتبعة من أجل اكتشاف الجريمة كفحص جهاز الجاني أو المشتبه به من قبل المحققين والهدف منها هو جمع الأدلة المطلوبة لكي تعطي للنيابة أثناء عملية التحقيق، لكنه يتسم بعدة معوقات يمكن أن تعرقل عملية التحقيق ويؤدي إلى نتائج سلبية، بحيث يستطيع المجرم الإفلات من الجهات الأمنية ولهذا سنتناول مجموعة هذه الصعوبات من خلال تقسيم هذا المطلب إلى فرعين، سنتناول صعوبة التحري عن كشف الجريمة في (الفرع الأول)، ضعف التعاون الدولي في مكافحة الجرائم الالكترونية في (الفرع الثاني).

الفرع الأول: صعوبة التحري عن كشف الجريمة

إن التحري في كشف غموض الجريمة الالكترونية تعترضه مجموعة من العقبات والصعوبات تتمثل في ما يلي:

---

[1]- مسرة خالد الحمد، الدليل الرقمي ومعايير جودته، ط1، مركز الكتاب الأكاديمي، عمان، 2014، ص 149.

[2]- ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق، المجلد 18، العدد2، كلية الحقوق، جامعة النهرين، جانفي 2016، ص 218.

[3]- محمد خليفة، المرجع السابق، ص 35.

أولا: ضخامة البيانات المتعين فحصها

يعتبر الكم الهائل للبيانات والمعلومات والتي هي بحاجة إلى فحص ودراسة لاستخلاص دليل الجريمة منها أحد مصادر الصعوبات التي تعيق عملية الإثبات في الجرائم الالكترونية، حيث أن طباعة كل ما هو موجود في الدعامات الممغنطة قد يتطلب مئات الآلاف من الصفحات، وفي نفس الوقت قد لا تقدم هذه الأخيرة أب فائدة للتحقيق، ولذلك على السلطات القائمة بالضبط والتحقيق أن لا تتمتع بالخبرة الفنية في مجال الحاسب الآلي فحسب، وإنما لابد أن تمتلك هذه السلطات أيضا القدرة على فحص الكم الهائل من المعلومات والبيانات المخزنة على أنظمة المعالجة الآلية[1].

ويسلك المحقق غير المدرب لمواجهة هذه الصعوبة أحد السبيلين:

1-إما حجز البيانات الالكترونية بقدر يفوق قدرة البشرية على مراجعتها أو التغاضي عن هذه البيانات كلها على أمل الحصول على اعتراف بالجريمة من المتهم[2].

2-لذلك وفي ظل تواضع القدرات التي يتمتع بها رجال الضبط والتحقيق، كان لزاما لهذه الجهات أن تستعين بالخبراء الذين يقومون بالتميز بين ما هو مفيد لتحقيق وبين ما هو خارج عن إطار التحقيق وما من شأنه تعطيل سير العدالة، حيث أن الاستعانة بالخبراء خاصة في هذا الإطار قد يضع المحقق في دائرة مغلقة من المعلومات وكم هائل من البيانات، قد لا يستطيع الخروج منها، خاصة إن لم يكن مسلحا بالتقنية والقدرة والخبرة المعلوماتية[3].

---

[1]- بثينة حبيباتني، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الانسانية، المجلد أ، العدد50، كلية الحقوق، جامعة الجزائر 1، ديسمبر 2018، ص 89.

[2]- عبد الله حسين على محمود، سرقة المعلومات المخزنة في الحاسب الآلي، ط2، دار النهضة العربية، القاهرة، 2002، ص 359.

[3]- ميسون خلف حمد الحمداني، المرجع السابق، ص 227.

ثانيا: طمس الهوية

عند استخدام شبكة الانترنت من طرف المجرم المعلوماتي يتعمد إخفاء هويته عن طريق استخدام بعض البرامج أو التطبيقات التي تعمل على طمس الهوية، مما يشكل صعوبة كبيرة أمام المحققين أو القضاء لاستخلاص الأدلة الجنائية الرقمية كذلك قد يلجأ الجناة إلى إخفاء المعلومات أو البيانات وهو ما يجعل عملية بناء الأدلة الرقمية أو استرجاعها أمر في غاية الصعوبة أمام الخبير[1].

ثالثا: قلة خبرة المحققين في الجرائم الالكترونية

تقع هذه الجرائم على التقنية التكنولوجية، وهذه التقنية دائمة التطور وبشكل سريع، حيث أن مرتكبي هذه الجرائم يتبعون كل جديد ويعملون على تطوير سبل إخفاء أدلة جرائمهم، ومن هنا يتوجب على المحقق أن يكون على دراية تامة ومواكبا للتطور فيما يتعلق بجرائم الحاسوب والانترنت، ولكن هذا الأمر لا يتحقق دائما وعليه فإن الصعوبات في هذا المجال هو[2]:

1- عدم التدريب: لقد اهتمت أجهزة الأمن في الكثير من دول العالم بمواجهة جرائم الحاسوب والانترنت والتحقيق فيها، ففي الولايات المتحدة الأمريكية تمثل أعلي نسبة من المستخدمين لنظم المعلومات في العالم وتعاني بشكل كبير من جرائم الحاسوب والانترنت، مما دعاها إلى إنشاء وحدة متخصصة للمكافحة والتحقيق في هذه الجرائم من ضمن مكتب التحقيقات الفيدرالي ويكون تدريب عناصر هذه الوحدة مستمرا ليواكب تطور جرائم الحاسوب والانترنت.

ففي المملكة الأردنية الهاشمية أنشأت مديرية الأمن العام قسما خاص بجرائم الحاسوب والانترنت منذ عام 1998 يتولي إجراءات المكافحة والاستدلال والتحقيق في الجرائم

---

[1]- منصور عبد السلام عبد الحميد حسان العجيل، الضوابط القانونية للإثبات الجنائي بالأدلة الرقمية (دراسة مقارنة) المجلة القانونية(مجلة متخصصة في الدراسات والبحوث القانونية)، ص 3400.

[2]- خالد عياد الحلبي، المرجع السابق، ص225.

المرتكبة بواسطة الحاسوب، وقد تم دعم هذا القسم بمختصين في مجال علوم وهندسة الحاسوب وزود بما يلزم من أجهزة ومعدات وبرمجيات تساعد في إجراءات التحقيق، وفي فحص الأجهزة المضبوطة في الجريمة والمحافظة على الأدلة[1].

2- عدم الاستعانة بالخبراء: إن عدم الاستعانة بالخبراء في مجال التحقيق في جرائم الحاسوب والانترنت يجعلها تفتقر إلى المعلومات الإحصائية على تلك الجرائم التي تساعد في تحديث القوانين التي تجرم وتعاقب على هذه الجرائم[2].

الفرع الثاني: ضعف التعاون الدولي في مكافحة الجرائم الالكترونية

بما أن الجريمة الالكترونية تخترق كل الحدود الإقليمية المعمول بها، كان من اللازم تفعيل سياسة التعاون الدولي والتنسيق بين الدول من أجل مكافحتها وإثباتها، لكن وعلى الرغم من المناداة بضرورة هذا التعاون إلا أنه هناك عوائق تجعل هذا التعاون صعبا من أهمها:

أولا: عدم وجود نموذج موحد للنشاط الإجرامي

فالأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم الالكترونية لا يوجد فها اتفاق عام وموحد حول نماذج إساءة استخدام نظم المعلومات وشبكة الانترنت الواجب تجريمها[3].

ونظرا لاختلاف المفاهيم الخاصة بها لاختلاف التقاليد والأعراف القانونية الدولية فإن هذا يضعف من منظومة القانون الدولي في مجال ضبط تلك الجرائم، وبالتالي يسهل على الجناة الإفلات من المسائلة الجنائية[4]، كما أن اختلاف طبيعة النظام القانوني بين البلدان أدي لاعتبار البعض للأفعال الجرمية على أنها مباحة وذلك راجع للطبيعة الخاصة

---

[1]- خالد عياد الحلبي، المرجع السابق، ص 225-226.

[2]- المرجع نفسه، ص 226.

[3]- الطيبي البركه، المرجع السابق، ص 279.

[4]- يوسف صغير، المرجع السابق، ص 133.

للمعلوماتية عبر الانترنت، بينما يراها العض الأخر غير مباحة ومن ثم يجرم الاعتداء عليها بالنقل والنسخ [1].

فعلي الرغم من إصدار العديد من الدول التشريعات التي تكافح الجريمة المعلوماتية إلا أنه لا يمكن اعتبارها جامعة مانعة والدليل على ذلك أن المؤسسات المحلية في فرنسا والولايات المتحدة الأمريكية وكندا تطالب في كل عام بإضافة صور أشكال جديدة من السلوك المعلوماتي والتي لم ينص عليها في التشريعات العقابية المعمول بها في هذا المجال، وبهذا يتبين عدم وجود اتفاق مشترك بين الدول حول صور الجريمة المعلوماتية[2].

ثانيا: عدم وجود تنسيق في النظم الإجرائية

إن اختلاف النظم الإجرائية التي يتم إتباعها في البحث والتحري والتحقيق في الجرائم الالكترونية يعد أحد المعوقات التي تقف أمام التعاون الدولي، وذلك راجع إلى أن الإجراءات التي تثبت فائدتها وفعاليتها في دولة ما قد تكون عديمة الفائدة في دولة أخري أو قد لا يسمح بإجرائها كما هو الحال بالنسبة للمراقبة الالكترونية، والتسليم المراقب والتنصت وغيرها من العمليات المتشابهة فإذا ما اعتبرت طريقة من طرق جمع الأدلة أو التحقيق أنها قانونية في دولة معينة، فإنه قد تكون ذات الطريقة غير مشروعة في دولة أخري[3].

ويعتبر أحسن مثال على اختلاف النهج القانونية بين الدول قضية الدودة الحاسوبية لوف باغ Love bug التي أعدت في الفلبين عام 2000 وقيل أنها عطلت ملاين

---

[1]- ميسون خلف حمد الحمداني، المرجع السابق، ص 225.

[2]- بثينة حبيباتني، المرجع السابق، ص 90.

[3]- براء منذر كمال عبد اللطيف، ناظر أحمد قنديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول تحولات القانون العام في مطلع الألفية الثالثة، كلية الحقوق، جامعة تكريت، العراق، 2009، ص 11.

الحواسيب في جميع أنحاء العالم، حيث أعاقت هذه القضية التحقيق بسبب أن ذلك العمل المؤذي والضار لم يكن آنذاك مجرما بشكل كاف في الفلبين[1].

ثالثا: عدم وجود معاهدات ثنائية أو جماعية بين الدول

حتى وإن كانت بعض الدول قد اتجهت إلى الانضمام إلى المعاهدات الثنائية أو الجماعية فإن هذه المعاهدات تبقي قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم برامج الحاسب وشبكة الانترنت[2]، وعليه فإن التطور السريع للجريمة الالكترونية قد يؤدي إلى إرباك المشرع الوطني، مما ينعكس بشكل سلبي على التعاون الدولي في مجال جمع وتبادل الأدلة الجنائية الرقمية[3]، كما يعطل ويعوق في ملاحقة ومحاكمة الجناة في الجرائم الالكترونية.

رابعا: مشكلة الاختصاص

تعتبر الجرائم الالكترونية من اكبر الجرائم التي تثير مسألة الاختصاص خاصة على المستوي الدولي على عكس المستوي الوطني أو المحلي الذي يتم الرجوع فيه إلى المعايير المحددة قانونا لذلك، بحيث تثار المشكلة بالنسبة للاختصاص على المستوي الدولي من حيث اختلاف التشريعات والنظم القانونية والتي قد ينجم عنها تنازع في الاختصاص بين الدول بالنسبة للجرائم المتعلقة بالانترنت التي تتميز بكونها عابرة للحدود فقد يحدث أن ترتكب الجريمة في إقليم دولة معينة من قبل أجنبي، فهنا تكون الجريمة خاضعة للاختصاص الجنائي للدولة الأولي استنادا لمبدأ الإقليمية، وتخضع كذلك لاختصاص الدولة الثانية على أساس مبدأ الاختصاص الشخصي في جانبيه، وقد تكون هذه الجريمة من الجرائم التي تهدد أمن دولة أخري فتدخل عندئذ في اختصاصها استنادا إلى مبدأ العينية[4].

---

[1]- مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد السلفادور بالبرازيل 12-19 أفريل 2010، رقم A/conf.213/9، ص 6.

[2]- ثنيان ناصر آل ثنيان، المرجع السابق، ص 130.

[3]- منصور عبد السلام عبد الحميد حسان العجيل، المرجع السابق، ص 3401.

[4]- بدري فيصل، مكافحة الجرائم المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتورا قانون علم كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، 2018/2017، ص 113.

خاتـمة

الخاتمة:

يتبين لنا من خلال دراستنا لموضوع الإثبات في الجريمة الإلكترونية أنها من أكثر وأخطر الجرائم التي تغزو العالم في الأونة الأخيرة وتهدد المجتمعات، فبانتشار تكنولوجيا المعلومات أصبحنا أكثر عرضة للوقوع كضحايا لها، فهذا الانتشار يعد بمثابة سلاح ذو حدين يمكن استخدامه من أجل تسهيل الاتصالات حول العالم، كما يمكنه استخدامه في التسبب بأضرار جسيمة للأشخاص أو المؤسسات من أجل تحقيق أهداف سياسية أو مادية شخصية .

لقد غيرت الجريمة الالكترونية النظرة التي كان ينظر بها للجرائم بصفة عامة وذلك لما تتسم به من طبيعة خاصة جعلتها تختلف عن الجرائم التقليدية كونها تقع في بيئة تقنية، كما تعتبر خصائص هذه الجريمة من أبرز العوامل التي ساعدت في تميزها عن باقي الجرائم العادية (التقليدية)، مما يجعل اكتشافها وإثباتها أمر في غاية الصعوبة بالأدلة التقليدية .

- **وعليه من خلال تطرقنا لهذه الدراسة خلصنا إلى مجموعة من النتائج أهمها:**

- عدم وجود تعريف شامل موحد بين الفقهاء للجريمة الالكترونية، بحيث تعددت التعاريف بين اتجاه مضيق لها يرتكز في تعريفه على موضوع الجريمة واتجاه موسع يرتكز في تعريفه علي أساس الوسيلة المرتكبة بها.
- المشرع الجزائري اعتمد علي معيار الجمع بين عدة معايير للتعريف بالجريمة كمعيار وسيلة الجريمة، موضوع الجريمة، وكذا معيار القانون الواجب التطبيق.
- محل ارتكاب هذه الجرائم ينصب على أنظمة المعالجة الآلية للمعطيات.
- من أهم خصائصها أنها تتمتع بصعوبة الاكتشاف و الإثبات ويمكن رد الأسباب وراء هذا إلى أنها جريمة تتم في بيئة تقنية لا تترك أي أثار خارجية مرئية.

– مجالات الجرائم الالكترونية عديدة ومخاطرها كثيرة نظرا لطبيعة استخدام التقنية الرقمية في شتى الميادين لاسيما المجالات المالية، وتنقسم الجرائم الالكترونية في قسمين: جرائم موجهة ضد النظام المعلوماتي، وجرائم تقليدية أداة ارتكابها النظام المعلوماتي .

– فيما يخص طرق الإثبات فقد نصت التشريعات المختلفة علي إجراءات متعددة تستهدف استخلاص الأدلة وتجميعها ولقد انقسمت التشريعات في مدى إمكانية تطبيق وسائل الإثبات التقليدية لاسيما التفتيش والضبط في الوسط الرقمي.

– تحتوي علي عدة مشكلات ومعوقات متعلقة بالدليل الرقمي في حد ذاته أهمها صعوبة الوصول إليه .

– عملية البحث والتحقيق تتخللها جملة من العقبات أهمها قلة خبرة المحققين في هذه الجرائم .

– ضعف التعاون الدولي لمكافحة هذه الجرائم.

– **وبناءا علي ما توصلنا إليه من نتائج نوصي بالأتي:**

– ضرورة الحفظ السريع للمعطيات وذلك باستخدام الوسائل الالكترونية المتاحة.

– تطوير وتكوين خبراء متخصصين في جمع الأدلة الجنائية الرقمية.

– القيام بدورات مكثفة إلي الخارج بقصد الاحتكاك بالبلدان التي لها خبرة في هذا المجال.

– إعطاء الفرصة للمواطنين للمشاركة في مكافحة الجرائم الالكترونية وذلك من خلال وضع خط يختص بتلقي البلاغات المتعلقة بهذه الجرائم.

– استحداث نص قانوني بخصوص أدلة الإثبات وإضافة الدليل الرقمي ضمنها خاصة وأن الجرائم الالكترونية لا يمكن إثباتها ل الأدلة التقليدية كالشهود ...الخ.

– تشديد العقوبة في قوانين الجرائم الالكترونية على كل الجاني معلوماتي بهدف مكافحة هذا النوع من الجرائم.

– ضرورة التعاون والعمل علي توحيد الجهود الدولية من اجل إنشاء قانون دولي موحد لمكافحة هذه الجرائم.

- ضرورة وجود قنوات اتصال بين الأجهزة الأمنية فيما بين الدول من أجل تسهيل عملية الحصول علي المعلومات.
- الحاجة إلي إبرام المزيد من الاتفاقيات والمعاهدات يتم من خلالها توحيد قواعد الاختصاص القضائي فيما يتعلق بالجرائم الالكترونية

قائمة المصادر والمراجع

المصادر:

الدستور:

1_ الدستور الجزائري، المؤرخ في 8 ديسمبر 1966، المعدل بالقانون رقم 16-01 المؤرخ في 26 جمادى الأول عام 1437 المواقف ل 6 مارس 2016، المعدل والمتمم في 15 جمادى الأولي عام 1442 الموافق ل 30ديسمبر 2020، الجريدة الرسمية الجمهورية الجزائرية، العدد82.

النصوص القانونية:

1_ الأمر رقم 156/66 المؤرخ في 18 صفر عام 1386، الموافق ل 8 يونيو 1966، المتضمن قانون العقوبات، المعدل والمتمم، ج ر، العدد 37.

2_ الأمر رقم 66/155 المؤرخ في صفر عام 1386 الموافق 8 يونيو سنة 1966، الذي يتضمن قانون الإجراءات الجزائية، الجريدة الرسمية الجمهورية الجزائرية، عدد48 بتاريخ 11 جوان1966، المعدل والمتمم.

3_ القانون رقم 09-04المؤرخ في 14شعبان عام 1430، الموافق ل 05أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، الجريدة الرسمية، العدد47.

وثائق الأمم المتحدة :

مؤتمر الأمم المتحدة الثاني عشر لمنع الجريمة والعدالة الجنائية، البند الثامن من جدول الأعمال المؤقت، التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما فيها الجرائم الحاسوبية، المنعقد سلفادور، بالبرازيل 12-19 أفريل 2010، رقم A/conf.213/9.

- المراجع

أ- الكتب:

1_ أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة الثانية، دار الفكر الجامعي، الإسكندرية، 2006

2_ أشرف عبد القادر قنديل، الإثبات الجنائي في الجريمة الإلكترونية، دون طبعة، دار الجامعة الجديدة للنشر، الإسكندرية، 2015.

3_ براء منذر كمال عبد اللطيف، ناظر أحمد قنديل، التعاون القضائي الدولي في مواجهة جرائم الانترنت، المؤتمر العلمي الأول، تحولات القانون العام في مطلع الألفية الثالثة، كلية الحقوق، جامعة تكريت، العراق، 2009.

4_ حسن الطوالبة، الجرائم الإلكترونية، الطبعة الأولى، جامعة العلوم التطبيقية، مملكة البحرين، 2008.

5_ خالد عياد الحلبي، إجراءات التحري والتحقيق في جرائم الحاسوب والانترنت، دون طبعة، دار الثقافة للنشر والتوزيع، الشرق الأوسط، 2011.

6_ خالد ممدوح إبراهيم، فن التحقيق الجنائي في الجرائم الالكترونية، دون طبعة، دار الفكر الجامعي، الإسكندرية، 2018.

7_ الديربي عبد العال، محمد صادق إسماعيل، الجرائم الاكترونية دراسة قانونية قضائية مقارنةط1، المركز القومي للإصدارات القانونية، القاهرة، 2012.

8_ رشيدة بوكر، جرائم الاعتداء على نظم المعالجة الآلية، الطبعة الأولى، منشورات الحلبي الحقوقية، الجزائر، 2012.

9_ عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي في القانون الجزائري والمقارن، دار الجامعة الجديدة، كلية الحقوق، جامعة الإسكندرية، 2006.

10_ عبد الرحمن بن عبد الله السند، الأحكام الفقهية لتعاملات الالكترونية الحاسب الآلي وشبكة المعلومات(الانترنت)، الطبعة الأولى، دار الوراق لطباعة والنشر والتوزيع، بيروت، 2004.

11_ عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في الجرائم الكمبيوتر والانترنت، د.ط، دار الكتب القانونية، مصر، دون سنة النشر.

12_ عبد الفتاح بيومي حجازي، جريمة غسيل الأموال بين الوسائط الالكترونية، دون طبعة، دار الفكر الجامعي، الإسكندرية، 2007.

13_ عبد الله حسين علي محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية، القاهرة، 2002.

14_ غانم مرضي الشمري، الجرائم المعلوماتية: ماهيتها، خصائصها، كيفية التصدي لها قانونا،الطبعة الأولى، دار العلمية الدولية للنشر والتوزيع، عمان، 2016.

15_ لينا محمد الأسدي، مدي فعالية أحكام القانون الجنائي في مكافحة الجريمة المعلوماتية(دراسة مقارنة)، دون طبعة، دار حامد، دون بلد النشر، دون سنة النشر.

16_ محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي، دون طبعة، دار الجامعة الجديدة للنشر، الإسكندرية، 2007.

17_ محمد سامي الشوا، ثورة المعلومات وانعكاساتها علي قانون العقوبات، دون طبعة، دار النهضة العربية، دون بلد النشر ، 1994.

18_ محمد عبد الرحيم، سلطان العلماء، جرائم الانترنت والاحتساب عليها، بحوث مؤتمر القانون والكمبيوتر والانترنت، المجلد3، الطبعة الثالثة، كلية الشريعة والقانون، جامعة الامارت العربية المتحدة، 2004.

19_ محمود عبد الحميد عبد المطلب، جرائم استخدام حاسب الآلي وشبكة المعلومات العالمية الجريمة عبر الانترنت، د.ط، مكتبة دار الحقوق، الشارقة، 2001.

20_ محمود نجيب حسني، شرح قانون العقوبات (القسم الخاص)، الطبعة16، دار النهضة العربية القاهرة، مصر، 1989

21_ مسرة خالد الحمد، الدليل الرقمي ومعايير جودته، الطبعة الأولى، مركز الكتاب الأكاديمي، عمان، 2014.

22_ مصطفى محمد موسى، المراقبة الالكترونية عبر شبكة الانترنت (دراسة مقارنة بين المراقبة الامنية التقليدية والالكترونية)، دار الكتب القانونية، مصر، 2005.

23_ ممدوح عبد الحميد عبد المطلب، بحث والتحقيق جنائي الرقمي في جرائم الكمبيوتر والانترنت، دار الكتب القانونية، مصر، 2006.

24_ نهلا عبد القادر المومني، الجرائم المعلوماتية، الطبعة الأولى، دار الثقافة للنشر وتوزيع، عمان، 2008.

25_ يزيد بو حليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري (في ضوء الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قانون العقوبات –قانون الإجراءات الجزائية –قوانين خاصة) دون طبعة، دار الجامعة الجديدة للنشر، الإسكندرية، 2019.

26_ يعيش تمام شوقي، الجريمة المعلوماتية (دراسة تأصيلية مقارنة)، الطبعة الأولى، مطبعة الرمال، الوادي(الجزائر)، جانفي2019.

27_

ب- المجلات والمقالات

1_ ابراهيم الغمار، السعادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1989.

2_ إسمهان بوضياف، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد11، سبتمبر، مسيلة، 2018.

3_ بثينة حبيباتني، معوقات مكافحة الجريمة المعلوماتية، مجلة العلوم الإنسانية، المجلد أ، العدد50، كلية الحقوق، جامعة الجزائر 1 ديسمبر 2018.

4_ جاسم خريبط خلف، صعوبات الدليل الجنائي في الجرائم المعلوماتية، مجلة القانون للدراسات والبحوث القانونية، المجلد2016، العدد12، جامعة ذي قار، كلية القانون، العراق، 30 يونيو 2016.

5_ حسين فريجة، الجرائم الالكترونية والانترنت، مجلة المعلوماتية، العدد36، أكتوبر، المسيلة، 2011.

6_ الطيبي البركة، إشكالية الإثبات في الجرائم الالكترونية، مجلة آفاق علمية، المجلد 11، العدد01، ادرار، 2019.

7_ عبير بعقيقي، فيصل نسيغة، الاثبات في الجرائم المعلوماتية على ضوء القانون 09/04، مجلة العلوم القانونية والسياسية، جامعة محمد خيضر، بسكرة، المجلد09، العدد02، جوان2018.

8_ مكتب الامم المتحدة المعني بالمخدرات والجريمة UNODC بفيينا، استخدام الانترنت في أغراض ارهابية، الامم المتحدة نيويورك، 2013

9_ منصور عبد السلام عبد الحميد حسان العجيل، الضوابط القانونية للإثبات الجنائي بالأدلة الرقمية دراسة مقارنة المجلة القانونية(مجلة متخصصة في الدراسات والبحوث القانونية).

10_ هشام محمد فريد رستم، "أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية موحدة لتدريب التخصصي"، مؤتمر القانون والكمبيوتر والانترنت المنعقد من 1-3 ماي 2000، كلية الشريعة والقانون، المجلد الثاني، ط3 جامعة الإمارات العربية المتحدة، 2004.

11_ ميسون خلف حمد الحمداني، مشروعية الأدلة الالكترونية في الإثبات الجنائي، مجلة كلية الحقوق، المجلد 18، العدد2، كلية الحقوق، جامعة النهرين، جانفي 2016.

ج- الرسائل الجامعية

- الدكتوراه

1_ بدري فيصل، مكافحة الجرائم المعلوماتية في القانون الدولي والداخلي، أطروحة لنيل شهادة دكتورا علوم تخصص قانون علم كلية الحقوق، جامعة الجزائر 01، بن يوسف بن خدة، 2018/2017.

2_ بن طالب ليندا، الدليل الالكتروني ودوره في الإثبات الجنائي (دراسة مقارنة)، أطروحة دكتورا، كلية الحقوق، جامعة مولود معمري، ، تيزي وزو، 2019.

3_ عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتورا، كلية الحقوق، جامعة ابوبكربلقايد، تلمسان، 2018/2017.

4_ هروال هبة نبيلة، جرائم الانترنت دراسة مقارنة، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان، 2014/2013.

5_ يرمش مراد، خصوصية الجريمة الالكترونية، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة، الجزائر1، 2021/2020.

- الماجستير

1_ ثنيان ناصر آل ثنيان، إثبات الجريمة الالكترونية دراسة تأصيلية تطبيقية، رسالة ماجستير، كلية الدراسات العليا قسم العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012.

2_ سليمان مهجع العنزي، وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، اكادمية نايف العربية العلوم الامنية، كلية الدراسات العليا، السعودية 2003.

3_ عبد الرحمن محمد بحر، معوقات التحقيق في جرائم الانترنت دراسة مسحية علي ضباط الشرطة في البحرين، رسالة مقدمة إلي معهد الدراسات العليا استكمالا لمتطلبات الحصول علي رسالة الماجستير في العلوم الشرطية، أكاديمية نايف العربية للعلوم الأمنية، معهد الدراسات العليا قسم العلوم الشرطية، الرياض، 1999،

4_ عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية (دراسة مقارنة)، رسالة ماجستير، جامعة الشرق الأوسط، الأردن، 2014

5_ علي عدنان الفيل، إجراءات التحري وجمع الأدلة والتحقيق الابتدائي في الجريمة المعلوماتية (دراسة مقارنة)ماجستير، كلية الحقوق، المكتب الجامعي الحديث، جامعة الموصل، الإسكندرية، 2012.

6_ نعيم سعيداني، آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري،رسالة ماجستير، كلية الحقوق، جامعة الحاج لخضر، باتنة، 2013/2012.

7_ يوسف صغير، الجريمة المرتكبة عبر الانترنت، رسالة ماجستير في القانون الخاص، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2013.

الماستر:

1_ اوساسي فؤاد، دور الدليل الرقمي في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، الجلفة، 20120/2019.

2_ بشري عواطة، حجية الدليل الالكتروني في الإثبات الجنائي، مذكرة ماستر، كلية الحقوق، جامعة 08 ماي 1945، قالمة، 2018/2017.

3_ بعرة سعيدة، الجريمة الإلكترونية في التشريع الجزائري، دراسة مقارنة، مذكرة ماستر، كلية الحقوق، جامعة محمد خيضر، بسكرة، 2016/2015.

4_ بن زرت أسيا، اثبات الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة ماستر، كلية الحقوق والعلوم السياسية، جامعة مستغانم، 2019.

5_ حكيمة شريد، مايسة ربيع، الجريمة المعلوماتية في التشريع الجزائري، مذكرة لنيل شهادة الماستر، كلية الحقوق، جامعة مولود معمري، تيزي وزو، 2016.

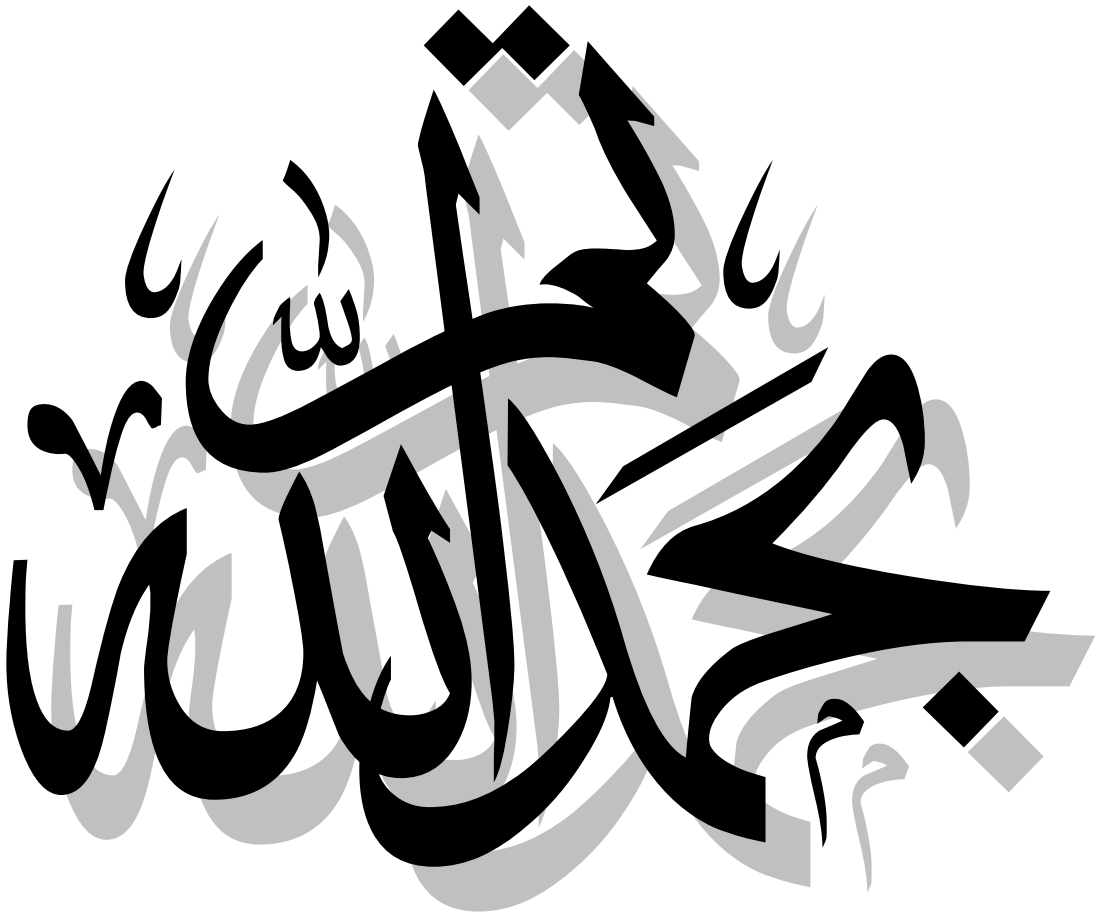
6_ طاهري عبد المطلب، الإثبات الجنائي بالأدلة الرقمية، مذكرة مكملة لمقتضيات نيل شهادة الماستر، كلية الحقوق، جامعة محمد بوضياف، مسيلة، 2015/2014.

7_ محمد بوعمرة، سيد علي بنيال، جهاز التحقيق في الجريمة الإلكترونية في التشريع الجزائري، مذكرة ماستر، كلية الحقوق، جامعة أكلي محند أولحاج، البويرة، 2020/2019.

8_ مدربل كريم، الإثبات بالدليل الرقمي في المسائل الجزائية، مذكرة لنيل شهادة الماستر، قسم الحقوق، جامعة اكلي محند اولحاج، البويرة، 2019.

فهرس المحتويات

فهرس المحتويات


بحمد الله

الملخص:

إن الإثبات هو إقامة الدليل علي وقوع الجريمة ونسبتها إلى المتهم وذلك وفق طرق مشروعة ومحددة قانونا، حيث يعد موضوع الإثبات في الجريمة الالكترونية الأساس الذي تبني عليه أي سياسة جنائية لمكافحة هذا النوع من الجرائم .

وتثير مسألة الإثبات صعوبات في مواجهة الجرائم الالكترونية، التي تقع علي العمليات الالكترونية بالوسائل الالكترونية، لكون هذه الجرائم تقنية تنشأ في الخفاء في بيئة رقمية، ينتج عنها مايسمى بالأدلة الإلكترونية التي تعتبر إحدى الأثار المهمة في الكشف عن هذه الجريمة و الربط بينها وبين مرتكبيها .

summary:

Evidence is establishing evidence of the occurrence of the crime and attributing it to the accused, according to legitimate and legally defined methods, as the subject of proof in electronic crime is the basis upon which any criminal policy is built to combat this type of crime.

The issue of proof raises difficulties in confronting electronic crimes, which fall on electronic operations by electronic means, because these crimes are technical crimes that arise in secret in a digital environment, resulting in the so-called electronic evidence, which is one of the important effects in detecting this crime and linking it with its perpetrators.