وزارة التعليم العالي والبحث العلمي

جامعة محمد البشير الإبراهيمي برج بوعريريج

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر

في الحقوق

تخصص: قانون الإعلام الآلي والأنترنت

الموضوع:

خصوصية الجريمة الإلكترونية في القانون الجزائري

إعداد الطلبة:

- بشان نسرين

- بلعباسي منال

تحت إشراف:

- الدكتور سي حمدي عبد المومن

لجنة المناقشة

(اللقب والاسم)	(الرتبة)	(الصفة)
- الدكتوراه لعوارم وهيبة	أستاذ محاضر - أ -	رئيسا
- الدكتور سي حمدي عبد المومن	أستاذ مساعد - ب -	مشرفا
- الأستاذ بلهامل عبد الفتاح	أستاذ مساعد - ب -	ممتحنا

السنة الجامعية: 2019- 2020

وزارة التعليم العالي والبحث العلمي

جامعة محمد البشير الإبراهيمي برج بوعريريج

كلية الحقوق والعلوم السياسية

قسم الحقوق

مذكرة مقدمة لاستكمال متطلبات شهادة الماستر

في الحقوق

تخصص: الإعلام الآلي والإنترنت

الموضوع:

خصوصية الجريمة الإلكترونية في القانون الجزائري

إعداد الطالبة:

بشان نسرين

بلعباسي منال

تحت إشراف:

الدكتور سي حمدي عبد المومن

السنة الجامعية: 2019-2020

((... وَمَا أُوتِيتُم مِّنَ الْعِلْمِ إِلَّا قَلِيلًا))

((سورة الإسراء: الآية 85))

شكر وعرفان

الحمد لله الذي تتم بنعمته الصالحات نشكره شكرا جزيلا طيبا مباركا فيه الذي وفقنا فيما نحن فيه الآن، والصلاة والسلام على رسوله الكريم ومن تبعه بإحسان إلى يوم الدين.

الشكر والتقدير للدكتور سي حمدي عبد المؤمن الذي قبل تواضعا وكرامة الإشراف على هذا العمل المتواضع .

كما نتقدم بالامتنان والعرفان للأساتذة الكرام أعضاء لجنة المناقشة الموقرة على تفضلهم لمناقشة هذه الرسالة

كما لا يفوتنا المقام هنا أن نسجل شكرنا إلى كل أساتذة كلية الحقوق والعلوم السياسية

بجامعة محمد البشير الإبراهيمي ببرج بوعريريج.

وإلى كل من ساعدنا من قريب أو بعيد على إنجاز هذه الرسالة.

إهـــداء

إلى من زرع في نفسي حب العلم وبذل الجهد في تحصيله من كان لي عونا وسندا ورفيقا

أبي العزيز

إلى الصدر الدافئ والقلب العطوف رمز الصبر والتضحية الجوهرة الغالية أمي الحبيبة

فاللهم ارحمهما كما رباني صغيرا.

إلى البنيان المرصوص أخواي وأختاي حفظهم الله ورعاهم

إلى كل أحبتي

إلى الأساتذة والزملاء

أهدي عملي هذا

بشان نسرين

إلى من أوصاني بهما ربي برا وإحسانا

والدي الكريمين حفظهما الله وأدام صحتهما وعافيتهما

إلى رفيق دربي زوجي العزيز

إلى إخوتي وأخواتي وكل أفراد عائلتي

إلى كل صديقاتي وإلى كل من أحب

إلى كل أساتذتي

بلعباسي منال

مقدمة

مقدمة:

يشكل استخدام الانترنت اليوم أحد أهم مظاهر عصرنا الراهن الذي نعيشه، من خلال زيادة عدد الأفراد المستخدمين لشبكة الانترنت، أو عدد صفحات الويب المتاحة على الشبكة أو ظهور أنشطة جديدة مرتبطة بالإنترنت، والتي تصاحبها في العادة جرائم تتم عبر الانترنت فبحلول العام 2020 وخاصة مع جائحة كورونا، فإن اشتراكات السكان عبر العالم في مواقع التواصل الاجتماعي والشبكة المعلوماتية والانترنت قد فاق التصورات، الأمر الذي أدى إلى ظهور مشكلات، وجرائم جديدة لم تكن موجودة، ولم يعرفها العالم لولا الانفجار الكبير لتكنولوجيا المعلومات والاتصالات.

لقد أصبحت الجريمة الالكترونية عابرة للحدود ترتكب من مسافات متباعدة، افتراضية لا تترك غالبًا أثرًا مرئيًا بل يمكن وفي لحظة إتلاف الدلائل فيها، وهي متغيرة مستحدثة متضاعفة هادئة لا تحتاج إلى عنف، بل كل ما تتطلبه القدرة على استغلال الوسائل التكنولوجية مما أعطى لها خصوصية في التشريعات والقوانين والقواعد العالمية، والوطنية بهدف ردعها وسد الهوة الضخمة التي تبتلع يوميا وبشكل رهيب آلاف الضحايا عبر العالم بصفة عامة والجزائر بصفة خاصة.

- أهمية اختيار الموضوع:

تكمن أهمية موضوع الدراسة في راهنيته اليوم على المستوى الدولي والوطني، وفي ارتباط الجريمة الإلكترونية بحياة الأفراد والمؤسسات، خاصة في ظل صعوبة تطبيق النصوص التقليدية على هذه الجرائم، وهو ما دفع إلى التدخل التشريعي من قبل الدول لمواجهة الجريمة الالكترونية بما فيها المشرع الجزائري، لذا فان إدراك ماهية الجريمة المعلوماتية واستظهار خصائصها يتخذ أهمية كبيرة واستثنائية لسلامة التعامل مع هذه الظاهرة.

أهداف الدراسة:

تسعى هذه الدراسة إلى المساهمة في الجهد الأكاديمي الذي يحاول التعرف على خصوصية الجريمة الالكترونية موضوعيا وإجرائيا، ذلك أن حداثة هذه الجرائم وما تتسم به من خصائص سوف المشرع في حيرة أمامها وكيفية التعامل معها، إذ لا شك أن تكييفها والإلمام بها يختلف عما هو الحال عليه في الجرائم التقليدية.

مبررات اختيار موضوع الدراسة:

هناك عوامل ذاتية وأخرى موضوعية دفعتنا إلى اختيار موضوع الدراسة أهمها:

أ- **مبررات موضوعية:** إن الوقوف على حقيقة التعامل مع الجريمة المعلوماتية من الناحيتين الموضوعية والإجرائية وخصوصيتها في كل ناحية، هو السبب الرئيسي لاختيارنا للموضوع حيث أن الكثير من الدراسات التي عنيت بهذه الجرائم باتت تركز على الجانب الموضوعي فقط دون الإجرائي لذا حاولنا في دراستنا إثراء النقاش القانوني حول هذا الموضوع الهام.

ب- **مبررات ذاتية:** يحظى موضوع خصوصية الجرائم الإلكترونية بمكانة مهمة لدى مختلف الباحثين، ومنه فطبيعة التخصص تجعل الباحث أكثر ميولا لدراسة المواضع المتعلقة بمجال الإنترنت.

إشكالية الدراسة:

لقد تسارعت وتيرة الانترنت بصورة كبيرة في عالمنا المعاصر اليوم، إلا أنه وبقدر ما قدمته التكنولوجيا المتطورة من تسهيل الحياة العامة إلا أنها قد خلفت مشكلات وتحديات وجرائم إلكترونية جديدة، تختلف عن الجرائم التقليدية، انعكست على واقع الأفراد والمؤسسات، وعليه نطرح الإشكالية التالية:

- **ما مدى تميز الجريمة الإلكترونية عن الجريمة العادية في التشريع الجزائري ؟**

وللإجابة على هذه الإشكالية يمكن طرح الأسئلة الفرعية التالية:

- ما هو مفهوم الجريمة الالكترونية في التشريع الجزائري ؟
- ما هي خصوصية الجريمة الإلكترونية في التشريع الجزائري ؟

- **مناهج الدراسة:**

ولمعالجة هذا الموضوع والإحاطة بجوانبه المتعددة ومنه الإجابة على الإشكالية المطروحة، اعتمدنا على المنهج الوصفي التحليلي الذي يقوم على جمع المعلومات والنصوص القانونية وتحليلها لإعطاء أكثر دقة حول موضوع خصوصية الجريمة الالكترونية في التشريع الجزائري.

- **محاور الدراسة:**

جاءت هذه الدراسة في فصلين كاملين، قسمنا الفصل الأول إلى ماهية الجريمة الالكترونية أما الفصل الثاني فتم تقسيمه إلى آليات مكافحة الجريمة الالكترونية.

- **صعوبات الدراسة:**

يصاحب كل بحث أو عمل جملة من الصعوبات التي واجهناها في هذا المجال والمتمثلة في حداثة موضوع البحث وقلة المصادر المرتبطة به من جهة، وصعوبة الحصول على المراجع الكافية بسبب غلق المكتبات وغيابها إلكترونيا، بسبب جائحة كورونا التي مست العالم والجزائر.

الفصل الأول

الفصل الأول: ماهية الجريمة الالكترونية:

نحاول في هذا الفصل توضيح ماهية الجريمة الإلكترونية لنتمكن فيما بعد من استجلاء خصوصية هذه الجريمة، حيث تعرضنا إلى المفاهيم والمضامين المختلفة للجريمة الإلكترونية (المبحث الأول)، ومن ثم تحديد خصائصها (المبحث الثاني).

المبحث الأول: مفهوم الجريمة الالكترونية

الجريمة الالكترونية بوصفها ظاهرة إجرامية ذات طبيعة خاصة، نسعى من خلال هذا المبحث إلى تحديد مفهوم للجريمة الالكترونية (المطلب الأول)، ثم تحديد أركان هذه الجريمة والتطرق فيما بعد إلى معرفة أنواعها ودوافع ارتكابها (المطلب الثاني).

المطلب الأول: تعريف الجريمة الالكترونية وأركانها.

سنتطرق في هذا المطلب إلى تعريف الجريمة الإلكترونية في الفقه والاتفاقيات الدولية وفي التشريع الجزائري (الفرع الأول)، ومن ثم نقوم بتحديد أركانها (الفرع الثاني).

الفرع الأول: تعريف الجريمة الالكترونية

أدى إطلاق مصطلح الجريمة الالكترونية لما كانت المعلومة في شبكة الإنترنت هي المحل الرئيسي التي تعتمد عليها الجرائم الناشئة عن الاستخدام غير المشروع للإنترنت.

ولقد ظهرت أقوال فقهية، واتفاقيات دولية وتعريفات قانونية وذلك لتسليط الضوء بشكل مباشر على هذا النوع من الجرائم، ودراسة جميع جوانبها وحصرها للتمكن من مواجهتها والحد من انتشارها وحماية معلومات وحقوق أصحابها.

1- تعريف الجريمة الإلكترونية فقها:

تضاربت الأوصاف القانونية أو المصطلح الدقيق للجريمة الالكترونية بين أقوال فقهاء القانون الجنائي، وذلك لتقارب المفاهيم فهناك الجريمة الالكترونية التي يأخذها البعض على أنها الحقل ألمفاهيمي الذي تنطوي فيه باقي المفاهيم: الجريمة المعلوماتية، الإجرام الالكتروني الغش المعلوماتي، الانحراف الذي يقع باسطة الجانب الآلي، الإجرام السيبراني المجرم ألمعلوماتي الجريمة الرقمية وغيرها من المصطلحات والتسميات التي تصب في هذا

الشأن.

حيث ترى الدكتورة غنية باطلي أن: مصطلح الجريمة الالكترونية من شانها أن يدخل في مفهومها جرائم الحاسوب وغيرها من الجرائم التي يسميها البعض بالجرائم المعلوماتية أو الغش ألمعلوماتي، وجرائم الاعتداء على معطيات الحاسب الآلي وجرائم الانترنت وبالتالي كان فيه من التوسع ما ينطوي بين جوانبه العديد من السلوكيات الضارة بالأفراد والجماعة.

مما جعل المشرع يعزز الحماية الجنائية، فلا يستطيع المجرم أن يتحايل ويحقق مآربه عن طريق استغلال التقدم العلمي، وما قد يجلبه من إمكانيات لم تكن في ذهن المشرع وقت وضع النصوص[1].

يعرف الفقيه ماور: الجريمة الالكترونية هي الفعل غير المشروع الذي يتورط الحاسب الآلي في ارتكابه [2]، كما عرفها الفقيه ماس بأنها: الاعتداءات القانونية التي ترتكب بواسطة المعلومات بغرض تحقيق ربح [3].

كما عرفها بعض الفقه على أنها: نشاط غير مشروع لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزونة داخل الحاسب أو التي تحول عن طريقه.[4]

جانب من الفقه كذلك عرفها على أنها: إتيان فعل غير مشروع أو الامتناع العمدي عن أداء فعل واجب الإتيان من خلال استخدام أي وسيلة الكترونية أو تكنولوجية بشكل غير مشروع يكون من نتيجتها الاعتداء على حق من حقوق الغير شخصية، مادية أو معنوية [5].

---

[1] لعاقل فريال، **الجريمة المعلوماتية في ظل التشريع الجزائري**، مذكرة مقدمة لنيل شهادة المستر في القانون العام، جامعة أكلي محند اولحاج–البويرة– كلية الحقوق و العلوم السياسية، 2014– 2015 ، ص8 .

[2] المرجع نفسه ، ص 8 .

[3] عادل يوسف عبد النبي الشكري، الجريمة المعلوماتية و أزمة الشرعية الجزائية، **مجلة دراسات الكوفة**، جامعة الكوفة العراق، العدد السابع 2008، ص 113 .

[4] عادل يوسف عبد النبي الشكري، نفس المرجع، ص 113.

[5] عصام حسني الأطرش، محمد محي الدين عساف، **معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجهة نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية**، مجلة جامعة الشارقة للعلوم القانونية، جامعة الاستقلال أريحا –فلسطين– ، المجلد 16 ، العدد1 ، يونيو 2019 ، ص 636 .

وعرف الفقيه روزونبلات الجريمة الإلكترونية بأنها: نشاط غير مشروع موجه لنسخ أو الوصول إلى المعلومات المخزنة داخل الحاسوب أو تغييرها أو حذفها أو التي تحول عن طريقه[1].

تعتبر منظمة التعاون والتنمية الاقتصادية OCDE من السباقين لوضع تعريف للغش المعلوماتي والجريمة الالكترونية والتي ذهبت إلى القول:

« Est considéré comme crime informatique tout comportement illégale ou contraire l'éthique, ou non autorisé qui concerne un traitement automatique de données. »[2]

2- الاتفاقيات الدولية:

حاولت العديد من الأعمال الأكاديمية تعريف الجريمة الالكترونية، ومع ذلك فلا تبدو التشريعات الوطنية مهتمة بتعريف دقيق للمصطلح، تاركة عبء تعريفها على الفقه. وهو الحال كذلك بالنسبة للاتفاقيات الدولية أو الإقليمية لم تحدد مصطلح دقيق للجريمة الالكترونية وبدلا من ذلك فالاستخدام الأكثر شيوعا في التشريعات هو مصطلح (جرائم الكمبيوتر، والاتصالات الإلكترونية، وتكنولوجيا المعلومات)، ومنها اتفاقية مجلس أوروبا للجرائم الالكترونية، واتفاقية جامعة الدول العربية، واتفاقية الاتحاد الإفريقي...، على سبيل المثال اتفاقية كومنولث الدول المستقلة لم تستخدم مصطلح (الجرائم الالكترونية) في تعريفها فعرفت (الجريمة المتصلة بمعلومات الحاسوب) بأنها: العمل الإجرامي الذي يستهدف معلومات الحاسوب.[3]

---

[1] يوسف خليل يوسف العفيفي، **الجرائم الالكترونية في التشريع الفلسطيني تحليلية مقارنة**، رسالة مقدمة لنيل الماجستير في القانون العام، كلية الشريعة والقانون، الجامعة الإسلامية –غزة، 2013، ص 8.

[2] د. دمان ذبيح عماد(جامعة عباس لغرور–خنشلة)، د. بهلول سمية(جامعة محمد لمين دباغين–سطيف)، **الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري**، مجلة الحقوق والعلوم السياسية، جامعة عباس الغرور–خنشلة، العدد13، جانفي 2020، ص 141.

[3] د.ذياب موسى البداينة، **مداخلة بعنوان: الجرائم الالكترونية: المفهوم والأسباب**، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 2–2014/4، عمان–المملكة الأردنية الهاشمية، 2014، ص 5–6.

3- في القانون الجزائري:

نجد المشرع الجزائري قد نص في قانونه 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 05 غشت سنة 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، المادة 02 منه:جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية [1].

نلاحظ أن المشرع أعطى تعريفا عاما للجريمة الواقعة على النظام ألمعلوماتي، أن هذا التعبير "نظام المعالجة الآلية للمعطيات " هو تعبير فني تقني متطور يصعب إدراك تقنيته فهو خاضع للتطورات السريعة والمتلاحقة في مجال الحاسبات الآلية والرقمية.

السبب الذي عزف عن تعريفه المشرعون واكتفوا بالنهل من الفقه والقضاء، وقد حسم المشرع موقفه إلى جانب الفقه.

الفرع الثاني: خصوصية أركان الجريمة الالكترونية.

للجريمة الالكترونية ثلاثة أركان هي:

1- الركن الشرعي:

ويقصد به الصفات غير المشروعة للفعل، حيث يكون هناك قاعدة تجريمية وعقوبات مفروضة على الجرائم الالكترونية المرتبطة بأنظمة المعلومات وذلك تحقيقا لمبدأ " لا جريمة ولا عقوبة إلا بنص " فإذا انتفى التجريم انتفت عن مرتكبها المسؤولية الجزائية، يعد هذا المبدأ ضمانا لمصلحة الأفراد فهو الحامي الحقيقي لحقوق الافراد و كفالة الحريات الفردية، فملاحقة الأفعال وتوقيع العقاب يجب أن ينتج عن قوانين صادرة من السلطة التشريعية تجرم الأفعال وتعاقب مرتكبيها.

---

[1] **القانون 04/09 المؤرخ في 05 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحته**، ج.ر.ج.ج، ع 47، المؤرخة في 16 غشت 2009.

أول نص تشريعي جزائري في مجال الإجرام ألمعلوماتي لم يظهر في قانون العقوبات إلا في 26 جويلية 2001، بموجب القانون رقم 01-09، المواد 144 مكرر و146 مكرر و144 مكرر 2 و146 من قانون العقوبات الجزائري والمتعلق بجريمة القذف والسب والإهانة إزاء رئيس الجمهورية أو فيما يخص دين الإسلام (الرسول وباقي الأنبياء أو ما هو معلوم من الدين) أو ضد الهيئات المؤسسة أو الهيئات العمومية، ومن خصوصيات المادة 144 مكرر ق.ع أن المشرع أدرج فيها لأول مرة مصطلح"...وسيلة الكترونية أو معلوماتية.."التي تسمح بتجريم الأفعال السالفة الذكر في محيط المعلوماتية والانترنت بالإضافة إلى المواد 144مكرر 1 و2 و146 قانون عقوبات جزائري.[1]

ولقد ورد العقاب في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون 15/04 المؤرخ في 10 نوفمبر 2004 في الفصل السابع مكرر من المواد 394مكرر إلى 394 مكرر7.[2] ولقد كان تعديل هذا القانون بموجب القانون رقم 04/09 المؤرخ في 14 شعبان 1430 الموافق ل 05 أوت 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.[3]

2- الركن المادي:

يمثل الركن المادي الوجه الخارجي الظاهر للجريمة، وبه يتحقق الاعتداء على المصلحة المحمية، وعن طريقه تقع الأعمال التنفيذية للجريمة، وحتى تنهض الجريمة مكتملة وتامة لابد من توافر عناصر ثلاثة وهي: السلوك الإجرامي، النتيجة الإجرامية والعلاقة

---

[1] شلاخ لطيفة، **انتشار الجريمة الالكترونية الماسة بالأشخاص في البيئة الجزائرية –دراسة ميدانية لبعض مستخدمي مقاهي النت بمدينة المسيلة**، مذكرة مكملة لنيل شهادة المستر في علوم الإعلام الآلي والاتصال تخصص صحافة مكتوبة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف –المسيلة، ماي 2017، ص 14.

[2] بموجب **المواد من 394 مكرر إلى 394 مكرر 7 من القانون 15/04 المؤرخ في 10 نوفمبر 2004** ج.ر.ج.ج، ع 71 مؤرخ في 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1966 المتضمن قانون العقوبات المعدل و المتمم، ص 11-12

[3] **القانون 04/09**، مرجع سبق ذكره.

السببية بينهما، وهي نفس العناصر في الجريمة الالكترونية، إلا أنهما يختلفان باختلاف سلوك مرتكبيها وشخصيته، وكذا صور الاعتداء.

أ- السلوك الإجرامي:

يعد السلوك الإجرامي أهم الأركان كونه يكشف عن سلوك مخالف لإرادة المجرم، ويبدو بمظاهر مادية في العالم الخارجي، أي أن الأفكار داخل النفس لا عقاب عليها إلا انه في جرائم المعلومات العمل التحضيري والنشاط الإجرامي يصعب التفرقة بينهما فالأمر يختلف من العالم الحقيقي والعالم الرقمي هذا الأخير الذي يعاقب المشرع على الأعمال التحضيرية فيه كشراء برنامج اختراق، ومعدات لفك الشفرات وكلمات المرور وحيازته صور دعارة للأطفال أو حتى بعض الفيروسات الالكترونية كلها جرائم في حد ذاتها[1].

ويتخذ الركن المادي في هذه الجرائم عدة صور مثلا:

- جريمة الإرهاب الالكتروني فان السلوك الإجرامي هنا هو إطلاق صفحات أو مواقع تدعو وتحرض على الانضمام لمثل هذه الجماعات، أو مثلا تبين كيفية صناعة قنابل.

- المواقع الإباحية كمثال أخر تزود مواقعها بصور وأفكار الشذوذ الجنسي وهناك مواقع تنشر فكرة الانتحار أو تشويه صورة الإسلام.

- جريمة الغش ألمعلوماتي الركن المادي فيها هو تغيير الحقيقة في مستند رسمي أو محرر رسمي وهي عبارة عن تسجيلات الكترونية أو محررات رسمية.

ب- النتيجة الإجرامية:

النتيجة الإجرامية في الجريمة التقليدية واضحة ذلك انه لا يكفي السلوك الإجرامي مهما بلغت جسامته ما لم يقترن بنتيجة، كجريمة القتل إن لم تنتج الوفاة كنا أمام جريمة الشروع في القتل.

---

[1]- الدكتور وليد طه، **التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست**، جمهورية مصر العربية، ص 17.

أما النتيجة الإجرامية في الجريمة الالكترونية يقوم النقاش فيما إذا كانت نتيجة الفعل الإجرامي في العالم الافتراضي أم في العالم الخارجي الحقيقي وكلاهما محتمل الحدوث وكذا النقاش حول مكان وزمان تحقق النتيجة الإجرامية وبالتالي تنازع القوانين. [1]

ج- العلاقة السببية: هي الصلة بين الفعل والنتيجة، وتثبت أن ارتكاب الفعل هو الذي أدى إلى النتيجة، فمثلا تشغيل الجهاز لاختلاس المعلومة تتحقق النتيجة بحصوله على المعلومة. فالعلاقة السببية في الجرائم الالكترونية هي العلاقة التقنية بين مرتكب الجريمة وبين الآلة محل الجريمة الالكترونية، وهي الأساس لتحديد نطاق المسؤولية الجزائية في كل الجرائم الالكترونية العمدية، ويقع عبء إثبات وجود الرابطة السببية من عدمها على النيابة العامة بما يقدم إليها من أدلة وبيّنات واستماع للشهود في مثل هذا النوع من الجرائم المستحدثة.[2]

وتتمثل صور الاعتداء المنصوص عليها في قانون العقوبات في:

- الدخول أو البقاء غير المشروع في نظام المعالجة الآلية للمعطيات:

-**الصورة البسيطة:** يتمثل النشاط الإجرامي في الأفعال الآتية:

-فعل الدخول: يتحقق فعل الدخول بمجرد الوصول إلى المعلومات المخزنة داخل النظام ودون علم ورضا صاحبه، لأن هذا النظام لا يسمح للدخول فيه إلا لأشخاص معينين أو يسمح بالدخول لكن مقابل نفقات.

-البقاء: معنى البقاء هو التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام، أو بتجاوز المدة المسموح له بالبقاء فيها، أو عدم الانسحاب فورا وقطع وجوده في نظام البيانات أو يطبع معلومات حين يسمح له بالرؤية فقط.

-**الصورة المشددة:** نصت المادة 394 مكرر في الفقرتين الثانية والثالثة من قانون العقوبات على ظروف تشديد عقوبة فعل الدخول والبقاء غير المشروع عندما ينتج عن هذين الفعلين

---

[1] الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الالكترونية، ص 4، على الرابط: *https://repository.najah.edu/handle/20.500.11888/1348 counsulté:08/09/2020* heur 12:26.

[2] د. لورنس سعيد الحوامدة، مرجع سبق ذكره، ص 23.

إما محو أو تحويل المعطيات التي يحتويها النظام، وإما عدم صلاحية النظام لأداء وظائفه من خلال تخريب نظام اشتغال المنظومة.

– **إدخال معطيات بطريق الغش:** يقصد به حسب المادة 394 مكرر1 من قانون العقوبات إضافة معطيات جديدة إلى نظام المعالجة الآلية أو التعديل من معلومات داخله كأن يتضمنه مسبقا فيغير فيها، ومثال ذلك حالة الاستخدام التعسفي لبطاقات السحب والائتمان سواء من صاحبها الشرعي أو عن غيره كحالة السرقة والتزوير.[1]

3 – الركن المعنوي:

يعد الحالة النفسية للجاني، والعلاقة التي تربط بين ماديات الجريمة وشخصية الجاني كما يمكن تعريف الركن المعنوي على أن: العلاقة التي تربط بين ماديات الجريمة وشخصية الجاني مرتكبها، وهذه العلاقة هي محل الإذناب في معنى استحقاق العقاب، ومن ثم يوجه إليها لوم القانون وعقابه.[2]

ويتمثل الركن المعنوي للجريمة الالكترونية في اتجاه إرادة الجاني لارتكاب جريمة من الجرائم الالكترونية مع علمه بأن المشرع يجرمها [3]، فهو الوسيلة الأساسية في تحديد طبيعة سلوك مرتكبها وتكييفه وتحديد العقوبة المقررة له، إذ أن انتفاء هذا الركن يوقعنا في جريمة واحدة هي جريمة الدخول أو الولوج غير المشروع.

في جريمة الاحتيال الالكتروني التي بدورها تعد جريمة عمدية يتطلب لقيامها توافر القصد الجنائي لقيام مسؤولية الجاني، والقصد الجنائي المشترط هو القصد الجنائي بنوعيه العام والخاص، فالمجرم يعلم بأنه يخالف القانون بسلوكه مع اتجاه نيته إلى تحقيق ربح غير

---

[1] عشاش حمزة، حمزة خضري، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، جامعة محمد بوضياف – المسيلة، مقال مقدم إلى مجلة الدراسات القانونية والسياسية تصدر عن جامعة عمار ثليجي بالأغواط–الجزائر، المجلد 06، العدد 02، 2020/06/05، ص186–185.

[2] عبد الله دغش العجمي، **المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة**، رسالة ماجستير في القانون العام بعنوان، جامعة الشرق الأوسط، 2014 ، ص 29 .

[3] وليد طه، مرجع سبق ذكره ، ص 17.

مشروع له أو للغير أو تجريد شخص آخر من ممتلكاته على نحو غير مشروع.[1]

وتبعا للقانون 394 مكرر، 394 مكرر1، 394 مكرر2 و394 مكرر5 فقد عبر عن الركن المعنوي في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات بالغش، العمد، والإعداد للجريمة. وهذا يدل على أن الجريمة الالكترونية جريمة عمدية ولا يفترض فيها الخطأ.

المطلب الثاني: أنواع الجريمة الالكترونية ودوافع ارتكابها

استحدث بموجب الثورة المعلوماتية الحاصلة أنواع جديدة من الجرائم ذات خصائص مغايرة عنها في الجرائم العادية ما دفع بالهواة والمجرمين إلى استغلالها في أفعالهم غير المشروعة لتحقيق مآربهم، وسنحاول تحديد أنواع الجريمة المعلوماتية وكذا تبيان دوافع المجرمين من ارتكابها.

الفرع الأول: أنواع الجرائم الالكترونية:

من الصعوبة تماما حصر الجريمة الالكترونية حيث أن أشكالها متعددة متنوعة وهي تزداد تنوعا وتعدادا كلما أوغل العالم في استخدام الحاسب الآلي وشبكة الانترنت، ما جعل المشتغلين بالفقه الجنائي في جدال حول تقسيم هذه الجرائم، فقد يكون النظام ألمعلوماتي هو نفسه موضوع أو محل الجريمة، فيما قد يكون أيضا هو أداة الجريمة ووسيلة تنفيذها.

أولا: الجرائم الواقعة بواسطة النظام ألمعلوماتي:

يعد الحاسب الآلي في هذا النوع من الجرائم وسيلة لتسهيل النتيجة الإجرامية ومضاعفا لجسامتها ويهدف الجاني من وراءها إلى تحقيق ربح مادي بطريقة غير مشروعة، تستخدم النظام ألمعلوماتي في حد ذاته أو برامجه كوسيلة لتنفيذ الجريمة.

وتنقسم هذه الجرائم بدورها إلى:

1/ الجرائم الواقعة على الأشخاص:

رغم تطور الحياة اليومية للأفراد والمجتمع بفضل استعمالهم للفضاء الافتراضي إلا أنه أصبح سلاحا فتاكا في يد المجرمين للدخول إلى المعلومات الخاصة للأشخاص، وعليه

[1] عشاش حمزة، حمزة خضري، مرجع سبق ذكره، ص186.

ظهرت عدة أنواع خاصة من الجرائم الالكترونية الواقعة على الأشخاص كجريمة التهديد والمضايقة والملاحقة. وهذا ما سنوضحه فيما يلي:

أ- **جريمة التهديد والمضايقة والملاحقة:** التهديد هو الوعيد بالشر، الذي يقصد به زرع الخوف في النفس بالضغط على إرادة الإنسان وتخويفه من أضرار ما سيلحقه أو سيلحق أشياء أو أشخاص له صلة به.

يعتبر تهديد الغير من خلال البريد الإلكتروني واحد من أهم الاستخدامات غير المشروعة للانترنت، حيث يقوم الفاعل بإرسال رسالة إلكترونية إلى المجني عليه تنطوي على عبارات تسبب خوفا له.[1]

تتم جرائم الملاحقة على شبكة الانترنت غالبا باستخدام البريد الالكتروني أو وسائل الحوارات الآلية المختلفة على الشبكة كالفايبر والفايس بوك والواتس آب، وتشمل الملاحقة وسائل تخويف ومضايقة تتفق مع مثيلاتها خارج الشبكة في الأهداف المجسدة في رغبة التحكم في الضحية، وتتميز عنها بسهولة إمكانية إخفاء هوية المجرم، علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة.[2]

ب- **إنتحال الشخصية والتغرير والاستدراج:** هي جريمة الألفية الجديدة كما سماها بعض المختصين في أمن المعلومات وذلك نظرا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية، تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية وتهدف إما لغرض الاستفادة من مكانة تلك الهوية أو لإخفاء هوية شخصية المجرم، لتسهيل ارتكابه جرائم أخرى. إن ارتكاب هذه الجريمة على شبكة الانترنت أمر سهل وهذه من أكبر سلبيات الانترنت الأمنية.[3]

---

[1] رزيق ليلة، رمضاني حميدة، **الجريمة الالكترونية واقع وتحدي**، مذكرة ماستر تخصص قانون جنائي وعلوم إجرامية، جامعة مولود معمري-تيزي وزو، 2018/07/09، ص 16.

[2] أستاذة نميدلي رحيمة، **خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة**، مداخلة مقدمة في مؤتمر الجرائم الالكترونية المنعقد في طرابلس، يومي 24-25 /03/ 2017، ص 95.

[3] د.فوزي شروق سامي، **تكنولوجيا الإعلام الحديث**، مؤسسة طيبة للنشر والتوزيع، طبعة1، القاهرة، 2014، ص 45.

أما التغرير والاستدراج فغالب ضحايا هذا النوع هم صغار السن من مستخدمي الشبكة، حيث يوهم المجرمون ضحاياهم برغبتهم في تكوين صداقة على الانترنت والتي قد تتطور إلى التقاء مادي بين الطرفين.[1]

ج- جرائم القذف والسب والتشهير وتشويه السمعة: يقوم المجرمون بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فردا أو مجتمع أو دين أو مؤسسة تجارية أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوبة نشرها أو إرسالها هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.[2]

د- الصناعة الإباحية: لقد وفرت شبكة الانترنت أكثر الوسائل فعالية وجاذبية لصناعة ونشر الإباحية، إن الانترنت جعلت الإباحية وسائل عرضها من صور وفيديوهات وحوارات في متناول الجميع، ولعل هذا يعد أكبر الجوانب السلبية للانترنت خاصة في مجتمع محافظ على دينه وتقاليده كمجتمعنا.

إن صناعة ونشر الإباحية تعد جريمة في كثير من الدول خاصة تلك التي تستهدف أو تستخدم الأطفال. لقد تمت إدانة مجرمين في أكثر من 200 جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات والتي انتهت في ديسمبر 1998م، تتعلق هذه الجرائم في تغرير الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهدة إباحية للأطفال.[3]

2/ الجرائم الواقعة على الأموال:

في ظل التحول من المعاملات التجارية التقليدية إلى المعاملات التجارية الالكترونية وتطور وسائل الدفع والوفاء، والتداول المالي الالكتروني، انجر عنه جملة من الجرائم منها:

أ-جرائم السطو على أرقام بطاقات الائتمان والتحويل الالكتروني غير المشروع: أدى استخدام البطاقات الائتمانية من خلال شبكة الانترنت إلى ظهور الكثير من المتسللين

---

[1] رزيق ليلة، رمضاني حميدة، مرجع سبق ذكره، ص 16.

[2] وائل رفعت علي خليل، **إشكاليات الإعلام ومعطيات الواقع**، المنهل، د.ب.ن، 2015، ص184.

[3] فوزي شروق سامي، مرجع سبق ذكره، ص 44-45.

للسطو عليها باعتبارها نقود الكترونية، خاصة أن الاستيلاء على هذه البطاقات ليس بالأمر الصعب، بحيث أن لصوص هذه البطاقات يستطيعون الآن سرقة مئات الألوف من أرقام البطاقات في يوم واحد من خلال شبكة الانترنت ومن ثم بيع هذه المعلومات للآخرين.

تتم عملية التحويل الالكتروني غير المشروع للأموال من خلال الحصول على كلمة السر المدرجة في ملفات أنظمة الكمبيوتر الخاصة بالمجني عليه، مما يسمح للجاني بالتوغل في النظام المعلوماتي والخدمات على الشبكة عن طريق تصريح كتابي أو تلفوني، بخصم القيمة على حساب بطاقة الدفع الالكتروني الخاصة به، وتتم العملية بدخول العميل أو الزبون إلى موقع التاجر ويختار السلع المراد شراؤها ويتم التعاقد بملأ النموذج الالكتروني ببيانات بطاقة الائتمان الخاصة بالمشتري.[1]

ب- القمار وتبييض الأموال عبر الانترنت: يعد غسيل الأموال من أبرز الأنشطة التي تقوم بها شبكات منظمة تحترف الإجرام الالكتروني، وتأخذ درجة عالية من التنسيق والتخطيط والانتشار في كافة أنحاء العالم، وتشير إحصائيات الأمم المتحدة وصندوق النقد الدولي إلى أن 30 مليار دولار أمريكي من الأموال القذرة تغسل سنويا عبر الشبكات الالكترونية مخترقة حدود ما يقارب أو أزيد عن 76 دولة في العالم.[2]

ج- جريمة السرقة والسطو على أموال البنوك: وتتحقق بواسطة استخدام المجرم الالكتروني بغرض الدخول إلى البنوك وغيرها من المؤسسات المالية، وتحويل الأموال من الحسابات الخاصة بالعملاء إلى حسابات أخرى، وقد يتم ذلك بكميات بسيطة بصفة متكررة بحيث لا يلفت الانتباه، وقد يتم دفعة واحدة.[3]

د- تجارة المخدرات عبر الانترنت: إن المخاوف من استخدام الانترنت لا تقتصر على ارتكاب الإنترنت في ارتكاب الجريمة بل تساهم بعض المواقع في انحراف الشباب وخصوصا

---

[1] رزيق ليلى، رمضاني حميدة، مرجع سبق ذكره، ص 14.

[2] رحموني محمد، **خصائص الجريمة الالكترونية ومجالات استخدامها**، جامعة أحمد دراية-أدرار، مجلة الحقيقة، العدد 41، 2018/01/10، ص 448.

[3] د.نعيمة دوادي، **الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)**، جامعة علي لونيسي-البليدة، مجلة مهد اللغات، جامعة حسيبة بن بوعلي بالشلف-الجزائر، المجلد 2، العدد 1، 2020/08/20، ص 51.

من المراهقين وذلك من خلال إنشاء مواقع الكترونية بقصد الاتجار بالمخدرات أو المؤثرات العقلية أو الترويج لها أو تعاطيها أو تسهيل التعامل فيها أو تعامل أو تفاوض بقصد إبرام الصفقات المتعلقة بالاتجار بها بأي شكل من الأشكال.[1]

3/ الجرائم الواقعة على أمن الدولة وجرائم ماسة بالأمن الفكري:

تعد هذه الجرائم من أخطر الجرائم الالكترونية، حيث استغلت الجماعات المتطرفة اتصالات الانترنت من أجل نشر أفكارها ومعتقداتها، بل تعدتها إلى تهديد أمن الدول من خلال الإرهاب والجرائم المنظمة وجرائم التجسس وجرائم الأمن الفكري:

أ- الجماعات الإرهابية: مما لا شك فيه أن ظاهرة الإرهاب أضحت عالمية، حيث ظهرت الكثير من التنظيمات بمختلف التسميات، تظهر العلاقة بين الإرهاب والجريمة الالكترونية من خلال تجنيد وتجييش أعضاء جدد في التنظيم أو حشد الهمم بواسطة استخدام مختلف وسائل التواصل الالكتروني.[2]

ب- الجريمة المنظمة: هي تكوين جماعة أو تنظيم بقصد ارتكاب أنشطة إجرامية خطيرة جدا. ويتبعون في ذلك طرق وأساليب محددة باستخدام العنف والتهديد لإخضاع العامة والحفاظ على أمن المنظمة الإجرامية لتحقيق مكاسب مالية، مستغلة في ذلك وسائل الاتصال والانترنت لتنفيذ عملياتها الإجرامية بيسر وسهولة.[3]

ج- الجريمة الماسة بالأمن الفكري: يبقى الأمن الفكري من بين أخطر الجرائم المرتكبة عبر الانترنت، حيث تعطي الانترنت فرصا للتأثير على معتقدات وتقاليد مجتمعات بأكملها مما يجعلها عرضة للهزيمة الفكرية وهو ما يسهل خلق الفوضى.[4]

---

[1] د.ليلى الجنابي،**فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية**، 2017، على الرابط التالي:
www.ahewar.org consulté le: 16 /09/2020 à 01 :03h.

[2] نعيمة داودي، مرجع سبق ذكره، ص 51.

[3] د.جيلالي الحسين، **التعاون الجنائي الدولي في مكافحة الجريمة العالمية**، مجلة القانون، المركز الجامعي أحمد زبانة- غليزان، العدد 02، 2018، ص 18-19.

[4] د.أحمد بن خليفة، ط. حفوظة الأمير عبد القادر، **الجريمة الالكترونية وآليات التصدي لها**، مجلة الامتياز لبحوث الاقتصاد والإدارة، العدد 01، جوان 2017، ص 158.

د- جريمة التجسس الإلكتروني: إن التطور في المجال الالكتروني ألمعلوماتي سهل من مهمة التجسس، فالمجرم الالكتروني سواء كان شخص واحد أو تنظيم يمكنه التجسس سواء على أشخاص أو منظمات وحتى دول. ويكون إما تجسس اقتصادي أو سياسي أو عسكري[1].

ثانيا: الجرائم الواقعة على النظام ألمعلوماتي:

إضافة إلى الجرائم المعلوماتية التي تقع باستخدام النظام ألمعلوماتي هناك نوع آخر من الجرائم المعلوماتية يمس النظام ألمعلوماتي ويستهدف إما المكونات المادية للنظام ألمعلوماتي أو المكونات المنطقية أو المعلومات المدرجة بالنظام ألمعلوماتي.

أ- الجرائم الواقعة على المكونات المادية للنظام المعلوماتي: إن الاعتداء على المكونات المادية للنظام ألمعلوماتي يتحقق إذا كان الحاسوب والأجهزة الملحقة به من معدات وكابلات، وشبكات الربط وآلات طباعة محلا للاعتداء، وتقوم الجريمة في هذه الحالة بإتيان أي فعل مادي من شأنه إخراج الحاسوب من حيازة مالكه وإدخاله في حيازة شخص آخر، أو إتلاف الجهاز وتدميره وغير ذلك من الأفعال المجرمة.

وهذه الجرائم هي جرائم تقليدية باعتبار أن هذه المكونات المادية محل الاعتداء تتمتع بالحماية الجزائية وفق النصوص التقليدية، باعتبارها من الأموال المادية المنقولة والتي تخضع سرقتها أو إتلافها للنصوص الجزائية التقليدية القائمة ويسأل مرتكبوها بموجب النصوص العقابية في قانون العقوبات، وعلى هذا الأساس فإن المكونات المادية للنظام ألمعلوماتي تخرج من نطاق المحل الذي ينصب عليه السلوك الإجرامي في الجرائم المعلوماتية.[2]

ب- **الجرائم الواقعة على البرامج الالكترونية:**وتنقسم هذه الجرائم بدورها إلى الجرائم الواقعة على البرامج التطبيقية، عن طريق تحديد البرنامج أولا ثم التلاعب به أو تعديله، ومن أمثلتها

---

[1] د.نعيمة داودي، نفس المرجع، ص 51.

[2] سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر-باتنة، 2012-2013، ص 36-37.

قيام أحد المبرمجين بالبنوك الأمريكية بتعديل برنامج بإضافة دولار واحد على كل حساب يزيد عن عشرة دولارات وقام بتقييد المصاريف الزائدة في حساب خاص به أطلق عليه اسم Zwicky.

وكذلك تضم هذه الجرائم الواقعة على برنامج التشغيل وهي البرامج المسؤولة عن عمل النظام ألمعلوماتي، ومن حيث قيامها بضبط ترتيب العمليات الخاصة بالنظام، وتقوم هذه الجريمة عن طريق تزويد البرنامج بمجموعة تعليمات إضافية للوصول إليها بشفرة تسمح بالدخول إلى جميع المعطيات التي يتضمنها النظام ألمعلوماتي ومثالها: جريمة تصميم برنامج وهمي من خلاله تنفذ الجريمة، ومثاله ما قامت به إحدى الشركات التأمين الأمريكية في مدينة لوس انجلوس بواسطة مبرمجها تصميم برنامج يقوم بتصنيع وثائق تأمين لأشخاص وهميين بلغ عددهم 46000 بهدف تقاضي هذه الشركة لعمولات من اتحاد شركات التأمين.[1]

ج- الجرائم الواقعة على المعلومات المدرجة بالنظام ألمعلوماتي: وتتحقق هذه الحالة عندما تكون مكونات الحاسب غير المادية المتمثلة في المعلومات بكل صورها من البيانات والبرامج المخزنة في ذاكرة الحاسب محلا للاعتداء، كأن يتم سرقتها أو إتلافها أو تزويرها والعبث بها وغير ذلك من الأفعال غير المشروعة. وهي الحالة التي تقف النصوص العقابية التقليدية قاصرة على تحقيق الحماية الكافية والمتكاملة للمعلومات.[2]

ومثالها ما قام به شخص يدعى *bluff Vladimir loriblitt* وهو موظف بوزارة المالية، حيث قام بإدخال بجريمة الغش أو التزوير ألمعلوماتي بإسرائيل باستخدام طريقة تدعى فواتير وهمية لا حصر لها وتحويل ما تم سداده من هذه الفواتير لحساب الشركات الوهمية التي قام بإنشائها.[3]

---

[1] نميدلي رحيمة، مرجع سبق ذكره، ص 96.

[2] سعيداني نعيم، مرجع سبق ذكره، ص 37.

[3] نميدلي رحيمة، مرجع سبق ذكره، ص 96.

الفرع الثاني: دوافع ارتكاب الجريمة الالكترونية:

لكل جريمة دافع يحفز المجرم على ارتكابها، فجريمة السرقة مثلا تكون جراء فقر أو احتياج أو ضائقة أصابت صاحبها دفعت به إلى نهب مال الغير، والجريمة الالكترونية كغيرها من الجرائم تكمن وراء ارتكابها جملة من الدوافع الشخصية أو الاجتماعية أو السياسية ولعل أهمها ما يلي:

1-استكشاف عالم شبكة المعلومات الدولية:نظرا للثورة التكنولوجية الحديثة وانتشارها في المجتمعات المتقدمة بصورة هائلة وما أدى ذلك إلى انبهار بعض المجرمين بهذه التقنية الحديثة إن كانوا ليسوا على درجة كبيرة من الخطورة الإجرامية إذ أنه لا يتوافر لديهم أي نوايا سيئة إلا أن غايتهم عند ارتكاب مثل هذه الجرائم هي غاية التعلم. ويرى بعض الباحثين أن الدافع قد يكون الرغبة في قهر أنظمة الشبكة،حيث يميل مرتكبي هذه الجرائم في حالة ظهور تقنية حديثة إلى إظهار تفوقهم وبراعتهم، فيحاولون إيجاد الوسيلة إلى تحطيم تلك تقنية أو التفوق عليها ويتزايد شيوع هذا الدافع لدى فئة صغار السن.[1]

2-دوافع مادية: ويتمثل تحقيق الكسب المادي، تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الانترنت، نظرا للربح الكبير وغالبا ما يكون الدافع لارتكاب هذه الجريمة هو وقوع الجاني في مشاكل مادية مثال على ذلك تحويل حساب مالي إلى حسابه.[2]

3-دوافع شخصية: وتتمثل في الرغبة في التعلم حيث يكرس مرتكبو هذه الجريمة وقتهم في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الأمنية للأنظمة الحاسوبية.

4- دافع التسلية: هي جريمة ترتكب من اجل التسلية وإشباع الفضول ولا يقصد منها أحداث جريمة.

5- دوافع ذهنية أو نمطية: الصورة الذهنية لمرتكبي جرائم الحاسوب والإنترنت غالبا هي

---

[1] د.غادة نصار، **الإرهاب والجريمة الإلكترونية**، طبعة 1، العربي للنشر والتوزيع، القاهرة، 2017، ص52.

[2] مجموعة الدكتور عبد الله اليحيى للمحاماة والاستشارات القانونية والتحكيم، ورقة عمل عن (الجرائم الالكترونية)، مقدمة إلى ملتقى الحقوق والعدالة للتعاملات الالكترونية بالرياض –السعودية، 2018/05/31.

صورة البطل والذكي، الذي يستحق الإعجاب لا صورة المجرم الذي يستوجب العقاب فمرتكبو هذه الجرائم يسعون إلى إظهار تفوقهم ومستوى ارتقاء براعتهم، لدرجة أنه إزاء ظهور أية تقنية مستحدثة فإن مرتكبي هذه الجرائم لديهم شغف الآلة، فيحاولون تحطيمها أو التفوق عليها.[1]

6- دافع الانتقام من رب العمل وإلحاق الضرر به: هناك آثار سلبية في سوق العمل من جهة وفي البناء الوظيفي من جهة أخرى، وقد لوحظ أن العاملين في قطاع التقنية أو المستخدمين لها في نطاق قطاعات العمل الأخرى ويتعرضون على نحو كبير لضغوطات نفسية ناجمة عن ضغط العمل والمشكلات المالية، ومن طبيعة العلاقات العمل المنفرة في حالات معينة، هذه الأمور قد تدفع إلى النزعة نحو تحقيق الربح لكنها في حالات كثيرة مثلث قوة محركة لبعض العاملين لارتكاب جرائم الكمبيوتر باعثها الانتقام من المنشأة أو رب العمل، أي أن الحقد على رب العمل الدافع المحرك لارتكاب الجريمة.[2]

7- دوافع سياسية وتجارية: وهي عموما محرك أنشطة الإرهاب الالكتروني فكثيرة هي المنظمات في عصرنا الحالي والتي تتبنى بعض الآراء والأفكار السياسية أو الدينية أو الإيديولوجية، ومن أجل الدفاع عن هذه الآراء تقوم بأفعال إجرامية ضد معارضيها. فمثلا هناك العديد من عمليات الاختراق تعود لأسباب عقائدية، حيث يقوم بعض المجموعات التي تتبنى فكرة الإصلاح، بعملية رقابة أخلاقية أو اجتماعية أو دينية، فتتجسس على المواقع التي تقدم خدمات أو معلومات تتعارض مع قناعتها، وتعمل على كشف أسرارها أو حتى تدميرها، فهناك مواقع تستهدف الأسرار الدبلوماسية والعسكرية، أما عن المعلومات التجارية فدافعها المنافسة.[3]

---

[1] لعاقل فريال، مرجع سبق ذكره، ص 25.

[2] رابحي عزيزة، **الأسرار المعلوماتية وحمايتها الجزائية**، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد–تلمسان، 2018/2017، ص 101.

[3] رابحي عزيزة، نفس المرجع، ص 101.

المبحث الثاني: خصائص الجرائم الالكترونية:

إن الانتقال من العالم المادي إلى عالم الرقميات غير من خصوصية الجريمة الواقعة في نظامه، فأعطى للجريمة الالكترونية سمات خاصة، تتحكم فيها الرقميات من جهة (المطلب الأول)، وسيمات مرتكبيها من جهة أخرى، (المطلب الثاني) وهذا ما نحاول تبيانه من خلال هذا المبحث.

المطلب الأول: خصائص خاصة بالجريمة الالكترونية:

تختلف الجريمة المعلوماتية عن الجريمة العادية ذلك من خلال الخصائص الخاصة التي تتسم بها، ولعل أهمها ما يلي:

1- **جريمة عابرة للقارات:** ذلك لقدرة تقنية المعلومات على اختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم، ما جعل مسرح الجريمة مكشوفا عالميا، فهي تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الأحيان إلى تحديات قانونية إدارية وفنية، بل وسياسية بشان مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية القيام بإعداد احد البرامج في بلد ما ثم يتم نسخ هذا البرنامج ويرسل إلى دول مختلفة من العالم. [1]

2- جرائم ناعمة: تتسم الجرائم الناشئة عن استخدام الانترنت بأنها ناعمة لخفتها ولكونها متسترة في أغلبها، كما أن الضحية لا يلاحظ ارتكابها رغم أنها قد تقع أثناء وجوده على الشبكة، فالجاني يتمتع بقدرات فنية تمكنه من تنفيذ جريمته بدقة، ومثال ذلك إرسال الفيروسات المدمرة وسرقة الأموال والبيانات الخاصة أو إتلافها والتجسس وغيرها من الجرائم.

ويستفيد المجرمون في مختلف مناطق العالم من الشبكة في تبادل الأفكار والخبرات الإجرامية فيما بينهم، ويظهر ذلك جليا في مختلف المواقع الإلكترونية ومنتديات قراصنة الهاكرز التي تضمن لهم الاتصال فيما بينهم بهدف تبادل الخبرات في مجال القرصنة، من

---

[1] ادهم باسم نمر بغدادي، **وسائل البحث والتحري عن الجرائم الالكترونية**، مذكرة مقدمة لنيل درجة ماجستير في القانون العام، كلية الدراسات العليا، جامعة النجاح الوطنية، نابلس–فلسطين، 2018، ص 11–13.

أجل ارتكابهم لجرائمهم بعيدا عن أعين الأمن.[1]

3- المساهمة في ارتكابها: إذ تتم الجريمة المعلوماتية من شخص لديه معرفة فنية في مجال الحاسوب، والذي يكون له دور إيجابي في المشروع الإجرامي، فمثلا يقوم الشخص المتخصص في تقنيات الحاسوب والانترنت بالجانب الفني من الجريمة، وبالتعاون مع شخص من محيط المؤسسة المجني عليها أو من خارجها لتغطية عملية التلاعب وتحويل المكاسب إليه. فعلى صعيد عمل المصارف يقوم موظف البنك، بتزويد العصابات بالبيانات الخاصة ببطاقات الائتمان الصحيحة والمتداولة، وذلك لغرض مساعدتهم في تقليد أو اصطناع هذه البطاقات، وبالتالي تتحقق الجريمة باصطناع أو تقليد بطاقات ائتمان مزورة، فالاشتراك بالجريمة المعلوماتية قد يكون إيجابيا وهو الغالب ويكون بتقديم مساعدة فنية أو مادية، وقد يكون الاشتراك سلبيا يتمثل بعدم الإبلاغ من جانب من علم بوقوع الجريمة محاولة منه تسهيل إتمامها.[2]

4- وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للبيانات: جرائم الالكترونية يمكن أن ترتكب أثناء أي مرحلة من مراحل التشغيل الأساسية وهي مراحل الإدخال أو المعالجة أو الإخراج.

- ففي مرحلة المدخلات يمكن ترجمة المعلومات إلى لغة مفهومة من قبل الحاسب، وبهذا يسهل إدخال معلومات غير صحيحة وعدم إدخال وثائق أساسية، وبذلك يمكن في مرحلة المدخلات ارتكاب الجانب الأكبر من الجرائم الالكترونية.

- وفي مرحلة المعاجلة يمكن إدخال أي تعديلات لتحقيق هدف إجرامي عن طريق التلاعب في برامج الحاسب، كتشغيل برامج جديدة أو دس تعليمات غير مصرح بها أو عمل برامج أصلية.

---

[1] أسامة مهمل، **الإجرام السيبيراني**، مذكرة لنيل شهادة المستر الأكاديمي، فرع القانون الجنائي، جامعة محمد بوضياف- المسيلة، 2018/2017، ص 12.

[2] ضرغام جابر عطوش آل مواش، **جريمة التجسس المعلوماتي: دراسة مقارنة**، المركز العربي للنشر والتوزيع، مكتبة دار السلام القانونية، السعودية، الطبعة الأولى، 2017، ص 33.

ويتطلب التشغيل في مرحلة المعالجة توافر معرفة فنية عميقة لدى الفاعل، والجرائم التي ترتكب في هذه المرحلة نادرا ما تكتشف، وقد يكون عامل المصادفة هو شبب اكتشافها.

– أما في مرحلة الإخراج فإن التلاعب يقع في النتائج التي يخرجها الحاسب عن طريق إدخال بيانات صحيحة، وتعالج فيه بطريقة صحيحة.[1]

5– الجرائم الالكترونية فادحة الأضرار: إن الاعتماد المتزايد على الحاسب الآلي في إدارة مختلف الأعمال في شتى المجالات ضاعف من الأضرار والخسائر التي تخلفها الاعتداءات على معطيات هذا الحاسب، لاسيما إذا كانت تمثل قيما مالية، خاصة مع ازدياد اعتماد البنوك والمؤسسات المالية ومختلف الشركات على الحاسب الآلي في تسييرها، وفي هذا الخصوص تشير الدراسات إلى أن الأضرار الناجمة عن جرائم المعطيات تفوق بكثير تلك الناجمة عن الجرائم التقليدية. ففي الولايات المتحدة وحسب مكتب التحقيقات الفيدرالي (FBI) فالجريمة المعلوماتية تكلف خسائر تقدر ب (150) ضعف ما تكلفه الجريمة العادية، وأن الخسائر الناجمة عن 139 عملية غش معلوماتي وقع على البنوك، بلغت 800 ألف دولار عام 1981 كما أن الغش المعلوماتي كان السبب في حدوث 50 حالة إفلاس في 354 بنكا بين شهري جانفي 1985 وجوان 1987.

وفي فرنسا قدرت الخسائر سنة 1991 حسب ما نشرته الجمعية الفرنسية لأمن المعلومات ب 10,4 مليار فرنك فرنسي، وفي سنة 1996 قدرة بحوالي 12,720 مليار فرنك فرنسي.[2]

6– تدني نسبة الإبلاغ عن تلك الجرائم من المجني عليه خاصة في شركات ومؤسسات الأعمال: نظرا لحساسية هذا النوع من الجرائم وما يتعرض له المجني عليه كطرف في الجريمة من تشهير فيما لو أبلغ عن الجريمة، فإن الإبلاغ عن هذا النوع من الجرائم قليل مقارنة مع غيرها من الجرائم، حيث أن معظم جرائم الانترنت والجرائم

---

[1] محمد علي سكيكر(رئيس محكمة الاستئناف)، **الجريمة المعلوماتية وكيفية التصدي لها**، طبعة 1، دار الجمهورية للصحافة، القاهرة، 2010، ص 40.

[2] الأستاذ محمد خليفة، **خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**، القانون الجنائي ألمعلوماتي بكلية الحقوق والآداب والعلوم الاجتماعية، جامعة 08 ماي 45–قالمة، ص 376–377.

المعلوماتية يتم اكتشافها مصادفة، وقد يكون هذا الاكتشاف بعد مدة طويلة من ارتكاب الجريمة، وهذا يدل على أن الجرائم التي لم تكتشف أكثر بكثير من الجرائم التي تم اكتشافها، وبعبارة أخرى فإن الفجوة كبيرة بين عدد هذه الجرائم الحقيقي وبين ما تم اكتشافه. فنقص الخبرة لدى الجهات المختصة أدى إلى ازدياد عدد الجرائم المعلوماتية بشكل ملحوظ، وذلك بسبب عدم قدرة هذه الجهات على التعامل مع هذا النوع من الجرائم المستحدثة بالوسائل الاستدلالية والإجراءات الجنائية التقليدية، وهذا أدى إلى عدم بذل الجهود الكافية من قبل رجال الشرطة للكشف عن هذه الجرائم لعدم الخبرة والمعرفة الفنية بطبيعتها وأهميتها.[1]

7- صعوبة إثبات الجريمة الالكترونية: يعد إثبات الجريمة الالكترونية من الصعوبة بمكان حيث يصعب تتبعها واكتشافها فهي لا تترك أثرا يقتفي، حيث تعتبر مجرد أرقام فمعظم الجرائم الالكترونية تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها، كما أنها تفتقر إلى الدليل المادي التقليدي كالبصمات مثلا.

ومن جهة أخرى فإن تعقبها يتطلب خبرة فنية يصعب تواجدها لدى المحقق العادي للتعامل معها، زيادة على ذلك يعمد مرتكب الجريمة الالكترونية إلى ممارسة التمويه عبد ارتكابها والتضليل والتحايل بغاية عدم التعرف على مرتكبها.[2]

8- سرعة محو الدليل وتوفر وسائل تقنية تعرقل الوصول إليه: تكون البيانات والمعلومات المتداولة عبر شبكة الانترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة لا تقرأ إلا بواسطة الحاسب الآلي، والوقوف على الدليل الذي يمكن فهمه بالقراءة والتوصل عن طريقه إلى الجاني يبدو أمرا صعبا لاسيما وأن الجاني يتعمد إلى عدم ترك اثر لجريمته، ضف إلى ذلك ما يتطلبه من فحص دقيق لموقع الجريمة من قبل مختصين في هذا المجال للوقوف على إمكانية وجود دليل ضد الجاني، وما يتبع ذلك من فحص للكم الهائل من الوثائق والمعلومات والبيانات المخزنة، التي تكون عبارة عن نبضات الكترونية غير مرئية تنساب

---

[1] د. لورنس سعيد الحوامدة، **الجرائم المعلوماتية أركانها وآلية مكافحتها-دراسة تحليلية مقارنة**، مجلة الميزان للدراسات الإسلامية والقانونية-السعودية، 2017/2016، ص 12.

[2] د. نعيمة دوادي، مرجع سبق ذكره، ص 49.

عبر النظام ألمعلوماتي، مما يجعل طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة.

يعيق المجرم في جرائم الانترنت سلطات التحقيق الوصول إلى الدليل بشتى الوسائل كمسح برامج أو وضع كلمات سرية ورموز وقد يلجا لتشفير التعليمات لمنع إيجاد أي دليل يدينه.[1]

9- نقص الخبرة لدى الأجهزة الأمنية والقضائية وعدم كفاية القوانين السارية: اختلافها عن الجريمة التقليدية أدى إلى تغيير آلية التحقيق وطرق جمع الأدلة من الجهات المخولة بالتحقيق وإضافة إلى أعباء تتعلق بكيفية الكشف عن هذه الجريمة وأدلتها، وكذا القضاء من خلال تعديل الكثير من مفاهيمه التقليدية سواء فيما يتعلق بالأدلة أو تطبيقاتها أو لقوتها في الإثبات أن تفعيل الحماية الأمنية والقضائية لم يتحقق بالقدر الكافي لدينا، نظرا لنقص المعارف التقنية وهو ما يتطلب تخصص في التقنية لتحصين الجهاز الأمني والقضائي.[2]

المطلب الثاني: خصائص المجرم الالكتروني:

المجرم الإلكتروني هو شخص يختلف عن المجرم العادي من حيث الشخصية والأفعال الإجرامية، والسؤال هنا هل هناك نموذج محدد للمجرم الالكتروني؟ أكيد هناك تمايز في زمرة المجرمين تحكمها جملة من السمات الخاصة بكل مجرم كما هناك صفات مشتركة بينهم وأهم السمات ما يلي:

1- **مجرم متخصص:** له قدرة فائقة في المهارة التقنية ويستغل مداركه ومهاراته في اختراق الشبكات كسر كلمات المرور أو الشفرات ويسبح في عالم الشبكات ليحصل على كل غال وثمين من البيانات والمعلومات الموجودة في أجهزة الحواسب ومن خلال الشبكات. [3]

---

[1] صغير يوسف، **الجريمة المرتكبة عبر الانترنت**، مذكرة مقدمة لنيل شهادة ماجستير، تخصص القانون الدولي للأعمال مدرسة الدكتوراه القانون الأساسي والعلوم السياسية، جامعة مولود معمري –تيزي وزو، 2013، ص 18، 19.

[2] المرجع نفسه، ص 20.

[3] إسراء جبريل رشاد مرعي، **الجرائم الالكترونية – الأهداف، الأسباب، طرق الجريمة ومعالجتها –** المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، 9 أغسطس 2016.

2- مجرم يعود للإجرام: يتميز المجرم ألمعلوماتي بأنه يعود للجريمة دائما فهو يوظف مهاراته في كيفية عمل الحواسيب وكيفية تخزين البيانات والمعلومات والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات ومرات فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء وإنما نتيجة شعوره بقدرته ومهارته في الاختراق.[1]

3- مجرم محترف: له من القدرات والمهارات التقنية ما يؤهله لان يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية وغيرها من الجرائم مقابل المال.[2]

4- المجرم الالكتروني كإنسان يتمتع بالمهارة والمعرفة والذكاء: المقصود بالإجرام ألمعلوماتي بالمعنى الدقيق هو الإجرام الذي ينشأ عن تقنيات التدمير الناعمة للمعلومات والبرمجيات، ولهذا يتميز المجرم الالكتروني غالبا بالذكاء، حيث أن الجريمة الالكترونية تتطلب مقدرة عقلية وذهنية عميقة، خاصة في الجرائم المالية التي تؤدي إلى خسارة كبيرة تلحق بالمجني عليه، فالمجرم الالكتروني يستخدم مقدرته العقلية ولا يلجأ إلى استخدام العنف أو الإتلاف المادي بل يحاول أن يحقق أهدافه بهدوء، فالإجرام ألمعلوماتي هو إجرام الأذكياء بالمقارنة بالإجرام التقليدي الذي يميل إلى العنف، فالمجرم الإلكتروني يسعى بشغف إلى معرفة طرق جديدة مبتكرة لا يعرفها أحد سواه، وذلك من أجل اختراق الحواجز الأمنية في البيئة الالكترونية، ومن ثم تحقيق مراده.[3]

- **المجرم الالكتروني شخص سوي واجتماعي:** يتميز بأنه إنسان اجتماعي، فهو لا يضع نفسه في حالة عداء مع المجتمع الذي يحيط به، بل على العكس من ذلك نجده إنسان متوافق مع مجتمعه ولكنه يقترف هذا النوع من الجرائم بدافع اللهو أو بغاية إظهار تفوقه

---

[1] د.علاء الرواشدة، د.أسماء ربحي العرب، **الجريمة في ظل العولمة: دراسة تحليلية للبنية وسياسات المواجهة**، كلية الإنسانيات والعلوم، جامعة عجمان، الإمارات العربية المتحدة، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، مجلد 18، عدد 2، جوان 2019، ص223.

[2] د.علاء الرواشدة، د.أسماء ربحي العرب، ص 223.

[3] حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة ماجستير، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر –باتنة، 2012/2011، ص 29-30.

على آلة الكمبيوتر أو على البرامج التي تتم تشغيله بها، أو بدافع الحصول على الأموال أو بهدف الانتقام.[1]

[1] د. رحموني محمد، مرجع سبق ذكره، ص 444.

الفصل الثاني

الفصل الثاني : آليات مكافحة الجريمة المعلوماتية

تسجل الدول بشكل يومي وعلى مدار24 ساعة آلاف الجرائم المعلوماتية لجميع مجالاتها، والجزائر كغيرها من الدول لم تسلم من الجريمة الالكترونية، لذلك سنحاول التعرف على آليات مواجهة مثل هذه الجرائم من خلال تناول الحماية الموضوعية (المبحث الأول) وتناول الحماية الإجرائية (المبحث الثاني)، واستخلاص خصوصية كل آلية حماية.

المبحث الأول: الحماية الموضوعية ضد الجريمة الالكترونية

لما كانت الجريمة المعلوماتية عالمية وعابرة للحدود كان من اللازم وجود اتفاقيات دولية وجهود فعالة للمنظمات الدولية كعقد عام لكبح الجريمة الالكترونية تنحدر تحت طائلته قوانين خاصة بكل وطن، ولم تكن الجزائر لتتغاضى بشكل عالمي أو سيادي عن هذه الاتفاقيات وسن قوانينها الخاصة.

المطلب الأول: الاتفاقيات والمنظمات الدولية لمكافحة الجريمة المعلوماتية:

تفاقمت الاعتداءات على الأنظمة المعلوماتية، ما انجر عليها تدخلا تشريعيا صريحا على المستوى الدولي وأولها اتفاقية بودابست لسنة 2001 حول الإجرام المعلوماتي بمختلف أشكاله حيث قسمت هذه الاتفاقية الجرائم إلى:[1]

- **الطائفة الأولى:** الجرائم التي تستهدف سرية و سلامة توفر المعطيات أي الجرائم التي تستهدف معطيات الكمبيوتر سواء بالاطلاع عليها أو إفشائها أو تصويرها أو إتلافها.
- **الطائفة الثانية:** وهي الجرائم المرتبطة بالكمبيوتر أي الجرائم التي يلعب فيها الكمبيوتر أو الحاسب الآلي دور الوسيلة كجرائم الاحتيال و التزوير الالكتروني.
- **الطائفة الثالثة:** الجرائم المرتبطة بالمحتوى أي يلعب فيها الكمبيوتر دور البيئة الجرمية كجرائم المواد الأخلاقية للأطفال وجرائم القمار وغسيل الأموال والمخدرات.
- **الطائفة الرابعة:**وهي الجرائم المتعلقة بحقوق الملكية الفكرية كحقوق المؤلف وهو نص

[1] **الاتفاقية المتعلقة بالجريمة الالكترونية–بودابست–، مجلس أوروبا، مجموعة المعاهدات الأوروبية –رقم** 185، صادرة بتاريخ 2001/11/23.

مكمل لما جاءت به قوانين الملكية الفكرية المقررة وطنيا و دوليا.

قانون الأونسترال النموذجي هو الآخر جاء استجابة لمحاولة الدول منع الجرائم الالكترونية ومكافحتها من خلال دراسة الأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به، وتم صياغة قانون الأونسترال النموذجي بشأن التجارة الإلكترونية، والآخر بشأن التوقيعات الالكترونية.[1]

وهناك البروتوكول المشترك للعناوين الالكترونية الدولية وهو أيضا يعد من المجهودات الدولية لمحاربة القرصنة الالكترونية وحماية مالكي العلامات التجارية وفي المقابل تم تكوين لجنة دولية خاصة بهدف الوصول إلى أفضل الحلول والاقتراحات. والعمل على خلق تعاون دولي شامل في حقل امتداد إجراءات التحقيق والملاحقة خارج الحدود وهي كانت ولا تزال محل اهتمام على الصعيدين الوطني والدولي.[2]

معاهدة برن (1971) تعتبر الحجر الأساس في مجال الحماية الدولية لحق المؤلف حيث تمنح لأصحاب حقوق المؤلف الحق في التصريح بعمل نسخ من هذه المصنفات بأي طريقة أو أي شكل كان، أو الترخيص أو منع أي ترجمة أو اقتباس أو بث إذاعي أو توصيل إلى الجمهور لمصنفه، وكذا تلزم الاتفاقية بتوقيع جزاءات سواء أكان المؤلف المعتدى عليه وطنيا أم أجنبيا.[3]

معاهدة تربس هي الأخرى من المعاهدات التي تم إنجازها في مجال حماية الملكية الفكرية من السطو عليها خصوصا مع انتشار عمليات السطو الإلكتروني على الأعمال الفنية دون إعطاء مالكيها أي من حقوقهم المادية أو المعنوية.[4]

---

[1] ليندة شرابشة، **السياسة الدولية و الإقليمية في مجال مكافحة الجريمة الالكترونية، الإتجاهات الدولية في مكافحة الجريمة الالكترونية**،أستاذة مساعدة في القانون العام، المركز الجامعي سوق أهراس، ص247.

[2] ليندة شرابشة، مرجع نفسه، ص 249.

[3] د.سعيداني سلامي، **تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية(وقائع ومقاربات)**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جوان 2018، ص 200.

[4] سعيداني سلامي، نفس المرجع، ص 201.

أكدت المنظمة الدولية للشرطة الجنائية الأنتربول على تعزيز وتشجيع التعاون بين أجهزة الشرطة بين الدول الأعضاء لمكافحة الجريمة الالكترونية، حيث يعتبر هذا الجهاز الأداة المثلى لتفعيل القوانين المختلفة وتنفيذها لما له من دور أساسي في المحافظة على الأمن العام لذلك فهو أيضا يتمتع بالمؤهلات اللازمة لقيامه بهذا الدور من خلال تعقب الجريمة والمجرمين.

أما إفريقيا فقد اجتمعت 54 حكومة افريقية على اتفاقية الاتحاد الإفريقي فيما يتعلق بمجال الأمن ألمعلوماتي وحماية البيانات الشخصية ، كما وافق مجلس وزراء الداخلية والعدل العرب في اجتماعهم بالقاهرة 2010 على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات ويتطرق في الفصل السابع منها للتعاون القانوني و القضائي في مكافحة هذه الجرائم صادقت عليها الجزائر سنة 2014، حيث تناولت الاتفاقية في فصلها الأول أحكاما عامة، بينت من خلالها الهدف وراء هذه الاتفاقية وأعطت تعريفات للمصطلحات الأكثر شيوعا في مجال الجرائم الالكترونية (تقنية المعلومات، مزود الخدمة، البرنامج المعلوماتي الشبكة المعلوماتية...).

كما بين مجالات تطبيق الاتفاقية في 4 حالات وهي: ارتكبت في أكثر من دولة، ارتكبت في دولة و تم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى، ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة، ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى. ذلك مع صون سيادة كل دولة وفقا لمبادئها الدستورية ونظمها الأساسية.

أما الفصل الثاني من الاتفاقية فقد عكف على تجريم الأفعال والسلوك لقوله تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل كجريمة الدخول والبقاء وجرائم الاعتداء على الأشخاص وغيرها، وتحديد المسؤولية الجنائية للأشخاص الطبيعية والمعنوية. [1]

[1] **الاتفاقية العربية لمكافحة جرائم تقنية المعلومات**، الأمانة العامة لجامعة الدول العربية–إدارة الشؤون القانونية–القاهرة، جمهورية مصر العربية، 2010/12/21. الشبكة القانونية العربية: *www.arablagalnet.org*

المطلب الثاني: التشريع الجزائري

حاول المشرع الجزائري سن قوانين داخلية مستنبطا من الجهود الدولية والاتفاقيات العالمية حتى يتفادى الوقوع في تنازع القوانين من جهة و سهولة توقيع العقاب من جهة أخرى غير انه لم يلمم بالشكل الكافي بكل الجرائم المستحدثة الماسة بنظام المعطيات. فقد تناول في نصوصه المستحدثة الاعتداءات الماسة بالأنظمة المعلوماتية و اغفل الاعتداءات الماسة بمنتجات الإعلام الآلي وذلك من خلال دراسة كل من القانونين 04 /15 المؤرخ في 10/11/2004 المتضمن تعديل قانون العقوبات[1]، والقانون 04/09 المؤرخ في 05 أوت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحتها .

جرمت المواد من 394 مكرر إلى 394 مكرر 7 من الفصل السابع من القانون 15/04: [2]

1- الدخول الاحتيالي إلى مجموع أو بعض نظام المعالجة الآلية للمعطيات أو البقاء فيه المادة 394 مكرر: يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 20000 دج

"تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة ".

- وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين و الغرامة من 50000 إلى 30000دج.

2- الإدخال بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها المادة 394 مكرر1: يعاقب بالحبس من ستة أشهر إلى 3 سنوات وبغرامة من 500000 إلى 4000000 دج.

---

[1] الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 يتضمن قانون العقوبات.

[2] المواد من 394 مكرر إلى 394 مكرر 7 من القانون 15/04 المؤرخ في 10 نوفمبر 2004، ج.ر.ج.ج، ع 71 مؤرخ في 10 نوفمبر 2004، ص 11و 12.

3- تصميم أو بحث أو تجميع أو اتجار أو توفير أو نشر معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية – حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم المادة 394 مكرر 2: يعاقب بالحبس من شهرين إلى 3 سنوات و بغرامة من 1000000 إلى 10000000 دج كل من يقوم بها عمدا أو عن طريق الغش .

_ إضافة إلى أن المشرع في المادة 394 مكرر 5 قد قرر نفس العقوبة المقررة للجريمة ذاتها لكل من شارك في مجموعة أو في اتفاق تالف بغرض الإعداد لجريمة أو أكثر و كان هذا التحضير مجسدا بفعل أو عدة أفعال.

وقد ضاعف المشرع العقوبة حيث:

– إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات الخاضعة للقانون العام فتطبق عقوبات اشد المادة 394 مكرر 3.

– كما يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها غرامة تعادل 5 أضعاف الحد الأقصى للغرامة المقررة للشخص الطبيعي المادة 394 مكرر4.

كما لم يغفل المشرع عن الحكم في الأجهزة والبرامج والوسائل المستخدمة وكذا المواقع والمحل أو مكان الاستغلال إذا ارتكبت الجريمة بعلم صاحبها من مصادرة وإغلاق دون المساس بالغير حسن النية المواد 394 مكرر 6، ومكرر 7.

كما لم ينسى المشرع الجزائري عن خضوع معطيات الحاسب الآلي لنصوص الملكية الأدبية والفنية للحماية: حيث نص في المادة 5 من القانون 03/05: [1]تعتبر أيضا مصنفات محمية الأعمال الآتية... وقواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى... تكفل الحماية لمؤلف المصنفات المشتقة دون المساس بحقوق مؤلفي المصنفات الأصلية.

[1] **المادة 5 من الأمر رقم 05/03 مؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف و الحقوق المجاورة**، ج.ر.ج.ج عدد44.

والمادة 4 من نفس القانون [1] : تعتبر على الخصوص كمصنفات أدبية أو فنية محمية المصنفات الأدبية المكتوبة مثل المحاولات الأدبية، والبحوث العلمية **والتقنية**، والروايات، والقصص، والقصائد الشعرية، **وبرامج الحاسوب**، والمصنفات الشفوية مثل المحاضرات والخطب والمواعظ وباقي المصنفات التي تماثلها.

العقوبات المقررة للاعتداء على حقوق الملكية الأدبية والفنية تشمل المواد من 153 إلى 156 إلى 159 من نفس القانون، قدرت العقوبة الأصلية بالحبس من 6 أشهر إلى 3 سنوات وغرامة من 500000 إلى 1000000 دج سواء تمت عملية النشر داخل الجزائر أو خارجها ومنح المشرع القاضي سلطة تقرير العقوبات التكميلية تتمثل في مصادرة المبالغ المساوية لمبلغ الإيرادات الناتجة عن الاستغلال غير الشرعي ليصنف أو أداء محمي ومصادرة وإتلاف كل عتاد انشأ خصيصا لمباشرة النشاط غير المشروع وكل النسخ المقلدة والمصادرة في هذه الحالة تكون وجوبيه، كما يمكن للقاضي أن يضاعف العقوبة في حالة العود مع إمكانية غلق المؤسسة التي يستغلها المقلد أو شريكه مدة لا تتعدى ستة أشهر.[2]

تطرق المشرع كذلك إلى تنظيم أحكام العلامات التجارية من خلال عدة قوانين آخرها الأمر رقم 06-03 المؤرخ في 19-07-2003 والمتعلق بالعلامات، وهي التسميات أو الرموز أو الأشكال التي توضع على البضائع التي يبيعها التاجر أو المصنعة أو المستصلحة المجهزة أو المختومة بغرض تمييزها عن بقية المبيعات أو الخدمات، ويشترط أن تكون مميزة وجديدة وغير مخالفة للنظام العام.[3]

وجاء في المادة 02 من الامر 03-07 الاختراع حل لمشكل معين في مجال التقنية يطلق عليه اختراع إذا أوفى شروطه (شرط الابتكار، شرط الجدة، القابلية للتطبيق

---

[1] المادة 4 من الأمر 05/03، مرجع سبق ذكره.

[2] نايري عائشة، **الجريمة الالكترونية في التشريع الجزائري** مذكرة مقدمة لنيل شهادة المستر، جامعة احمد دراية –أدرار– 2016-2017، ص 34، 36.

[3] **أمر رقم 03-06 المؤرخ في 19 جويلية 2003 والمتعلق بالعلامات**، ج.ر.ج.ج، ع 44، المؤرخة في 23 جويلية 2003.

الصناعي والمشروعية) [1]

رغم الجهود الدولية الفقهية أو القضائية و كذا التشريع الجزائري و ما جاء به في القانون 04/09، إلا أن الخصائص المميزة للجريمة الالكترونية كانت بمثابة الكابح الذي وقفت القوانين والنظم القانونية عاجزة عن مكافحتها ، نظرا للعدد الهائل من هذه الجرائم المتطورة بتطور تقنية المعلومات، حيث أصبح مبدأ (لا جريمة ولا عقوبة إلا بنص) لا يتسع لمكافحة هذا النوع من الجرائم، بل يجب التوسع في تفسيره لإيجاد التكييف القانوني السليم للجرائم الالكترونية المستحدثة.

وتكمن خصوصية التجريم في غالبية وقوع هذه الجرائم على العالم الافتراضي دون المادي، وذلك حتى مع ملامسة بعضها للعالم المادي، فإنها تبقي من الخصوصية لما يجعلها متمايزة عن غيرها من الجرائم التي تتطلب خصوصية في التجريم لئلا يفلت مقترفها من العقاب.

المبحث الثاني: الحماية الإجرائية ضد الجريمة الالكترونية:

بالرجوع إلى خصائص جرائم العصر الرقمي الحديث فان متابعتها إجرائيا يعد هاجسا أمام التشريعات الدولية العالمية أو الداخلية، ومحاولة تدارك هذا النقص الهائل يعد تحديا في حد ذاته، فالجريمة الالكترونية لا تترك أثرا ماديا في مسرح الجريمة كما أن مرتكبيها محترفون في إتلاف أو تغيير أو إضاعة الدليل في فترة قصيرة .

المطلب الأول : طرق ووسائل البحث والتحري في الجريمة الإلكترونية.

ككل جريمة تكون مراحل جمع الأدلة كما حددها القانون على سبيل الحصر وذلك لما فيها من مساس بحرية الأفراد وحقوقهم الأساسية، وهي: المعاينة، الخبراء، التفتيش، ضبط الأشياء مراقبة المحادثات والمراسلات وتسجيل وسماع الشهود والاستجواب والمواجهة إلا أن التحقيق في الجرائم المعلوماتية له خصوصية خاصة، لأنه يتم في بيئة رقمية.

---

[3] **المادة 02 من القانون 03-07 المؤرخ في 19-07-2003 يتعلق ببراءات الاختراع** ، ج.ر.ج.ج، ع 44، الصادرة في 23-07-2003 .

الفرع الأول: جمع الأدلة (المعاينة و التفتيش و ضبط الأدلة):

إن مسرح الجريمة الرقمية هي البيئة الرقمية، وبالتالي فان جمع الأدلة فيها يكون من ذات طبيعتها التقنية، حتى يقوى الدليل على إثباتها، و تحيط بعملية جمع الأدلة الكثير من العوائق والصعوبات ذلك راجع للخصائص المميزة لهذه الجريمة، إلا انه لا مفر من مواصلة جمع الأدلة مع التطوير المستمر لوسائل البحث، وتكييف جمع الأدلة مع طبيعة الجرائم المعلوماتية.

1- المعاينة:

من خصائص الجريمة الالكترونية أنها قلما تخلف آثارا مادية إضافة إلى لزوم وقت طويل لاكتشافها، ما يعطي الفرصة لمرتكبي هذه الجرائم أن يضروا أو يتلفوا أو يعبثوا بالآثار المادية للجريمة إن وجدت، وهو الأمر الذي يولد الشك في دلالة الأدلة المستسقاة من المعاينة في الجريمة الالكترونية، فعند تلقي البلاغ عن وقوع إحدى الجرائم الالكترونية وبعد التأكد من البيانات الضرورية في البلاغ، يتم الانتقال إلى مسرح الجريمة الالكترونية، ومن ذلك مراعاة (تحديد الأجهزة المحتمل تورطها في الجريمة، إعداد الفريق المتخصص للمعاينة من خبراء، رجال امن ومحققين وغيرها[1]

2-التفتيش:

إجراء يباشره موظف مختص بهدف البحث عن أدلة مادية لجناية أو جنحة، تحقق وقوعها في محل يتمتع بحرمة، وذلك وفقا للضمانات والقيود المقررة قانونا، ويعد تفتيش نظم المعالجة الآلية من اخطر المراحل، لأنه يكون على طابع غير مادي، ولا يعدو إلا أن يكون معلومات الكترونية ليس لها مظهر محسوس خارجيا، والتفتيش ينصب على الجانب المادي والمنطقي للحاسوب معا.

أ/ تفتيش المكونات المادية للحاسوب: لا توجد فيه مشكلة في التنفيذ، لأنه يرد على أشياء مادية، لا خلاف فيها لقواعد القانون لأنه تطبق عليه القواعد التقليدية، لكن مع الأخذ بعين

[1] رابح وهيبة، **الجريمة المعلوماتية في التشريع الإجرائي الجزائري**، كلية الحقوق و العلوم السياسية جامعة عبد الحميد بن باديس-مستغانم، مجلة الباحث للدراسات الأكاديمية ، العدد الرابع، ديسمبر 2014، ص 326.

الاعتبار الإجراءات الخاصة بضبط هذه الأجهزة لحساسيتها وإمكانية إتلافها، ونظام التفتيش تنطبق عليه الضمانات المقررة قانونا.

ب/تفتيش المكونات المنطقية للحاسوب : قام المشرعون بسن قوانين إجرائية جديدة تنص على إمكانية تفتيش المكونات المنطقية للحاسوب، وقد صرحت الاتفاقية الأوروبية المتعلقة بجرائم تقنية المعلومات انه يحق للدول الأعضاء تفتيش نظام الحاسوب أو جزء منه أو المعلومات المخزنة فيه ووسائط التخزين، والتفتيش في البيئة الرقمية يخضع لشروط شكلية وأخرى موضوعية تختلف عن شروط التفتيش في البيئة التقليدية. [1]

نص المشرع على التفتيش في المادة 45 فقرة 7 من قانون الإجراءات الجزائية، يعتبر التفتيش في المنظومة المعلوماتية مغايرا عن التفتيش العادي وإن كان إجراء من إجراءات التحقيق قد أحاطه المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 51 فقرة 6 وكذا على اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5.[2]

3- ضبط الأدلة:

ضبط الأدلة في الجريمة الالكترونية يكون عن طريق:

- نسخ المعطيات محل البحث على دعامة تخزين قابلة للحجز(وسائط تخزين البيانات والمعطيات والبرمجيات) مع الحفاظ على سلامة المعطيات في المنظومة المعلوماتية.
- الحجز عن طريق منع الوصول إلى المعلومات .
- الحجز على المكونات المادية للحاسوب وملحقاته والمعدات المستعملة في الشبكة كجهاز المودم .[3]

---

[1] خلف فاروق، **الآليات القانونية لمكافحة الجريمة المعلوماتية**، مداخلة مقدمة في الملتقى حول الجريمة المعلوماتية بين الوقاية والمكافحة –جامعة محمد خيضر –بسكرة، 16-17 نوفمبر 2015، ص 2-3 .

[2] المواد 45 فقرة 7،51 فقرة 6 و65 مكرر5 من الأمر رقم 66-155 المؤرخ في 8 يونيو 1966،مرجع سبق ذكره.

[3] المقدم عز الدين عز الدين، **مداخلة بعنوان الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها**، الملتقى الوطني حول الجرائم المعلوماتية، بسكرة في 16 نوفمبر 2015.

كما أن قانون الإجراءات الجزائية نص على انه لا يجوز ضبط الأدلة إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير انه طبقا لقانون الإجراءات الجزائية المعدل والمتمم في الفصل الرابع تحت عنوان في اعتراض المراسلات وتسجيل الأصوات والتقاط الصور نصت المادة 65 مكرر 5 فقرة 3 على انه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية أن يأذن بالاعتراض ووضع ترتيبات تقنية دون موافقة المعنيين من اجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة. أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة العادية [1] .

الفرع الثاني: وسائل الإثبات (الخبرة، الشهود، الاستجواب)

تختلف وسائل الإثبات في الجريمة المعلوماتية عنها في الجريمة التقليدية، فوسائل الثبات تدخل في إطار اختصاص القضاء، والذي يثبت ويدعم من خلالها القضاء الجريمة المعلوماتية المرتكبة من طرف المجرمين، والتي هي محل التحقيق.

1- الخبرة:[2]

الخبرة الفنية إجراء من إجراءات التحقيق يتم بموجبه الاستعانة بشخص يتمتع بقدرات فنية ومؤهلات علمية لا تتوافر لدى جهات التحقيق و القضاء ، من اجل الكشف عن دليل أو قرينة تفيد في معرفة الحقيقة بشان وقوع جريمة أو نسبتها إلى المتهم .

يخضع الخبير إلى إجراءات قانونية هي :

- اختياره من طرف جدول الخبراء (المادة 147 من قانون الإجراءات الجزائية الجزائري).
- على الخبير أداء اليمين القانونية (المادة 145 من قانون الإجراءات الجزائية الجزائري).

---

[1] بشير حماني ، **خصوصية التحقيق في الجريمة الالكترونية**، مذكرة تخرج مقدمة لنيل شهادة الماستر بعنوان : ، جامعة محمد بوضياف –المسيلة– 2019/2018 ، ص 20 .

[2] براهيمي جمال، **التحقيق الجنائي في الجرائم الالكترونية**، أطروحة مقدمة لنيل شهادة دكتوراه، كلية الحقوق و العلوم السياسية جامعة مولود معمري –تيزي وزو– ، 2018/06/27، ص من 67 – 81.

الجوانب الفنية للخبرة الالكترونية :

1- تقنيات انجاز الخبرة الالكترونية : هناك تقنيات أساسية التي يتعين على الخبير الالكتروني إتباعها لجمع الأدلة الرقمية، فحصها وتحليلها، ومن ثم كتابة النتائج المتوصل إليها في التقرير والتي تتلخص في :

- تقنيات ما قبل التشغيل والفحص (التأكد من صلاحيات وحدات نظام الأجهزة الالكترونية التحقق من مطابقة محتويات إحراز المضبوطات لما هو مدون عليها، تسجيل وتوثيق معطيات وحدات المكونات المضبوطة ، كالنوع والطراز و الرقم التسلسلي).

-تقنيات التشغيل والفحص (وضع نسخة لكل دعائم التخزين المضبوطة، تحديد أسماء وأنواع المجموعات البرمجية، إظهار الملفات المخبأة والنصوص المخفية داخل الصور تحديد الخصائص المميزة لكل جزء من الأدلة الرقمية وإعداد قائمة لها...).

2- الوسائل العلمية لإنجاز الخبرة الالكترونية: تتمثل في:

- بروتوكول الانترنت (IP): أو ما يسمى بعنوان الانترنت يعتمد عليه الخبير من خلال إتباع المسار ألتراسلي للبروتوكول للبحث عن رقم الجهاز المستعمل في الجريمة، و ثم تحديد موقعه و منه معرفة الجاني.

- نظام البروكسي هو وسيط بين شبكة الانترنت ومستخدميها يضمن توفير خدمات الذاكرة الجاهزة، ومنه تمكن الخبير من اقتناء دليل الإثبات بما تحتفظ به وتخزنه الذاكرة في كل عمليات التنزيل التي تمت على النظام .

- برنامج(Trace rout): برنامج مدرج في نظام تشغيل الحاسب الرئيسي، يحدد بدقة الأجهزة الالكترونية التي اشتركت في نقل البيانات على الانترنت بتحديد مساراتها وصولا إلى المرسل إليه، كما يمكنه أن يستدعي ويحيط بالملفات التي تم الولوج إليها وكافة عمليات الاختراق والعبور أو التجاوز خلال الإعداد للجريمة وغيرها.

- أنظمة كشف الاختراق (IDS): يكمن دورها في مراقبة العمليات التي تحدث على الأجهزة الالكترونية المرتبطة بشبكة الانترنت وتسجيلها فور وقوعها في سجلات خاصة داخل هذه

الأجهزة.

– برامج مراجعة العماليات الحاسوبية واسترجاعها(Auditing Tools) برامج تستخدم لمراقبة مختلف العماليات التي تجري على ملفات وأنظمة تشغيل حاسب معين و تسجيلها في ملفات تسمى(Logs) واسترجاع هذه الملفات في حالة محوها وحذفها.

– برنامج الدمج و فك الدمج(pk zip) يستعين به الخبير عادة لفك البرامج المدمجة قصد التعرف على طبيعة البيانات التي تحتويها وتحليلها.

– الذكاء الصناعي وهي تقنيات وبرامج الحاسب الآلي التي يستعين بها الخبير لحصر الأسباب والفرضيات المتعلقة بالجريمة...

2– الاستجواب: وهو مساءلة المتهم ومناقشته عن الوقائع المنسوبة إليه ارتكابها ومجابهته بالأدلة وسماع ما لديه من دفوع للتهمة المنسوبة إليه، واستجواب المتهم في الجرائم المعلوماتية تحكمه نفس القواعد العامة للاستجواب في الجرائم التقليدية، لا بد أن تكون السلطة المختصة التي تتولى الاستجواب مؤهلة للتحقيق في الجرائم المعلوماتية حتى يمكن الاستيعاب والتعامل مع مفرداتها وقد أحاط المشرع الاستجواب بعدة ضمانات ملزمة لضمان حقوق المتهم.[1]

من الإجراءات المستحدثة لمواجهة الجريمة الالكترونية في التشريع الجزائري تمديد التوقيف تحت النظر الممنوح لضباط الشرطة القضائية مرة واحدة إذا تعلق بالجريمة الالكترونية طبقا لنص المادة 5/51 من الأمر 15–02 المؤرخ في 23 جويلية 2015، مع العلم أن هذا الإجراء بوليسي يقوم به الضابط ضد كل شخص تتوافر دلائل قوية على ارتكابه الجريمة في الجريمة المتلبس بها بوضع شخص في مركز الشرطة أو الدرك لمدة يحددها المشرع كلما دعته الضرورة لذلك، على أنه لا يجوز أن تتجاوز مدة التوقيف للنظر 48 ساعة ماعدا بعض الجرائم الخطيرة التي خصها المشرع باستثناءات.[2]

[1] خلف فاروق ، مرجع سبق ذكره، ص 4.

[2] سعيدة بوزنون، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، جامعة الإخوة منتوري –قسنطينة، مجلة العلوم الإنسانية عدد52، المجلد ب، ص.ص.47–57، ديسمبر 2019، ص 52.

3- سماع الشهود:

سماع الشهود كسائر إجراءات التحقيق في الطريقة التقليدية، فالقاضي له أن يسمع الشهود أو يستغني عنهم، فإذا قرر سماعهم فهو الذي يحدد من يجب الاستماع إليه ومن يمكن الاستغناء عنه، والأمر متروك للسلطة التقديرية للقاضي، والشاهد في الجرائم المعلوماتية يطلق عليه اسم الشاهد المعلوماتي تميزا له عن الشاهد التقليدي، والمقصود بالشاهد في الجريمة المعلوماتية هو الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسوب، والذي تكون لديه معلومات جوهرية أو هامة لازمة للولوج في نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة، وتضم طائفة الشهود مشغلوا الحاسوب، خبراء البرمجة، محللو البيانات، مهندسو الصيانة، مديرو النظم. [1]

المطلب الثاني: الأجهزة المكلفة بالتحري والبحث عن الجريمة الالكترونية.

سنتطرق في هذا المطلب إلى الأجهزة المكلفة بالتحري والبحث عن الجريمة الالكترونية، على المستوى الدولي (الفرع الأول)، وعلى المستوى الوطني (الفرع الثاني)

الفرع الأول: على المستوى الدولي:

المنظمة الدولية للشرطة الجنائية الانتربول من أهم أجهزة مكافحة الإجرام، تهدف هذه المنظمة إلى ضرورة التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال، ومنع ومكافحة جرائم القانون العام، وخاصة الجرائم العابرة للحدود الوطنية للدول، كما تعمل على تفعيل دور المؤسسات الأمنية على المساهمة في الوقاية من جرائم القانون العام والحد من خطورتها، تقوم على وسيلتين:

1- تجميع البيانات والمعلومات المتعلقة بالجريمة والمجرم عن طريق المكاتب المركزية الوطنية الموجودة في أقاليم الدول الأطراف.

2- التعاون في ملاحقة المجرمين الفارين وإلقاء القبض عليهم وتسليمهم للدول التي تطالب بتسليمهم.

[1] خلف فاروق، مرجع سبق ذكره، ص 4 .

وخلال وباء كوفيد -19 و ما بعده أطلق الانتربول أكاديميته الافتراضية لتوفير التدريب الالكتروني لأجهزة إنفاذ القانون في العالم يقدمها مدربون مؤهلون و حلقات دراسية شبكية موجهة لأفراد إنفاذ القانون في بلدان الانتربول أل 194 الأعضاء و أهم المواضيع التي تتناولها الدورات: العملات المشفرة، و الطائرات المسيرة، والأدلة الجنائية الرقمية و الجريمة السيبرية،

والشبكة الخفية، ومكافحة الإرهاب، والجريمة المنظمة، والمستجدات في قدرات الانتربول الشرطية.

أما المجلس الأوروبي هو الأخر فقد انشأ سنة 1991 شرطة أوروبية تختص بملاحقة الجرائم العابرة للحدود سمي بالمنظمة الدولية للبوليس الجنائي ، يضم 156 دولة كأعضاء فيها.

أما ما جاء في الاتفاقية العربية في المادة الثالثة و الأربعون فقد نص على ضرورة وجود جهاز متخصص و متفرغ في كل دولة طرف على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات المتعلقة بجرائم تقنية المعلومات أو لجمع الأدلة بشكلها الالكتروني في جريمة معينة. كما يجب أن يكون لدى الجهاز في أي دولة طرف القدرة على الاتصالات مع الجهاز المماثل في دولة طرف أخرى بصورة عاجلة، يجب على هذا الجهاز القدرة على التنسيق مع سلطات الدولة بصورة عاجلة. على كل دولة طرف ضمان توفر العنصر البشري الكفء من اجل تسهيل عمل الجهاز.[1]

الفرع الثاني: على المستوى الوطني:

1-**إنشاء هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال و مكافحته** حسب المادة 13من القانون 04/09 وهي سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع لدى الوزير المكلف بالعدل في الجزائر العاصمة .

[1] الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، مرجع سبق ذكره.

تتولى هذه الهيئة مهام خاصة هي حسب المادة 14 من نفس القانون: [1]

1- تنشيط و تنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

2- مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال بما في ذلك تجميع المعلومات وانجاز الخبرات القضائية.

3- تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المعلوماتية وتحديد مكان تواجده.

2/- **الهيئات القضائية الجزائية المتخصصة:** أنشئت بموجب القانون 04/14المؤرخ في 10 نوفمبر 2004 [2] تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد 32، 37 و 40 من قانون الإجراءات الجزائية الجزائري تتمتع بمباشرة مهامها في دائرة الاختصاص الإقليمي الموسع، بحيث تنظم في القضايا المتصلة بتكنولوجيات الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا، إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون 04/09 .

وعليه يمتد الاختصاص الإقليمي لوكيل الجمهورية و لقاضي التحقيق إلى محاكم أخرى –عن طريق التنظيم- قد تكون تابعة لنفس المجلس أو مجلس أخر، المشرع لم ينص على ذلك صراحة لكن يفهم من خلال نصوص المواد 40 مكرر إلى 40 مكرر 5 انه يمتد الاختصاص حتى إلى محاكم أخرى خارج دائرة المجلس الذي تنتمي إليه محكمة وكيل الجمهورية أو قاضي التحقيق.

إذا اعتبر النائب العام للمجلس القضائي المختص في الأصل أن الجريمة تدخل ضمن اختصاص المحكمة التي تم توسيع اختصاصها المحلي، يطالب فورا بالإجراءات اللازمة ويضع تحت تصرف وكيل الجمهورية لهذه المحكمة ضباط الشرطة القضائية لتنفيذ

---

[1] المواد 13-14 من القانون 04/09 المؤرخ في 5 غشت 2009، مرجع سبق ذكره

[2] القانون رقم 04 – 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66 – 155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 71 بتاريخ 10 نوفمبر 2004.

تعليماتهم.

وإذا فتح تحقيق قضائي لدى محكمة مختصة، يجب أن يصدر قاضي التحقيق لديها أمرا بالتخلي عن الإجراءات لصالح قاضي التحقيق لدى المحكمة التي تم توسيع اختصاصها المحلي، وفي هذه الحالة يتلقى ضباط الشرطة القضائية العاملون بدائرة اختصاص هذه المحكمة (محكمة القاضي المتخلي) التعليمات مباشرة من قاضي التحقيق المتخلى له عن هذه القضية .[1]

عزز المشرع الجزائري بموجب القانون 22/06 نشاط الضبطية القضائية بإجراءات خاصة لمواجهة بعض الجرائم، عرفها الفقه على أنها الإجراءات والتقنيات التي تتخذها الشرطة القضائية بغية البحث والتحري عن الجرائم الخطيرة المقررة في قانون العقوبات وجمع الأدلة والكشف عن مرتكبيها وذلك دون علم و رضا الأشخاص المعنيين [2] .

قسم المشرع هذه الأساليب وحصرها بالصور التالية: المراقبة واعتراض المراسلات والأصوات والتقاط الصور ثم التسرب، وأضاف القانون 01/06 المتضمن قانون الفساد بمقتضى المادة 56 منه الصور التالية: إذا تعلق الأمر بجرائم الفساد والتسليم المراقب والترصد الالكتروني والاختراق.

3/- الوحدات التابعة للمديرية العامة للأمن الوطني و الدرك الوطني:

أ/- المديرية العامة للأمن الوطني: تتكون من مصلحة مركزية وفرق محلية، إضافة إلى المخبر المركزي للشرطة العلمية بشاطوناف بالجزائر العاصمة ومخبرين جهويين بكل من قسنطينة ووهران وتحتوي على فروع تقنية من بينها خلية الإعلام الآلي.

ب/- الوحدات التابعة للدرك الوطني : يضع الدرك وحدات متنوعة وعديدة على مستوى القيادة العادة، أو على مستوى القيادات الجهوية والمحلية وذلك حفاظا على الأمن والنظام

---

[1] حابت أمال، **مداخلة بعنوان : الطابع الخصوصي للإجراءات الجزائية في شأن الجرائم الالكترونية في القانون الجزائري** مقدمة في الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة ، 16-17 نوفمبر 2015 ، ص 6-7 .

[2] بموجب القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل و المتمم للأمر رقم 66-155 المؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية.

العام ومحاربة الجريمة بكافة أنواعها (المصالح والمراكز العلمية والتقنية، هياكل التكوين، المصلحة المركزية للتحريات الجنائية، المعهد الوطني لعلم الإجرام).

يوجد بالمعهد الوطني للأدلة الجنائية وعلم الإجرام ببوشاوي التابع للقيادة العامة للدرك الوطني قسم الإعلام والإلكترونيك الذي يقوم بالتحقيق في الجرائم الالكترونية بتحليل الأدلة وذلك من خلال تحليل الدعامة الالكترونية، وانجاز المقاربات الهاتفية، وتحسين التسجيلات الصوتية والفيديو والصورة وذلك لتسهيل استغلالها، بالإضافة إلى مراكز الرقابة من جرائم الإعلام الآلي والجرائم المعلوماتية ومكافحتها ببئر مرادرايس والتابع لمديرية الأمن العمومي للدرك الوطني [1].

وكنتيجة محققة مثلا: سنة 2016 سجلت مديرية الشرطة القضائية بالمديرية العامة للأمن الوطني وجود 11 قضية متعلقة بالإرهاب الالكتروني اغلبها خاصة بتهديدات داعش الإرهابي، وبالبحث والتحري بين مختلف القطاعات المختصة تم توقيف 58 شخص متورط في قضايا الإرهاب الالكتروني تمت إحالتهم على القضاء وقد استطاع أيضا الجيش الالكتروني الجزائري من توقيف ما يزيد عن 160 جزائري لهم علاقة مباشرة مع تنظيم داعش في العراق وسوريا وليبيا، من خلال فك شفرات الرسائل المتبادلة عبر الفيس بوك والتويتر.

تتميز الجريمة الالكترونية بخصوصيات إجرائية تحددها اختصاصات الأقطاب المخصصة بها، وتوسع صلاحيات الشرطة القضائية بشأنها وذلك من خلال (مراقبة الأشخاص، اعتراض المراسلات، تسجيل الأصوات والصور والتسرب).

فمن ناحية نجد خصوصية الإثبات في هذا النوع من الجرائم فإنها لا تخلو من الصعاب العديدة والتي تكتنف رصد واحتواء الدليل المتحصل عليه من مسرح الجريمة سواء المادي أو الافتراضي، وذلك كون الأدلة الرقمية صعبة الاحتواء وسهلة الاختفاء والمحو، وكذلك انه يمكن التضليل بشان كشفها أو الاطلاع على مضمونها.

[1] بشير حماني ، مرجع سبق ذكره ، ص 35- 37 .

وأما خصوصية الملاحقة فإنها تتبع من الجانب التقني لهذه الجرائم والتي تتطلب قدرات خاصة لدى الأشخاص المتخصصين بالمتابعة والملاحقة لمثل هذا النوع من الجرائم، وكذلك الآليات القانونية التي يجب إقرارها في التنقيب عن الأدلة الالكترونية، ومشروعية الإجراء الذي يمكن إتباعه للكشف عن الدليل و هذا عوضا عن مشروعية الدليل نفسه.

خاتمة

خاتمة:

يشهد عالمنا اليوم ثورة تكنولوجية هائلة سهلت الحياة العملية من جهة، لكن في المقابل فتحت بابا لا يغلق من جهة أخر بسبب ما صاحبها من جرائم إلكترونية جعلتها أكثر تعقيدا من الجرائم التقليدية.

وأمام هذا الوضع كان لابد على الجزائر الإسراع في اتخاذ الإجراءات اللازمة لتطوير آليات التصدي لمثل هذه الجرائم، إلا أن جاء به المشرع الجزائري في هذا الصدد لا يكفي لسد الهوة التي فتحتها المنظومات المعلوماتية، بل يجب إصدار قانون خاص بها يفصل فيه المفاهيم الخاصة بالجريمة ومرتكبيها والعقوبات المقررة لها، كما يجب أن تكون مرنة جدا لتتماشى والتطورات السريعة لتكنولوجيات الإعلام والاتصال.

كما أن مسألة إفراد الجريمة الالكترونية بقواعد خاصة تنسجم مع طبيعتها وخصوصياتها أملتها مجموعة من الاعتبارات، كان من بينها الاختلاف الذي يطبع القواعد الإجرائية العادية عن نظيرتها في مجال البحث والتحري عن الجريمة الالكترونية من جهة والصعوبات التي تعترض أجهزة إنفاذ القانون لضبط هذه الجريمة من جهة أخرى.

إن المعالجة القانونية لهذه الجرائم يجب أن تتم في إطار شمولي، ذلك أن اعتماد المحاور الرئيسية للحماية الجزائية في ما بينها لا تخلو من التكامل، حيث أن خصوصية التجريم يلزمها خصوصية في الإثبات وكذلك خصوصية في البحث والملاحقة.

- قائمة المصادر والمراجع :

1- المصادر

أ- المواثيق الدولية:

- قرار لجنة الأمم المتحدة للقانون التجاري الدولي رقم 162/51 معتمد من قبل جمعيتها العامة بناء على تقرير اللجنة السادسة 1996/12/16.

- الاتفاقية المتعلقة بالجريمة الالكترونية-بودابست-، مجلس أوروبا، مجموعة المعاهدات الأوروبية -رقم 185، صادرة ب 2001/11/23.

- الاتفاقية العربية لمكافحة جرائم تقنية المعلومات،الأمانة العامة لجامعة الدول العربية-إدارة الشؤون القانونية-القاهرة، جمهورية مصر العربية، 2010/12/21. الشبكة القانونية العربية: *www.arablagalnet.org*

ب-القوانين:

أ- النصوص التشريعية:

1- الأمر رقم 05/03 مؤرخ في 19 يوليو 2003 يتعلق بحقوق المؤلف والحقوق المجاورة، ج.ر.ج.ج عدد44.

2- القانون 03-07 المؤرخ في 2003/07/19 يتعلق ببراءات الاختراع، الجريدة الرسمية عدد 44 صادرة في 32-07-2003 .

3- القانون رقم 04 - 14 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر رقم 66-155 المتضمن قانون الإجراءات الجزائية، ج.ر.ج.ج عدد 71 بتاريخ 10 نوفمبر 2004.

4- الأمر رقم 66-155 المؤرخ في 8 يونيو 1966،المتضمن قانون الإجراءات الجزائية،ج.ر.ج.ج عدد 71 بتاريخ 10 نوفمبر 2004.

5- القانون 15/04 المؤرخ في 10 نوفمبر 2004 (جريدة رسمية عدد 71 مؤرخة في 10 نوفمبر 2004، ص 11-12) المعدل و المتمم للأمر رقم 66-156 المؤرخ في 8 يونيو 1996 المتضمن قانون العقوبات المعدل و المتمم.

6- القانون رقم 06-22 المؤرخ في 20 ديسمبر 2006 المعدل والمتمم للأمر رقم 66-155 المؤرخ في 08 يونيو 1996 يتضمن قانون الإجراءات الجزائية .

7- القانون 09-04 المؤرخ في 5 غشت 2009 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

8- الأمر رقم 66-155 مؤرخ في 8 يونيو 1966 يتضمن قانون الإجراءات الجزائية .

9- الأمر رقم 66-156 المؤرخ في 8 يونيو 1966 يتضمن قانون العقوبات.

10- الأمر رقم 03-06 المؤرخ في 19 جويلية 2003 والمتعلق بالعلامات التجارية ، جريدة رسمية عدد44 صادرة ب 23 جويلية 2003 .

2- المراجع:

أ- الكتب

1- ضرغام جابر عطوش آل مواش، **جريمة التجسس المعلوماتي: دراسة مقارنة**، المركز العربي للنشر والتوزيع، مكتبة دار السلام القانونية، الطبعة الأولى، 2017، ص 33.

2- د.غادة نصار، **الإرهاب والجريمة الإلكترونية**، طبعة 1، العربي للنشر والتوزيع، القاهرة، 2017.

3- د.فوزي شروق سامي، **تكنولوجيا الإعلام الحديث**، مؤسسة طيبة للنشر والتوزيع، طبعة1، القاهرة، 2014.

4- محمد علي سكيكر(رئيس محكمة الاستئناف)، **الجريمة المعلوماتية وكيفية التصدي لها**، طبعة 1، دار الجمهورية للصحافة، القاهرة، 2010.

5- وائل رفعت علي خليل، **إشكاليات الإعلام ومعطيات الواقع**، المنهل، د.ب.ن، 2015.

ب- مذكرات التخرج الجامعية:

أولا: أطروحات الدكتوراه.

1-براهيمي جمال، أطروحة دكتوراه في العلوم تخصص القانون بعنوان: التحقيق الجنائي في الجرائم الالكترونية، لكلية الحقوق و العلوم السياسية، جامعة مولود معمري -تيزي وزو، 2018/06/27.

2- رابحي عزيزة، **الأسرار المعلوماتية وحمايتها الجزائية**، أطروحة دكتوراه في القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد-تلمسان، 2018/2017.

ثانيا- مذكرات الماستر:

1- ادهم باسم نمر بغدادي، مذكرة تخرج درجة ماجستير بعنوان: وسائل البحث والتحري عن الجرائم الالكترونية، في القانون العام، كلية الدراسات العليا جامعة النجاح الوطنية نابلس - فلسطين، 2018.

2- أسامة مهمل، مذكرة لنيل شهادة الماستر الأكاديمي: **الإجرام السيبيراني**، فرع القانون الجنائي، جامعة محمد بوضياف-المسيلة، 2018/2017.

3- بشير حماني، مذكرة تخرج لنيل شهادة الماستر بعنوان: **خصوصية التحقيق في الجريمة الالكترونية**، جامعة محمد بوضياف -المسيلة، 2019/2018.

4- حمزة بن عقون، **السلوك الإجرامي للمجرم المعلوماتي**، مذكرة لنيل شهادة ماجستير، كلية الحقوق و العلوم السياسية، جامعة الحاج لخضر -باتنة، 2012/2011.

5- رزيق ليلة، رمضاني حميدة، **الجريمة الالكترونية واقع وتحدي**، مذكرة ماستر تخصص قانون جنائي وعلوم إجرامية، جامعة مولود معمري-تيزي وزو، 2018/07/09.

6- سعيداني نعيم، **آليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري**، مذكرة ماستر في العلوم القانونية، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر- باتنة، 2012-2013.

7- شلاخ لطيفة، قريشي الحاج العربي إبراهيم، **انتشار الجريمة الالكترونية الماسة بالأشخاص في البيئة الجزائرية –دراسة ميدانية لبعض مستخدمي مقاهي ألنت بمدينة المسيلة**، مذكرة مكملة لنيل شهادة الماستر في علوم الإعلام الآلي والاتصال تخصص صحافة مكتوبة، كلية العلوم الإنسانية والاجتماعية، جامعة محمد بوضياف –المسيلة، ماي 2017.

8- صغير يوسف، مذكرة تخرج لنيل شهادة ماجستير بعنوان: **الجريمة المرتكبة عبر الانترنت**، تخصص القانون الدولي للأعمال، مدرسة الدكتوراه –القانون الأساسي والعلوم السياسية، كلية الحقوق والعلوم السياسية جامعة مولود معمري –تيزي وزو، 2013/03/06.

9- عبد الله دغش العجمي، رسالة ماجستير في القانون العام بعنوان: المشكلات العملية والقانونية للجرائم الالكترونية دراسة مقارنة، جامعة الشرق الأوسط، 2014.

10- لعاقل فريال، مذكرة لنيل شهادة الماستر في القانون العام بعنوان: الجريمة المعلوماتية في ظل التشريع الجزائري، كلية الحقوق والعلوم السياسية، جامعة أكلي محند اولحاج – البويرة، 2014-2015.

11-- نايري عائشة، مذكرة لنيل شهادة الماستر بعنوان: **الجريمة الالكترونية في التشريع الجزائري**، جامعة احمد دراية –أدرار، 2017/2016.

12- يوسف خليل يوسف العفيفي، رسالة ماجستير في القانون العام بعنوان: الجرائم الالكترونية في التشريع الفلسطيني (دراسة تحليلية مقارنة)، كلية الشريعة والقانون الجامعة الإسلامية –غزة، 2013.

ج- المجلات والمقالات:

1- د.أحمد بن خليفة، ط. حفوظة الأمير عبد القادر، **الجريمة الالكترونية وآليات التصدي لها**، مجلة الامتياز لبحوث الاقتصاد والإدارة، العدد 01، جوان 2017.

2- د.جيلالي الحسين، **التعاون الجنائي الدولي في مكافحة الجريمة العالمية**، مجلة القانون، المركز الجامعي أحمد زبانة-غليزان، العدد 02، 2018.

3- الأستاذة حابت أمال (أستاذة محاضرة بجامعة مولود معمري -تيزي وزو)، مداخلة بعنوان: **الطابع الخصوصي للإجراءات الجزائية في شان الجرائم الالكترونية في القانون الجزائري**، مطوية الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، جامعة محمد الصديق بن يحيى -جيجل، 16-17 نوفمبر 2015.

4- خلف فاروق، مداخلة بعنوان: **الآليات القانونية لمكافحة الجريمة المعلوماتية**، كلية الحقوق والعلوم السياسية جامعة حمد لخضر-الوادي، مطوية الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة -جامعة محمد خيضر بسكرة، 16-17 نوفمبر 2015.

5- د. دمان ذبيح عماد(جامعة عباس لغرور-خنشلة)، د. بهلول سمية(جامعة محمد لمين دباغين-سطيف)، **الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري**، مجلة الحقوق والعلوم السياسية، جامعة عباس الغرور-خنشلة، العدد13، جانفي 2020.

6- د.ذياب موسى البداينة، **مداخلة بعنوان: الجرائم الالكترونية: المفهوم والأسباب**، الملتقى العلمي: الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 2-2014/4، عمان-المملكة الأردنية الهاشمية، 2014.

7- رابح وهيبة، **الجريمة المعلوماتية في التشريع الإجرائي الجزائري**، كلية الحقوق والعلوم السياسية جامعة عبد الحميد بن باديس-مستغانم، مجلة الباحث للدراسات الأكاديمية، العدد الرابع، ديسمبر 2014.

8- رحموني محمد، **خصائص الجريمة الالكترونية ومجالات استخدامها**، جامعة أحمد دراية-أدرار، مجلة الحقيقة، العدد 41، 2018/01/10.

9- د.سعيداني سلامي، **تطور التشريعات والاتفاقيات الدولية في مجال الجرائم المعلوماتية(وقائع ومقاربات)**، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، جوان 2018.

10- سعيدة بوزنون، **مكافحة الجريمة الالكترونية في التشريع الجزائري**، جامعة الإخوة منتوري –قسنطينة، مجلة العلوم الإنسانية عدد52، المجلد ب، ص.ص.47-57، ديسمبر 2019.

11- المدرس المساعد عادل يوسف عبد النبي ألشكري، **الجريمة المعلوماتية وأزمة الشرعية الجزائية**، جامعة الكوفة كلية القانون، العدد السابع (الجريمة المعلوماتية)، 2008.

12- الدكتورة عباس كريمة –كلية الحقوق جامعة قسنطينة1، **جرائم المساس بأنظمة المعالجة الآلية للمعطيات**، مجلة البيبان للدراسات القانونية والسياسية، كلية الحقوق والعلوم السياسية جامعة محمد البشير الإبراهيمي –برج بوعريريج- الجزائر، العدد الرابع، ديسمبر 2017.

13- عبد الحكيم، مولاي براهيم، **الجرائم الالكترونية**، مجلة الحقوق والعلوم الإنسانية جامعة زيان عاشور بالجلفة- الجزائر، عدد 13، 23 جوان 2015.

14- عشاش حمزة، حمزة خضري، **خصوصية أركان الجريمة المعلوماتية في التشريع الجزائري**، جامعة محمد بوضياف –المسيلة، مقال مقدم إلى مجلة الدراسات القانونية والسياسية تصدر عن جامعة عمار ثليجي بالأغواط-الجزائر، المجلد 06، العدد 02، 2020/06/05.

15- المقدم عز الدين عز الدين، مداخلة بعنوان: **الإطار القانوني للوقاية من الجرائم المعلوماتية ومكافحتها**، الملتقى الوطني حول الجرائم المعلوماتية، بسكرة، في 16 نوفمبر 2015.

16- عصام حسني الأطرش ومحمد محيي الدين عساف، **معوقات مكافحة الجرائم المعلوماتية في الضفة الغربية من وجه نظر العاملين في أقسام الجرائم المعلوماتية في الأجهزة الأمنية**، مجلة جامعة الشارقة للعلوم القانونية، جامعة الاستقلال، أريحا، فلسطين، المجلد 16، العدد 1، يونيو 2019.

17- مجموعة الدكتور عبد الله اليحيى للمحاماة والاستشارات القانونية والتحكيم، ورقة عمل عن (الجرائم الالكترونية) مقدمة إلى ملتقى الحقوق والعدالة للتعاملات الالكترونية بالرياض -السعودية، 2018/05/31.

18- د.علاء الرواشدة، د.أسماء ربحي العرب، **الجريمة في ظل العولمة: دراسة تحليلية للبنية وسياسات المواجهة**، كلية الإنسانيات والعلوم، جامعة عجمان، الإمارات العربية المتحدة، مجلة الحقيقة للعلوم الاجتماعية والإنسانية، مجلد 18، عدد 2، جوان 2019.

19- د. لورنس سعيد الحوامدة، **الجرائم المعلوماتية أركانها وآلية مكافحتها-دراسة تحليلية مقارنة**، مجلة الميزان للدراسات الإسلامية والقانونية-السعودية، 2017/2016.

20- أستاذة نشناش منية، الركن المفترض في الجريمة المعلوماتية محور المداخلة : **المحور الإطار ألمفاهيمي للجريمة المعلوماتية**، بجامعة محمد الصديق بن يحيى-جيجل- مطوية الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-17 نوفمبر 2015.

21- د. نعيمة دوادي، **الجريمة الالكترونية (خصائصها ومجالات استخدامها، وأهم سبل مكافحتها)**، جامعة علي لونيسي-البليدة، مجلة مهد اللغات، جامعة حسيبة بن بوعلي بالشلف-الجزائر، المجلد 2، العدد 1، 2020/08/20، ص 49.

22- أستاذة نميدلي رحيمة، مداخلة بعنوان: **خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة**، جامعة محمد لمين دباغين سطيف 2 -الجزائر، كتاب أعمال مؤتمر الجرائم الالكترونية المنعقد في طرابلس/لبنان، يومي 24-2017/03/25 2017/04/08.

23- السيد الدكتور وليد طه، التنظيم التشريعي للجرائم الالكترونية في اتفاقية بودابست جمهورية مصر العربية.

د- مواقع إلكترونية:

1- الإشكاليات الموضوعية والإجرائية في النظام القانوني الفلسطيني في الجريمة الالكترونية على الرابط:

https://repository.najah.edu/handle/20.500.11888/1348 counsulté:08/09/2020 heur 12:26 .

2- د.ليلى الجنابي،**فعالية القوانين الوطنية والدولية في مكافحة الجرائم السيبرانية،** على الرابط التالي: *www.ahewar.org consulté le: 16 /09/2020 à 01 :03h*

3- ليندة شرابشة، **السياسة الدولية والإقليمية في مجال مكافحة الجريمة الالكترونية، الإتجاهات الدولية في مكافحة الجريمة الالكترونية**،أستاذة مساعدة في القانون العام، المركز الجامعي سوق أهراس، مقال منشور على موقع دراسات وأبحاث: *https://www.asjp.cerist.dz*

4- الأستاذ محمد خليفة، **خصوصية الجريمة الالكترونية وجهود المشرع الجزائري في مواجهتها**، القانون الجنائي المعلوماتي بكلية الحقوق والآداب والعلوم الاجتماعية، جامعة 08 ماي 45-قالمة، مقال منشور على موقع الدراسات والأبحاث: *https://www.asjp.cerist.dz*

5- إعداد الباحثة إسراء جبريل رشاد مرعي، الجرائم الالكترونية-الأهداف، الأسباب، طرق الجريمة ومعالجتها، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، 09 أغسطس 2019.مقال منشور على:

.https://democraticac.de/wp-content/uploads/2019/08

فهرس المحتويات