جامعة مولود معمري – تيزي وزو–
كلية الحقوق والعلوم السياسية
قسم حقوق

# إشكالية القانون الواجب التطبيق على الجريمة الإلكترونية

***مذكرة لنيل شهادة الماستر في القانـــــــــون***
***تخصص: قانون جنائي وعلوم جنائية***

**إعداد الطالب:**
**دالي رياض**

**إشراف الأستاذة:**
**د/ تاجر كريمة**

**لجنة المناقشة:**

**د/ دراني ليندة ..... أستاذة محاضرة (أ)، جامعة مولود معمري، تيزي وزو .....رئيسا؛**

**د/ تاجر كريمة.....أستاذة محاضرة (ب)، جامعة مولود معمري، تيزي وزو..... مشرفا ومقررا؛**

**د/ القبي حفيظة .... أستاذة محاضرة (أ)، جامعة مولود معمري، تيزي وزو،..... ممتحنا.**

**تاريخ المناقشة: 2024/06/12.**

# الإهـــــــداء

ها أنا اليوم أقف على عتبة تخرجي أقطف ثمار تعبي و أرفع قبعتي بكل فخر، فاللهم لك الحمد إذا رضيت ولك الحمد بعد الرضا، لأنك وفقتني على إتمام هذا النجاح وتحقيق حلمي....

وبكل حب أهدي ثمرة نجاحي وتخرجي:

إلى الذي زين إسمي بأجمل الألقاب، من دعمني بلا حدود و أعطاني بلا مقابل، إلى من علمني أن الدنيا كفاح و سلاحها العلم والمعرفة، داعمي الأول في مسيرتي وسندي و قوتي و ملاذي بعد الله، فخري و إعتزازي" والدي".

إلى من جعل الله الجنة تحت أقدامها، و احتضنني قلبها قبل يدها وسهلت لي الشدائد بدعائها، إلى القلب الحنون و الشمعة التي كانت لي في الليالي المظلمات، سر قوتي ونجاحي جنتي "والدتي"

إلى من ساندتني بكل حب عند ضعفي و أزاحت عن طريقي المتاعب ممهدة لي الطريق زارعة الثقة والإصرار بداخلي "بن مني هدى"

إلى ملائكة رزقني الله بهن لأعرف من خلالهن طعم الحياة الجميلة، تلك الملائكة التي غيرن مفاهيم الحب و الصداقة و السند في حياتي أخواتي

"فريد، نادية، هاني، هالة"

إلى جميع من أمدوني بالقوة والتوجيه و أمن بي ودعمني في الأوقات الصعبة لأصل إلى ما أنا عليه الأن زملائي وزميلاتي وفقهم الله.

# الشكـــر والعرفـــان

أتقدم بالشكر و التقدير و العرفان بالجميل مع الإحترام للأستاذة الفاضلة الدكتورة "تاجر كريمة" التي تفضلت بالإشراف على مذكرتي، والتي لم تبخل علي بالنصائح القيمة والتوجيهات السديدة و المعاملة الطيبة طيلة مشوار إنجاز هذا العمل المتواضع.

فاللهم أجزيها منا خير الجزاء وبارك لها في صحتها ورزقها وأهلها.

كما أتوجه بالشكر والتقدير إلى الأساتذة الكرام أعضاء لجنة المناقشة على تفضلهم بقبول مناقشة هذه المذكرة فجزاكم الله كل خير.

تعد الجريمة الإلكترونية أحد منتجات ثورة المعلومات التي عرفها العالم في الأونة الأخيرة، وهي نتيجة للتطورات التكنولوجية في مجال تبادل ونقل المعلومات بين الأفراد والمؤسسات والدول عامة، فهذه التطورات المشهودة أفرزت لنا جريمة جديدة مستحدثة و مجرم جديد بطابع وتركيبة جديدة يختلف عن المجرم التقليدي في إطار علم الإجرام والقانون الجنائي، فسببت هذه الجريمة الكثير من الخسائر للعديد من الشركات والبنوك، وأصبحت تشكل تهديدا مباشرا لحرمة الحياة الخاصة سواء للأفراد أو المؤسسات.

فبروز هذه الجريمة أصبح واقع يهدد جميع الأفراد والبلدان، وذلك راجع في المقام الأول إلى الوسائل المتقدمة التي يستخدمها المجرم الإلكتروني، التي تأثرت هي الأخرى بالتطورات المشهودة في مجال تكنولوجيا الإعلام و الإتصال، ولقد إختلف الدراسون لهذه الظاهرة في تسميتها ووصفها وتشخصيها، بل وتعدد أراء فقهاء القانون بين مؤيد ومعارض فيما إذا كانت القوانين القائمة تكفي لمجابهة هذا النوع من الجرائم أم لا، لذلك لاتزال العديد من الدول تعاني من الفراغ التشريعي الذي يعالج هذا النوع من الجرائم المستحدثة،

إضافة إلى ذلك تتمتع الجريمة الإلكترونية بعدة خصائص ميزتها عن باقي الجرائم التقليدية، ومن أبرز هذه الخصائص انها جريمة عابرة للحدود لا تحدها حدود جغرافية، فهذه الخاصية أفضت عليها طبيعة خاصة، تتجلى في قدرة الجاني على إرتكابها عن بعد، أي أن يكون الجاني في مكان و المجني عليه في مكان أخر، فالجريمة الإلكترونية ليس لها مقر ثابت و معين بل تنتشر في كل دول العالم، لذلك يمكن أن يتوزع السلوك الإجرامي على عدة دول في أن واحد، إضافة إلى اختلافا لمسرح التي تتم فيه الجريمة الإلكترونية الذي يعتبر مسرح غير مادي أي مسرح إفتراضي عكس الجرائم التقليدية.

وعليه ونظرا للطبيعة الإفتراضية التي تتميز بها الجريمة الإلكترونية وبعدها الدولي لم تعد مخاطرها و أثارها محصورة في النطاق الإقليمي لدولة بعينها، الأمر الذي بات يثير بعض العقبات أمام الأجهزة المعنية لمكافحة هذه الظاهرة، ذلك أن متابعة الجناة والكشف عن جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم في نطاق إقليم دولة أخرى ، وهو ما يتعارض مع مبدأ السيادة

الإقليمية للدول المنصوص عليه في المادة الثالثة من قانون العقوبات "يطبق قانون العقوبات على كافة الجرائم التي ترتكب في أراضي الجمهورية، كما يطبق على الجرائم التي ترتكب في الخارج إذا كانت تدخل في إختصاص المحاكم الجزائية الجزائرية طبقا لأحكام قانون الإجراءات الجزائية"[1] ، مما يؤدي كنتيجة إلى تنازع الاختصاص القضائي بسبب صعوبة تحديد مكان وقوع الجريمة الإلكترونية عبر الوطنية وبالتبعية بروز إشكالية القانون الواجب التطبيق على هذه الجريمة .

انطلاقا مما سبق ذكره، إن الغرض المنشود من وراء البحث في موضوع إشكالية القانون الواجب التطبيق على الجريمة الإلكترونية، هو تسليط الضوء في المقام الأول على الإشكالية التي تثيرها الجريمة الإلكترونية في مجال تحديد النص الجنائي الواجب التطبيق، حيث أن الطبيعة الخاصة التي تتميز بها هذه الجرائم بإعتبارها جريمة لا تحدها حدود جغرافية و جريمة تقع في بيئة إفتراضية، جعلت الكثير من التشريعات الوطنية في حيرة بخصوص تحديد مكان وقوع هذه الجريمة و بالتالي تحديد القانون الواجب التطبيق، كما وتسمح لنا هذه الدراسة في التعرف على بعض الحلول التي وجدت في سبيل تجاوز عقبات تحديد النص الجنائي الواجب التطبيق على هذه الجريمة

يعتبر هذا البحث من المواضيع الجديدة و المهمة في القسم الإجرائي من القانون الجنائي، كما أنه من المواضيع التي لا تزال في بدايتها ولم تتم دراستها وفحصها على مستوى القانون الجنائي، حيث أن معظم الأبحاث التي أجريت في مجال الجرائم الإلكترونية، إقتصرت على دراسة جوانبها الموضوعية دون محاولة الخوض في الإشكاليات التي تثيرها هذه الجريمة ، لا سيما إشكالية القانون الواجب التطبيق في حالة إمتداد أثارها إلى عدة أقاليم دولية.

يمكن إرجاع اختيارنا لهذا الموضوع إلى أسباب ذاتية و أخرى موضوعية تتمثل فيما يلي:

**1.**الأسباب الذاتية: تتمثل في ميولي الخاص إلى دراسة القانون الجنائي والعلوم الجنائية، كذلك الرغبة الشديدة في البحث في الجرائم المستحدثة لاسيما منها الجريمة الإلكترونية التي تتسع رقعتها الجغرافية يوما بعد يوم،

[1] الأمر رقم 66-156 مؤرخ في 18 صفر 1386، الموافق 8 يونيو سنة 1966، المتضمن قانون العقوبات، المعدل والمتمم، الجريدة الرسمية رقم 49 الصادرة بتاريخ 21 صفر 1386.

2.الأسباب الموضوعية: رغبتي وفضولي في إكتشاف حقيقة التعامل مع المشكلات التي تطرحها هذه الجريمة، فالعديد من الدراسات التي أنجزت في الجريمة الإلكترونية لم تركز على العوائق التي تشكلها هذه الجريمة، حيث كانت تقريبا جل الأبحاث تركز على الجوانب الموضوعية لهذه الجريمة

الجدير بالإشارة، ونظرا لنقص الدراسات المتخصصة بخصوص إشكالية القانون الواجب التطبيق على الجريمة الإلكترونية، فقد واجهنا العديد من الصعوبات في إنجاز هذا البحث، حيث وجدنا نقصا من حيث المؤلفات التي أنجزت في هذا الصدد، ولقد حاولت قدر الإمكان من خلال بحثي هذا إثراء النقاش القانوني حول المعوقات التي تثيرها الجريمة الإلكترونية.

إن إمتداد تأثير تكنولوجيا المعلومات إلى الجوانب الإجرائية من القانون الجنائي، يثير إشكالية قانونية، وذلك راجع أن نصوص هذا القانون صيغت من أجل تطبيقها على الجرائم التقليدية، التي ترتكب في بيئة مادية ملموسة على عكس الجريمة الإلكترونية التي تقع في بيئة إفتراضية غير مادية مختلفة تماما عن المسرح التقليدي، إضافة إلى ذلك وباعتبار أن هذه الجريمة ذات صبغة دولية، ففي غالب الأحيان يكون سلوكها الإجرامي موزع على العديد من الأقاليم الدولية في أن واحد مما يثير إشكالية تحديد مكان وقوعها و كذا القانون الواجب التطبيق في هذه الحالة، هذه المشكلات والعقبات القانونية جعلت مسألة تحديد القانون الواجب التطبيق على الجريمة الإلكترونية فعلا مسألة شائكة ومعقدة، وعليه كانت إشكالية الباحث كالاتي:

**إلى أي مدى يمكن إيجاد قانون موحد يطبق على الجريمة الإلكترونية العابرة للحدود أمام العقبات التي تطرحها الطبيعة الخاصة لهذه الجريمة ؟.**

بالنظر إلى درجة التعقيد التي تتميز بها الجريمة الإلكترونية و ما أثارته من إشكاليات قانونية وكذا دور التشريعات الوطنية في معالجة هذه الإشكاليات تم إتباع المناهج التالية في معالجة الموضوع:

المنهج الوصفي في توضيح مفاهيم الجريمة الإلكترونية الفقهية والتشريعية، وكذا وصف مختلف أنواع الجريمة الإلكترونية، كما تم إستخدام المنهج التحليلي من أجل دراسة وتحليل مختلف المعلومات المتوصل إليها، وذلك من خلال تحليل النصوص القانونية ودراسة أهم ما جاء بها، أما

بالنسبة للمنهج المقارن تم إستخدامه على إعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود و جريمة عالمية، فقد نالت بلا شك حظها من المعالجة التشريعية على مستوى التشريعات المقارنة، لذلك حاولت من خلال هذه الدراسة مقارنة بعض المفاهيم التي إعتمدها المشرع الجزائري مع بعض التشريعات الأخرى.

حتى نجيب عن الإشكالية المطروحة في موضوع بحثنا، ويكون العمل متكاملا قدر الإمكان وملما بجميع المعلومات قسمنا الدراسة إلى فصلين، حيث عالجنا في الفصل الأول الإطار المفاهيمي للجريمة الإلكترونية، أما بخصوص الفصل الثاني فقد تناولنا عقبات تحديد القانون الواجب التطبيق على الجريمة الإلكترونية العابرة للحدود مع الحلول المقترحة لها.

# الفصل الاول : الإطار المفاهيمي للجريمة الإلكترونية

انتشرت شبكات الحاسوب والمعلومات في جميع أنحاء العالم سواء في الدول المتقدمة او الدول النامية، حيث أصبحت جزء لا يتجزأ من الحياة اليومية للأفراد ودخلت تطبيقاتها في بيئة المجتمعات المعاصرة، وأسهمت شبكات الحاسوب والمعلومات في تعزيز التواصل الحضاري وتعزيز التفاهم الإنساني وساهمت أيضا في تسهيل التواصل بين الشعوب، و في هذا الإطار استفحلت ظاهرة إجرامية جديدة تعرف بإسم الجريمة الإلكترونية والتي أصبحت تحديا حديثا يواجه مختلف المجتمعات، فتسبب التطور التكنولوجي المتسارع في تزايد من هجمات هذه الجريمة.

نظرا لخطورة هذه الأخيرة وسرعة إنتشارها وكذا سهولة إرتكابها، أصبحت موضع اهتمام الكثير من رجال الفقه والقانون، حيث أخذت هذه الظاهرة حيزا كبيرا من الدراسات من أجل ضبط مفهوم لها بالإضافة إلى إنفراد هذه الجريمة بخصائص تميزها عن باقي الجرائم التقليدية مما أضفى عليها ميزة الطابع الدولي كونها جريمة عابرة للقارات زيادة على مختلف الخصائص الأخرى التي تتميز بها(المبحث الأول)، مثلما لهذه الجريمة عدة صور تختلف باختلاف الزاوية التي ينظر إليها إزاء الإعتداء الموجه ضد ضحاياها(المبحث الثاني).

## المبحث الأول: مفهوم الجريمة الإلكترونية

إن دراسة أية ظاهرة قانونية يتطلب تأصيلها، حيث بالرجوع إلى أساس تحديد مفهوم الجريمة الإلكترونية نجد أنها تتمثل في الممارسات الدولية عن طريق الإتفاقيات الإقليمية و الدولية أو التوصيات والمؤتمرات و الدراسات الأكاديمية التي بذلت جهدا كبيرا لتحديد مفهوم الجريمة الإلكترونية ولكن ليس بالضرورة أن تقف على المفهوم الحقيقي لهذه الجريمة، لذلك لا يوجد مصطلح قانوني موحد للجريمة الإلكترونية، بل برزت مصطلحات عديدة ابتداء من إصطلاح "إساءة إستخدام الكمبيوتر" مرور بـ "الجرائم المعلوماتية، جرائم تكنولوجيا الإعلام و الإتصال، الجريمة السيبرانية...إلخ"، فإختلاف المصطلحات يعني إختلاف الدلالات، حيث يتنوع مفهوم الجريمة الإلكترونية بين المفهوم الواسع والضيق للجريمة الإلكترونية (المطلب الأول)، وتتميز هذه الجريمة بالعديد من الخصائص التي تميزها عن باقي الجرائم (المطلب الثاني).

### المطلب الأول: تعريف الجريمة الإلكترونية

ظهرت الجريمة الإلكترونية نتيجة للثورة الرقمية المتسارعة، ونظرا لحداثة هذه الجريمة إختلف الفقه و التشريعات في تعريف الجريمة الإلكترونية، فكل يعرفها وفقا للمعيار الذي إعتمد عليه، وفي سبيل ذلك ظهرت عدة دلالات دالة عن هذه الظاهرة وبالتبعية ظهرت العديد من التعاريف في هذا الشأن، منها تعاريف فقهية (الفرع الأول)، وكذا تعاريف تشريعية (الفرع الثاني).

#### الفرع الأول: التعريف الفقهي للجريمة الإلكترونية

إختلف فقهاء القانون الجنائي في ضبط تعريف الجريمة الإلكترونية وذلك لإختلاف الأسس الفقهية وتباين الأنظمة القانونية، حيث بذلوا جهودا متواصلة للوصول إلى تعريف صريح لهذه الجريمة، فانقسموا إلى إتجاهين، الإتجاه الأول يضيق من مفهوم الجريمة الإلكترونية (أولا)، و الإتجاه الثاني يوسع من تعريفها (ثانيا).

**أولا: الإتجاه الفقهي المضيق لمفهوم الجريمة الإلكترونية**

يركز أنصار هذا الإتجاه على تعريف الجريمة الإلكترونية على الجانب الفني، والذي بدوره يجعل من المنظومة المادية المعلوماتية حقل للجريمة، وهي الهدف المباشر للمجرمين، والجريمة الإلكترونية ضمن هذا التعريف هي عبارة "**عن نشاط إجرامي تستخدم فيه تقنية الحاسب الألي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي**"[1].

أو هي "**كل الفعل غير مشروع يتورط في إرتكابه الحاسب، أو الفعل الإجرامي الذي يستخدم في إرتكابه الحاسوب كأداة رئيسية**"[2].

فحسب التعريف المقدم من أنصار هذا الإتجاه، توصف الجريمة بأنها إلكترونية عندما تكون الأداة المستخدمة هي الحاسب الألي الذي بواسطته تتحقق النتيجة الإجرامية المستهدفة.

كما عرف البعض الأخر الجريمة الإلكترونية على أنها " **كل فعل غير مشروع يتطلب درجة عالية من التقنية الحاسوبية لارتكابه من ناحية، ولملاحقته من ناحية أخرى**"[3]، فبهذا يضيق هذا التعريف من نطاق الجريمة الإلكترونية حيث يتطلب من مرتكبيها أن يتمتعوا بمستوى عال من المعرفة بتكنولوجيا المعلومات، وهو ما لا يتحقق في كثير منها لأن تبسيط وسائل المعالجة وتحويل الأجهزة المعقدة فيما سبق إلى أجهزة سهلة الإستخدام مكنت الفاعل إرتكاب جريمته دون معرفة كبيرة بالمعلوماتية[4].

---

[1] حمالي سمير، "**التحديات القانونية لمواجهة الجرائم السيبرانية**"، مداخلة منشورة في المسطرة الإجرائية لأشغال الملتقى الوطني الإفتراضي حول "الجرائم الإلكترونية في المجتمع الجزائري"، كلية العلوم الإنسانية و الإجتماعية، جامعة يحي فارس، المدية، 15 مارس 2022، منشور على الموقع الإلكتروني https://www.univ-medea.dz ، تم الإطلاع عليه بتاريخ 2024/01/23 على الساعة 12.30، ص 23.

[2] نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أحمد دراية، أدرار، 2017/2016 ص7.

[3] حرزون ليلة، هدروق أسماء، التنظيم القانوني للجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري، مذكرة لنيل شهادة ماستر، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2022/2021، ص06.

[4] عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي ( دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2010، ص ص 33-34.

فمن وجهة نظرنا أن هذا التعريف المقدم بشأن اشتراط المعرفة التقنية للمعلومات في الفاعل يشوبه نوع من النقص وذلك راجع أنه في بعض الحالات قد يتوفر هذا الشرط عند إرتكاب الجريمة الإلكترونية ويكون الفاعل متمكن في مجال تقنية المعلومات ولكن في غالب الأحيان قد لا يتوفر هذا الشرط و يرتكب الفعل الإجرامي في بيئة إلكترونية دون أن يكون الفاعل على قدر كبير من المعرفة في مجال تقنية المعلومات، فبمقدور الجاني أن يرتكب جريمة تخريب البيانات المخزنة في الحاسب الألي (مثل حذفها أو نقلها أو تغييرها) دون الحاجة إلى قدر كبير من المعرفة في هذا المجال، كذلك في السنوات الأخيرة انتشرت على موقع التواصل الإجتماعي (Face book) روابط ملغمة ومحملة بفيروسات تم إنشاؤها على مواقع متخصصة الغرض منها إختراق حسابات شخصية في الفايسبوك(الحصول على العنوان البريدي الإلكتروني وكلمة السر) فبمجرد إرسالها إلى شخص ما و يتم الدخول إلى هذا الرابط يخترق الحساب الخاص بالمستقبل للرسالة، فهذا الفعل لا يتطلب مهارات عالية ومعرفة كبيرة ، فلذلك فإن أنصار الإتجاه المضيق للجريمة الإلكترونية لم يوفقوا باشتراطهم للمعرفة العالية بتقنية المعلومات.

تجدر الإشارة أن أنصار هذا الإتجاه يرون أنه لا داعي لإنشاء نصوص جديدة للتعامل مع الجرائم التي تفتقر إلى المعرفة بالحاسب الألي لأنها جرائم عادية تغطيها النصوص التقليدية للقوانين الجنائية، على عكس الجرائم التي يتطلب فيها هذه المعرفة فهي بحاجة إلى نصوص خاصة تتلاءم وطبيعتها التي تختلف عن غيرها من الجرائم التقليدية[1].

فمن خلال ما سبق انصار هذا الإتجاه من خلال تعريفهم للجريمة الإلكترونية أخذوا بالوسيلة كأداة لإرتكاب هذه الجريمة فالتعريفات المقدمة من طرف أنصار هذا الإتجاه حصرت من نطاق الجريمة الإلكترونية في الأداة المستعملة في إرتكاب الفعل الإجرامي، والشي المعاب على التعريفات

[1] حشيفة عبد الهادي، التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، 2020/2019، ص10.

المقدمة أنها أخرجت الكثير من الأفعال الغير مشروعة التي يستخدم فيها الحاسب الألي كوسيلة لإرتكابها من نطاق الجريمة الإلكترونية مثل جريمة الإحتيال المعلوماتي[1].

**ثانيا: الإتجاه الفقهي الموسع لمفهوم الجريمة الإلكترونية**

إثر الانتقادات التي وجهت لأصحاب الإتجاه الضيق في تعريف الجريمة الإلكترونية ذهب بعض الفقهاء لمحاولة إعطاء تعريف موسع للجريمة الإلكترونية.

حيث عرفها البعض من أنصار هذا الإتجاه بأنها "**جميع الأعمال الإجرامية التي ترتكب بمساعدة الكمبيوتر**"، او هي "**كل عمل إجرامي يتم في محيط أجهزة الكمبيوتر**"[2]، أو هي" **مجموعة من الأفعال و السلوكيات غير المشروعة التي تتم عبر شبكة الأنترنت أو البث من خلال محتوياتها** "[3].

فمن خلال هذه التعريفات يتبين لنا أن هذا الإتجاه يوسع نوعا ما من مفهوم الجريمة الإلكترونية عكس الإتجاه المضيق، حيث لم يحصر نطاق هذه الجريمة في الحاسوب أو مستخدمه، وإنما وسعوا من نطاقها لتشمل كل فعل إجرامي يتم عن طريق المعلوماتية تصبغ عليه صفة الجريمة الإلكترونية، ونظرا لتسارع التطور التكنولوجي والذي تتطور معه هذه الجريمة بالتبعية نرى أن أصحاب هذا الإتجاه أصابوا بتوسيعهم من نطاق التجريم للجريمة الإلكترونية للإلمام بأكبر قدر من صور الجريمة الإلكترونية المستحدثة.

يوجد أيضا من بين التعريفات الموسعة للجريمة الإلكترونية تعريف الخبير الأمريكي "باركر" حيث عرفها بأنها" **كل عمل إجرامي متعمد بغض النظر عن علاقته بالمعلوماتية و ينتج عن هذا العمل خسارة تلحق بالمجني عليه و ربح يحققه الجاني**"[4].

---

[1] نصت المادة 08 من إتفاقية بودابست لمكافحة الجرائم المعلوماتية والأنترنت على أن الإحتيال المعلوماتي هو "**القيام بإدخال أو حذف أو تعديل أو التعدي على عمليات الشبكة المعلوماتية بهدف الحصول على منفعة مادية لنفسه او لغيره**".

[2] بوديسة بجاد عبد الرؤوف، أليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة ماستر، تخصص قانون الإعلام الالي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2022/2021، ص 10.

[3] عائشة بن قارة مصطفى، مرجع سابق، ص33.

[4] وردي طيب، الإختصاص القضائي في جرائم الأنترنت، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الطاهر مولاي، سعيدة، 2015/2014، ص 3.

بينما إعتمد مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين التعريف التالي للجريمة الإلكترونية " **أية جريمة يمكن ارتكابها من خلال نظام حاسوبي، أو شبكة حاسوبية، والجريمة تلك تشمل من الناحية المبدئية جميع الأفعال الإجرامية التي يمكن ارتكابها في بيئة إلكترونية**"[1].

بعد عرض التعريف الفقهي للجريمة الإلكترونية بين إتجاه مضيق و أخر موسع، فالتباين الحاصل بين الاتجاهين مرجعه إلى طبعة النظام القانوني للإثبات، فهناك نظام أنجلوسكسوني و نظام لاتيني، فالأول يأخذ بالإثبات المقيد، والثاني يأخذ بنظام الإثبات الحر، وعليه ففي نظام الإثبات القانوني الأنجلوسكسوني (المقيد) فالقاضي مقيد بقيد موضوعي متمثل في "لا جريمة و لا عقوبة إلا بنص"، وقيد إجرائي وهو ضرورة حصوله على الدليل الذي يثبت الوقائع المتجددة، ولذلك فهذه الدول تسعى لتوسيع مفهوم الجريمة الإلكترونية للوصول إلى الدليل الذي يثبت الصلة بينها وبين المجرم، بالإضافة لتسهيل التعاون الدولي في مجال الجريمة الإلكترونية، بينما التضيق في مفهوم الجريمة الإلكترونية يثير صعوبات في التعاون الدولي فتسليم المجرم الإلكتروني مثلا مقرون بازدواجية التجريم، وبناءا على المفهوم الضيق تكون الجريمة الإلكترونية مباحة في بلد ومجرمة في بلد أخر[2].

وللوقوف على المفهوم الدقيق للجريمة الإلكترونية نتساؤل عن المصلحة الجديرة بالرعاية أو المحمية من قبل المشرع؟، ماهي المصلحة المحمية التي يسعى المشرع لحمايتها في الجريمة الإلكترونية؟.

وردا عن هذا التساؤل فإذا تم الأخذ بالمفهوم الضيق للجريمة الإلكترونية فالمصلحة الجديرة بالحماية هي البيانات والمعطيات، أما إذا تم الأخذ بالمفهوم الواسع فيجب البحث عن كل جريمة بأركانها لتحديد المصلحة الجديرة بالحماية، وعليه فالمصلحة الجديرة بالحماية هو المعيار الأمثل

---

[1] مونة مقلاتي، راضية مشري، "**الجريمة الإلكترونية (دلالة المفهوم وفعالية المعالجة القانونية)**"، مجلة أبحاث قانونية وسياسية، المجلد 6 ، العدد 01، جامعة 0 ماي 1945 قالمة، 2021، ص 494.

[2] محمد عدنان علي الزير، الجرائم الإلكترونية (المحاضرة الأولى): مفهومها وخصائصها و أركانها والمصلحة المحمية فيها، المدونة القانونية، فيديو منشور على الموقع الإلكتروني www.youtube.com/@DrMohammedAadnan، تم الإطلاع عليه بتاريخ 24/04/ 2024 على الساعة 14.36.

للوقوف على تحديد مفهوم الجريمة الإلكترونية و الحيلولة دون التوسع فيها والوقوع في التعدد الصوري لواقعة واحدة، والجدير بالقول أيضا أن المفهوم الواسع لهذه الجريمة له خلفيات و أهداف وهي السعي لتكاثف جهود كل الدول لمكافحة الجريمة الإلكترونية، وختاما لهذا العرض نقول أن الجريمة الإلكترونية لها طبيعة مزدوجة إذ تعد جريمة إلكترونية محضة تستهدف الأنظمة والبيانات المعلوماتية، كما أنها تعد جريمة عادية (كلاسيكية) مرتكبة بواسطة تقنية المعلومات[1].

**الفرع الثاني: التعريف التشريعي للجريمة الإلكترونية**

لم تتطرق معظم التشريعات الجنائية المقارنة إلى تعريف الجريمة الإلكترونية، وإنما إكتفت بتحديد العديد من المظاهر والسلوكيات التي تشكل جرائم إلكترونية، محددة أركانها و الجزاءات المقررة لها، لذلك بالعودة إلى أحكام القانون الفلسطيني نجد أنه لم يورد تعريفا جامعا للجريمة الإلكترونية، غير أنه بالرجوع للنصوص القانونية المنظمة بموجب القرار بقانون رقم (10) لسنة 2018 بشأن الجرائم الإلكترونية، نجد أنه نص على العديد من المظاهر و الأفعال التي تشكل بحد ذاتها جرائم إلكترونية و نص أيضا على العقوبات المقررة على مرتكبي تلك الجرائم[2]، ونفس الشيء بالنسبة للتشريع العماني حيث عدل المشرع العماني قانون الجزاء بالمرسوم السلطاني 2001/72 أين أضاف إلى قانون الجزاء الفصل الثاني مكرر وجرم بموجب هذا التعديل جملة من التصرفات التي يتعرض لها الحاسب الألي وحصرها في بعض الصور نذكر منها على سبيل المثال" الإلتقاط غير المشروع للمعلومات والبيانات، الدخول غير المشروع على أنظمة الحاسب الألي للتجسس والتنصت على البيانات والمعلومات، تسريب المعلومات والبيانات، جمع المعلومات والبيانات و إعادة

[1] محمد عدنان علي الزير، الجرائم الإلكترونية (المحاضرة الأولى): مفهومها وخصائصها و أركانها والمصلحة المحمية فيها، المدونة القانونية، فيديو منشور على الموقع www.youtube.com/@DrMohammedAadnan، تم الإطلاع عليه بتاريخ 04/24/ 2024 على الساعة 14.50.

[2] صهيب ياسر محمد شاهين، بشرى محمد حسن أبو ترابي، "**الجريمة الإلكترونية وبعدها القانوني (دراسة مقارنة بين التشريع الجزائري والفلسطيني)**"، مجلة نوميروس الأكاديمية، ، العدد الأول، المجلد الثاني جامعة عباس لغرور، خنشلة، الجزائر، 2021، ص 153

إستخدامها"[1]، وكذلك الأمر بالنسبة للتشريع الكويتي الذي أوضح المشرع من خلال قانون رقم 63 لسنة 2015 المتضمن مكافحة جرائم تقنية المعلومات العديد من المصطلحات المرتبطة بالجريمة الإلكترونية مثل (البيانات الإلكترونية، الشبكة المعلوماتية، وسيلة تقنية المعلومات، الدخول غير المشروع، التوقيع الإلكتروني) وحاول أيضا توضيح بعض النصوص المتعلقة بهذا النوع من الجرائم من خلال هذا القانون[2]، أما بخصوص المشرع المصري إكتفى ايضا بذكر الجرائم الإلكترونية والعقوبات المقررة لها من خلال القانون رقم 175 لسنة 2018 في الباب الثالث منه المادة 12 [3].

أما المشرع الجزائري فقد خالف كل هذه التشريعات، إذ يعتبر قانون العقوبات الجزائري من القوانين العربية السباقة التي تطرقت لهذا الموضوع بل أنه من التشريعات المواكبة للتشريعات الغربية على خطى التشريع الأمريكي والإنجليزي والفرنسي، فالمشرع الجزائري بادر إلى تعديل قانون العقوبات بمقتضى القانون رقم 04-15[4] المؤرخ في 10 نوفمبر 2004 بإدراجه القسم السابع مكرر والذي يتضمن المواد 394 مكرر إلى المادة 394 مكرر 7 ولم يكتف المشرع الجزائري بذلك بل قطع أشواطا أخرى في سبيل فرض حماية جنائية على الحياة الخاصة للأفراد حيث بادر بتعديل جديد لقانون العقوبات وهو الذي جاء به القانون رقم 06-23[5] المؤرخ في 20 ديسمبر 2006 والذي مس المادة 303 وإقراره المادة 303 مكرر إلى المادة 303 مكرر 3 وهو بذلك يضع سياجا لحماية

---

[1] بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة المسيلة،2014/2013، ص 14.

[2] مخلد إبراهيم الزغبي، **فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية** "**دراسة مقارنة**"، المجلة العربية للنشر العلمي، العدد 37،2021 ، ص 279.

[3] القانون رقم 175، لسنة 2018 ، المتضمن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد32 مكرر (ج)، الصادرة في 14 أوت 2018، ص 08.

[4] القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية رقم 71، الصادرة بتاريخ 10 نوفمبر 2004.

[5] قانون رقم 06-23 مؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006 يعدل ويتمم الامر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966.

خصوصية الأفراد تحسبا للإستخدام السيء للوسائل التكنولوجية الحديثة عن طريق الكمبيوتر أو الهاتف النقال وما يرتبط بها من تقنيات مثل ما يسمى بالبلوتوث وغيره[1].

بالرجوع للقانون رقم 04-15 المؤرخ في 10 نوفمبر2004 المتمم والمعدل للأمر 66-156[2]المتضمن قانون العقوبات، قام المشرع الجزائري بتجريم ما أسماه بـ "المساس بأنظمة المعالجة الألية للمعطيات" حماية لأنظمة المعالجة الألية للمعطيات من كافة أشكال الإعتداءات التي تقع على مكوناتها غير المادية وهو الامر الذي دفع بالمشرع الجزائري إلى تعديل قانون العقوبات بموجب القانون السالف الذكر، حيث خصص له القسم السابع مكرر بعنوان –المساس بأنظمة المعالجة الألية للمعطيات– يحتوي هذا القسم على ثمانية مواد بدأ من المادة 394 مكرر إلى المادة 394 مكرر 07.[3]

ونظرا لخطورة هذه الظاهرة التي أصبحت تهدد المجتمع قام المشرع الجزائري في سبيل الحد من هذه الجريمة بإصدار قانون خاص مستقل وهو القانون 09-04 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها[4]، أطلق على الجريمة الإلكترونية تسمية الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، وعرفها في المادة 02 الفقرة (أ) على أنها " جرائم المساس بأنظمة الألية للمعطيات المحددة في قانون العقوبات وأي جريمة ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية ".

وعليه نلاحظ أن المشرع الجزائري إنتقل من المفهوم الضيق للجريمة الإلكترونية الذي كان ينحصر في الجرائم التي تقع على أنظمة المعالجة الألية للمعطيات وذلك في القانون 04-15 إلى المفهوم الواسع للجريمة الإلكترونية بسنه القانون 09-04 المتعلق بالوقاية من جرائم تكنولوجيا

---

[1] زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر،2011، ص48

[2]القانون رقم 04- 15، مرجع سابق.

[3] يرمش مراد، خصوصية الجريمة الإلكترونية، أطروحة لنيل شهادة دكتورة علوم في القانون الخاص، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة، السنة الجامعية 2021/2020، ص ص 25-26.

[4] القانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، الجريدة الرسمية، العدد47، الصادرة بتاريخ 16 غشت 2009، ص 05 .

الإعلام والإتصال بنصه على ان الجرائم الإلكترونية ترتكب في نظام معلوماتي أو يسهل إرتكابها عليه وهو الأمر الذي وسع من دائرة التجريم في مجال الإجرام الإلكتروني، فأدخل كل الجرائم التقليدية المرتكبة بإستعمال وسيلة تكنولوجية لذلك أطلق البعض عليها تسمية بالجرائم تقليسيبرانية.

**المطلب الثاني: خصائص الجريمة الإلكترونية**

تمثل الجريمة الإلكترونية تهديدا متزايدا في عصرنا الحديث، فالجريمة الإلكترونية تختلف عن الجرائم التقليدية من عدة نواحي سواء من ناحية طبيعة الجريمة في حد ذاتها أو من ناحية مرتكبي هذه الجريمة الذين يمتازون بعدة صفات تجعلهم ينفردون بها غيرهم من المجرمين التقليديين، فعليه قسمنا هذا المطلب إلى فرعين، السمات الخاصة بالجريمة الإلكترونية (الفرع الأول)، ثم تطرقنا إلى المميزات المرتبطة بالمجرم الإلكتروني (الفرع الثاني).

**الفرع الاول: السمات الخاصة بالجريمة الإلكترونية**

تتميز الجريمة الإلكترونية بسمات خاصة فريدة بنوعها تميزها عن باقي الجرائم الأخرى، فالجريمة الإلكترونية لا يمكن حصرها بمكان معين فهي جريمة عابرة للحدود الوطنية (أولا) صعبة الضبط و الإثبات (ثانيا)، وهادئة (ثالثا).

**أولا: الجريمة الإلكترونية جريمة منظمة وعابرة للحدود الوطنية**

يتميز الفضاء المعلوماتي بالحدود الجغرافية غير محددة أي لا تعرف أي حدود، فهي بيئة منفتحة عبر شبكات تخترق الزمان والمكان، من غير أن تكون تحت أي حراسة خصوصا بعد ظهور شبكات المعلومات الدولية" الأنترنت"، بحيث يمكن نقل كم هائل من المعلومات بين عدة أنظمة عن بعد و يفصل بينها ألاف الأميال، ونتيجة لذلك تأثرت عديد من دول بالجريمة الإلكترونية الواحدة في أن واحد[1].

لذلك فإن الجريمة الإلكترونية لا ترتبط بمكان محدد لإرتباطها بالشبكة الإلكترونية، وفي أغلب الأحيان يكون مرتكب الجريمة في مكان والضحية في مكان أخر والضرر في مكان ثالث، حيث قد تتأثر دول ومؤسسات وشركات كثيرة بهذه الجريمة في الوقت نفسه وفي أماكن متعددة، ومن هنا سميت بالجريمة العابرة للحدود الوطنية أو الدولية، وهو ما أدى إلى ضرورة التعاون الدولي للحد من

[1] عائشة بن قارة مصطفى، مرجع سابق، ص ص 44-45.

هذه الجريمة[1]، فقدرة تقنية المعلومات على إختصار المسافات وتعزيز الصلة بين مختلف أنحاء العالم إنعكست على طبيعة الأعمال الإجرامية التي يعمد فيها المجرمون إلى إستخدام هذه التقنيات في خرقهم للقانون، مما يعني أن مسرح الجريمة الإلكترونية لم يعد محليا بل أصبح عالميا، إذ أن الفاعل لا يتواجد على مسرح الجريمة بل يرتكب جريمته عن بعد، وهو ما يعني عدم التواجد المادي لحصول الجريمة الإلكترونية في مكان الجريمة، ومن ثم تتباعد المسافات بين الفعل الذي يتم من خلال جهاز كمبيوتر الفاعل، وبين المعلومات محل الإعتداء[2].

يصف علماء القانون الجريمة الإلكترونية بالجريمة العابرة للدول والقارات أو الجريمة العابرة للحدود، على الرغم من أن هذا النوع من الجرائم لا ينفرد لوحده بهذه الميزة حيث أن هناك بعض الجرائم الأخرى التي تشترك بهذه الخاصية، مثل جرائم الإرهاب الدولي وجرائم المخدرات وغسيل الأموال إلا أنها تختلف عنها في كونها لا تستلزم الإنتقال عبر الحدود والخضوع لإجراءات التفتيش والمراقبة كما هو الشأن في الجرائم التقليدية[3].

الجدير بالإشارة أن الأمم المتحدة في إحدى دراستها توصلت من خلال إستقراء الممارسات الدولية من خلال التطبيقات القضائية والجرائم المبلغ عنها أن نسبة 50% إلى 100 % من الجرائم الإلكترونية المرتكبة هي جريمة عابرة للحدود[4].

تختلف الجريمة الإلكترونية عن الجرائم الأخرى من حيث أنها ذات بعد دولي (عابرة للحدود) وكونها جريمة لا تعرف حيز مكاني معين فعلى سبيل المثال يمكن أن يكون الجاني مرتكب جريمة "إختراق المواقع الإلكترونية الحكومية" يقيم بدولة تونس وإرتكب جريمة إختراق موقع الإلكتروني لفرع

---

[1] عبد الله ذيب محمود، أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2020، ص 27 .

[2] نعيمة داودي، "**الجريمة الإلكترونية(خصائصها ومجالات إستخدامها، وأهم سبل مكافحتها)**"، مجلة مهد اللغات، المجلد 2، العدد1، كلية لغات الاجنبية، جامعة حسيبة بن بوعلي، الشلف، 2020، ص 48.

[3] يرمش مراد، مرجع سابق، ص35.

[4] محمد عدنان علي الزير، الجرائم الإلكترونية (المحاضرة الأولى): مفهومها وخصائصها و أركانها والمصلحة المحمية فيها، المدونة القانونية، فيديو منشور على الموقع www.youtube.com/@DrMohammedAadnan، تم الإطلاع عليه بتاريخ 04/24/ 2024 على الساعة 15.50

بنكي متواجد بإقليم دولة الإمارات وهذا الفرع البنكي تابع لدولة مصر، ففي هذه الحالة نرى أن الجاني يتواجد بدولة تونس والضرر كان في دولة الإمارات والمجني عليه هي الحكومة المصرية.

**ثانيا: الجريمة الإلكترونية صعبة الضبط و الإثبات**

من أهم خصائص الجريمة الإلكترونية التي تميزها عن غيرها من الجرائم أنه من الصعب إكتشافها وإثباتها لأسباب ترجع إلى الجاني أو إلى المجني عليه، وإلى وسيلة إرتكابها، حيث تتم هذه الجريمة بشكل منظم من إقليم دولة واحدة بإستخدم الأنترنت، أضف إلى أن الجاني مجرم محترف يتصف بالذكاء و مثقف لا يترك أثارا جانبية خارجية للجريمة مما يصعب إثباتها، كما أن المجني عليهم وهم غالبا مؤسسات عامة او خاصة يحجمون عن الإبلاغ عنها تجنبا للإساءة إلى السمعة وهز الثقة، فضلا عن إمكانية تدمير الدليل في مدة زمنية قياسية[1].

فإذا تم ضبط الجريمة الإلكترونية فلا يكون إلا بمحض الصدفة، نظرا لعدم وجود أثر كتابي لما يجرى خلال تنفيذها من عمليات حيث يتم بالنبضات الإلكترونية نقل المعلومات، ولذلك يستطيع الجاني تدمير دليل الإدانة في أقل من ثانية، إلى جانب إمكانية إرتكابها عبر الوطنية والدول والقارات وذلك بإستخدام شبكات الإتصال ودون تحمل عناء الإنتقال كما سبق و أشرنا في الخاصية الأولى(البعد الدولي للجريمة الإلكترونية)، وإلى جانب ذلك الرغبة في إستقرار حركة المعاملات ومحاولة إخفاء أسلوب الجريمة حتى لا يتم تقليدها من جانب الأخرين، فكل هذه الأسباب تدفع المجني عليه في الجرائم الإلكترونية إلى الإحجام عن مساعدة السلطات المختصة في إثبات الجريمة والكشف عنها، وحتى في حالة الإبلاغ فإن المجني عليه لا يتعاون مع جهات التحقيق خوفا مما يترتب عليه من دعاية مضرة وضياع ثقة المساهمين حيث يكون المجني عليهم عادة من البنوك والمؤسسات المالية كما سبق وأشرنا[2].

فضبط الجريمة الإلكترونية ليس بالأمر السهل ولكن في حالة ما تم إكتشاف وقوع هذه الجريمة والإبلاغ عنها فإن إثباتها أمر يحيط به كذلك الكثير من الصعاب، فهذه الجريمة تكون في بيئة غير

---

[1] بن لعربي أسماء، خصوصية الجريمة الإلكترونية، مذكرة نيل شهادة ماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة إبن خلدون، تيارت، 2021/2020، ص 21-22 .

[2] محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004، ص 53.

تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والأنترنت مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والمتابعة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن موجات ونبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليا من قبل الفاعل أمر في غاية السهولة [1].

أيضا تجدر الإشارة أن وسائل المعاينة وطرقها التقليدية لا تنجح غالبا في إثبات الجريمة الإلكترونية نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالجريمة التقليدية لها مسرح تجري عليه الأحداث، حيث تخلف أثار مادية تقوم عليها الأدلة وهذا المسرح يعطي المجال أمام سلطات الإستدلال والتحقيق الجنائي في الكشف عن الجريمة، وذلك عن طريق المعاينة والتحفظ عن الأثار المادية التي تخلفها الجريمة، لكن مسرح الجريمة الإلكترونية مسرح إفتراضي يتضاءل دوره في الإفصاح عن الحقائق المؤدية للأدلة المطلوبة ولذلك لسببين:

- أن الجريمة لا تخلف أثار مادية
- أن كثير من الأشخاص يترددون على مسرح الجريمة خلال فترة من زمن وقوع الجريمة وحتى ضبطها أو التحقيق فيها، وهي فترة طويلة نسبيا، الأمر الذي يعطي مجالا للجاني أو للأخرين أن يغيروا أو يتلفوا أو يعبثوا بالآثار المادية إن وجدت، الأمر الذي يورث الشك في الأدلة المستقاة من المعاينة في الجريمة الإلكترونية[2].

**ثالثا: الجريمة الإلكترونية جريمة ناعمة (هادئة)**

تختلف الجرائم الإلكترونية عن الجرائم التقليدية التي تتطلب أحيانا إستخدام العنف، كما هو الحال في جرائم القتل والضرب والجرح والسرقة وجرائم الإرهاب، إلا أن الجرائم المتصلة بالكمبيوتر تمتاز بأنها جرائم ناعمة لا تتطلب عنفا، بل تتطلب مواصفات خاصة كالذكاء و امتلاك الوسائل المناسبة وقدرة التعامل مع شبكة الأنترنت، فنقل بيانات من كمبيوتر إلى أخر أو المساس بأنظمة المعالجة الألية للمعطيات او الدخول الغير المشروع للحاسوب أو القرصنة أو السطو الإلكتروني

[1] نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010، ص 56.

[2] يرمش مراد، مرجع سابق، ص 40.

على الأرصدة وبيانات بطاقات الإئتمان، لا يتطلب أي عنف سواء مادي أو معنوي ولا يبذل فيه الجاني أي جهد عضلي، فهي جرائم هادئة بطبيعتها فلا يحتاج المجرم الإلكتروني إلى العنف، و إنما يحتاج إلى مهارة وفن ودقة في إستعمال تقنية المعلومات مثل إستخدام ما يعرف بالقنابل المنطقية والفيروسات المعلوماتية، كما أن معظم هؤلاء من الشباب المثقفين ذوي الإختصاصات العالية في مجال الحاسوب مما يخلق صعوبات إضافية لملاحقتهم[1].

خلاصة لما سبق إن الجريمة الإلكترونية جريمة ليست مثل باقي الجرائم كونها جريمة ذات بعد دولي فبإمكان مرتكبيها أن يباشر نشاطه الإجرامي من أي مكان دون الحاجة للتواجد في مسرح الجريمة، إضافة إلى تمتعها بخاصية صعوبة الكشف و الإثبات تميزها عن الجرائم التقليدية الأخرى، أي يستطيع مرتكبها الإفلات من المتابعة بكل بساطة دون أن يترتب على فعله الإجرامي أية مسائلة جزائية .

ففي كثير من الأحيان لا يكتشف ضحايا الجرائم الإلكترونية تعرضهم مثلا لإختراق حسابتهم وسرقة معلوماتهم الشخصية نتيجة جهلهم بتقنيات الحماية الأمنية للمعطيات، وفي المقابل أيضا في حالة لذلك يمتنعون في غالب الأحيان عن التبليغ خوفا من العواقب المترتبة عن ذلك، أيضا هذه الجريمة صعبة الإثبات نظرا لعدة عوامل منها ما يتعلق بطابع الجريمة نفسها ومنها ما يتعلق مثلا بنقص الخبرة الفنية للمحققين في هذا المجال، والجريمة الإلكترونية ليست مثل الجريمة التقليدية التي تتطلب في غالب الأحيان نوع من المجهود البدني لتحقيق النتيجة الجريمة بينما الجريمة الإلكترونية لا تتطلب هذا المجهود البدني لذلك تعرف بالجرائم الناعمة.

**الفرع الثاني: المميزات المرتبطة بالمجرم الإلكتروني**

يتميز المجرم الإلكتروني عن غيره من المجرمين التقليدين بصفات وسمات مختلفة جعلت منه محل العديد من الأبحاث والدراسات.

المتمثلة في المهارة المطلوبة للتنفيذ (أولا)، المعرفة (ثانيا)، الوسيلة (ثالثا)، التنظيم والتخطيط (رابعا)، الباعث وراء إرتكاب الجريمة (خامسا).

[1] يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة ، مصر، 2019، ص 57.

**أولا: المهارة والإحترافية المطلوبة لتنفيذ الجريمة الإلكترونية**

يتطلب تنفيذ النشاط الإجرامي في الجريمة الإلكترونية توفر المهارة لدى مرتكبها والتي تعد من أبرز خصائص المجرم الإلكتروني، و هذه الميزة قد يكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو عن طريق الخبرة المكتسبة في مجال تكنولوجيا المعلومات أو بمجرد التفاعل الاجتماعي مع الآخرين، ولا يعني بالضرورة أن يكون المجرم الإلكتروني على قدر كبير من العلم والمعرفة في هذا المجال، بل إن الواقع العملي والدراسات قد أثبتت أن بعض أنجح مجرمي المعلوماتية لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل في هذا المجال[1].

يتمتع المجرم الإلكتروني بإحترافية في تنفيذه لنشاطه الإجرامي، لأن إرتكابه لهذه الجرائم عن طريق الحاسوب يقتضي الكثير من التدقيق والتخصص والإحترافية في هذا المجال للتوصل إلى التغلب على برامج الحماية التي وضعها المتخصصون لحماية أنظمة الحاسوب، كما في حالة البنوك والمؤسسات الأمنية و العسكرية[2].

ففي أغلب الأحيان نجد أن المجرم الإلكتروني يتمتع بموهبة أو فطرة خاصة تميزه عن باقي المجرمين التقليدين، فيكون مولوعا بالتكنولوجيا وكل ما يخص الحاسب الألي وشبكة الأنترنت، فدائما ما يسعى إلى اكتساب و تطوير مهاراته في مجال التكنولوجيا والإتصال و استغلالها في البحث عن الثغرات الأمنية للمواقع الإلكترونية سواء الخاصة بالأفراد أو المؤسسات بمختلف أنواعها و قد يصل الأمر حتى إلى المؤسسات الأمنية.

**ثانيا: المعرفة بأنظمة المعالجة للمعطيات**

يتميز المجرم الإلكتروني أيضا بخاصية المعرفة التي تمكنه من تكوين تصور كامل لجريمته، إذ يستطيع أن يطبق جريمته على أنظمة مماثلة كتلك التي يستهدفها وذلك قبل تنفيذ جريمته، حتى لا يتفاجأ بأمور غير متوقعة من شأنها إفشال مخططاته أو الكشف عنها، فعادة ما يلجأ المجرم المعلوماتي إلى التمهيد لارتكاب جريمته بالتعرف على المحيط الذي تدور فيه، وكذا الظروف التي

[1] خالد داودي، الجريمة المعلوماتية، الطبعة الأولى، دار الإعصار العلمي للنشر والتوزيع، عمان–الأردن،2018، ص 33.

[2] يرمش مراد، مرجع سابق، ص 48.

تحيط بالجريمة المراد تنفيذها وامكانيات نجاحها واحتمالات فشلها، ويساعده في ذلك درجة المهارة التي يتمتع بها[1].

نظرا لميزة الذكاء التي يتمتع بها المجرم الإلكتروني بإمكان هذا الأخير إجراء محاكاة (Simulation) لمسرح الجريمة قبل إرتكابها وتقدير نسبة نجاح أو فشل الجريمة، وكذا التخمين في مختلف العوائق التي قد تواجهه عند مباشرته للنشاطه الإجرامي وسبل التغلب عليها، اي أن المجرم الإلكتروني يستطيع التحقق من الوصول إلى النتيجة الإجرامية قبل وقوعها وهي الميزة التي لا يتمتع بها المجرم في الجرائم التقليدية.

**ثالثا: الوسيلة المتطلبة لتنفيذ الجريمة الإلكترونية**

أما بخصوص الوسيلة فيقصد بها الإمكانية التي يتزود بها مرتكب الجريمة لإتمام جريمته فمجرمو تكنولوجيا المعلومات الحديثة يتميزون بالقدرة على الحصول على ما يحتاجون إليه أو ابتكار الأساليب التي تقلل من الوسائل اللازمة لإتمام النشاط الإجرامي، والحقيقة أنه كلما كان نظام المعالجة الألية المستهدفة غير مألوف كانت الوسيلة المتطلبة أكثر صعوبة في الحصول عليها لإقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام[2].

**رابعا: التنظيم والتخطيط المسبق**

تتميز الجريمة الإلكترونية عادة بوجود أكثر من فاعل للنشاط الإجرامي الواحد، إذ ترتكب أغلب الجرائم الإلكترونية من عدة أشخاص يحدد لكل شخص منهم دور معين، ويتم العمل بينهم وفقا لتخطيط وتنظيم سابق على ارتكاب الجريمة، فقد تحتاج جريمة نسخ برامج الحاسب الآلي مثلا إلى من يقوم بنسخ تلك البرامج والى من يقوم بعملية بيعها.

كما أنه من الملاحظ أن الأشخاص الذين يقومون بخلق أو تعديل البرامج لأغراض غير مشروعة ليسوا دائما المستفيدين بطريقة مباشرة من النشاط الإجرامي، فجرائم المعلوماتية تتطلب عادة

---

[1] دواد وسيلة، الجريمة الإلكترونية على ضوء قانون العقوبات الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد إبن باديس–مستغانم–2019، ص14.

[2] شاهين خضر، رضوان سعادة، الجريمة الإلكترونية و إجراءات مواجهتها، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد بوضياف المسيلة، 2021/2020، ص28.

شخصين على الأقل أحدهما متخصص في الحاسبات الآلية يقوم بالجانب الفني من المشروع الإجرامي وشخص آخر من المحيط ذاته أو من خارج المؤسسة المجني عليها لتغطية عملية التلاعب وتحويل المكاسب، وأحيانا أخرى يمكن تجنيد المجرم المعلوماتي القادر على إختراق نظم المعلومات ضمن عصابات الجريمة المنظمة عن طريق شبكة الإنترنت، ويمكن من خلال هذه الشبكة تبادل أفكار ومعلومات التطرف والإرهاب، كما يمكن الاتفاق معه على ارتكاب إحدى الجرائم الأخلاقية أو التلاعب في الحسابات أو بطاقات الائتمان[1].

**خامسا: الباعث وراء إرتكاب الجريمة**

لا يختلف الباعث من وراء إرتكاب الجريمة الإلكترونية في كثير من الأحيان عن الباعث لإرتكاب غيرها من الجرائم التقليدية الأخرى، فالرغبة في تحقيق الربح المادي بطريق غير مشروع يظل الباعث الأول وراء إرتكاب الجريمة الإلكترونية، ثم يليه بعد ذلك مجرد الرغبة في قهر نظام الحاسب وتخطي حواجز الحماية المضروبة حوله، وأخيرا الإنتقام من رب العمل أو أحد الزملاء، حيث يفرق مرتكبو الجرائم الإلكترونية بين نوعين من الأضرار، ضرر يصيب الأشخاص وهو الأمر الذي يعدونه غاية لا أخلاقية، وبين ضرر يلحق بمؤسسات أو جهات والتي في إستطاعتها اقتصاديا تحمل نتائج تلاعبهم، وهو ما يطلق عليه أعراض روبن هود The roben hood syndrome[2].

[1] دواد وسيلة، مرجع سابق، ص ص 14-15.

[2] خالد داودي، مرجع سابق، ص 34.

## المبحث الثاني: معايير تصنيف صور الجريمة الإلكترونية

تعتبر الجريمة الإلكترونية ظاهرة حديثة برزت في العالم ككل، فبالرغم من المجهودات المبذولة من رجال الفقه وكذا التشريعات الجنائية المقارنة في ضبط تعريف لها إلى أنه لحد الأن لا يزال هناك اختلافات في تعريف هذه الجريمة، ونفس الشيء نجده بالنسبة لصور هذه الجريمة حيث أنه ليس هناك تصنيف دولي للجريمة الإلكترونية لكن في المقابل هناك بعض الممارسات الدولية التي أخذت تصنيف معين وأصبح معتمدا في كثير من الاتفاقيات الدولية.

منها القائم على المعلوماتية كوسيلة لإرتكاب الجريمة (المطلب الأول)، ثم التصنيف الثاني القائم على المعلوماتية كمحلا للجريمة (المطلب الثاني).

### المطلب الأول: المعلوماتية كوسيلة لإرتكاب الجريمة الإلكترونية

أحيانا تكون المعلوماتية أداة لإرتكاب الجريمة، وذلك عن طريق إعتماد الجاني على وسائل تقنية حديثة في مباشرة سلوكه الإجرامي، وعليه من خلال هذا الطرح سنحاول على سبيل المثال لا على سبيل الحصر تقديم بعض الجرائم التي تكون المعلوماتية وسيلة لإرتكاب الجريمة منها

الجرائم الإلكترونية التي تستهدف الأشخاص (الفرع الأول)، الجرائم الإلكترونية التي تستهدف الأموال (الفرع الثاني)، وبعض الجرائم الإلكترونية التي تستهدف أمن الدولة (الفرع الثالث).

#### الفرع الأول: الجرائم الإلكترونية المستهدفة للأشخاص

تتمثل الجرائم الإلكترونية التي يكون فيها الأفراد هم المستهدفين في الجرائم الغير جنسية (أولا)، الجرائم الجنسية (ثانيا).

##### أولا: الجرائم الإلكترونية غير جنسية

أحيانا تكون شبكة الأنترنت وسيلة لإرتكاب سلوكيات إجرامية مخالفة للقوانين والأخلاق دون ان تكون مرتبطة بالجنس أو العنف الجنسي وهو ما يعرف بالجرائم الإلكترونية غير الجنسية، فهذا النوع من الجرائم يستهدف الأشخاص وتشمل التشهير بالأشخاص المعنويين أو الحقيقين من بث أخبار كاذبة وأفكار ومعلومات وفضائح ملفقة ليس لها من الصحة ، والتي من يترتب عنها الإضرار الأدبي والنفسي وأحيانا المادي والشخصي للجهة المقصودة، كما يمكن لمرتكب هذه الجرائم أن ينتهك

الحقوق الملكية و الفكرية لبرامج الحاسب والمصنفات الفنية بإستخدام الحواسيب الألية وشبكة الأنترنت، ومن أمثلة الجرائم التي تتم كذلك عبر الأنترنت على سبيل المثال لا الحصر نجد جريمة التخابر أو الإتصال من أفراد منظمة أو نشاط يهدد أمن و إستقرار الدول كالدعارة، المخدرات والتهريب، ...إلخ[1]،

كما يمكن أن تشمل الجرائم الإلكترونية الغير جنسية جريمة القتل عن طريق الكمبيوتر، فالقتل لم يبق محصورا بإستخدام وسائل مادية لتحقيق النتيجة بل أصبح يمكن تحقيقه عن بعد وذلك عن طريق التسبب في الوفاة بالتحريض على الإنتحار بإستخدام شبكة الأنترنت، ومن أبرز أمثلة عن ذلك لعبة الحوت الأزرق أو لعبة تحدي الحوت الأزرق والتي ظهرت في سنة 2016 على مواقع التواصل الإجتماعي، حيث تتكون هذه اللعبة من تحديات لمدة خمسين يوما وفي التحدي الأخير يطلب من اللاعب الإنتحار وإلا يعتبر خسر التحديات السابقة، ولقد تسبب هذا الأمر في إنتحار بعض الاطفال بعد أيام من الإدمان على هذه اللعبة[2].

**ثانيا: الجرائم الإلكترونية الجنسية**

الجرائم الإلكترونية الجنسية هي السلوكيات المنافية للأخلاق والمخالفة للقوانين وأعراف المجتمعات المحافظة والتي ترتكب بإستخدام الحاسب الألي مع توفر شبكة الأنترنت، وتتضمن هذه الجرائم ( حث وتحريض القاصرين على أنشطة جنسية غير مشروعة، إفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية، تلقي أو نشر المعلومات عن القاصرين عبر الحاسب الالي، التحرش الجنسي بالقاصرين عبر الحاسب الألي والوسائل التقنية الحديثة، نشر وتسهيل نشر و إستضافة المواد الفاحشة عبر الأنترنت بوجه عام وللقاصرين تحديدا، المساس بالحياء عبر الأنترنت... إلخ)، والقارئ لهذه الصفات وبإمعان النظر فيها يجد أنها شاملة لصورة واحدة ألا وهي ترويج الدعارة أو إثارة الفحش وإستغلال الأطفال والقصر في الأنشطة الجنسية الغير المشروعة عن

[1] الطيب بلواضح، الجريمة في الفضاء الإلكتروني، الطبعة الأولى، دار وائل للنشر والتوزيع، 2010، ص 59 .

[2] مرجع نفسه، ص 59.

طريق إستغلال الأنترنت والحاسب الألي[1]. ذلك أن فئة الأطفال هم المستهدفون بدرجة اولى في الجرائم الإلكترونية الجنسية وذلك لعدة إعتبارات منها الفقر والتهميش الإجتماعي الذي يجعل هذه الفئة عرضة للاستغلال من طرف مرتكبي هذه الجرائم.

**الفرع الثاني: الجرائم الإلكترونية المستهدفة للأموال**

أحيانا يكون باعث المجرم الإلكتروني من وراء إرتكابه الجريمة هو الربح المالي غير المشروع وتتمثل الجرائم الإلكترونية التي تستهدف الأموال في النصب والإحتيال الإلكتروني (أولا)، القمار وغسيل الأموال عبر الأنترنت(ثانيا)، جرائم السطو على أرقام بطاقات الإئتمان والتحويل الإلكتروني غير المشروع للأموال(ثالثا).

**أولا: النصب و الإحتيال الإلكتروني**

يلجأ بعض مرتكبي الجريمة الإلكترونية إلى إستخدام وسائل وطرق إحتيالية طمعا في تحقيق الربح المادي السريع، مستخدما في ذلك إسما وهوية مستعارة أو منتحلا صفة على غير الحقيقية بغرض الحصول على مال منقول أو منفعة، كالإختلاس وسرقة الأموال عن طريق الحصول على البيانات الشخصية مثل رقم الحساب والبطاقات المصرفية، ولقد ذهب رأي من الفقه إلى تعريف هذه الجريمة بأنها " إدعاءات كاذبة تدعمها مظاهر كاذبة أو أعمال خارجية، من شأنها حمل المجني عليه للتصديق وتسليم المال"[2].

وعرفها أيضا جانب من الفقه بأنها " كل سلوك إحتيالي أو خداعي يرتبط بعملية التحسيب الإلكتروني يهدف إلى كسب فائدة أو مصلحة مادية"[3].

فجريمة النصب والإحتيال الإلكتروني أصبحت تشكل تهديدا خطيرا على مستخدمي الشبكة العنكبوتية، حيث عالجت فرق مكافحة الجرائم المعلوماتية للأمن الوطني بالجزائر 152 قضية نصب

---

[1] غانم مرضى الشمري، الجرائم المعلوماتية(ماهيتها، خصائصها، كيفية التصدي لها قانونيا) الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2016، ص 57.

[2] أحمد أبو زيد شحاتة، "**الجريمة المعلوماتية أنواعها وسبل مواجهتها**"، مجلة العلوم القانونية والاقتصادية، العدد الثاني، جويلية 2023، ص 719.

[3] تيسير أحمد حسين الزغبي، جريمة الإحتيال الإلكتروني، مذكرة لنيل شهادة ماجيستير في القانون العام، كلية الدراسات القانونية، قسم القانون، جامعة جدارا، الأردن، 2010 ص93.

وإحتيال عبر الأنترنت خلال فترة 09 أشهر لسنة 2020 وهذا العدد في تزايد مستمر نظرا للتعامل في التجارة الإلكترونية[1].

**ثانيا: القمار وغسيل الأموال عبر الأنترنت**

أصبح من اليسير تبادل القيم النقدية عبر الأنترنت، واصبح قطاع البنوك كأي قطاع تجاري يتداول الأموال من خلال وسائل التكنولوجيا الحديثة مما جعل عصابات الجريمة وغاسلوا الأموال يستفيدون من مزايا هذه التكنولوجيا، وبالمقابل تغيرت أساليب ووسائل غسل الأموال وأصبحت تبتعد تدريجيا عن الأساليب التقليدية[2].

و تعرف جريمة غسيل الأموال التي تتم عبر الأنترنت بأنها "غسل الأموال الذي ينفذ عبر الشبكة العنكبوتية ، ويعرف بأنه النزع الصفة القذرة والغير المشروعة للأموال الناتجة عن جرائم متعلقة بالتجارة غير المشروعة كالمخدرات والإرهاب وإستخدامها عبر الانترنت كوسيلة لإظهارها وإخفاء مصدرها غير الشرعي، و غالبا ما تتم هذه العمليات من طرف عصابات الجريمة المنظمة، حيث تمتلك هذه الجماعات اموالا كبيرة ناتجة عن عملياتهم الإجرامية المحظورة مثل المخدرات وأنشطة الفساد، إذا تعمد إلى إدخال هذه الأموال القذرة إلى الحركة المالية عن طريق إستعمال شبكة الأنترنت[3].

وكثيرا ما ترتبط عملية غسيل الأموال مع ممارسة القمار على شبكة الأنترنت وهو الأمر الذي أدى إلى إنتشار أندية القمار الإفتراضية، فأصبحت مواقع الكازينوهات الإفتراضية على الأنترنت محل شبهة ومراقبة، ومن البديهي أن يستغل المجرمون تطور تقنيات التكنولوجيا لخدمة أنشطتهم

[1] نادية شريف، الجرائم المعلوماتية، مقال متوفر على الموقع الإلكتروني https://www.aps.dz ، تم الإطلاع عليه بتاريخ 04/23/ 2024 على الساعة 17.20.

[2] أعشب علي، الإطار القانوني لمكافحة غسل الأموال، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 2007، ص 35.

[3] بن نقي سفيان، "**جريمة غسل الأموال بين الوسائط الإلكترونية والنصوص التجريمية**"، مجلة الأبحاث القانونية والسياسية، المجلد 03، العدد02، جامعة طاهري محمد، الجزائر، 2021، ص157.

الإجرامية ويشمل ذلك بالطبع سبل غسيل الأموال التي إستفادت من عصر التقنية فلجأت إلى الأنترنت لتوسعة وتسريع أعمالها في غسيل أموالها غير المشروعة[1].

**ثالثا: جرائم السطو على أرقام بطاقات الإئتمان والتحويل الإلكتروني غير المشروع للأموال:**

لعل من أبرز التطبيقات الحديثة المبتكرة في مجال المعلوماتية هي تقنية الدفع الإلكتروني للأموال فهذه الأخيرة كسرت حاجز التعامل بالنقود وكذلك عوائق ومشاكل المبادلات المالية، فأصبحت تتم بسهولة وسيولة كبيرة مع ميزة كسب الوقت عند التعامل بهاته التقنية حيث لا تستغرق من الزمن سوى لحظات، ولكن الجانب السلبي في هذه المعاملات أنها وبرغم من تأمينات المؤسسة المالية وحرصها على تأمين هذه المعاملات إلا أنها تبقى الهدف الأول للمجرم الإلكتروني، نظرا لما تدره من أرباح دون اللجوء إلى الأساليب التقليدية للسرقة[2].

عملية التحويل الإلكتروني غير المشروع للأموال تكون من خلال لجوء المجرم الإلكتروني الحصول على كلمة السر المدرجة في ملفات انظمة الكمبيوتر الخاصة بالمجني عليه، مما يمكن و يسمح للجاني التوغل والولوج إلى النظام المعلوماتي والخدمات على الشبكة عن طريق تصريح كتابي او تلفوني، وتتم العملية بدخول العميل او الزبون إلى موقع التاجر ويختار السلع المراد شراؤها ويتم التعاقد بملأ النموذج الإلكتروني ببيانات بطاقة الإئتمان الخاصة بالمشتري[3]، فالمجرم الإلكتروني مثلما أشرنا سابقا يتميز بالذكاء والمعرفة ويرتكب سلوكه الإجرامي في هذه الحالة بإستعمال أسلوب الخداع حيث يقوم بإنشاء مواقع وهمية خاصة بقراصنة الأنترنت، تكون هذه المواقع مشابهة ومماثلة للمواقع الأصلية للشركات والمؤسسات التجارية والمالية المتعاملة بالتسويق الإلكتروني من المواقع

---

[1] صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجيستر في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية، جامعة مولود معمري-تيزي وزو-2013، ص ص46-47.

[2] بلعيد منصورية، النظام الإجرائي للجريمة المعلوماتية في التشريع الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2020، ص32.

[3] بشان نسرين، بلعباسي منال، خصوصية الجريمة الإلكترونية في القانون الجزائري، مذكرة مقدمة لإستكمال متطلبات شهادة الماستر في الحقوق، تخصص قانون الإعلام الألي والأنترنت، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد البشير الإبراهيمي، الجزائر،2019-2020، ص17.

site على شبكة الويب web أو من تطبيقات التجارة الإلكترونية المشهورة في العالم الإفتراضي مثل تطبيقين (Amazon. Ali expresse)، ويتم من خلال هذه المواقع الوهمية على شبكة العنكبوتية إستقبال جميع المعاملات التجارية والمالية، من بينها البيانات الشخصية والمعلومات الخاصة و السرية الخاصة لضحايا هذه الأسلوب مثل البيانات الخاصة ببطاقة الدفع (رقم البطاقة و كلمة السر) والرسائل الإلكترونية المتعلقة بالموقع الأصلي، حيث يظهر الموقع الوهمي بمظهره[1].

ومن بين القضايا التي عرفها العالم في هذه الجريمة هو رفع دعاوى قضائية من طرف الشركة المشهورة " مايكروسوفت " للبرمجيات ضد 118 موقعا على الأنترنت حاولت الإيقاع بالمستخدمين للشبكة الدولية وخداعهم بإستدراجهم لتقديم بيانات و معلومات شخصية تخص حساباتهم وبطاقاتهم الائتمانية مثل إسم المستخدم، رقم البطاقة وكلمة السر...إلخ[2].

**الفرع الثالث: الجرائم الإلكترونية المستهدفة لأمن الدولة**

لم تسلم الدول هي الأخرى من ظاهرة الجرائم الإلكترونية المستحدثة، فأصبح أمنها مهدد من هذا النوع من الجرائم، وتتمثل الجرائم الإلكترونية التي تستهدف أمن الدولة في جريمة الإرهاب الإلكتروني (أولا)، جريمة التجسس (ثانيا)، جريمة الإتجار بالبشر عبر الشبكة الإلكترونية(ثالثا).

**أولا: جريمة الإرهاب الإلكتروني**

يشهد عصرنا الحالي قفزة نوعية من ناحية التقدم و الإزدهار في المجال المعلوماتي ومع تطور الحكومات الإلكترونية كما هو الحال في عديد من الدول المتقدمة، فتبعا لذلك تحول نمط الحياة وتغيرت معه أشكال الأشياء وأنماطها، ومثلما لهذا التقدم العديد من الإيجابيات له كذلك العديد من السلبيات والتي من أبرزها تغير أشكال الجريمة والتي قد لا يتغير الاسم التقليدي لبعض الجرائم لكن يكون هناك تغيير جوهري أو بسيط في طرق إرتكابها، ومن هذه الجرائم الحديثة في طرقها القديمة في إسمها نجد جريمة الإرهاب والتي أخذت منحى حديث يتماشى مع التطور التقني، فظهرت جريمة حديثة تسمى بالإرهاب الإلكتروني فالسلوك الإجرامي الخاص بهذه الأخيرة يكون بإقتحام

[1] محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)،الطبعة الأولى، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 2002، ص169.

[2] أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008، ص 84.

المواقع وتدميره وتغير محتوياته والدخول على الشبكات والعبث بمحتوياتها بإزالتها أو بالإستيلاء عليها أو الدخول على شبكات الإتصال أو شبكات المعلومات بهدف تعطيلها عن العمل أطول فترة ممكنة أو تدميرها نهائيا أصبح هو أسلوب الإرهاب حاليا في محاولة الوصول إلى أغراضه[1].

وعليه فالإختلاف بين جريمة الإرهاب التقليدي و الإرهاب الإلكتروني كجريمة مستحدثة، يكمن في الطريقة التي يلجأ إليها الفاعل لإرتكاب السلوك الإجرامي، فالأولى ترتكب بوسائل تقليدية أما الأخيرة فترتكب بوسائل تقنية وعن بعد.

فيعرف الإرهاب الإلكتروني على أنه " العدوان أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد والذي يرتكب على الإنسان بسبب دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، بإستخدام الموارد المعلوماتية والوسائل الإلكترونية بشتى أصناف العدوان وصور الإفساد الذي يستهدف جهة الحكومة[2].

وقدمت أيضا موسوعة المعرفة تعريفا لجريمة الإرهاب الإلكتروني بأنها " إستخدام و إستعمال التقنيات الرقمية لإخافة ونشر الرعب و إخضاع الأخرين، أو هو القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو إقتصادية أو أمنية أو عرقية أو دينية"[3].

**ثانيا: جريمة التجسس**

يعتبر التجسس وسيلة من وسائل الحرب أي حرب معلومات التي هي فرع من فروع العمليات المعلوماتية تتمثل في القيام بأعمال التي لها التأثير على معلومات سواء من الدول أو الأفراد او لها غايات سياسية أو دينية أو شخصية، فالقصد من التجسس هو إستغلال والقيام بجميع الإجراءات التقنية لغرض الوصول والحصول على البيانات المخزنة فالحاسب أو التلاعب فيها أو إتلافها أو

[1] غانم مرضي الشمري، مرجع سابق، ص ص 87-88.

[2] بواب بن عامر، لخضر إدريس خوجة، "**المواجهة التشريعية للإرهاب الإلكتروني في الجزائر**"، مجلة البحوث القانونية والسياسية، جامعة مولاي الطاهر، سعيدة، الجزائر، العدد 09، ديسمبر 2017، ص284.

[3] سليماني مباركة، "**الإرهاب الإلكتروني وطرق مكافحته**"، مجلة الحقوق والعلوم السياسية، العدد 08، الجزء 01، جامعة عباس لغرور خنشلة، 2017 ص343.

تشويهها او حذفها أو الحصول على البيانات التي تستخدم أو تنقل عن طريق أحد الأجهزة وتتميز هذه الجريمة بأن المعلومات هي التي تكون محل التأثير والاعتداء عليها[1].

فجريمة التجسس تندرج ضمن فئة الجرائم الخطيرة التي تمس وتهدد الامن القومي للدولة كنتيجة لما قد يترتب عن هاته الجريمة من تعريض المصالح المختلفة للدولة لعدة مخاطر، والذي بدوره قد يؤدي إلى العدوان عليها من دول أخرى، فبالرغم من أن تلك الأنظمة عادة ما تكون محمية بأنظمة حماية قد تكون متطورة في نظر المؤسسات أو الدول التي تستخدمها، إلا أنها لا تقف حائلا من تلك الإختراقات[2].

في الأونة الأخيرة زادت عمليات الهجوم على أجهزة الحاسوب ، ووصل الأمر إلى الأجهزة ذات الطابع السري في المجال العسكري ومجال البورصة والبنوك، والتعرف على حسابات العملاء ووصل الأمر إلى إختراقها في بعض الأحيان، مما ينذر بإندلاع حرب قد يطلق عليها مجازا "الحرب الإلكترونية الباردة"[3].

مثلما إكتشفت بعض حالات التجسس الدولي وفي الأونة الاخيرة إكتشف عن مفتاح وكالة الأمن القومي الأمريكي NSA المعروفة ببراعتها في نظام التشغيل الشهير وندوز(Windows)، كما أظهرت أخيرا النقاب عن منظمة دولية ضخمة للتجسس الإلكتروني تعمل تحت إشراف وكالة الأمن القومي الأمريكية بالتعاون مع أجهزة الإستخبارات والتجسس في العديد من البلدان مثل كندا وبريطانيا وإستراليا ونيوزيلندا، لرصد والتجسس على المكالمات الهاتفية والرسائل بكافة أنواعها و إصطلح عليها إسم (ECHELON)[4].

[1] حسين طاهري، الجرائم الإلكترونية، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، الجزائر، 2022، ص24.

[2] فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2010/2009،ص18 .

[3] مرجع نفسه،ص18.

[4] أمير فرج يوسف، مرجع سابق، ص126.

**ثالثا: جريمة الإتجار بالبشر عبر الشبكة الإلكترونية**

لقد قدمت شرطة الانتربول الدولية تعريفا لجريمة الإتجار بالبشر التقليدية بأنها" إشراك الأشخاص أو نقلهم أو تنقيلهم أو إستقبالهم، بإستعمال التهديد والترهيب بالقوة أو حتى إستعمالها أو غير ذلك، من انواع القسر أو الإختطاف أو الإحتيال أو الخداع أو إساءة إستعمال السلطة أو إساءة إستغلال حالة إستضعاف لدى ضحايا هاته الجريمة، أو بإغراء وإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص أخر، لغرض الإستغلال مثل إستغلالهم في الدعارة أو سائر أشكال الإستغلال الجنسي أو السخرة أو الخدمة قسرا أو الإسترقاق أو الممارسات الشبيهة بالرق، أو بالإستبعاد أو نزع الأعضاء"[1].

أما بخصوص تعريف جريمة الإتجار بالبشر عبر الشبكة الإلكترونية فيمكن تعريفها "بأنها السلوك الإجرامي الذي يقوم من خلاله الجاني بإنشاء موقع إلكتروني عبر الشبكة المعلوماتية من أجل تجنيد أشخاص أو نقلهم أو تنقيلهم أو إيوائهم أو إستقبالهم، بواسطة إستعمال التهديد بالقوة أو بإستعمالها أو غير ذلك من أشكال القسر، أو الإختطاف أو الإحتيال أو الخداع أو إساءة إستعمال السلطة، أو إستغلال حالة استضعاف أو بإعطاء أو تلقي مبالغ مالية أو مزايا لنيل موافقة شخص له سيطرة على شخص أخر لغرض الاستغلال، ويشمل الإستغلال كحد أدنى إستغلال دعارة الغير أو سائر أشكال الإستغلال الجنسي أو لسخرة أو الخدمة قسرا او الإسترقاق أو الممارسات الشبيهة بالرق أو الإستبعاد، أو نزع الأعضاء[2] "

كما ورد أيضا تعريف لجريمة الإتجار بالبشر عبر شبكات الأنترنت على أنه " **التجارة بالبشر هي بكل بساطة إبرام صفقات تجارية عبر وسيلة إلكترونية يستعين بها المجرمون لغرض بيع سلعة المتمثلة في الإنسان**" فعندما نقول تجارة فهذه دلالة على ان الفضاء الإلكتروني هو سوق مفتوح على مصراعيه تعرض فيه منتجات بشرية تخضع لقواعد العرض والطلب فيه و الشيء المريح

[1] حنان ريحان مبارك المضحكي، الجرائم المعلوماتية –دراسة مقارنة– الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014، ص288.

[2] نبيلة كردي، "**الإتجار بالبشر عبر الأنترنت**"، مجلة الأبحاث، المجلد 7، العدد 2، جامعة العربي التبسي، الجزائر،2022، ص 525.

في العملية المتعاملين والذي هم المشتري والبائع الذين وفرت عليهما التكنولوجية المعلوماتية ربح الوقت و التخلص من عناء السفر والتنقل ودون ان يكون لقاء بين المتعاملين ويكون الدفع بواسطة بطاقات إئتمان فعوائق المكان والزمان تلاشت لصالح الإجرام المنظم إذ اصبح من الصعب إثبات الجريمة وجمع الادلة لان منتحل الشخصية قد يكون في دولة تأوي موقع غير دولة إقامته[1].

**المطلب الثاني: المعلوماتية محلا للجريمة الإلكترونية**

يكون الحاسب الألي في هذه الحالة هو محل الجريمة، حيث يكون السلوك الإجرامي المرتكب من طرف المجرم الإلكتروني منصب على النظام المعلوماتي ، فهناك جرائم إلكترونية واقعة على نظام المعالجة الالية للمعطيات(الفرع الأول)، و جرائم إلكترونية واقعة على المعلومات داخل أنظمة المعالجة الألية (الفرع الثاني).

**الفرع الأول: الجرائم الإلكترونية الواقعة على نظام المعالجة الالية للمعطيات**

تعتبر جريمة الدخول او البقاء غير المشروع للنظام المعلوماتي من أهم جرائم الواقعة على نظام المعالجة الألية للمعطيات على العموم، ذلك أن أغلب هذه الجرائم لا يمكن إرتكابها إلا بعد الدخول للنظام، ولهذا كانت جريمة الدخول هي الباب والحد الفاصل بين الجاني وبين إرتكابه لمختلف جرائم المعطيات الأخرى، لذلك أولت التشريعات إهتماما كبيرا بهذه الجريمة، وهناك من التشريعات ما يجعلها الجريمة الأساسية وما باقي الجرائم إلا نتائج لها[2].

الأمر الذي يستدعي التركيز على جريمة الدخول غير المشروع للنظام المعلوماتي (أولا)، ثم على جريمة البقاء غير مصرح به في النظام المعلوماتي (ثانيا).

**أولا: الدخول غير المشروع للنظام المعلوماتي**

يمكن تعريف جريمة الدخول غير المشروع للنظام المعلوماتي بأنها الدخول إلى محتويات جهاز الكمبيوتر ذاته، أي إجراء إتصال بالنظام محل الحماية بالطرق الفنية اللازمة لذلك، وليس معناه الدخول إلى القاعة الموجود بها جهاز الكمبيوتر وقد أشار المؤتمر 15 للجمعية الدولية لقانون العقوبات المنعقد في

[1] زمال وصال، جريمة الإتجار بالبشر عبر الأنترنت، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي التبسي، الجزائر، 2022/2021، ص32-33.

[2] علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الألي، الطبعة الأولى، الدار الجامعية، بيروت،1999، ص 118.

البرازيل سنة 1994 بشأن جرائم الكمبيوتر إلى هذا المعنى، حيث إعتبر أن الدخول غير المشروع هو التوصل أو الولوج دون تصريح إلى نظام أو مجموعة نظم عن طريق إنتهاك إجراءات الأمن، كما لم يحدد كل منهما وسيلة أو طريقة الدخول، لذا فإن الجريمة تقع بأي وسيلة فقد يلجأ الجاني إلى إدخال برنامج فيروس أو يدخل عن طريق إستخدام الرمز السري لشخص أخر أو عن طريق تجاوز نظام الحماية إذا كان ضعيفا، ويستوي أن يتم الدخول مباشرة أو بطريق غير مباشر كما هو الحال في الدخول عن طريق شبكات الإتصال الهاتفية، وأيضا لا عبرة في هذه الجريمة بصفة مرتكب الفعل الإجرامي، فقد يكون الفاعل يعمل في مجال الأنظمة أو لا يعمل، سواء كان يفهم أو لا يفهم في أسلوب تشغيل النظام، فيكفي أن يكون الجاني ليس ممن لهم الحق في الدخول إلى النظام حتى تتوفر جريمة الدخول غير المشروع[1].

وتتم عملية الدخول غير المشروع في النظام المعلوماتي بعدة طرق أهمها:

- إستخدام برامج مبرمجة خصيصا لإختراق انظمة الحماية الفنية في الحالات الطارئة، لأن إدارة وتشغيل هذه البرامج تفرض وجود نوع معين من البرامج يمكن إستخدامها لتتجاوز جدار الحماية في الحالات الطارئة، أو في حالة اختلال وظائف الحاسب الألي أو تعطيله عن العمل و أشهر هذه البرامج ما يسمى بـ (Superzab)، والجدير بالإشارة ان هذا النوع من الأنظمة في حالة ما وقع في أيدي غير مصرح لها بإستعمالها فإن هذا يسمح لها بالتغلغل في منظومة الحاسب الألي ولو كان محمي،
- أبواب المصيدة (trap–doors) ويقصد بها الفواصل التي يتعمد واضعو البرامج تركها أثناء إعدادها لتستخدم في إضافة ما يحلو لهم لاحقا.
- إستعمال ما يرمي في بصناديق القمامة دون حذفه نهائيا
- طريقة المختصرات (raccourci) تتم باستغلال نقاط ضعف بالنظام للدخول إليه
- القناع وذلك أن يقوم الفاعل بإقناع الحاسوب بأنه شخص مرخص له بالدخول
- إستخدام برامج خبيثة يتم دمجها في إحدى البرامج الأصلية للحاسب الألي بحيث يعمل في جزء منه ليقوم بتسجيل الشفرات

[1] شنين صالح ، الحماية الجزائية لبرامج الحاسب الألي، مذكرة مكملة لنيل شهادة الماجيستير في الحقوق، تخصص قانون جزائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2007/2006، ص 86.

- إستخدام ألة طابعة مرفقة بجهاز الحاسب الألي لاستخراج قائمة البرامج الموجودة داخل النظام[1].

**ثانيا: جريمة البقاء غير المصرح به في النظام المعلوماتي**

بخصوص جريمة البقاء غير المصرح به في النظام المعلوماتي هو التواجد في النظام ضد إرادة من له الحق في السماح بالبقاء، وقد يقترن البقاء بالدخول غير الشرعي منذ البداية كما يتحقق مع دخول شرعي غير مصرح به إذا إستمر البقاء لغير المدة المحددة وهذا ما يعرف بتجاوز التصريح فتجريم كل منهما غير مرتبط بالأخر ومثال ذلك أن يحصل الجاني خدمة تلفونية لمدة أطول من المدة التي دفع مقابلها عن طريق إستخدام وسائل وتقنيات غير مشروع، وكذلك يتضح الهدف من تجريم البقاء بالنسبة للجاني الذي لم يقصد الدخول عن طريق الغش للنظام ومع ذلك يبقى داخل النظام وتنصرف إرادته إلى ذلك والذي يمكن أن يغادر[2].

**الفرع الثاني: الجرائم الواقعة على المعلومات داخل أنظمة المعالجة الألية للمعطيات**

هي الجرائم التي تحدث داخل أنظمة المعالجة الألية للمعطيات يمكن أن تشمل مجموعة واسعة من الأنشطة الغير قانونية التي تستهدف البيانات والأنظمة الرقمية ومن هذه الجرائم جريمة سرقة المال المعلوماتي (أولا)، جريمة إتلاف معلومات وبرامج الحاسب الألي (ثانيا)، و جريمة التزوير المعلوماتي (ثالثا).

**أولا: سرقة المال المعلوماتي**

ظهرت جريمة السرقة المعلوماتية المتمثلة في سرقة المعلومات من برامج وبيانات مخزنة من دائرة الكمبيوتر أو نسخ برامج المعلومات بصورة غير شرعية، بعد تمكن مرتكب هذه الجريمة من الحصول على كلمة السر أو بواسطة إلتقاط موجات كهرومغناطيسية الصادرة عن الحاسب الألي أثناء تشغيله أو بإستخدام نهايات طرفية تتصل بالحاسب الألي، وبالرجوع إلى تحليل جريمة السرقة التقليدية نجد أن المال فيها منقولا، فتنقل حيازته من المالك إلى السارق، ومعظم التشريعات لا تعترف بسرقة المعلومات بل الوصول غير المصرح لها و إختراقها وتقليدها والاستلاء عليها ونسخها نسخا

[1] دليلة مزرقن، جريمة المساس بأنظمة المعالجة الألية للمعطيات، مذكرة نيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة،2016/2015، ص ص 37-38.

[2] جدي نسيمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماجيستر في القانون الجنائي، تخصص قانون جنائي، كلية الحقوق، جامعة وهران،2014/2013، ص 53.

غير مشروعا يعد جريمة، هذا ما نراه بوجوب عدم قياس نصوص السرقة التقليدية على السرقة المعلوماتية مما يدعو إلى إقتراح أن يتدخل المشرع بنص صريح لمواجهة هذه الظاهرة الإجرامية المعاصرة[1].

تمتاز جريمة السرقة المعلوماتية بمجموعة من الخصائص أهمها:

- يكون مرتكبي السرقة المعلوماتية يكونون بالعادة من ذوي الإختصاص في مجال تقنية المعلومات، أو يكون الجاني لديه قدر من المعرفة في التعامل مع الوسائل الإلكترونية
- ترتكب هذه الجريمة بعد تدبير وتخطيط مسبق ولا تأتي بشكل عفوي، حيث تتصف بالتنظيم
- صعوبة إكتشاف جرائم السرقة التي تحدث بإستخدام الوسائل الإلكترونية، ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مع مثل هذا النوع من الجرائم
- تتميز السرقة بالوسائل الإلكترونية أنه قد يتعاون أكثر من شخص على إرتكابها
- عادة ما تتطلب هذه الجريمة وجود حاسب ألي متصل بالشبكة المعلوماتية ومزود ببعض البرامج السابقة
- يكون عادة الهدف من إرتكابها الحصول على الربح السريع[2].

**ثانيا: جريمة إتلاف معلومات وبرامج الحاسب الألي**

يعرف الإتلاف بأنه "**جعل الشي غير صالح للإستعمال أو بإعدام صلاحيته أو تعطيله (وقف عمله) سواء بصفة كلية او جزئية**"، ويقصد كذلك بالإتلاف "**إفناء مادة الشيء تماما على أن يؤدي منفعته ولو لم تفن مادته سواء كان هذا التوقف كليا او جزئيا ويكون الشيء غير صالح للإستعمال بجعله لا يقوم بوظيفته المرصود لها على النحو الأكمل**"، كما يقصد أيضا بإتلاف معلومات وبرامج الحاسب الألي" **إتلاف أو محو تعليمات البرامج والبيانات ذاتها يطلق عليها مصطلح تدمير نظم المعلومات وعادة لا يستهدف مرتكب هذا الإعتداء فائدة مالية لنفسه بل لمجرد**

[1] داود إدريس، شيبان إلياس، جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون إعلام ألي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2023/2022 ص 26.

[2] محمد عبد المحسن بن طريف، "**جريمة السرقة المعلوماتية**"، مجلة الدراسات والبحوث القانونية، المجلد 07، العدد 02، جامعة عمان العربية، الأردن، 2022، ص 19.

**إعاقة نظام المعلومات**"، ويمكن القول أن الإتلاف لا يتحقق فقط في التأثير على مادة الشي بل يتحقق كذلك حتى في حالة الإنتقاص من قيمة الشيء الإقتصادية مما يعني أن الحكمة من الإتلاف هي ليس التعرض لمادة الشي وإنما العبرة بقيمته المالية ذلك أن الفعل الذي يترتب عنه فقدان الشي لقيمته المالية أو الانتقاص منها هو الذي يحقق الإعتداء الذي يعاقب عليه القانون على إعتبار أنه قد ذهب بأهمية الشي بالنسبة لمالكه[1].

وترتكب جرائم إتلاف معلومات وبرامج الحاسب عن طريق قنابل منطقية، أو عن طريق برنامج الدودة والفيروس الذي يقصد به "برنامج تم إعداده من قبل شخص أو أكثر على درجة متقدمة من العلم بالبرمجة بإستخدام تقنيات متطورة، بحيث يكون من خصائص هذا البرامج الإنتقال إلى أجهزة الحاسب الألي والتكاثر والإنتشار فيها وهي برامج غير مرئية بالطرق العادية وتحتاج إلى أسلوب علمي للكشف عنها[2].

**ثالثا: جريمة التزوير المعلوماتي**

إن موضوع التزوير هو المحرر، الذي لا بد من توافر شروط فيه، تتمثل في الكتابة من قبل شخص وأن ينتج أثاره القانونية هذه من الناحية التقليدية لجريمة التزوير، لكن في مجال المعلوماتية فالأمر يختلف فجريمة التزوير المعلوماتي تقع على المستندات المعلوماتية .كما أن الغاية من تجريم أفعال التزوير هو حماية الثقة العامة، التي تنشأ من تعامل الأفراد بالمحررات بمفهومها التقليدي، ووضع نص خاص بالتزوير المعلوماتي يحقق الحماية للنظام المعلوماتي فقط دون الحفاظ على الثقة العامة، وبذلك فإن المحررات المعلوماتية تخرج من المفهوم التقليدي للمحرر مما ينقص من ثقة المتعاملين بها، لذلك فإن إلغاء النص يخضع المحررات المعلوماتية إلى النصوص التقليدية الخاصة بالتزوير بالمفهوم الجديد للمحررات، كذلك فالنشاط الإجرامي المكون لجريمة التزوير المعلوماتي

---

[1] أحمد بن مسعود، "**جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري**"، مجلة الحقوق والعلوم الإنسانية، المجلد 10، العدد 01، جامعة الجلفة، 2017، ص ص 486-487 .

[2] الدزيري هيبة، جريمة الدخول الغير مشروع لنظام المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس ، مستغانم، الجزائر، 2020/2019، ص 34.

يتمثل في فعل تغيير الحقيقة ويعني استبدالها بما يخالفها واذا انتفى هذا التغيير انتفى التزوير، وإن تزوير البرنامج أو قواعد البيانات لا يعد تزويرا بل يقع تحت طائلة نصوص قانون حقوق المؤلف والحقوق المجاورة[1].

[1] عباسة محمد ياسين، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسة، قسم القانون العام، جامعة عبد الحميد بن باديس مستغانم،2021/2020، ص 47.

## الفصل الثاني: معوقات تحديد القانون الواجب التطبيق على الجريمة الإلكترونية مع الحلول المقترحة لها

تواجه مختلف التشريعات الجنائية المقارنة في كثير من الأحيان صعوبة كبيرة في مواكبة تطورات الجريمة الإلكترونية و التي بالتبعية تتأثر هذه الأخيرة بالتطورات الي يشهدها مجال تكنولوجيا المعلومات، فحتى الأساليب المستعملة في إرتكاب هذه الجريمة شهدت هي الأخرى تطورا ملحوظا، ونظرا للطبيعة الخاصة التي تتميز بها الجريمة الإلكترونية بإعتبارها جريمة عابرة للحدود وتقع في مكان لامادي، فصار بإمكان الجاني إرتكاب سلوكه الإجرامي بكبسة زر فقط و دون عناء التنقل إلى المكان المراد تحقيق نتيجته الجرمية فيه، وكذلك في غالب الأحيان يتوزع الركن المادي لهذه الجريمة وتصيب عدة دول مختلفة في أن واحد.

هذه الميزة التي تتمتع بها الجريمة الإلكترونية سهلت من جهة على المجرمين لإرتكاب الجرائم والإفلات من اكتشافهم، ومن جهة أخرى صعبت من مأمورية المحققين و القضاء في تحديد مكان وقوع هذه الجريمة و بالتبعية تحديد القانون الواجب التطبيق عليها، ذلك أن ملاحقة الجناة وكشف جرائمهم عبر الحدود يقتضي من الناحية العملية أن يتم في نطاق إقليم دولة أخرى، وهو ما يصطدم بمبدأ السيادة الإقليمية للدول عملا بمبدأ إقليمية النص الجنائي( المبحث الأول) ، لذلك كان لا بد من البحث عن الحلول المناسبة لتجاوز هذه العقبات وتكون هذه الحلول تتوافق مع طبيعة الجريمة الإلكترونية(المبحث الثاني).

## المبحث الأول: عقبات تحديد القانون الواجب التطبيق على الجريمة الإلكترونية

الجريمة الإلكترونية جريمة مستحدثة ظهرت نتيجة للتطورات التي يشهدها المجال التكنولوجي، وكنتيجة لذلك أثارت مكافحة هذه الجريمة الكثير من العقبات نظرا لطبيعتها الخاصة التي تميزها عن باقي الجرائم التقليدية، فالرغم من الدراسات التي أنجزت في سبيل الوصول إلى تعريف شامل و موحد لم يستطع فقهاء القانون الجنائي الوصول إلى إتفاق موحد في هذا الصدد(المطلب الأول)، وكذا بإعتبارها جريمة لا تحدها حدودا جغرافية مثلما أشرنا سابقا، ففي كثير من الأحيان تثار الإشكالية المتعلقة بتحديد مكان إرتكابها(المطلب الثاني).

### المطلب الأول: العقبات التشريعية

تثير الجريمة الإلكترونية الكثير من العقبات التشريعية، من بين هذه العقبات صعوبة ضبط مدلولها (الفرع الأول)،إضافة إلى ذلك عدم قدرة النصوص التقليدية على معالجة هذه الظاهرة ، فبالرغم من اختلافها في الطبيعة والطريقة والوسيلة التي ترتكب بها عن الجرائم التقليدية، إلا أنها في كثير من الأحيان تتداخل مع الجرائم التقليدية(الفرع الثاني).

#### الفرع الأول: صعوبة ضبط مدلول الجريمة الإلكترونية

إن من بين الصعوبات التي تثيرها الجريمة الإلكترونية ضبط مدلول واضح وشامل لها هذه الصعوبة تساهم في إشكالية تحديد القانون الواجب التطبيق، حيث أنه لا يوجد إجماع على تعريف هذه الجريمة من حيث كيف تعرف أو ما هي الافعال التي تندرج ضمن الجريمة الإلكترونية، فمثلما يقول العالم فان دير هلست وونيف " هناك غياب لتعريف عام و إطار نظري متسق في هذا الحقل من الجريمة... وفي أغلب الأحيان تستخدم مصطلحات إفتراضية والحاسوب و الإلكترونية والرقمية وكلها تعكس فجوات مهمة في التعريف"[1].

[1] خلوفي رشيد، بولحية شهرزاد، "**تحديات الجريمة الإلكترونية في الجزائر**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، جامعة الجزائر، 2019، ص ص 1974-2003، ص1978.

في هذا الصدد بذلت العديد من الجهود في سبيل الوصول إلى تعريف محدد شامل للجريمة الإلكترونية، أين أصر البعض من الفقهاء إلى ترجيح عدم وضع تعريف لهذه الجريمة وحجتهم في ذلك أن هذا النوع هي جرائم تقليدية وليست جريمة واحدة ترتكب بإستعمال وسائل إلكترونية، و مما لا شك فيه أن عدم الإتفاق حول ضبط مدلول الجريمة الإلكترونية، هو خشية من حصر نطاقها داخل إطار تجريمي محدد قد يضر بها خاصة في ظل التطور المستمر للتقنية المعلوماتية والذي نلمسه كل يوم، فما يتم تجريمه قد يصبح غير ذي أهمية بالنسبة للصور مستحدثة أخرى قد ظهرت نتيجة إستخدام تقنيات حديثة[1].

فلذلك تعددت المصطلحات الدالة على هذه الظاهرة، حيث أن هناك من يصطلح على الجريمة الإلكترونية بمصطلح الجريمة المعلوماتية والمغزى منها هو التعبير عن الجريمة التي يكون فيها موضوع الحق المعتدى عليه هو المعلومة، كما أن هناك من يستخدم مصطلح جرائم الانترنت فهو استخدام ضيق لأنه سيقصر هذه الجرائم على سلوكيات غير مشروعة ترتكب عن طريق الولوج إلى شبكة الانترنت دون الجرائم التي يمكن أن نتصور إمكانية ارتكابها عن طريق جهاز الكمبيوتر دون الحاجة إلى استخدام الانترنت، أما من يستخدم مصطلح الجريمة الإلكترونية فيقصد بها الجرائم المرتكبة عن طريق الكمبيوتر وغيره من وسائل الاتصال الحديثة[2]

فوصفت الجريمة الإلكترونية بأنها جريمة تقاوم التعريف، لإختلاف التعريفات المقدمة في سبيل ضبط مدلول لها، حيث تعددت الآراء والأفكار بشأن هذا التعريف، فهناك من إعتمد في تعريفه على

[1] نواصرية ليلي، سليم نصيرة، التفتيش في الجرائم المعلوماتية، مذكرة لنيل شهادة ماستر، تخصص قانون إعلام ألي و أنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج ، 2023/2022، ص6 .

[2] شفيقة خنيفر، **الإجرام الإلكتروني**، كفاءات ضائعة في عالم التقنية، مداخلة منشورة في المسطرة الإجرائية للمؤتمر العلمي الافتراضي الأول: الجريمة الإلكترونية (الواقع والتداعيات)، كلية العلوم الإنسانية والاجتماعية ،جامعة محمد الشريف مساعدية –سوق أهراس، 2022، منشور على الموقع الإلكتروني https://www.univ-soukahras.dz، من دون ترقيم.

الجانب الفني، بينما إعتمد البعض على الجانب القانوني، في حين إعتمد البعض الأخر على معايير أخرى مختلفة[1].

مما سبق نقول أن فقهاء القانون لم يتفقوا على تعريف واحد يكون هذا التعريف شامل و ملم بجميع صور الجريمة الإلكترونية، وكنتيجة لهذا الإختلاف تعددت التعاريف المقدمة للجريمة الإلكترونية، فكل يعرفها وفقا للمعيار الذي إعتمد عليه، فهذا الاختلاف أثر أيضا بجزء على ضبط مدلول هذه الجريمة.

لذا فمدلول هذه الجريمة لا يزال غير مكتمل وغير متجانس، ففي حالة ما إذا تم تعريف الجريمة الإلكترونية وفقا لأحد المنهاج سواء مناهج العلوم السياسية أو القانونية أو علم الإجتماع أو علم الإجرام فإن التعاريف المقدمة لوصف هذه الجريمة ستكون مختلفة، فهذا التنوع الموجود في تعريف هذه الجريمة يصعب في فهمها، فغالبا ما يطرح التساؤل حول ما إذا تم إستخدام او عدم إستخدام التعاريف القانونية لهذه الجريمة، حيث أن ما يعتبر إنحرافا أو إجراما بالنسبة لدولة ما يمكن أن يكون مباحا في دولة أخرى والعكس صحيح، لذلك يختار بعض علماء الجريمة عدم إستخدام التعاريف القانونية التي تكون "مصطنعة" إلى حد ما، في حين أن بعض الأخرين يتبنون تحليلاتهم على التعريف القانوني للعمل الإجرامي المتمثل في الجريمة الإلكترونية[2].

مثلما اشار العالم "ديفيد وول" فإن مفهوم الجريمة الإلكترونية لا يرتبط على وجه التحديد بمصطلح قانوني لأنه لن يتمكن علماء الجريمة من الإعتماد على التعريف القانوني لدراسة الجريمة الإلكترونية فحسب بل سيواجهون تحديا إضافيا هو فحص ظاهرة تحدث في مكان جديد تماما وغير معروف لهم حتى الأن، وبالتالي فإن النقاش المفاهيمي المهم في أبحاث علم الجريمة هو ما إذا كان

[1] حوالف حليمة، مهاجي فاطمة الزهراء، "**معالم الجريمة المعلوماتية في القانون الجزائري**"، مجلة البحوث القانونية والسياسية، مجلد 03، العدد 16، 2021، ص ص 140-155، ص142.

[2] Prévention de la criminalité et sécurité quotidienne:prévenir la cybercriminalité, 6 eme rapport international, center international pour prévention de la criminalité, page 90.

مفهوم الجريمة الإلكترونية يشكل شكلا جديدا من أشكال الجريمة أو ما إذا كان يشير إلى نوع موجود بالفعل من الجريمة يتحذ شكلا جديدا عند ممارسته في بيئة جديدة.

وأيضا بالنسبة لهذا العالم فإن بعض أشكال الجريمة الإلكترونية المرتكبة في العالم الإفتراضي تجد نظيرتها في العالم الحقيقي وخير مثال جريمة الإحتيال، فالجريمة بصفة عامة سواء إرتكبت في بيئة افتراضية أو بيئة حقيقية تظل مع ذلك كما هي ولذلك فإن الجريمة ليست هي التي تتغير بل البيئة التي تحدث فيها الجريمة هيا التي تتغير.

فتعريف الجريمة الإلكترونية أمر صعب للغاية والنقاش لا يزال مفتوحا بخصوصه، حيث يتفق الباحثون على أن الفضاء الإلكتروني وتقنيات الكمبيوتر تستخدم لتسهيل الأعمال الإجرامية والانحراف، ومن ناحية أخرى فإنهم يختلفون على أنواع الجرائم التي ينبغي أن يشملها التعريف، وصعوبة فهم مفهوم الجريمة الإلكترونية يتفاقم بسبب ارتباطها بمجموعة كاملة من الأنشطة غير المشروعة وليس فقط بحقيقة محضة وبسيطة[1].

فمن خلالنا بحثنا على تعريف هذه الجريمة صادفنا الكثير من التعاريف المقدمة في هذا الإطار، وكل من تطرق إلى تعريفها يعرفها انطلاقا من وجهة نظر معينة، وهذا الشيء لا يسعف التشريعات للبدء في تجريم هذه الجريمة، لذلك تتجنب معظم التشريعات النص على تعريف لهذه الجرائم مكتفية بالنص على السلوك الذي يندرج ضمنها بالتحديد والنص على تجريمه وتحديد الجزاء المناسب للفعل، وإذا كانت هناك مساع أو توجهات للوقوف على تعريف محدد يجب تجنب التعاريف ذات المفهوم الضيق قدر الإمكان، والأخذ بالتعاريف الواسعة المتوازنة التي تحقق الغرض منها بتجريم الفعل ولا تمثل إنتهاكا للحقوق والحريات[2].

[1] Ibid,p 91.

[2] حنان ريحان مبارك المضحكي، مرجع سابق، ص 358.

**الفرع الثاني: عدم ملاءمة النصوص الجزائية التقليدية مع خصوصية الجريمة الإلكترونية**

سبق و أوضحنا أن المعلوماتية قد تكون كوسيلة لإرتكاب الجريمة أو محل لهذه الجريمة، وفي كلتا الحالتين قد يشكل هذا الإعتداء جريمة الأمر الذي يقتضي تدخل القانون الجنائي لمواجهتها، ولكن التساؤل الذي يطرح في هذه الحالة هل تكفي نصوص قانون العقوبات لمواجهة هذه الجرائم أو أية قوانين خاصة معمول بها للوقوف أمام مرتكبي الجرائم الإلكترونية؟، فمن حيث المبدأ فلا يمكن الجزم بإمكانية القانون الجنائي بوضعه الراهن على مواجهة هذه الجرائم المستحدثة، وذلك لأن النصوص التقليدية وضعت لتطبق وفق معايير معينة (منقول مادي) في حين أن بعض القيم في مجال المعلومات لها طبيعية غير مادية مثل المعلومات، يضاف إلى ذلك مما تتميز به من الأساليب الفنية التي تستخدم في إرتكاب هذا النوع الجديد من الجرائم من ذاتية خاصة[1].

تجدر الإشارة أيضا أن التطور التكنولوجي كان أسرع من أن يسايره أي مشرع، حيث لم تظهر القوانين الخاصة بالمعلوماتية إلا بعد فترة طويلة نسبيا، أين تمت مواجهة الجريمة الإلكترونية بالإعتماد على النصوص الجزائية التقليدية قبل أن تصدر النصوص الملائمة لها، ولكن الاستمرار في تطبيق النصوص التقليدية اثار العديد من المشاكل لم تكن تتلاءم مع الاشكال الجديدة للإجرام المعلوماتي، وفي هذا الإطار قررت المحاكم الامريكية أن الدخول غير المشروع للحاسوب لا يمكن إعتباره إنتهاك حرمة عقار، لأن هذه الجريمة تفترض أن يتجاوز عضو من أعضاء الإنسان عتبة الملكية المنتهكة، وهو امر يختلف تماما عن فعل الدخول غير المشروع الذي يحدث في وسط إفتراضي، كما ان جريمة السرقة تفترض حرمان الضحية من إستعمال ملكيتها وهو أمر لا يحدث عند سرقة المعطيات الإلكترونية من داخل الأنظمة المعلوماتية[2].

[1] محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت(دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2009، ص57.

[2] مختار الأخضري، "الإطار القانوني لمواجهة جرائم المعلوماتية"، نشرة القضاة تصدرها المديرية العامة للشؤون القضائية والقانونية، مديرية الدراسات القانونية والمواثيق، العدد 66، سنة 2011/2010، صادرة عن وزارة العدل، الجزائر، ص 57-58.

ولقد ثار تساؤل في فرنسا عن مدى إنطباق بعض نصوص التجريم الخاصة ببعض الجرائم التقليدية كالسرقة أو خيانة الأمانة على الإعتداء على مثل هذه الصور من المعلومات، فمن بين أمثلة ذلك صدور حكم من المحاكم الفرنسية بإعتبار قيام موظف بإحدى الشركات بتصوير التصميمات الخاصة بألة لتصنيعها وتسويقها بمشروع اخر بالإستعانة بهذه التصميمات سرقة وذلك دون أن يبحث فيما إذا كانت هذه التصميمات محمية ببراءة الإختراع أو لا، وفي نفس السياق أدانت محكمة النقض الفرنسية بتهمة خيانة الأمانة موظفا سابقا في مكتب متخصص في الخبرة المحاسبية لأنهم إكتشفوا بحوزته بعض المستندات التي كان قد حصل عليها من ملفات العملاء الخاصة بمكتب الخبرة الذي كان يعمل فيه، وذلك لأن هذه المستندات كانت مسلمة إليه بسبب وظيفته من أجل عمل محدد[1].

وبناءا على قضايا كثيرة طرحت أمام القضاء في كثير من الدول، تبلورت فكرة وضع نصوص قانونية خاصة، غير أن ما يلاحظ أن هناك إختلاف بين الدول في أسلوب المعالجة التشريعية لهذه المشكلة، فهناك من قام بتعديل قانون العقوبات بشكل يسمح بتعميم القواعد التقليدية على الجرائم التي ترتكب بواسطة الحاسوب وهو الأسلوب المتبع في غالبية الدول، في حين نجد دولا أخرى إستحدثت قواعد خاصة بالجرائم المعلوماتية، أما في الجزائر فتم استحداث فصل جديد تحت عنوان " المساس بأنظمة المعالجة الألية للمعطيات " والنص على أهم الجرائم التي تستهدف الأنظمة المعلوماتية (م 394 مكرر) وكذلك إصدار قانون خاص يتضمن قواعد خاصة للوقاية من الجرائم الإفتراضية علما ان القواعد الوقائية هي التي دعت إلى وضع قانون خاص.

وفي محاولة الإجابة على التساؤل المطروح في هذا الصدد (هل تكفي نصوص قانون العقوبات لمواجهة هذه الجرائم أو أية قوانين خاصة معمول بها للوقوف أمام مرتكبي الجرائم الإلكترونية؟) نرى أنه من الأجدر على التشريعات سن قوانين خاصة تكون مواكبة لتطورات هذه الجريمة ونظرا لصعوبة

[1] محمد عبيد الكعبي، مرجع سابق، ص 58-59.

هذا الأمر، نقول أنه بالإمكان تطبيق القواعد التجريمية التقليدية على بعض صور الجريمة الإلكترونية وليس كلها وذلك في حالة ما لم تكن هذه الجريمة تتعارض مع هذه النصوص.

**المطلب الثاني: العقبات المرتبطة بتحديد مكان إرتكاب الجريمة الإلكترونية**

تطرح مسألة تحديد مكان وقوع الجريمة الإلكترونية عندما ترتكب هذه الأخيرة من طرف أجنبي فوق إقليم الدولة، أو ترتكب في الخارج ضد مصلحة الدولة أو رعاياها أو من طرف رعاياها، وعندها تطرح مسألة تحديد الإختصاص القضائي وبالتبيعة تحديد القانون الواجب التطبيق على الجريمة الإلكترونية ذات العنصر الأجنبي، لذلك على العموم توجد أربعة مبادئ تحدد إطار السلطان المكاني للنص التجريمي، بالإضافة إلى تفعيل مبدأ أخر من بعض التشريعات سواء العربية منها أو الأجنبية وهو مبدأ عالمية النص الجنائي، وهذه المبادئ هي المبادئ العامة لتطبيق قانون العقوبات من حيث المكان(الفرع الأول)، وأيضا أنه في بعض الحالات يتوزع السلوك الإجرامي على عدة أقاليم دولية بإعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود، مما يخلق مشكلة تنازع القوانين من حيث المكان و تأثيرها على مسألة الإختصاص القضائي (الفرع الثاني).

**الفرع الأول: المبادئ العامة الضابطة للنطاق المكاني ومدى تطبيقها على الجريمة الإلكترونية**

تعد المبادئ العامة للتطبيق الإقليمي للقانون الجنائي أساسا مهما لتحديد نطاق القانون الجنائي الوطني، وتضمن هذه المبادئ مجتمعة أن القانون الجنائي يحمي النظام العام، وسلطة الدولة بشكل فعال، وحقوق الأفراد سواء داخل الحدود الوطنية أو خارجها، مع مراعاة التعاون الدولي و الاعتراف بالسيادة المتبادلة بين الدول، وتتمثل هذه المبادئ في مبدأ الإقليمية ومدى صلاحيته لتحديد القانون الواجب التطبيق (أولا)، مبدأ شخصية النص الجنائي (ثانيا)، مبدأ عينية النص الجنائي (ثالثا). مبدا عالمية النص الجنائي (رابعا).

**أولا: مبدأ الإقليمية ومدى صلاحيته لتحديد القانون الواجب التطبيق**

للوصول إلى تحديد القانون الواجب التطبيق على الجريمة الإلكترونية لابد من تحديد المكان الذي وقعت فيه الجريمة وهو ما يسمى بمبدأ إقليمية النص الجنائي، وتعد قواعد القانون الجنائي

بشقيه الموضوعي و الإجرائي مظهرا من مظاهر سيادة الدولة، لذلك فإن تطبيقها من حيث المكان يخضع لمبدأ مستقر ألا وهو مبدأ الإقليمية، فإذا كان تطبيق هذا المبدأ بالنسبة للجرائم التقليدية لا يثير إشكالا، فالتساؤل يطرح حول مدى إمكانية الأخذ بهذا المبدأ كمعيار لتحديد القانون الواجب التطبيق على الجريمة الإلكترونية، بما أن هذه الأخيرة تختلف اختلافا تاما على الجرائم التقليدية.

فيقصد بالإقليم ذلك المكان الذي يمتد إليه السلطة السياسية للدولة طبقا لأحكام القانون الدولي العام، ويتكون إقليم الدولة من الأراضي التي تحدها الحدود السياسية للدولة وكذلك المياه الإقليمية حسب ما هو مقرر في قانون البحار وكذلك الإقليم الجوي المتمثل في طبقات الجو التي تعلو الإقليم الأرضي والمائي إلى مالا نهاية في الارتفاع[1].

أما بخصوص مبدأ الإقليمية فمفاده أن الدولة تقوم بتطبيق قانون العقوبات الخاص بها على جميع الجرائم التي تقع داخل نطاقها الإقليمي بغض النظر عن جنسية مرتكبيها سواء أكان وطنيا أم أجنبيا، وسواء أكان المجني عليه وطنيا أم أجنبيا، وسواء هددت مصلحة تلك الدولة صاحبة السيادة على إقليمها أو هددت مصلحة دولة أجنبية[2]، ولهذا المبدأ معنيان أحدهما معنى إيجابي و أخر معنى سلبي، فالمعنى الإيجابي يقصد به سريان القانون الجنائي للدولة على جميع ما يقع من جرائم، أيا كانت جنسية مرتكبها، سواء كان وطنيا أم أجنبيا، أما المعنى السلبي لا سلطان للقانون الجنائي للدولة على ما يقع خارج إقليمها من جرائم مهما كانت صفة مرتكبها أو جنسيته إلا إستثناءا[3].

و تأخذ غالبية الدول بمبدأ الإقليمية كأصل في سريان القانون الجنائي من حيث المكان، فتطبيقا لهذا المبدأ يطبق القانون الجنائي على كافة الجرائم التي ترتكب في إقليمها أو جزء من

---

[1] بارش سليمان، شرح قانون العقوبات الجزائري، الجزء الأول شرعية التجريم، سلسلة القانون الجنائي الجزائري، 1992، ص 65.

[2] عبد المومن بن صغير، "**تطبيق النص الجنائي بين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة**"، مجلة العلوم القانونية و السياسية، المجلد 10، العدد03، جامعة سعيدة، الجزائر، ص 62 .

[3] سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي (دراسة مقارنة)، الطبعة 01، دار الكتب القانونية، القاهرة، مصر،2010، ص 128.

إقليمها بصرف النظر عن جنسية فاعلها، وهو المبدأ المنصوص عليه في المادة 03 من قانون العقوبات الجزائري (يطبق قانون العقوبات على كافة الجرائم التي ترتكب في الأراضي الجمهورية)[1].

فتطبيق مبدأ الإقليمية على الجريمة الإلكترونية يثير العديد من الإشكالات والصعوبات المتمثلة في صعوبة تحديد مكان إرتكاب هذه الجريمة (أ)، وكذا بعض الإشكالات المرتبطة بتحديد مكان بعض صور الركن المادي للجريمة الإلكترونية (ب).

**أ: صعوبة تحديد مكان إرتكاب الجريمة الإلكترونية لوقوعها في عالم إفتراضي**

يعتبر تحديد المكان الذي وقعت فيه الجريمة الإلكترونية من الأساسيات لتحديد القانون الواجب التطبيق، غير أن الطبيعة الخاصة لهذه الجريمة و إرتكابها في مسرح الإفتراضي شكلت فعلا عائقا جعلت تحديد مكان إرتكابها عقبة من العقبات، مما اثر هذا الأمر سلبا على مسألة تحديد القانون الواجب التطبيق عليها.

إن مكان إرتكاب الجريمة الإلكترونية يكون في عالم إفتراضي غير ملموس، بواسطة شبكة الأنترنت مما يسهم في صعوبة تحديد مكان إرتكاب الجريمة، ففي جريمة الإبتزاز مثلا هي جريمة تقليدية غير أنها ترتكب بإستعمال وسائل تكنولوجية كالأنترنت والاتصالات الهاتفية و الرسائل النصية، وبالتالي يتحول مكان وقوع الجريمة من إطاره المادي المحدد إلى بيئة إفتراضية غير ملموسة، فالتهديد تم سماعه هاتفيا وهو يشكل أحد عناصر تكوين الجريمة، فالركن المادي للجريمة الذي يعد كمعيار لتحديد مكان إرتكابها قد وقع ضمن نطاق بيئة إفتراضية وهو الأمر الذي يعقد من مسألة تحديد مكان إرتكابها[2].

[1] لموسخ محمد،" **تنازع الإختصاص في الجرائم المعلوماتية**" ،مجلة دفاتر السياسة والقانون، المجلد 07، العدد، 02، 2009، ص 148.

[2] يوسف قجاج، إشكالية الإختصاص في الجريمة الإلكترونية، مقال متوفر على منبر هسبريس، https://www.hespress.com ، تم الإطلاع عليه بتاريخ يوم 2024/04/28، على الساعة 17.10.

كذلك بالنسبة لجرائم التزوير ففي السابق كانت هذه الجرائم تقع على المحررات الورقية، ومع تطور المشهود في تكنولوجيا المعلومات أصبحت هذه الجريمة تستهدف بطاقات الإئتمان ويتخذ من الحاسب الألي وسيلة لها، مما عقد من عملية تحديد مكان إرتكاب الجريمة[1].

حيث أن العديد من الجرائم الإلكترونية يتم الفعل الإجرامي فيها من مسافات بعيدة نظرا لطبيعة هذه الجريمة، وذلك بإستخدام وحدات طرفية أو إتصال هاتفي يستطيع الجاني من خلالها من إعطاء تعليمات للحاسب الألي تمكنه من إختراق شبكات المعلومات في مناطق اخرى، مما يترتب على ذلك إثارة مشكلة تتمثل في صعوبة الوصول إلى مرتكب هذا الفعل وتحديد مكان تواجده، وأيضا يمكن لهذا الجاني إلغاء وطمس كل ما يدل على جريمته من خطوات[2].

والجدير بالإشارة أيضا أن المجرم المعلوماتي في حالة تمكنه من الحصول و معرفة كلمة السر للوسائل الإلكترونية التي تتصل بالشبكات العالمية، يستطيع إختراق هذه الشبكات والعبث بمعلوماتها بغض النظر عن مكان تواجده، وعليه فإن الصبغة العالمية التي تتصل بتنظيم المعالجة الألية للمعلومات تثير إشكالية تحديد الإختصاص المكاني لهذه الجرائم، من حيث المحكمة المختصة و كذلك سريان القانون الوطني من حيث المكان[3].

فعليه تكمن المشكلة الأساسية في تحديد مكان إرتكاب الجريمة الإلكترونية في أنها جريمة تتميز بالطابع الدولي أي أنها جريمة لا تحدها حدودا جغرافية مثلما سبق و أشرنا في خصائصها، وفضلا عن ذلك أن الشبكة الأنترنت نظرا لسمة التعقيد التي تتمتع بها وكذا طرق إستخدامها المتنوعة مما يؤدي كنتيجة إلى صعوبة تحديد مكان إرتكاب الجريمة الإلكترونية، ففي الجرائم التقليدية والتي

[1] مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، دراسة مقارنة، دار الخلدونية، الجزائر، 2021، ص 100

[2] عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنت، دار الكتب القانونية، مصر، 2007، ص 16.

[3] مرجع نفسه، ص 31.

عند وقوعها تتكفل القواعد التنظيمية المنصوص عليها في القواعد الجنائية بتحديد مكان إرتكاب الجريمة، وهذه القواعد من الصعب إعمالها على الجريمة الإلكترونية[1].

مما سبق يتضح أن من بين العوامل التي تجعل من تحديد مكان وقوع الجرائم الإلكترونية صعبا هي طبيعة البيئة الإفتراضية التي تتميز بها هذه الجريمة بإعتبار أن هذه الأخيرة يمكن أن تحدث في أي مكان يتوفر فيه إتصال بالأنترنت، عكس الجرائم التقليدية التي عادة لا تثير أية صعوبة في تحديد مكان إرتكابها، فعليه يعتبر موضوع تحديد مكان وقوع الجريمة الإلكترونية تحديا للأنظمة القانونية، والذي لاتزال هذه النقطة تثير كثيرا من الجدل نظرا لتأثيرها على التحقيقات و تطبيق القانون.

إضافة فإن تحديد مكان وقوع الجرائم الإلكترونية يتطلب إطار تشريعي محدد يختلف عن القواعد التقليدية التي سنت في هذا الشأن، فالطبيعة الخاصة للجريمة الإلكترونية التي تختلف عن الجرائم التقليدية في كثير من النقاط تفرض ذلك، وعليه نرى أنه يجب إصدار تشريعات جديدة تتناسب مع الواقع الحالي للتكنولوجيا و الجرائم الإلكترونية.

إن موضوع تحديد مكان إرتكاب الجريمة الإلكترونية والقانون الواجب تطبيقه على الفعل لا يحظى دائما بالوضوح أو القبول أمام حقيقة أن غالبية هذه الجريمة ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات معلومات أو أنظمة معلومات خارج الحدود بل حتى عندما يرتكبها شخص من داخل الدولة على نظام الدولة نفسها، وهو ما يبرز أهمية إختبار مدى ملاءمة قواعد تحديد مكان إرتكاب الجريمة وكذا القانون الواجب التطبيق، وما إذا كانت النظريات والقواعد

[1] أسامة أحمد محمد النعيمي، هايس سويلم صلبي الشمري، "**قواعد الإختصاص الموضوعي في الجرائم المعلوماتية-دراسة مقارنة-**"، مجلة جامعة تكريت للحقوق، المجلد 07، العدد01، كلية الحقوق، جامعة الموصل، نينوى، العراق، 2022، ص ص 114-115.

القائمة في هذا المجال تطال هذه الجرائم، أم يتعين إفراد قواعد خاصة بها مثلما أشرنا سابقا في ضوء الخصوصية التي تمتع بها هذه الجريمة، و ما تثيره من إشكاليات في تحديد مكان إرتكابها[1].

و في هذا الشأن عالج القضاء المغربي قضية تنطبق وقائعها على هذه العقبة، حيث تعود وقائعها أن الأمر يتعلق بجريمة التهديد بإفشاء أو نشر أمور شائنة(الابتزاز)، أين عرضت القضية على المحكمة الابتدائية بمدينة سلا، وان هذه الجريمة إرتكبت من طرف جناة ينحدرون من مدينة أخرى تسمى واد زم، والضحية يقطن بمدينة سلا، وتمثلت أداة إرتكاب الجريمة في وسائل التواصل و الإتصال، مما تكون معه أن الجريمة قد انتقلت من جريمة عادية تقليدية إلى جريمة إلكترونية تم إقترافها بوسائل إلكترونية، وهو ما يتماشى مع الجريمة الإلكترونية.

أيضا ما يلاحظ من وقائع الجريمة أن السلوك المادي للجريمة توزع بين مدينتين ( واد زم، سلا) وبالتالي كل مدينة قد تحقق فيها أحد عناصر الركن المادي للجريمة، وبالرجوع إلى قانون المسطرة الجنائية المغربي فالمشرع المغربي عالج مسألة تحديد مكان إرتكاب الجريمة في مواد عدة من خلال القاعدة الثلاثية وذلك في المواد 44 و55و 259 باختلاف الجهة القضائية (- مكان إرتكاب الجريمة، – محل إقامة أحد الأشخاص المشتبه في مشاركته للجريمة، – مكان إلقاء القبض على أحد هؤلاء الأشخاص ولو تم القبض عليه لسبب اخر.)

عليه في ظل غياب الإطار الذي ينظم موضوع الإختصاص في الجرائم الإلكترونية دفع هذا النقص إلى إعمال قواعد الإختصاص المحلي متلما أشرنا إليه، وهو الأمر الذي يطرح صعوبة من ناحية البيئة المرتكب فيها الجريمة، فقواعد الإختصاص المحلي تنظم في إطار بيئة تقليدية بينما الجريمة الإلكترونية فالبيئة المرتكب فيها الجريمة هي بيئة افتراضية غير ملموسة، وهو الأمر الذي تفطنت له المحكمة الابتدائية بمدينة سلا.

أين قضت بعدم الإختصاص المكاني والذي أيدته محكمة الاستئناف موضوع الطعن بالنقض، حيث ان الجرائم محل المتابعة نظمها المشرع المغربي في المادتين 538 و 129 من القانون

[1] عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية –دراسة مقارنة–، مذكرة لنيل شهادة ماجستير في القانون العام، جامعة الشرق الأوسط، المملكة الأردنية، 2014، ص 86.

الجنائي وهي جرائم تقليدية، بينما الوسائل التي اعتمدها المتهمون والمتمثلة في الإتصالات الهاتفية و الرسائل النصية وشبكة الأنترنت قد نقلت الجريمة من إطار مادي محدود جغرافيا إلى بيئة افتراضية غير ملموسة، والتهديد محل الواقعة تم عبر رسائل الإتصال عن بعد والتي حولته من نطاق جغرافي محدود بمدينة واد زم إلى بيئة افتراضية غير ملموسة، فتم إستقبال التهديد من طرف الضحية بمدينة سلا مما يجعل المحكمة الابتدائية بسلا صاحبة ولاية هي الأخرى مكانيا للنظر في الجرائم موضوع المتابعة.

لذلك فتطبيق قاعدة مكان إرتكاب الجريمة بمفهومها التقليدي لا تتلاءم مع طبيعة الجريمة الإلكترونية وخصوصيتها حيث يصعب تحديد مكان وقوع الفعل الإجرامي في هذه الجرائم( بإعتبار أن الجريمة الإلكترونية تتم في مسرح إفتراضي وكذا بتميزها بأنها جريمة لا تحدها حدود جغرافية)، فعلى إعتبار أن هذه القاعدة صيغت لكي تحدد الإختصاص المتعلق بجرائم قابلة للتحديد المكاني وبالتالي لا ينبغي إعمالها بشأن الجريمة الإلكترونية والتي ترتكب في فضاء مادي غير ملموس يبقى معه أمر تحديد مكان إرتكاب الجريمة في غاية الصعوبة، ويجعلها تستعصي على الخضوع للقوالب القانونية التي تحكم مسألة الإختصاص المكاني[1].

وفي المقابل تبذل جهودا كبيرة للوصول إلى حل لهذه العقبة، وفي هذا الصدد باشر مكتب التحقيقات الفيدرالي FBI بإنشاء موقع إلكتروني وهو عبارة عن منتدى مخصص للحديث حول تقنيات تزوير البطاقات البنكية، حيث تم وضعه قيد التشغيل في شهر جوان 2010 تحت إسم Carder projet، والذي بواسطته تم تحديد هوية ومكان تواجد المحتالين على البطاقات البنيكة[2].

[1] يوسف قجاج، الجريمة الإلكترونية و إشكالية الإختصاص القضائي _مكان إرتكاب الجريمة نموذجا _ المفهوم الجديد لمكان إرتكاب الجريمة الإلكترونية– مقال متوفر على الموقع الإلكتروني ،https://www.mrlatalib.com، تم الاطلاع عليه بتاريخ 2024/04/22 على الساعة 16:05.

[2] مناصرة يوسف، مرجع سابق، ص 100.

**ب: الإشكالات المرتبطة بتحديد مكان بعض صور الركن المادي للجريمة الإلكترونية**

إن كان من الصعب تحديد مكان إرتكاب الجريمة الإلكترونية نظرا لخصوصيتها والمتمثلة في أنها جريمة ترتكب في العالم اللامادي والافتراضي، فإن هناك إشكالات أخرى تثار بشأن بعض صور الركن المادي للجريمة الإلكترونية، حيث يقتضي تحديد مكان إرتكاب الركن المادي للجريمة الإلكترونية تحديدا دقيقا لعناصر الركن المادي، مثل حالة الشروع في الجريمة الإلكترونية، الإشتراك في الجريمة الإلكترونية ،الجريمة الإلكترونية المستمرة، الجريمة الإلكترونية المركبة، وجريمة الإعتياد.

**01 الشروع في الجريمة الإلكترونية:**

إذا وقف نشاط الجاني عند حد الشروع، فإن فعله يعتبر قد حدث في الإقليم الذي قام فيه بالأفعال التحضيرية، أي البدء في التنفيذ و الأصل أنه لا يعتد بالمكان الذي ينوي الجاني تحقيق نتيجة نشاطه فيه مادامت هذه النتيجة لم تتحقق، ورغم ذلك فقد ذهبت بعض التشريعات إلى إعتبار مكان جريمة الشروع إما مكان وقوع النشاط أو المكان الذي كان ينوي فيه الجاني تحقيق نتيجته الإجرامية، وهذا المكان الأخير محل نظر لأنه مادامت النتيجة لم تتحقق فلم يقع إذن أي إخلال بالنظام العام في الإقليم الذي كان يراد تحقيقها فيه، مما لا مبرر معه لإخضاع الشروع لقانون هذا الإقليم[1].

ففي جريمة سرقة الدعامات أو البرامج مثلا، فالمكان الذي يتم فيه البدء في تنفيذ الركن المادي هو المكان الذي تم فيه البدء بفعل الإختلاس للدعامات، وأيضا بخصوص جريمة الإتلاف فالمكان الذي يتم فيه البدء تنفيذ الركن المادي هو مكان البدء في إدخال برنامج الفيروس على الشبكة المعلوماتية المراد إتلافها[2].

[1] أحمد فتحي سرور، الوسيط في قانون العقوبات (القسم العام)، الطبعة السادسة، دار النهضة العربية، مصر، 2015، ص 258.

[2] بن عودة صليحة، "**الشروع في الجرائم المعلوماتية بين الوقاية والردع**"، مجلة دفاتر الحقوق والعلوم السياسة، المجلد 01، العدد 02، جامعة أبوبكر بلقايد تلمسان، ص 81.

**02 -الإشتراك في الجريمة الإلكترونية:**

تنص المادة 585 من قانون الإجراءات الجزائية المعدل والمتمم على أنه " كل من كان في إقليم الجمهورية شريكا في جناية أو جنحة مرتكبة في الخارج يجوز أن يتابع من أجلها ويحكم عليه بمعرفة جهات القضاء الجزائرية إذا كانت الواقعة معاقب عليها في كلا القانونين الأجنبي والجزائري بشرط أن تكون تلك الواقعة الموصوفة بأنها جناية أو جنحة قد ثبت إرتكابها بقرار نهائي من الجهة القضائية الأجنبية "[1].

فتبعا لذلك يجد هذا المبدأ صعوبة في التطبيق بالنسبة للجريمة الإلكترونية نظرا لطبيعتها، إذا يتطلب الأمر لمسائلة الشريك الموجود في الجزائر وفقا للقانون الجزائري، أن تكون الواقعة معاقب عليها في كلا الإقليمين الأجنبي و الجزائري و أن يصدر حكم الإدانة على الفاعل الأصلي في البلد المنشأ، لذلك نرى أن تطبيق نص المادة السالفة الذكر على الجريمة الإلكترونية يصطدم بعقبة تتمثل في صعوبة تحديد مكان وقوع الفعل الأصلي الذي يعتبر شرطي مبدئي لعقد الإختصاص للقاضي الوطني وبالتبعية تطبيق قانون العقوبات، لأن ذلك يثير إشكالية معرفة ما إذا كان الفعل مباحا أو مجرما في ذلك البلد.

**03 -الجريمة المستمرة:**

في حالة ما إذا إستمر النشاط المادي للجاني وقتا طويلا، كأن يقوم بعرض الكتابات أو الصور الممقوتة في موقعه الخاص الذي قام بإنشائه، ويبقى هذا العرض مستمرا إلى غاية أن يقرر الجاني إيقاف و إنهاء الوضع الإجرامي، فهنا يعتبر مكانا للجريمة كل محل تقوم فيه حالة الإستمرار، وتكون كل محكمة تحققت الجريمة في دائرتها مختصة بالنظر في هذه الجريمة، وذلك راجع أن الركن المادي للجريمة ينطوي على إستمرار زمني ومكاني في أن واحد، فيكون الإقليم الذي وقعت أو تحققت فيه حالة الإستمرار يكون له السلطان عليها، كجرائم النشر بواسطة الإعلام الألي مثلا فقد

[1] الأمر رقم 66-155، المؤرخ في 18 صفر 1386، الموافق لـ8 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

إعتبرها البعض من الجرائم المستمرة[1]، كذلك بالنسبة لجريمة الدخول أو البقاء غير المشروع في نظام معالجة الألية للمعطيات فإن المكان يتحدد بكل محل يقع فيه الإستمرار[2].

ففي هذا الصدد يمكن إيضاح هذا الطرح بمثال عن الاحتيالات المالية التي تتم في الوسط الإلكتروني مثل سرقة أرقام بطاقات الإئتمان وإستغلالها لفترة طويلة لغرض إجراء عمليات الشراء بهذه البطاقة.

**04 الجريمة المركبة:**

تكون الجريمة مركبة في حالة ما إذا إرتكبت بأكثر من عمل ذي طبيعة مختلفة، كجريمة النصب الإلكتروني مثلا، فهذه الجريمة تقوم في ركنها المادي على عنصرين هما الوسائل الإحتيالية و الاستيلاء على المال، وفي هذا الصدد قضت محكمة النقض الفرنسية بأن هذه الجريمة تعد مرتكبة في فرنسا مادام أحد عناصرها قد إرتكبت في الإقليم الفرنسي[3].

**05 جريمة الإعتياد:**

يكون الإعتياد في حالة إرتكاب الفعل الإجرامي أكثر من مرة واحدة، وقد ثار التساؤل عن القانون الواجب التطبيق إذا توزعت الأفعال المكونة للإعتياد في أقاليم مختلفة أي في أكثر من إقليم، فإختلف الفقه في حل هذه الشأن، فذهب البعض إلى القول بأنه ما لم يتوافر الإعتياد في إقليم دولة معينة فإن قانونها لا ينطبق على الجريمة وأنه لا يجوز الإكتفاء بتوافر فعل واحد من أفعال الإعتياد في إقليم الدولة حتى يقال بإنطباق قانونها على هذه الجريمة، وإلا إختلط الأمر بين جريمة الإعتياد والجريمة المستمرة، اما رأي أخر فذهب للقول بإنطباق قانون الإقليم الذي وقع فيه الفعل الأخير من أفعال الإعتياد بحجة أن الجريمة تقع به منظورا إلى ما سبقه من أفعل[4].

---

[1] يعقوب عبد العزيز الصانع، التلبس في الجرائم الإلكترونية، منصة القبس، مقال متوفر على الموقع الإلكتروني، https://www.alqabas.com ، تم الإطلاع عليه يوم 2024/05/05 على الساعة 14.20

[2] حسين بن سعيد بن يوسف الغافر، السياسة الجنائية في مواجهة جرائم الأنترنت، دراسة مقارنة، جامعة عين شمس، القاهرة ، مصر، 2010، ص 464.

[3] بارش سليمان، مرجع سابق، ص 67.

[4] أحمد فتحي سرور، مرجع سابق، ص 260

ومن أمثلة ذلك قيام مجموعة من القراصنة الإلكترونيين متخصصة في تنفيذ عمليات الإحتيال المالي بواسطة الإختراقات التي تمس الحسابات المصرفية وسرقة المعلومات التي تخص البيانات المالية، فتقوم هذه المجموعة بممارسة مهامها بشكل مخطط وبإستمرار مما يجعلها في هذه الحالة نموذجا لجريمة الإعتياد في هذه الفئة من الجرائم.

**ثانيا: مبدأ شخصية النص الجنائي**

يقوم هذا المبدأ على وجوب سريان النص على كل من يحمل جنسية الدولة ولو إرتكبت الجريمة خارج إقليمها ويعبر عن هذا الوجه بالوجه الإيجابي لمبدأ شخصية النص الجنائي، ومن ناحية أخرى يطبق قانون الدولة إذا كان المجني عليه من رعاياها ولو وقعت الجريمة في الخارج ويعبر عن هذا الوجه بالوجه السلبي لمبدأ الشخصية، والجدير بالإشارة أن المشرع الجزائري أخذ بمبدأ شخصية النص الجنائي بشقيه الإيجابي والسلبي ونفس الشي بالنسبة للمشرع الفرنسي من خلال المادة 113 الفقرتين 06 و 07 من قانون العقوبات الفرنسي، فمن خلال هذا العرض نطرح التساؤل الأتي.

يعتمد هذا المبدأ بصفة أساسية على الجاني من حيث الكشف على هويته ومن ثم التعرف على جنسيته وهذه المعلومات صعبة في الجرائم الإلكترونية حيث أن المجرمون يستعملون التشفير والأسماء المستعارة، و غالبا ما يعتمد المحققون في إطار البحث عن مرتكبي هذه الجرائم من خلال عنوان الجهاز المستخدم في إرتكاب الجريمة (برتوكول الأنترنت IP)، ولكن نظرا للذكاء الذي يتمتع به المجرم المعلوماتي فإنه عند إرتكابه للجريمة يستخدم الشبكة الإفتراضية الخاصة المعروفة إختصارا بـ VPN وهذه الشبكة تعمل على إخفاء بيانات الخاصة بالمجرم وكذا إرسالها إلى خوادم في بلدان أخرى لإخفاء هويته، مما يؤدي هذا الأمر إلى تعقيد عملية تتبع مكان هذا المجرم، إلا أنه رغم هذه الصعوبة فالمسألة ليست مستحيلة على القائمين بالتحريات والتحقيق في هذه الجرائم الذين يستعملون نفس الوسائل لفك التشفير والتعرف على المتورطين الذي يختفون وراء هذه الأسماء، أيضا أن هذا المبدأ قد يكتنفه بعض المخاطر مثل تطبيق القانون الجنائي الوطني على الجرائم التي تقع

في الخارج التي يختص بها القانون الأجنبي في ذات الوقت أنها تؤدي ايضا إلى المساس بمبدأ عدم جواز محاكمة الشخص عن نفس الفعل مرتين [1].

**ثالثا: مبدأ عينية النص الجنائي**

يقوم هذا المبدأ على وجوب سريان قانون الدولة على كل الجرائم التي ترتكب في الخارج، وتشكل اعتداء على مصالحها الأساسية بصرف النظر عن جنسية مرتكبها، وتلجأ الدولة إلى الأخذ بمبدأ العينية وذلك لإعطاء نصوصها سلطانا ونطاق للتطبيق لا يتسع له مبدأ الإقليمية.

وعلى هذا الاساس قد يطبق هذا المبدأ على الجرائم الإلكترونية إذا كانت تمس مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني[2]، غير أن تطبيق هذا المبدأ قد يصادفه العديد من الإشكاليات التي تعيق التنفيذ، من ناحية تعارض الاختصاص وفقا لمبدأ العينية مع الاختصاص وفقا لمبدأ الإقليمية، وذلك في حالة أن تكون الجريمة المرتكبة وفقا لمبدأ العينية مجرمة في قانون الدولة الأخرى التي اقترفت فيها، فهنا تثار مسألة تنازع الاختصاص ما بين الدولة المقترفة فيها الجريمة وفقا لمبدأ الإقليمية والدولة الأخرى التي تعد تلك الجريمة من الجرائم التي ترى أنه يناط بقضائها النظر فيها وفقا لمبدأ العينية كونها تمس بأمن مؤسساتها أو دفاعها الوطني أو مصالحها الإستراتيجية، وبالتالي فقد يحاكم الشخص على فعله مرتين.

ايضا من المشكلات هي أن اختصاص القضاء بالنظر في الجرائم الإلكترونية والقانون الواجب تطبيقه على الفعل دائما يشوبه نوعا من الغموض وعدم الإيضاح أمام حقيقة أن غالبية الأفعال ترتكب من قبل أشخاص من خارج الحدود، أو أنها تمر عبر شبكات معلومات وأنظمة معلومات خارج الحدود، وهو ما يبرز أهمية إمتحان قواعد الإختصاص والقانون الواجب التطبيق وما إذا كانت النظريات والقواعد القائمة تطال هذه الجرائم أم أنه يتعين إفراد قواعد خاصة بها في ضوء

[1] بثينة حبيباتي، "**معوقات مكافحة الجريمة المعلوماتية**"، مجلة العلوم الإنسانية، المجلد أ، العدد 50، كلية الحقوق، جامعة الجزائر 01، ص93.

[2] لموسخ محمد، مرجع سابق، ص 150.

خصوصيتها وما تثيره من مشكلات تتعلق بالإختصاص القضائي[1]، وعليه نقول أن تطبيق مبدأ العينية على الجريمة الإلكترونية يثير العديد من الصعوبات ناحية تسليم المجرمين و كذا إشتراط إزدواجية التجريم، لذلك تسعى الدول إلى توسيع من مفهوم الجريمة الإلكترونية حتى تتمكن من التصدي لهذه الظاهرة.

والجدير بالإشارة أن المشرع الأمريكي أخذ أيضا بمبدأ العينية حين قرر إمداد التشريع الأمريكي إلى الجرائم الواقعة في الخارج والتي من شأنها المساس بالمصالح الأمريكية المنصوص عليها في قانون العلاقات الخارجية The foreign relations Law of the USA، حيث جعل الإختصاص الأمريكي والقانون الأمريكي هو المطبق طالما كان هناك سلوك ذو تأثير على الإقليم الأمريكي[2].

**رابعا: مبدأ عالمية النص الجنائي**

نظرا لأن القانون الجنائي يسري على إقليم الدولة فقط كقاعدة عامة مثلما سبق و أشرنا، فإن تلك الضوابط تقف عاجزة في حالة إرتكاب جريمة عالمية مثلما هو لحال بالنسبة للجريمة الإلكترونية بإعتبارها جريمة عالمية، وانتهاك مصالح وقيم المجتمع الدولي ولأن ملاحقة المجرمين في حالة فرارهم إلى دول أخرى فعل يمس سيادة الدولة أو عدم رغبة سلطات الدولة التي إرتكب فيها الفعل الإجرامي أو عدم قدرتها على ملاحقة الجاني، الأمر الذي يقتضي مد مجال الولاية القضائية وفقا لضوابط أخرى تمكن بمعاقبة جناة لا يمكن أن يخضع لقضائها، وعليه فإن إمتداد الإختصاص يعد بمثابة علاج قانوني نظرا لعدم كفاية المبادئ التقليدية لمجابهة أنواع معينة من الجرائم كالجريمة الإلكترونية[3].

[1] فايز محمد راجح غلاب، مرجع سابق، ص 392.

[2] حسين بن سعيد بن يوسف الغافر، مرجع سابق، ص 460

[3] أميمة خديجة حميدي، عبد المجيد لخداري، "**إمكانية تفعيل مبدأ العالمية على الجريمة الإلكترونية**"، مجلة الحقوق والحريات، المجلد 10، العدد01 ، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة ، 2022،ص 1933.

ومن ضوابط إعمال مبدأ عالمية النص الجنائي، التي يمكن التمييز بين ثلاث منها كما يأتي:

أ -يعد مبدأ عالمية النص الجنائي صورة عاكسة للتضامن الدولي في مكافحة الجريمة التي تفنن المجرمون في اقترافها بالاستفادة من التطور العلمي الذي أتاح لهم ممارستها على مستوى دولي كالإتجار في المخدرات والقرصنة والجريمة المنظمة، وعليه فلا يوجد ما يبرره سوى فكرة حماية المصالح العامة والمشتركة للبشرية، وهو ما أدى إلى انحصار هذا المبدأ في نطاق ضيق من الجرائم

ب -يفترض تطبيق مبدأ العالمية أن يقبض على المتهم في إقليم دولة معينة، أو يقبض عليه في مكان لا يخضع لسيادة دولة أخرى كالبحر العام، كما يلزم ألا يكون استرداد الأجنبي قد طلب أو قبل على أساس أن المقصود بهذا النص هو مواجهة الإجرام الدولي بتقرير قاعدة تسري بصفة احتياطية على الجرائم التي تخضع في الأصل لقوانين أجنبية، فإذا طلبت الدولة صاحبة السلطان الأصلي استرداد المجرم فلا يجوز إعمال النص الاحتياطي.

ج- يشترط أن تكون الجريمة المرتكبة جناية أو جنحة معاقب عليها في شريعة الدولة التي اقترفت في أرضها هذه الجرائم[1].

**الفرع الثاني: تنازع القوانين الإجرائية من حيث المكان و تأثيرها على مسألة الإختصاص القضائي**

إن شبكة الأنترنت ليس لها مقر في دولة معينة، فهي لا تخضع لرقابة دولة معينة، ولا يوجد قانون جنائي موحد يحكمها بل تتعدد القوانين الجنائية التي تحكمها بتعدد الدول المرتبطة بها، إذ يمكن التنقل من شبكة إلى أخرى والنفاذ إلى قواعد البيانات عبر قارات ودول مختلفة وهنا يثار التساؤل حول القانون الواجب التطبيق، هل يطبق قانون الدولة التي إرتكب على إقليمها الفعل المجرم أم يطبق القانون الدولة التي حصل الضرر على إقليمها؟[2].

بالرجوع إلى القواعد العامة التي تنظم مسألة تطبيق القانون من حيث المكان نجد المبدأ الأساسي وهو مبدأ الإقليمية، وعليه عملا بهذا المبدأ فإن كل دولة تمارس سيادتها على إقليمها تقوم بتطبيق قوانينها داخل حدودها بصرف النظر عن جنسية مرتكب الجريمة مثلما سبق و تطرقنا إليه،

[1] عزيزة شبري، "**تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية**"، مجلة الاجتهاد القضائي، العدد15، جامعة محمد خيضر بسكرة، 2017، ص 93.

[2] حسين بن سعيد بن يوسف الغافر، مرجع سابق، ص 455.

الأمر الذي يحتمل تنازع القوانين إتجاه الواقعة الواحدة ويستبعه بالضرورة تنازع الإختصاص القضائي، فجريمة السب مثلا عبر الرسائل الإلكترونية Email تقع أحيانا في بلد ويتلقاها الضحية في بلد أخر، فهذه الرسائل تمر أحيانا بأكثر من دولة قبل وصولها إلى بلد الإستقبال، فكل دولة تعمل على تطبيق قانونها على هذه الجريمة، فيحدث هنا تنازع إيجابي للقوانين في التطبيق.

غير أن تطبيق هذا المبدأ (مبدأ الإقليمية) على الجرائم الإلكترونية قد يثير بعض المشكلات منها مشكلة تنازع الإختصاص القضائي لأكثر من دولة، كما لو قام الجاني ببث الصور الخليعة ذات الطابع الإباحي من إقليم دولة معينة فلتكن مثل من الجزائر وتم الإطلاع عليها في دولة أخرى ولتكن تونس ففي هذه الحالة يثبت الإختصاص وفقا لمبدأ الإقليمية لكل دولة من الدول التي مستها الجريمة والمتمثلة في دولتين (الجزائر وتونس)[1].

ايضا من الإشكاليات المثارة في تطبيق القانون الوطني على الجرائم التي تقع كلها أو جزء منها في إقليم الدولة، إزدواجية الإختصاص حيث يختص بها القانون الأجنبي في نفس الوقت الذي تدخل في إختصاص القانون الوطني، وذلك قد يؤدي إلى الإطاحة بمبدأ عدم جواز محاكمة الشخص عن الفعل أكثر من مرة، كما أن من المشكلات التي تعيق تطبيق الإختصاص القضائي القائم على مبدأ على مبدأ الإقليمية في مجال الجرائم الإلكترونية تتمثل في حالة أن يكون مزود الأنترنت الأساسي موجود في دولة بينما المزودات الفرعية في أكثر من دولة، فأي من قضاء تلك الدول يكون مختصا، وأي من القوانين يكون واجب التطبيق؟[2].

وكذلك بافتراض أنه لو قام شخص ما بإرتكاب جريمة إلكترونية على إقليم دولة لا يحمل جنسيتها، فقد يحدث التنازع بين قانون الدولة التي إرتكبت الجريمة على إقليمها، وقانون الدولة التي ينتمي إليها لأن كل دولة تأخذ بمبدأ معين، وعليه فالفعل الواحد يتنازعه قانونان، قانون دولة الإقليم على أساس مبدأ الإقليمية وفي نفس الوقت قد يخضع لقانون دولة الجاني عملا بمبدأ الشخصية في شقه الإيجابي، بل قد ينعقد الإختصاص ويطبق قانون دولة ثالثة متى كانت الجريمة ماسة بمصالحها

[1] فايز محمد راجح غلاب، مرجع سابق، ص 382.

[2] مرجع نفسه، ص 383.

الحيوية وذلك طبقا لمبدأ العينية[1]، فهذه الإشكالية حاول كل من الفقه والقضاء والتشريع المقارن إيجاد حلولا لها كما سنرى لاحقا.

من بين الأمثلة تنازع القوانين في هذه الجريمة يمكن أن نفترض مثلا أن يقوم شخص يقطن بالجزائر بإقتحام الحسابات الخاصة بالمؤسسات المالية لعديد من الدول لنفرض مثلا المؤسسات المالية في الدول الأتية (تونس، مصر، المغرب، ليبيا)، حيث يقوم الجاني بتطوير فيروس وزرعه في الحواسيب الخاصة بهذه المؤسسات وسرقة الحسابات البنكية لهم، ففي هذه الحالة نلاحظ أن الركن المادي قد توزع بين عدة دول حيث كان السلوك الإجرامي في الجزائر أما النتيجة فتحققت في كل من الدول الأتية (تونس ، مصر، المغرب و ليبيا)، ففي هذا المثال يقع تنازع من ناحية القوانين، بحيث في هذه الحالة يكون القضاء الجزائري مختصا في النظر في القضية وفقا لمبدأ الإقليمية، وكذلك القضاء التونسي والمصري والمغربي والليبي وفقا لمبدأ العينية، ففي هذه الحالة نطرح التساؤل ما هو القانون الواجب التطبيق في هذه الحالة بإعتبار أن الجريمة توصف بأنها جريمة إلكترونية تمت عن طريق الحاسوب ومست العديد من الدول ؟.

إن إعمال السريان المكاني للقانون الجنائي وفقا لاحد المبادئ المعمول بها ، لا يخلو من الصعوبات التي تفضي إلى إثارة تنازع إيجابي في الإختصاص بين أكثر من تشريع وطني، وأيضا قيام تنازع سلبي في الإختصاص يخرج معه إختصاص أي من الدول بملاحقة الجاني، وهذا النوع الأخير من التنازع نادر الوقوع لأن التشريعات الوطنية تعقد إختصاصها وفقا لمعايير الإختصاص المعروفة، ففي حالة قيام تنازع إيجابي في الإختصاص بين أكثر من دولة لملاحقة نفس النشاط الإجرامي، أو في حالة يثور فيها التنازع كما في الجرائم عبر الوطنية(مثل الجرائم الإلكترونية) التي يتوزع فيها السلوك الإجرامي المادي للجريمة في إقليم أكثر من دولة، أو في حالة تجرد بعض عناصر هذا السلوك من خصيصتها المادية، كما هو الحال في القرصنة في مجال الحوسبة، وصور

[1] برتيل علي، مدوري نبيل، يعلاوي زهر الدين، القانون الواجب التطبيق على الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد لمين دباغين، سطيف 2023/2022، ص 17.

المساهمة الجنائية التي تتم بإستخدام أجهزة الإتصالات الحديثة، مثل هذه الظاهرة تفرض تنازعا في الإختصاص بل غموضا في تحديد معياره[1].

ومن القضايا التي لفتت النظر إلى هذه المشكلة قضية (R.V.THOMP-SON) وتتلخص وقائعها في قيام مبرمج إنجليزي يعمل في أحد البنوك بدولة الكويت بالتلاعب في نظام الحاسوب الالي الخاص بالبنك، لإجراء خصومات في أرصدة العملاء ثم يودعها في حسابه الخاص، وبعد رجوع المتهم إلى بلده بإنجلترا يراسل البنك الذي يعمل فيه، سائلا إياه تحويل الحساب الخاص به إلى عدة حسابات بنكية في إنجلترا، وهو ما قام به البنك بالفعل، وبعد ذلك قدم للمحكمة بتهمة الحصول على أموال الغير بطرق الإحتيال (المادة 15 من القانون الإنجليزي المجرم لفعل السرقة لعام 1968) وحكم عليه بعقوبة السجن إلا أنه طعن في الحكم إستنادا إلى عدم إختصاص القضاء الإنجليزي بالفصل في الجريمة، حيث أن فعلي السحب والإيداع تما بدولة الكويت وليس في إنجلترا، وقد رفضت محكمة الاستئناف الطعن المقدم منه، وجاء في حيثيات رفضها أن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل، وما أسفر عنه من حصوله على الاموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية[2].

[1] عبد الله العجمي الدغشي، مرجع سابق، ص 95.

[2] جمال محمد خلفان محمد النقبي، سلطان محمد سالم عوض هيسان المصعبي، "**التعاون الوطني والدولي في الجرائم الإلكترونية المشكلات والحلول**"، مجلة المعهد العالي للدراسات القانونية، المجلد 3، العدد 16، 2023، ص 5504-5505.

## المبحث الثاني: الحلول المقترحة لمواجهة إشكالية تحديد القانون الواجب التطبيق على الجريمة الإلكترونية

بذلت التشريعات الوطنية جهودا كبيرة في سبيل البحث عن حلول لمجابهة هذه الظاهرة وما تثيره من الإشكاليات قانونية، ومن أبرزها التي واجهها المشروعون هي القانون الواجب التطبيق على هذه الجريمة، فحاولت بعض التشريعات لتقديم بعض الحلول بخصوص مشكلة الإختصاص القضائي وبالتبعية مسألة القانون الواجب التطبيق، فكان للفقهاء نصيب من الحلول الفقهية والقضائية المقترحة بشأن النص الجنائي الواجب التطبيق (المطلب الأول)، وايضا كان للقانون الدولي والداخلي لبعض الدول العديد من المواقف بخصوص مسألة القانون الواجب التطبيق على الجريمة الإلكترونية (المطلب الثاني).

### المطلب الأول: الحلول الفقهية والقضائية المقترحة بشأن النص الجنائي الواجب التطبيق على الجريمة الإلكترونية

حاول فقهاء القانون الجنائي وكذا بعض التشريعات من خلال الإجتهادات القضائية إلى التوصل لحل لمعضلة تنازع القوانين الإجرائية من حيث المكان بخصوص الجريمة الإلكترونية، بإعتبار أن هذه الأخيرة جريمة لا تحدها حدود جغرافية، ويمكن أن يصيب الضرر الناتج عنها عدة دول في أن واحد، عليه قدم بعض الفقهاء حلولا فقهية للتغلب على هذه الإشكالية (الفرع الأول)، وكذا قدمت بعض التشريعات حلول في هذا الشأن(الفرع الثاني).

## الفرع الأول: الحلول الفقهية

بإعتبار الجريمة الإلكترونية جريمة عابرة للحدود، فهذه الخاصية تثير في غالب الأحيان مسألة تنازع القوانين من حيث المكان، ولقد حاول الفقه الوصول إلى حل للتغلب على هذه الإشكالية و إنقسم الرأي في هذا الشأن إلى مذهب السلوك او النشاط الإجرامي بوصفه معيار لتحديد مكان إرتكاب الجريمة (أولا)، مذهب مكان تحقق النتيجة كمناط لتحديد الاختصاص وبالتبعية تحديد القانون الواجب التطبيق (ثانيا)، المذهب المختلط الذي أخذ بكلا المذهبين (ثالثا).

### أولا- مذهب السلوك أو النشاط الإجرامي بوصفه معياراً لتحديد مكان وقوع الجريمة

ينعقد الاختصاص وفقاً لهذا المعيار في المحكمة التي يقع في نطاقها النشاط الإجرامي، وليس مكان حصول النتيجة أو الآثار المترتبة عليه، فعلى سبيل المثال إذا قام شخص من الجزائر بإرتكاب جريمة التهديد والإبتزاز والتشهير الإلكتروني ضد شخص يقطن بدولة أخرى ولتكن مثلا دولة تونس، فوفقا لهذا المعيار القانون الواجب التطبيق هو القانون الجزائري بإعتبار أن السلوك الإجرامي كان في الجزائر والنتيجة تحققت في دولة تونس.

ولقد دافع أنصار هذا الإتجاه عن موقفهم بدعوى أن اتخاذ آثار الفعل (النتيجة الإجرامية) كمناط لتحديد مكان وقوع الجريمة تكتنفه بعض الصعوبات ؛ يمكن إجمالها في أنه معيار مرن وفضفاض ، فضلاً عن أن حصول النشاط الإجرامي كمعيار لتحديد مكان إرتكاب الجريمة يعتبر الأنسب من الناحية الإجرائية حيث يسهل عملية الإثبات وجمع أدلة الجريمة، وأيضا المحكمة التي لها ولاية نظر الدعوى تكون قريبة من مسرح الجريمة[1].

يضيف المؤيدون لهذا المنهج، أن الضرر الذي يحدث في مكان محدد غالبا ما يكون نتيجة لعوامل خارجة عن إرادة الفاعل، وكذلك تطبيق قانون الدولة التي يحدث فيها الضرر قد لا يتوافق مع اعتبارات العدالة نظراً لجهل الجاني بهذا القانون الذي يتم إعماله بحقه ، وفي الغالب ليس ممكناً

[1] موسى مسعود أرحومة، **الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية**، ورقة بحثية مقدمة إلى المؤتمر المغاربي حول (المعلوماتية والقانون)،أكاديمية الدراسات العليا، طرابلس، ليبيا، يومي 28 و 2009/10/29، منشور على الموقع الإلكتروني https://iefpedia.com، تم الإطلاع عليه بتاريخ 2024/04/24 على الساعة 17.30، ص 15.

العلم به، إذ حينما أقدم على ارتكاب الفعل الذي أتاه يعتقد مشروعيته وفقاً لقانون البلد الذي وقع فيه السلوك ، وإذا به غير ذلك من منظور قانون البلد الذي تحقق فيه الضرر.

وقد نال هذا الاتجاه تأييدا واسعا من الفقهاء في كل من فرنسا أو مصر، وليس هذا فحسب ، بل قامت بعض التشريعات المقارنة بتبنيه، ومن هذا القبيل القانون الدولي الخاص النمساوي الصادر سنة 1979 والمجري الصادر في السنة ذاتها[1].

فهذا الإتجاه يشوبه نوع من العيوب، نجملها في أن الجريمة الإلكترونية عكس الجرائم التقليدية التي يمكن أن يطبق فيها هذا المعيار للتخلص من التنازع الواقع، لكن بخصوص الجريمة الإلكترونية فكثير من الأحوال يتوزع النشاط الإجرامي و يشترك فيه كثير من الفاعلين بإختلاف مكانهم فعلى السبيل المثال يمكن أن يشترك الفاعلون في إرتكاب جريمة واحدة مثل جرائم الإختراق ومن اماكن متفرقة مثل الجزائر و تونس و المغرب لهدف تحقيق نتيجة إجرامية واحدة تكون في دولة إسرائيل مثلا. فهنا لا يمكن إعمال هذا المعيار في هذه الحالة وبدورنا لا نميل إلى هذا المعيار لحل هذه الإشكالية.

**ثانيا- مذهب مكان تحقق النتيجة كمناط لتحديد الاختصاص وبالتبعية تحديد القانون الواجب التطبيق**

واجه الإتجاه الأول (مذهب السلوك أو النشاط الإجرامي بوصفه معياراً لتحديد مكان وقوع الجريمة) الكثير من الانتقادات من جانب فريق أخر من الفقه، بالرغم من الحجج التي ساقها مؤيدو المذهب الأول، وتركزت هذه الانتقادات على أن هذا المذهب لم تول إهتماما كافيا للمكان الذي وقع فيه الضرر أو للأثر الذي كان الجاني يسعى لتحقيقه، فالآثار الضارة هي التي تبعث الفزع في نفوس الناس، بينما يعتبر مكان وقوع الفعل مجرد مصدر للضرر ليس إلا، كما أن تمام الجريمة لا يكون إلا في المكان الذي ظهرت فيه آثارها الضارة التي كان الجاني يقصدها أو يرغب في تحقيقها، والجدير بالإشارة أنه من بين الأسباب التي قدمت لدعم هذا الإتجاه أنه يحقق وحدة الجريمة ولا

[1] نفس المرجع، ص 15.

الفصل بين عناصرها، وكذلك يعتبر هذا الاتجاه في نظر المدافعين عنه بأنه أكثر واقعية على اعتبار أن الضرر له مظهر خارجي ملموس خلافاً للنشاط الذي قد لا يكون كذلك متى ما اتخذ صورة الامتناع أو السلوك السلبي، وتجدر الإشارة أن هذا الإتجاه لقي ترحيبا من بعض الفقه إلى جانب ذلك تم تبنيه من بعض التشريعات المقارنة ، ومنها القانون الألماني الصادر في 5 ديسمبر 1975[1].

وبخصوص رأينا في هذا الإتجاه، أننا لا نتفق معه إلى حد ما، وحجتنا في ذلك أن هناك بعض الأفعال التي تتم عبر الوسائل الإلكترونية تكون مشروعة في موطن الفاعل، بينما في مكان تحقق النتيجة تكون غير مشروعة ومثال ذلك إنتحال الهوية الرقمية في ببعض الدول يعتبر سلوك مشروع بينما في المقابل هناك بعض من دول تجرم هذا الفعل، وأيضا جريمة التمييز وخطاب الكراهية.

**ثالثا- المذهب المختلط**

في ظل الإنتقادات التي وجهت للمنهجين السابقين، ظهر منهج ثالث يقر أن الجريمة تعد واقعة في مكان حصول النشاط (العمل التنفيذي)، وكذلك المكان الذي تحققت فيه النتيجة أو الذي من المتوقع أو من المنتظر تحققها فيه، ونال هذا الاتجاه الغالبية العظمى من الفقهاء، ويجد مبرره في أن الركن المادي للجريمة يقوم على ثلاثة عناصر، وهي (الفعل (النشاط) ، والنتيجة ، وعلاقة السببية)، ما يعني أن الجريمة تعد واقعة في كل مكان تحقق فيه عنصر من عناصر الركن المادي، أي في مكان النشاط ومكان النتيجة على حد سواء .

وهذا الاتجاه أخذت به بعض التشريعات المقارنة، ومنها قانون العقوبات النرويجي وكذلك الدنماركي، والصيني والألماني والإيطالي لسنة 1930[2]، وكذلك الأمر بالنسبة لقانون العقوبات الجزائري.

خلاصة لما سبق ومن خلال عرضنا للمناهج الثلاثة و الحلول التي قدموها بشأن مسألة تنازع القوانين الإجرائية من حيث المكان، نرى في هذا الصدد أن المعيار المختلط هو الأنسب لحل هذه

[1] عراب مريم، "**الإختصاص القضائي في الجرائم المعلوماتية**"، مجلة حوليات كلية الحقوق والعلوم السياسية، المجلد07، العدد 03 كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد، وهران، 2015، ص 278.

[2] موسى مسعود ارحومة، مرجع سابق، ص 16.

الإشكالية، حيث جمع ميزات كلا من المذهبين، ووسع من مجال الإختصاص وهو ما يتطابق مع الطبيعة الخاصة للجرائم الإلكترونية التي في كثير من الأحيان يتوزع نشاطها الإجرامي و كذا النتيجة الإجرامية على أماكن متفرقة.

وقد تصدى جانب أخر من الفقه الجنائي لمسالة تحديد الدولة صاحبة الولاية القضائية في متابعة الجناة حيث استندوا إلى معيارين وهما:

- **معيار القانون الأكثر ملائمة** : أي اختصاص الدولة الأكثر عرضة للأعمال الإجرامية، حيث إعتمد أصحاب هذا الاتجاه على مدى الضرر الذي سببته الجريمة الإلكترونية، فإذا امتد هذا الضرر لأكثر من دولة، ففي هذه الحالة يرى في التفاوت الحاصل في نسبة الضرر بين الدول المتضررة، ويكون الاختصاص للدولة الأكثر تضررا من هذه الجريمة، إلا أن ما يعاب على هذا المعيار هو محدوديته في التعامل مع كل حالات الضرر الذي تسببت فيه الجريمة الإلكترونية، لأنه قد يتساوى الضرر لدى أكثر من دولة.

- **معيار الضرر المرتقب:** أي الضرر الذي تتسب فيه الجريمة المرتكبة عبر الإنترنت يمكن أن يحدث في أي دولة تكون متصلة بالمجال الرقمي، لأن وجهة الجريمة الإلكترونية غير معين ومحدد، الأمر الذي قد تتضرر منه العديد من الدول بنفس المستوى من الضرر، وبالتالي نكون أمام وضعية يستحيل معها تطبيق قوانين الدول المتضررة على الواقعة، لذلك يرجع الاختصاص إلى محاكم الدولة التي ارتكبت فيها الجريمة الإلكترونية، وهذا التوجه هو الذي أكد عليه المجلس الأوربي للعدل في أحد قراراته حيث جاء فيه أن المعلومات المنشورة في شبكة الإنترنت يمكن معاينتها من قبل جميع الدول الموصولة بها ومن دون أن تكون موجهة بالضرورة محددة، لكن طبيعة هذه الوسيلة الإعلامية الجديدة لا يجب أن ينتج عنها تطبيق لجميع القوانين الموجودة بل يجب أن نطبق معيار الارتقاب على المسئول عن المعلومات الضارة فيها[1].

[1] جمال زين العابدين أمين أحمد، "**الإختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية، "دراسة مقارنة""**، مجلة مستقبل العلوم الإجتماعية، العدد 04، جامعة عبد الملك السعدي، المغرب،2021، ص ص 76-135، ص 91.

**الفرع الثاني: الحلول القضائية:**

نال القضاء كذلك نصيبه في محاولة الوصول لإيجاد حل لمشكلة تنازع القوانين بخصوص الجريمة الإلكترونية، فمن خلال هذا الفرع سنحاول عرض بعض السوابق القضائية في هذا الشأن بالنسبة للقضاء الأمريكي (أولا)، القضاء الإنجليزي (ثانيا)، القضاء الفرنسي (ثالثا).

**أولا: بالنسبة للقضاء الأمريكي**

من السوابق القضائية التي شهدتها محاكم الولايات المتحدة في هذا الصدد، قضى قضاء مسيوتا بخصوص قضية بث موقع ألعاب القمار عبر الأنترنت من لاس فيغاس بولاية نيفادا على تجريم الفعل طالما أن ولاية مسيوتا يحظر قانونها مثل هذه الألعاب، فقد إعتبر أن القانون الواجب التطبيق هو القانون الأمريكي في حالة ما إذا تحققت أثار الجريمة في الولايات المتحدة، إضافة إلى أنه يكفي لإمتداد ولاية القضاء الأمريكي إلى جريمة وقعت في الخارج، إذا كانت أثارها مست مصالح أمريكية أو عرضتها للخطر[1].

**ثانيا: بالنسبة للقضاء الإنجليزي**

نص قانون مكافحة إساءة إستخدام الحاسب البريطاني على بعض المعايير التي تساهم في تحديد مكان وقوع الجرائم الإلكترونية وبما ينسجم مع الطبيعة الخاصة لهذه الجرائم، وبالشكل الذي من شأنه أن يساعد في تذليل الصعوبات التي تواجه المحاكم عند تحديد مكان إرتكاب الجريمة الإلكترونية، حيث نص في هذا الصدد على مكان إرتكاب جريمة تعديل مواد الحاسب الألي غير المصرح بها، والذي يتحدد بمكان بدء السلوك الإجرامي، وفي نفس السياق نص على أن مكان إرتكاب جريمة التحريض عبر الشبكة المعلوماتية لا يكون بمكان إرتكاب السلوك، بل بمكان تحقق

[1] خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2019، ص 131-132.

النتيجة الإجرامية، فيطبق القانون الإنجليزي ويكون القضاء البريطاني مختصا وفقا للمادتين (3 و 4) طالما هناك إرتباطا بين الواقعة وبريطانيا[1].

**ثالثا: بالنسبة للقضاء الفرنسي**

أيضا كان للقضاء الفرنسي مجموعة من الاجتهادات في مجال تحديد مكان إرتكاب الجريمة، فبخصوص جرائم الصحف المرتكبة عبر الشبكة المعلوماتية يحدد مكان إرتكابها بمحل تمركز الموقع الذي تم نشر الأقوال أو الأفعال أو المعلومات بواسطته، أي المكان الذي تم التلفظ فيه بالتهديد وليس في الدول التي نقل فيها الخبر عبر التلفاز او الصحافة المكتوبة أو الإلكترونية والتي من خلالها علم الشخص، أما بالنسبة للجرائم الماسة بحقوق الملكية الفكرية فقد إعتبر مكان إرتكابها بالمكان الذي إرتكب فيه التقليد مكان نشره أو معيار إمكانية الوصول للموقع كأساس لاختصاص المحكمة في حالة الإعتداء على حقوق المؤلف، بواسطة الشبكة المعلوماتية[2].

في هذا الصدد صدر قرار عن الغرفة الجنائية بمحكمة النقض الفرنسية بتاريخ 8 ديسمبر 2009 اعتبر في إحدى حيثياته " أن مكان ارتكاب الجريمة هو المكان الذي تم فيه التلفظ بالتهديد (توجيه التهديد) و ليس في الدول التي نقل الخبر فيها عبر التلفاز أو الصحافة المكتوبة أو الإلكترونية و التي من خلالها علم الشخص "[3].

وفي سياق ذات صلة صدر قرارين عن محكمة النقض الفرنسية بخصوص الإختصاص في الجرائم المرتبطة بحقوق الملكية الفكرية، حيث صدر الأول بتاريخ 9 ديسمبر 2003 قبلت من خلاله اختصاص محكمة فرنسية للنظر في إصلاح الضرر الناتج عن جريمة تقليد علامة تجارية في موقع إسباني و لكنه قابل للوصول إليه من فرنسا و رفضت الدفع المثار من أجل عدم إختصاص القضاء الفرنسي"، و صدر الثاني بتاريخ 5 أبريل 2012 اعتبرت فيه أن التقليد المتنازع بشأنه تم نشره على

[1] يوسف قجاج، الجريمة الإلكترونية وإشكالية الإختصاص القضائي- مكان إرتكاب الجريمة الإلكترونية نموذجا- المفهوم الجديد لمكان إرتكاب الجريمة الإلكترونية، مقال منشور على الموقع الإلكتروني https://www.mrlatalib.com تم الإطلاع عليه بتاريخ 24-04-2024 على الساعة 17.35.

[2] أسامة أحمد محمد النعيمي، هايس سويلم صلبي الشمري، مرجع سابق، ص 117.

[3] مرجع نفسه.

موقع للأنترنيت يمكن الوصول إليه من فرنسا، و بالتالي فإن القضاء الفرنسي هو صاحب الإختصاص في النازلة "، و في نفس الإتجاه ذهبت محكمة الاستئناف بباريس من خلال القرار الصادر عنها بتاريخ 25 شتنبر 2007 إلى القول " بأن القانون الجنائي الفرنسي هو المطبق و القضاء الفرنسي هو المختص في واقعة التقليد التي قام بها موقع إيطالي و رفضت الدفع المثار بعد إختصاص المحاكم الفرنسية على اعتبار غياب أي فعل مكون للجريمة تحقق في الأراضي الفرنسية و أن الطرف المدني الوحيد هو من جنسية إيطالية[1].

[1] يوسف قجاج، الجريمة الإلكترونية وإشكالية الإختصاص القضائي– مكان إرتكاب الجريمة الإلكترونية نموذجا– المفهوم الجديد لمكان إرتكاب الجريمة الإلكترونية، مرجع سابق.

## المطلب الثاني: موقف القانون الدولي والداخلي لبعض الدول بخصوص مسألة القانون الواجب التطبيق للجريمة الإلكترونية

يسعى القانون الدولي للوصول إلى توازن بين حماية سيادة الدول وتوفير إطار فعال لمجابهة الجرائم الإلكترونية العابرة للحدود، وذلك من خلال تعزيز التعاون الدولي وتطوير التشريعات المتناسبة مع التطورات التكنولوجية، وإلى جانب ذلك تتبنى التشريعات في مختلف الدول مواقف متنوعة بخصوص معالجة مسألة القانون الواجب التطبيق على الجريمة الإلكترونية العابرة للحدود، فهناك تعارض فيما بينها بخصوص القانون الواجب التطبيق مستندة إلى مبادئ قانونية مختلفة مثل مبدأ الإقليمية و الشخصية والعينية إضافة إلى مبدأ العالمية الذي أصبح معمول به من طرف بعض التشريعات، فكان موقف القانون الدولي من مسألة القانون الواجب التطبيق على الجريمة الإلكترونية ظاهرا عن طريق العديد من الإتفاقيات الدولية والإقليمية(الفرع الأول)، وكذا موقف القانون الداخلي من مسألة القانون الواجب التطبيق على الجريمة الإلكترونية مثلما هو الحال للتشريع المصري والجزائري(الفرع الثاني).

### الفرع الأول: موقف القانون الدولي من مسألة القانون الواجب التطبيق على الجريمة الإلكترونية

إن إشكالية القانون الواجب التطبيق على الجريمة الإلكترونية يستوجب البحث على موقف القانون الدولي منها والحل الذي اقترحه بشأنها من خلال الإتفاقيات الدولية والإقليمية.

من بينها إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية (أولا)، القانون العربي النموذجي لمكافحة تقنية أنظمة المعلوماتية (ثانيا)، إتفاقية بودابست (ثالثا)، الإتفاقية العربية لمكافحة جرائم تقنية المعلومات (رابعا).

#### أولا: إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية

بالرجوع إلى إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للوطنية، فإنها فصلت في هذه المسألة بنصها من خلال المادة 15 منها وفقا لما يلي " يتعين على كل دولة طرف أن تعتمد ما قد يلزم من تدابير لتأكيد سريان ولايتها القضائية على الجرائم المقرر في الحالات الأتية:

- عندما يرتكب الجرم في إقليم تلك الدولة
- عندما يرتكب الجرم ضد أحد مواطني تلك الدولة
- عندما يرتكب الجرم أحد مواطني تلك الدولة"[1].

فهذه الإتفاقية ركزت على مبدأ الإقليمية و مبدأ الشخصية في المقابل لم تأخذ هذه الإتفاقية بمبدأ العينية.

**ثانيا: القانون العربي النموذجي لمكافحة تقنية أنظمة المعلوماتية**

أما بخصوص القانون العربي النموذجي فقد أخذ بمبدأ إقليمية النص الجنائي في تحديد القانون الواجب التطبيق بالنسبة لجرائم الكمبيوتر و الأنترنت، بالإضافة إلى مبدأ العينية وطبقا لهذا المبدأ يمتد التشريع الجنائي للدولة ليطبق على الجرائم التي ترتكب في الخارج بصرف النظر عن جنسية مرتكبها، حيث يستند هذا الامتداد إلى ما للدولة من حق في الدفاع الذاتي ضد كافة صور الإعتداء على مصالحها الأمنية والمالية ولو وقعت خارج إقليمها خاصة و أن السلطات الأجنبية التي وقعت هذه الجرائم فوق إقليمها قد تتقاعس عن العقاب عليها[2].

لذلك فلقانون العربي النموذجي لمكافحة تقنية أنظمة المعلوماتية لم يأخذ بمبدأ الشخصية.

**ثالثا: إتفاقية بودابست لمكافحة الجريمة المعلوماتية**

بالرجوع إلى إتفاقية بودابست نجد أن الباب الثالث بعنوان الإختصاص القضائي نص في المادة 22 منها على أن:"

- يعتمد كل طرف ما قد يلزم من تدابير تشريعية وتدابير أخرى وذلك لإقرار الإختصاص بشأن أي جريمة تنص عليها المواد من 02 إلى 11 من هذه الإتفاقية وذلك عندما ترتكب الجريمة: ( في إقليمه، على متن إحدى السفن ترفع علم ذلك الطرف، على متن إحدى الطائرات المسجلة بموجب

[1] إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من قبل الجهة العامة لمنظمة الامم المتحدة، بتاريخ 15 نوفمبر 2000 تمت المصادقة عليه من طرف الجزائر بتحفظ، بموجب المرسوم الرئاسي رقم 02-55 المؤرخ في 05 فبراير 2002.

[2] عبد الفتاح بيومي حجازي، مرجع سابق، ص 50.

قوانين ذلك الطرف، من جانب أحد مواطنيه، إذا كانت الجريمة معاقبا عليها بموجب القانون الجنائي بمكان إرتكابها، أو في حالة إرتكاب الجريمة خارج الإختصاص القضائي الإقليمي لأي دولة)

- يجوز لكل طرف الإحتفاظ بالحق في عدم تطبيق، أو التطبيق فقط في حالات أو بشروط معينة قواعد الإختصاص المنصوص عليها في الفقرات (ب-د)

- يعتمد كل طرف ما قد يلزم من تدابير تشريعية و تدابير أخرى وذلك لإقرار الإختصاص القضائي بشأن الجرائم المشار إليها في المادة (02/23) من هذه الإتفاقية، وفي الحالات التي يكون فيها الجاني المزعوم موجودا في إقليمه، ولا يقوم بتسليمه أو تسليمها لطرف أخر على سند جنسيته أو جنسيتها، وذلك بعد طلب التسليم.

- لا تستبعد هذه الإتفاقية أي إختصاص جنائي يمارسه أحد الأطراف وفقا لقانونه الوطني

- في حالة مطالبة أكثر من طرف من الأطراف بالإختصاص القضائي بشأن جريمة ما تقرها هذه الإتفاقية يقوم الأطراف المعنيون، متى كان ذلك ملائما بالتشاور بغرض تحديد الإختصاص القضائي الأكثر ملائمة للمحاكمة"[1].

وفقا لهذه المادة، وحتى لا يفلت مرتكبو الجرائم من العقاب بسبب النزاعات التي قد تنشأ بين الدول بشأن من لديه سلطة متابعة مرتكبي هذه الجرائم، تسعى الدول الأطراف في اتفاقية بودابست إلى الاتفاق على دولة تتحقق شرط الأفضلية في ممارسة الإختصاص القضائي على الجريمة الإلكترونية وهو ما يسميه الفقه الإختصاص طبقا للكفاءة الإفتراضية نسبة للمسرح الإفتراضي الذي ترتكب فيه هذه الجريمة[2].

**رابعا: الإتفاقية العربية لمكافحة جرائم تقنية المعلومات**

نصت المادة 30 من الفصل الرابع بعنوان التعاون القانوني والقضائي للإتفاقية العربية لمكافحة جرائم تقنية المعلومات على أن " تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد

[1] إتفاقية بودابست، (مكافحة الجرائم المعلوماتية المنبثقة عن اجتماع المجلس الأوروبي ببودابست)، بتاريخ 21/ نوفمبر/ 2001، المجر رقم 185.

[2] جمال زين العابدين أمين أحمد، مرجع سابق، ص 89.

إختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الإتفاقية وذلك إذا إرتكبت الجريمة كليا أو جزئيا أو تحققت:

-في إقليم الدولة الطرف

-على متن سفينة تحمل علم الدولة الطرف

-على متن طائرة مسجلة تحت قوانين الدولة الطرف

-من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان إرتكابها أو إذا إرتكبت خارج منطقة الإختصاص القضائي لأية دولة

-إذا كانت الجريمة تمس أحد المصالح العليا للدولة "[1].

في حين أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات قد منحت للبلدان المتضررة الحق في متابعة مرتكبي الجرائم الإلكترونية، فإن هذه المتطلبات تكون عاجزة عن تحديد الجهة التي يعود لها الاختصاص القضائي للنظر في الجريمة في حالة تضرر أكثر من دولة[2].

**الفرع الثاني: موقف القانون الداخلي من مسألة القانون الواجب التطبيق على الجريمة الإلكترونية**

بعد التعرض لموقف الفقه والقضاء حول هذه المسألة كان لا بد أن يكون للقانون الداخلي موقف هو الأخر، موقف المشرع الجزائري (أولا)، موقف المشرع المصري (ثانيا).

**أولا: موقف المشرع الجزائري من إشكالية تنازع الإختصاص القضائي وبالتبيعة القانون الواجب التطبيق**

تناول المشرع الجزائري مسألة الإختصاص القضائي بأن الأصل هو أن المحاكم الجزائرية تكون هي صاحبة الاختصاص الأصيل بالنظر في الجرائم الإلكترونية والتي يقع على إقليمها السلوك الإجرامي كله أو جزء منه، بغض النظر عن شخص المتهم وهو المبدأ المنصوص عليه في المادة

[1] الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن إجتماع مجلس وزراء الداخلية والعدل العرب بصفة مشتركة بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، صادقت الجزائر على الإتفاقية العربية عن طريق المرسوم الرئاسي رقم 14-252 بتاريخ ديسمبر سنة 2010.

[2] جمال زين العابدين أمين أحمد، مرجع سابق، ص 90.

الثالثة (03) الفقرة الأولى من قانون العقوبات الجزائري، حيث يعتبر هذا المبدأ مظهرا من مظاهر سيادة أي دولة، ويسمى بمبدأ إقليمية النص الجنائي والمقصود منه مثلما أشرنا سابقا أن القانون الجزائي لدولة ما يطبق على كل جريمة ترتكب على إقليم هذه الدولة سواء كان الجاني يحمل جنسية هذه الدولة أم يحمل جنسية دولة أجنبية وسواء كان المجني عليه مواطنا أم أجنبيا، فهذا المبدأ هو الأصل الذي تعمد الدولة من خلاله حماية مصالحها على الإقليم الوطني.

كذلك وفقا لنص المادة 586 من القانون رقم 17-07 المؤرخ في 27 مارس 2017 المعدل والمتمم لقانون الإجراءات الجزائية فإن المشرع الجزائري وضع أحكاما خاصة تطبق في حالة تعدد أقاليم إرتكاب الجريمة حيث نصت " تعد مرتكبة في الإقليم الجزائري كل جريمة يكون عمل من الأعمال المميزة لأحد أركانها المكونة لها قد تم في الجزائر".

وعليه يمكن القول أن القانون العقوبات الجزائري هو الذي يطبق على الكثير من الجرائم المتعلقة بالأنترنت، طالما أن أحد العناصر المكونة للجريمة قد وقع على هذا الإقليم، ففي جريمة نشر صور إباحية وبثها عبر شبكة العنكبوتية، فإن القانون الجزائري هو الذي يطبق بصرف النظر عن الدولة التي وقعت فيها طالما أنه يمكن الدخول إليها من الجزائر، فتلقي مستخدم الأنترنت لهذه الصورة على الإقليم الوطني يعتبر من أحد العناصر المكونة للجريمة[1]، أما في حالة ما إذا شكلت الإعتداءات تهديدا لمصالحها وخارج حدود إقليمها لابد من إعمال مبادئ استثنائية مثلما هو متعارف عليه في باقي التشريعات حماية لمصالحها و مواطنيها، وبالمقابل احترام و عدم الإعتداء على سيادة دولة أخرى[2].

فكان موقف المشرع الجزائري بخصوص الجريمة الإلكترونية التي يمتد سلوكها خارج الإقليم الجزائري وتمس بمصالحها، أنه أخذ بمبدأ العينية حيث نص في المادة 15 من القانون 09-04 على أنه" أنه وفضلا عن الإختصاص المنصوص عليه في قانون الإجراءات الجزائية تختص المحاكم الجزائرية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال المرتكبة خارج الإقليم

[1] عبد الفتاح بيومي حجازي، مرجع سابق، ص 45.

[2] بوديسة بجاد عبد الرؤوف، مرجع سابق، ص 83.

الوطني عندما يكون مرتكبها أجانب وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الإستراتيجية للإقتصاد الوطني" [1].

يفهم من إستقراء فحوى المادة السالف ذكرها أن المشرع الجزائري ركز على الجرائم التي تمس بسيادة ومصالح الدولة الجزائرية، و أن المحاكم الجزائرية وحدها تختص بالنظر في الجرائم الإلكترونية وذلك في حالة توفر الشروط التالية:

- أن يتعلق الأمر بجرائم تكنولوجيا الإعلام والإتصال وهي التسمية التي إصطلح عليها المشرع الجزائري على الجرائم الإلكترونية
- أن ترتكب الجريمة في خارج الإقليم الجزائري
- أن يكون الجاني أجنبي
- أن يكون الغرض من الجريمة استهداف مؤسسات الدولة الجزائرية الدفاع الوطني المصالح الإستراتيجية للإقتصاد الوطني.

إن المشرع الجزائري في سبيل حماية مصالح الدولة و مواطنيها أخذ بمبدأ العينية على الجرائم الإلكترونية التي يمتد سلوكها إلى خارج الإقليم الجزائري وبهذا أصاب المشرع بإعماله هذا المبدأ في مجابهة هذا النوع من الجرائم، خاصة وأن السلطات الأجنبية قد تتقاعس عن العقاب عليها، لكن ما يلاحظ ان المشرع الجزائري لم يوسع الحماية لتشمل رعاياها إذا كانوا ضحايا خاصة و أن المشرع الجزائري عدل المادة 588 من خلال القانون رقم 15-02 المعدل والمتمم لقانون الإجراءات الجزائية[2]، لذلك لتوسيع الحماية للرعايا الجزائريين فإنه يتعين قياسا على المادة 15 من القانون 09-04 منح الإختصاص للمحاكم الجزائرية بخصوص الجرائم التي يقع الجزائري في الخارج ضحية لها،

[1] عراب مريم، مرجع سابق، ص ص 285-286.

[2] المادة 588 من القانون العقوبات المعدلة والمتممة بالقانون رقم 15-02 المؤرخ في 23 يوليو2015 على أنه: " يجوز متابعة ومحاكمة كل أجنبي، وفقا لأحكام القانون الجزائري، إرتكب خارج الإقليم الجزائري بصفة فاعل أصلي أو شريك في جناية أو جنحة ضد أمن الدولة الجزائرية أو مصالحها الأساسية او المحلات الدبلوماسية والقنصلية الجزائرية أو اعوانها، أو تزييفها لنقود أو أوراق مصرفية وطنية متداولة قانونا في الجزائر أو أي جناية أو جنحة ترتكب إضرار بمواطن جزائري"

وليس في ذلك إنتهاك لمبدأ الشرعية لأن الأمر يتعلق بقاعدة إجرائية، كل هذا تأسيسا على أن حماية الرعايا هي صورة لحماية مصالح الدولة في الخارج[1].

وفي هذا الإطار وبالرجوع إلى بعض القوانين الخاصة نلاحظ أن المشرع الجزائري مدد هذه الحماية لتشمل رعاياه عندما يكونون ضحايا جرائم معينة مرتكبة في الخارج، إذ بالرجوع إلى نص المادة 21 من القانون رقم 20-05 المتعلق بالوقاية من التمييز و خطاب الكراهية ومكافحتهما نجد أنها نصت على أن "زيادة على قواعد الإختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختص الجهات القضائية الجزائرية بالنظر في الجرائم المنصوص عليها في هذا القانون المرتكبة خارج الإقليم الوطني، إذا كانت الضحية جزائريا، أو أجنبيا مقيما بالجزائر"[2].

**ثانيا: التشريع المصري**

سار المشرع المصري على نفس خطى المشرع الجزائري بالأخذ بمبدأ الإقليمية على الجرائم التي ترتكب داخل الإقليم الوطني، فيطبق قانون العقوبات على أية جريمة تقع داخل الإقليم المصري بغض النظر عن جنسية المتهم أو المجني عليه في هذه الجريمة، ففي هذا الشأن نصت المادة الأولى من هذا القانون على أنه " تسري أحكام هذا القانون على كل من يرتكب في الإقليم المصري جريمة من الجرائم المنصوص عليها فيه"، أما في حالة ما إذا إرتكب جريمة في الإقليم المصري وكان الجاني في الخارج ففي هذا الشأن حسمت المسألة المادة 2 الفقرة 1 من قانون العقوبات المصري التي نصت على أنه " تسري أحكام هذا التشريع على كل من إرتكب في خارج القطر فعلا يجعله فاعلا أو شريكا في جريمة وقعت كلها أو بعضها في القطر المصري"، فيستخلص أن العبرة في تحديد إقليمية القاعدة الجنائية هي بوقوع الجريمة كاملة أو جزء منها على الإقليم المصري (السلوك والنتيجة)، وتجدر الإشارة ان القانون العربي النموذجي أخذ بمبدأ إقليمية النص الجنائي بالنسبة لجرائم الكمبيوتر والأنترنت، إضافة إلى مبدأ العينية وطبقا لهذا المبدأ يمتد التشريع الجنائي

[1] بارش سليمان، مرجع سابق، ص73.

[2] القانون رقم 20-05، المؤرخ في 05 رمضان عام 1441، الموافق لـ 28 أبريل سنة 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية عدد25، المؤرخة في 29 أبريل سنة 2020، ص 07.

للدولة ليطبق على الجرائم التي ترتكب في الخارج بصرف النظر عن جنسية مرتكبيها، ويستند هذا الإمتداد إلى ما للدولة من حق في الدفاع الذاتي ضد جميع صور الإعتداء على مصالحها الأمنية والمالية ولو وقعت خارج إقليمها، خاصة وأن السلطات الأجنبية التي وقعت هذه الجرائم فوق إقليمها قد تتقاعس عن العقاب عليها[1].

وفي نفس السياق بالرجوع لنص المادة الثالثة من قانون رقم 175 لسنة 2018 المتضمن مكافحة جرائم تقنية المعلومات نصت كما يلي " مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على من إرتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها في هذا القانون، متى كان الفعل معاقبا عليه في الدولة التي وقع فيها تحت أي وصف وذلك في أي من الأحوال التالية:

- إذا إرتكب الجريمة على متن أي وسيلة من وسائل النقل الجوي أو البري أو المائي وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها
- إذا كان المجني عليهم أو أحدهم مصريا
- إذا تم الإعداد للجريمة او التخطيط أو التوجيه أو الإشراف عليها او تمويلها في جمهورية مصر العربية
- إذا إرتكب بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية في أكثر من دولة من بينها جمهورية مصر العربية
- إذا كان من شأن الجريمة إلحاق ضرر بأي من مواطني جمهورية مصر العربية أو المقيمين فيها أو بأمنها أو بأي من مصالحها في الداخل أو الخارج
- إذا وجد مرتكب الجريمة في جمهورية مصر العربية، بعد إرتكابها ولم يتم تسليمه[2].

فتطبيق قانون مكافحة جرائم تقنية المعلومات يقتضي إذا الإلتزام بالقواعد الأتية:

[1] عبد الفتاح بيومي الحجازي، مرجع سابق، ص 49-50.

[2] القانون رقم 175، لسنة 2018، المتضمن مكافحة جرائم تقنية المعلومات، سالف الذكر.

- عند وقوع فعل على الإقليم المصري، فإنه يجب الرجوع إلى القانون المصري لمعرفة ما إذا كان الفعل المرتكب يعد جريمة والعقوبة المقررة له، فإن كان الفعل يعد جريمة فعلى القاضي ان يطبق على مرتكب الجريمة العقوبة المقررة في هذا القانون
- عدم تطبيق قواعد أي قانون أجنبي على جريمة من الجرائم الواردة بقانون مكافحة جرائم تقنية المعلومات وقعت على الإقليم المصري.

وعليه إذا وقعت جريمة من هذه الجرائم على إقليم مصري فلا يجوز تطبيق أي قانون خلاف القانون المصري أيا كان مرتكبها أو المجني عليه، وأيا كانت المصلحة المضارة من إرتكاب الجريمة، وهذا يعني أن القانون الوطني يطبق على اي جريمة ترتكب فوق هذا الإقليم بصرف النظر عن جنسية الجاني أو المجني عليه وسواء كانت الجريمة قد هددت مصالح الدولة صاحبة السيادة على الإقليم أو هددت مصالح دولة أجنبية[1].

والجدير بالذكر أيضا أن المشرع المصري من خلال القانون رقم 175 لسنة 2018 المتضمن مكافحة جرائم تقنية المعلومات تبنى مبدأ مغاير لما هو متعارف عليه، وهو مبدأ العينية وجعل أحكام ونصوص هذا القانون تسري على الجرائم المرتكبة (الجرائم المتعلقة بالمصالح الجوهرية للدولة) حتى ولو خارج الإقليم المصري من غير مصريين متى كان معاقبا على ذات الفعل في قانون الدولة التي إرتكبت على أراضيها تحت أي وصف(إزداوجية التجريم )، ولم يكتفي المشرع المصري بهذا فقط بل أخذ من خلال هذا القانون بتطبيق مبدأ عالمية النص الجنائي ولكن بشكل مقيد أي سريان أحكام هذا القانون على هذه الجرائم التي تتعلق بتقنية المعلومات والتي تقع خارج البلاد حتى وإن كان الفاعل غير مصري (الإختصاص السلبي) الذي يسمح للدولة بالمتابعة الجنائية ضد مرتكبي الجرائم على اساس جنسية المجني عليهم، فالجدير بالإشارة أيضا أن البحث في النطاق المكاني لتطبيق قانون مكافحة جرائم تقنية المعلومات من أهم وابرز الأمور التي نظمها المشرع المصري وحرص على النص عليها صراحة و إدراجها ضمن نصوص قانون مكافحة تقنية المعلومات وتبنيه مبدأ العينية

[1] خالد حسن أحمد لطفي، مرجع سابق، ص 161-162.

بدلا من مبدأ الإقليمية وبالتالي إسناد مهمة الإختصاص القضائي للقاضي الوطني، حتى وإن كان لم يرد النص على هذا الإختصاص صراحة فهو أمر يفهم من نص المادة 03 السالفة الذكر[1].

فمن خلال ما سبق نرى أن المشرع المصري كان أكثر توسعا من المشرع الجزائري و أخذ في مواجهة الجريمة الإلكترونية التي تمتد أثارها خارج الإقليم المصري بمبدأ العينية، حيث إختلف عن المشرع الجزائري من خلال تفعيله لمبدأ العالمية و هنا نظن أن المشرع المصري كان أدق من المشرع الجزائري في سبيل البحث في النطاق المكاني لتطبيق القانون الوطني وتوسيع نطاق تطبيق قانونه.

[1] حاتم أحمد محمد بطيخ، "**تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات**"، مجلة الدراسات القانونية والإقتصادية، المجلد 07، العدد 01، جامعة عين شمس مصر، 2021، ص ص 30-31.

يتجلى من خلال دراستنا لموضوع إشكالية القانون الواجب التطبيق على الجريمة الإلكترونية، أن هذه الجريمة تعتبر من بين الجرائم التي أثارت جدلا واسعا بين فقهاء القانون الجنائي ورجال القضاء و أغلب التشريعات الوطنية ، فالجريمة الإلكترونية جريمة وليدة للتطورات التكنولوجية التي لم يستطيع أي مشرع مسايرتها، مما نتج عنه العديد من الإشكاليات التي واجهتها مختلف التشريعات لعل أبرزها مدى قدرة القواعد التقليدية على مواكبة الجريمة الإلكترونية من ناحية النص الجنائي الواجب التطبيق.

على ضوء الإشكاليات التي أظهرتها الدراسة خلصت في الإجابة عنها إلى جملة من النتائج تمثلت فيما يلي:

- أن فقهاء القانون الجنائي واجهوا صعوبة في وضع تعريف لهذه الجريمة لدرجة أنه وصفت هذه الجريمة بأنها جريمة تقاوم التعريف، ففي إطار وضع تعريف للجريمة الإلكترونية الفقهاء إلى فريقين، فريق يضيق من نطاقها بتعريفه لها مركزين في ذلك على الوسيلة المستخدمة لإرتكاب هذه الجريمة إلى جانب اشتراطهم ان يتوفر في المجرم الإلكترونية المعرفة التقنية في مجال الحاسوب، وفريق يوسع من نطاق الجريمة الإلكترونية لتشمل كل الأفعال الإجرامية المرتكبة في البيئة الإلكترونية.
- المشرع الجزائري وفي سبيل مجابهة هذه الجريمة قام بتعديل قانون العقوبات بمقتضى القانون رقم 04-15 وإدراجه لقسم يتضمن 08 مواد عن طريقها تم تجريم ما أسماه بـ "المساس بأنظمة المعالجة الألية للمعطيات"، إلى جانب هذا قام بإصدار قانون خاص مستقل وهو القانون رقم 09-04 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، من خلاله إصطلح على الجريمة الإلكترونية بإسم الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال، وعرفها من خلال المادة 02 من هذا القانون الجريمة الإلكترونية على جرائم المساس بأنظمة المعالجة الألية للمعطيات المحددة في قانون العقوبات بالإضافة إلى كل جريمة ترتكب أو يسهل إرتكابها بواسطة منظومة معلوماتية وهذه الأخيرة في الغالب ما تكون جرائم تقليدية.

- تتسم الجريمة الإلكترونية بعدة خصائص ميزتها عن باقي الجرائم التقليدية مثل أنها جريمة دولية أو جريمة لا تعترف حدود جغرافية، جريمة يصعب كشفها و إثباتها بإعتبار أنها لا تخلف أثار مادية، جريمة ناعمة تختلف بذلك عن الجريمة التقليدية التي تتطلب العنف في إرتكابها.
- يتميز المجرم الإلكتروني عن غيره من المجرمين التقليدين بصفات وسمات خاصة، فمن أهم هذه الصفات أنه مجرم يتسم بالمهارة نظرا للاحترافية التي يتمتع بها في مجال تكنولوجيا الإعلام والإتصال، كذلك المعرفة والتي بواسطتها يستطيع عمل محاكاة للجريمة على أنظمة مماثلة قبل شروعه في الجريمة وذلك لتأكد من تحقيق نتيجة الإجرامية، إضافة إلى خاصية الوسيلة فهي الميزة التي يكتسبها المجرم الإلكتروني والتي عن طريقها يتزود بالإمكانيات اللازمة لإتمام عمله الإجرامي، زيادة على ذلك يتمتع المجرم الإلكتروني بميزة التنظيم و التخطيط حيث عادة ما ترتكب الجريمة الإلكترونية بواسطة عدة فاعلين و كل فاعل له دور خاص به، و في الأخير يكون باعث المجرم الإلكتروني من وراء إرتكاب جريمته رغبة في كسب الربح المادي الغير مشروع وكذا رغبة نفسية في قهر نظام الحاسب فهو بهذه الميزات يختلف عن المجرم التقليدي.
- للجريمة الإلكترونية العديد من الصور و الأنواع التي استفحلت في العالم نظرا للتطورات السريعة التي يشهدها مجال تكنولوجيا الإعلام و الإتصال، ومن بين التصنيفات التي وضعت في هذا الصدد تصنيف الجريمة الإلكترونية عندما تكون المعلوماتية كوسيلة لإرتكاب الجريمة والتي تضم العديد من صور الجرائم الإلكترونية التي تستهدف الأشخاص و الأموال و أمن الدولة، أما التصنيف الأخر فتكون المعلوماتية كمحل لهذه الجريمة عندما يكون السلوك الإجرامي المرتكب من طرف الجاني ينصب على النظام المعلوماتي.
- أن الجريمة الإلكترونية بالرغم من الدراسات التي أنجزت في سبيل وضع تعريف موحد ويكون شامل لجميع صور هذه الجريمة، إلا أنه كل هذه الدراسات بائت بالفشل في ضبط مدلولها، وفي سبيل ذلك ظهرت العديد من المصطلحات الدالة على هذه الجريمة " الجرائم السيبرانية، الجرائم الرقمية، جرائم الغش، جرائم تقنية المعلومات، جرائم الكمبيوتر و الأنترنت وغيرها من التسميات".

- نظرا لكون النصوص الجزائية التقليدية إنما تم وضعها للتعامل مع الجرائم التي تنصب على محل مادي وملموس، فإن الأمر استتبعه قصور و عجز هذه النصوص في مجابهة الجريمة الإلكترونية نظرا لكون مسرحها يختلف تماما عن مسرح الجرائم التقليدية.
- أن هذا القصور لم يعتر النصوص الموضوعية فقط ولم يقف عند الشق الموضوعي للقانون الجنائي، بل امتد حتى إلى الشق الجزائي، فقد أثارت هذه الجريمة العديد من الإشكاليات في نطاقه وذلك راجع ان نصوص قانون الإجراءات الجزائية وضعت لتحكم إجراءات المتعقلة بالجرائم التقليدية التي لا توجد صعوبة في تحديد مكان وقوعها وبالتبعية تحديد القانون الواجب التطبيق، عكس الجريمة الإلكترونية العابرة للحدود الوطنية المتخذة للعالم اللامادي مسرحا لها و التي في كثير من الأحيان يتوزع سلوكها الإجرامي على عدة دول، مما يثير صعوبة في تحديد مكان وقوعها وبالتبعية تحديد القانون المنطبق عليها في هذه الحالة.
- في سبيل تجاوز هذه العقبة و عدم إفلات مرتكبي هذه الجريمة استغلالا منهم لهذه العقبة، حاول فقهاء القانون الجنائي إلى جانب بعض التشريعات الوطنية من خلال الإجتهادات القضائية إلى الوصول إلى معايير جديدة للتغلب على إشكالية تحديد مكان وقوع الجريمة الإلكترونية و كذا القانون الواجب التطبيق عليها، ومن جهة أخرى كان للقانون الدولي عدة مواقف في تبيان مسألة النص الجنائي الوجب التطبيق على الجريمة الإلكترونية من خلال الاتفاقيات الدولية و القوانين التي صدرت في سبيل مكافحة الجريمة الإلكترونية .
- أن المجتمع الدولي من منطلق الرغبة في الحد من الجريمة الإلكترونية لا يهتم بالقانون الواجب التطبيق بقدر اهتمامه بالتعاون لكشف مرتكب هذه الجرائم ومعاقبتهم، في إطار احترام التوازن بين السيادة الوطنية للدول ومقتضيات التعاون الدولي.
- للتغلب على هذه الإشكالية وجب تعزيز التعاون الدولي في مجابهة هذه الجريمة بإعتبارها جريمة عابرة للحدود.

وعلى ضوء ما توصلت إليه في هذه الدراسة من نتائج فإنه قد بدا لي ان أقدم بعض المقترحات أمل أن أكون موفقا في طرحها

- نظرا لخطورة الجريمة الإلكترونية و إنتشارها في الأونة الأخيرة بإنتشار مواقع التواصل الإجتماعي و كذا ثقافة التجارة الإلكترونية، فإنني أرى ضرورة إنشاء مواقع إلكترونية خاصة تكون تحت إشراف السلطات الأمنية أو القضائية للتبليغ عن هذه الجرائم، خاصة أمام إحجام الضحايا عن التبليغ خوفا من تشويه سمعتهم في المجتمع.
- بإعتبار أن الجريمة الإلكترونية جريمة عابرة للحدود فإنه من الضروري تفعيل مبدأ عالمية النص الجنائي في مجال التصدي و مكافحة هذه الظاهرة.
- بما أن الجريمة الإلكترونية في تطور مستمر، فأقترح القيام بعملية تحديث للقوانين الخاصة بمكافحة هذه الجريمة تتماشى مع التطورات التكنولوجية، لتفادي إستغلال الجناة لأي ثغرة قانونية.
- بإعتبار هذه الجريمة جريمة دولية عابرة للحدود، فلتغلب على الإشكالات التي تثيرها أقترح توحيد الجهود الدولية في سبيل مواجهة الجريمة الإلكترونية.

- **باللغة العربية**

**أولا: المصادر**

**01 -الإتفاقيات**

01 -إتفاقية بودابست، (مكافحة الجرائم المعلوماتية المنبثقة عن اجتماع المجلس الأوروبي ببودابست)، بتاريخ 21/ نوفمبر/ 2001، المجر رقم 185.

02 – إتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية المعتمدة من قبل الجهة العامة لمنظمة الامم المتحدة، بتاريخ 15 نوفمبر 2000 والمصادق عليها بموجب مرسوم رئاسي رقم 02-55 المؤرخ في 05 فبراير 2002.

03 –الإتفاقية العربية لمكافحة جرائم تقنية المعلومات، المنبثقة عن إجتماع مجلس وزراء الداخلية والعدل العرب بصفة مشتركة بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة، صادقت الجزائر على الإتفاقية العربية عن طريق المرسوم الرئاسي رقم 14-252 بتاريخ ديسمبر سنة 2010.

**02 -القوانين**

01 -الأمر رقم 66-155، المؤرخ في 18 صفر 1386، الموافق لـ8 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

02 -قانون رقم 06-23 مؤرخ في 29 ذي القعدة 1427 الموافق 20 ديسمبر 2006 يعدل ويتمم الامر رقم 66-156 المؤرخ في 18 صفر 1386 الموافق 8 يونيو 1966.

03 –القانون رقم 04-15 المؤرخ في 27 رمضان عام 1425 الموافق 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، الجريدة الرسمية رقم 71، الصادرة بتاريخ 10 نوفمبر 2004.

04 -القانون رقم 09-04، المؤرخ في 14 شعبان 1430 الموافق لـ 5 غشت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحتها، الجريدة الرسمية، العدد47، الصادرة بتاريخ 16 غشت 2009.

05 -القانون رقم 175، لسنة 2018، المتضمن مكافحة جرائم تقنية المعلومات المصري، الجريدة الرسمية، العدد32 مكرر (ج)، الصادرة في 14 أوت 2018.

06 -القانون رقم 20-05، المؤرخ في 05 رمضان عام 1441، الموافق لـ 28 أبريل سنة 2020، المتعلق بالوقاية من التمييز وخطاب الكراهية ومكافحتهما، الجريدة الرسمية عدد25، المؤرخة في 29 أبريل سنة 2020.

**ثانيا: المراجع**

**01 - الكتب**

**أ -الكتب العامة**

1.أحمد فتحي سرور، الوسيط في قانون العقوبات (القسم العام)، الطبعة السادسة، دار النهضة العربية، مصر، 2015.

2.بارش سليمان، شرح قانون العقوبات الجزائري، الجزء الأول شرعية التجريم، سلسلة القانون الجنائي الجزائري، 1992.

**ب -الكتب المتخصصة**

1.أعشب علي، الإطار القانوني لمكافحة غسل الأموال، ديوان المطبوعات الجامعية، بن عكنون، الجزائر، 2007.

2.الطيب بلواضح، الجريمة في الفضاء الإلكتروني، الطبعة الأولى، دار وائل للنشر والتوزيع، 2010.

3.أمير فرج يوسف، الجرائم المعلوماتية على شبكة الأنترنت، دار المطبوعات الجامعية، الإسكندرية، مصر، 2008.

4.حسين بن سعيد بن يوسف الغافر، السياسة الجنائية في مواجهة جرائم الأنترنت، دراسة مقارنة، جامعة عين شمس، القاهرة ، مصر، 2010.

5.طاهري حسين ، الجرائم الإلكترونية، الطبعة الأولى، دار الخلدونية للنشر والتوزيع، الجزائر، 2022.

6.حنان ريحان مبارك المضحكي، الجرائم المعلوماتية –دراسة مقارنة– الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت، لبنان، 2014.

7.خالد حسن أحمد لطفي، القانون الواجب التطبيق على الجريمة المعلوماتية، دار الفكر الجامعي، الطبعة الأولى، الإسكندرية، مصر، 2019.

8.خالد داودي، الجريمة المعلوماتية، الطبعة الأولى، دار الإعصار العلمي للنشر والتوزيع، عمان– الأردن،2018.

9.زبيحة زيدان، الجريمة المعلوماتية في التشريع الجزائري والدولي، دار الهدى للطباعة والنشر والتوزيع، عين مليلة، الجزائر،2011.

10. سامي جلال فقي حسين، الأدلة المتحصلة من الحاسوب وحجيتها في الإثبات الجنائي (دراسة مقارنة)، الطبعة الأولى، دار الكتب القانونية، القاهرة، مصرة، 2011.

11. عائشة بن قارة مصطفى، حجية الدليل الإلكتروني في مجال الإثبات الجنائي ( دراسة مقارنة)، دار الجامعة الجديدة، مصر، 2010.

12. غانم مرضى الشمري، الجرائم المعلوماتية(ماهيتها، خصائصها، كيفية التصدي لها قانونيا) الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2016.

13. عبد الله ذيب محمود، أسامة إسماعيل دراج، الوجيز في الجرائم الإلكترونية القواعد الموضوعية والإجرائية، الطبعة الأولى، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2020.

14. عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر الإنترنت، دار الكتب القانونية، مصر، 2007.

15. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الألي، الطبعة الأولى، الدار الجامعية، بيروت،1999.

16. محمد أمين أحمد الشوابكة، جرائم الحاسوب والأنترنت (الجريمة المعلوماتية)،الطبعة الاولى، مكتبة دار الثقافة للنشر والتوزيع، عمان، الأردن، 2002.

17. محمد عبيد الكعبي، الجرائم الناشئة عن الإستخدام غير المشروع لشبكة الأنترنت(دراسة مقارنة)، دار النهضة العربية، القاهرة، مصر، 2009.

18. محمد علي العريان، الجرائم المعلوماتية، دار الجامعة الجديدة للنشر، مصر، 2004.

19. مختار الأخضري، الإطار القانوني لمواجهة جرائم المعلوماتية، نشرة القضاة تصدرها المديرية العامة للشؤون القضائية والقانونية، مديرية الدراسات القانونية والمواثيق، العدد 66، سنة 2011/2010، صادرة عن وزارة العدل، الجزائر.

20. مناصرة يوسف، الدليل الإلكتروني في القانون الجزائي، دراسة مقارنة، دار الخلدونية، الجزائر، 2021.

21. نهلا عبد القادر المومني، الجرائم المعلوماتية، طبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، الأردن، 2010.

22. يزيد بوحليط، الجرائم الإلكترونية والوقاية منها في القانون الجزائري، دار الجامعة الجديدة ، مصر، 2019.

**02 الرسائل والمذكرات الجامعية**

**أ - أطروحات الدكتوراه**

1.فايز محمد راجح غلاب، الجرائم المعلوماتية في القانون الجزائري واليمني، أطروحة من أجل الحصول على شهادة الدكتوراه في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق، جامعة الجزائر1، 2010/2009.

2.يرمش مراد، خصوصية الجريمة الإلكترونية، أطروحة لنيل شهادة دكتورة علوم في القانون الخاص، فرع الملكية الفكرية، كلية الحقوق، جامعة الجزائر 1 بن يوسف بن خدة، السنة الجامعية 2021/2020.

**ب - رسائل الماجيستير**

01. تيسير أحمد حسين الزغبي، جريمة الإحتيال الإلكتروني، مذكرة ماجيستير في القانون العام، كلية الدراسات القانونية، قسم القانون، جامعة جدارا، الأردن، 2010.

02. جدي نسيمة، جرائم المساس بأنظمة المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماجيستر في القانون الجنائي، تخصص قانون جنائي، كلية الحقوق، جامعة وهران،2014/2013.

03. شنين صالح ، الحماية الجزائية لبرامج الحاسب الألي، مذكرة مكملة لنيل شهادة الماجيستير في الحقوق، تخصص قانون جزائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر، بسكرة، 2007/2006.

04. صغير يوسف، الجريمة المرتكبة عبر الأنترنت، مذكرة لنيل شهادة الماجيستر في القانون، تخصص القانون الدولي للأعمال، كلية الحقوق والعلوم السياسية، مدرسة الدكتوراه "القانون الأساسي والعلوم السياسية، جامعة مولود معمري–تيزي وزو–2013.

05.عبد الله دغش العجمي، المشكلات العلمية والقانونية للجرائم الإلكترونية –دراسة مقارنة–، مذكرة لنيل شهادة ماجستير في القانون العام، جامعة الشرق الأوسط، المملكة الأردنية، 2014.

**ج –مذكرات الماستر**

1. الدزيري هيبة، جريمة الدخول الغير مشروع لنظام المعالجة الألية للمعطيات، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم القانون العام، جامعة عبد الحميد بن باديس ، مستغانم، الجزائر، 2020/2019.

2.بخي فاطمة الزهراء، إجراءات التحقيق في الجريمة الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة المسيلة،2014/2013

3. بوديسة بجاد عبد الرؤوف، أليات التحري عن الجريمة الإلكترونية في القانون الجزائري، مذكرة لنيل شهادة ماستر، تخصص قانون الإعلام الالي والأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي برج بوعريريج، 2022/2021.

4. برتيل علي، مدوري نبيل، يعلاوي زهر الدين، القانون الواجب التطبيق على الجريمة الإلكترونية، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد لمين دباغين، سطيف 2023/2022.

5. بشان نسرين، بلعباسي منال، خصوصية الجريمة الإلكترونية في القانون الجزائري، مذكرة مقدمة لإستكمال متطلبات شهادة الماستر في الحقوق، تخصص قانون الإعلام الألي والأنترنت، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد البشير الإبراهيمي، الجزائر،2019–2020.

6. بلعيد منصورية، النظام الإجرائي للجريمة المعلوماتية في التشريع الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد بن باديس مستغانم، الجزائر، 2020.

7. بن لعربي أسماء، خصوصية الجريمة الإلكترونية، مذكرة نيل شهادة ماستر في الحقوق، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة إبن خلدون، تيارت، 2021/2020 .

8. حرزون ليلة، هدروق أسماء، التنظيم القانوني للجريمة الإلكترونية طبقا لأحدث التعديلات في القانون الجزائري، مذكرة لنيل شهادة ماستر، تخصص علوم جنائية، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمان ميرة، بجاية، 2022/2021.

9. حشيفة عبد الهادي، التعاون الدولي في مجال مكافحة الجرائم الإلكترونية، مذكرة لنيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور الجلفة، 2020/2019.

10. داود إدريس، شيبان إلياس، جريمة الدخول إلى النظام المعلوماتي في القانون الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون إعلام ألي وأنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج، 2023/2022.

11. دليلة مزرقن، جريمة المساس بأنظمة المعالجة الألية للمعطيات، مذكرة نيل شهادة الماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد خيضر بسكرة،2016/2015.

12. دواد وسيلة، الجريمة الإلكترونية على ضوء قانون العقوبات الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون قضائي، كلية الحقوق والعلوم السياسية، قسم القانون الخاص، جامعة عبد الحميد إبن باديس–مستغانم–2019.

13. شاهين خضر، رضوان سعادة، الجريمة الإلكترونية و إجراءات مواجهتها، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة محمد بوضياف المسيلة، 2021/2020

14. عباسة محمد ياسين، الجريمة المعلوماتية في ظل التشريع الجزائري، مذكرة نيل شهادة الماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسة، قسم القانون العام، جامعة عبد الحميد بن باديس مستغانم،2021/2020.

15. زمال وصال، جريمة الإتجار بالبشر عبر الأنترنت، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي وعلوم جنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة العربي التبسي، الجزائر، 2022/2021.

16. نايري عائشة، الجريمة الإلكترونية في التشريع الجزائري، مذكرة لنيل شهادة الماستر في القانون الإداري، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة أحمد دراية، أدرار، 2017/2016.

17. نواصرية ليلي، سليم نصيرة، التفتيش في الجرائم المعلوماتية، مذكرة لنيل شهادة ماستر، تخصص قانون إعلام ألي و أنترنت، كلية الحقوق والعلوم السياسية، جامعة محمد البشير الإبراهيمي، برج بوعريريج ، 2023/2022.

18. وردي طيب، الإختصاص القضائي في جرائم الأنترنت، مذكرة لنيل شهادة ماستر، تخصص قانون جنائي والعلوم الجنائية، كلية الحقوق والعلوم السياسية، قسم الحقوق، جامعة الطاهر مولاي، سعيدة،2015/2014.

**03 المقالات العلمية**

1. أحمد أبو زيد شحاتة، "**الجريمة المعلوماتية أنواعها وسبل مواجهتها**"، مجلة العلوم القانونية والاقتصادية، العدد الثاني، جويلية 2023، ص ص 685- 755.

2. أحمد بن مسعود، "**جرائم المساس بأنظمة المعالجة الألية للمعطيات في التشريع الجزائري**"، مجلة الحقوق والعلوم الإنسانية، المجلد 10، العدد 01، جامعة الجلفة، 2017، ص ص 482- 491.

3. أسامة أحمد محمد النعيمي، هايس سويلم صلبي الشمري، "**قواعد الإختصاص الموضوعي في الجرائم المعلوماتية**-دراسة مقارنة-"، مجلة جامعة تكريت للحقوق، المجلد 07، العدد01، كلية الحقوق، جامعة الموصل، نينوى، العراق، 2022، ص ص 105-145.

4. أميمة خديجة حميدي، عبد المجيد لخداري، "**إمكانية تفعيل مبدأ العالمية على الجريمة الإلكترونية**"، مجلة الحقوق والحريات، المجلد 10 ، العدد 01، كلية الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة ، 2022،ص ص 1917.1942

5. بثينة حبيباتي، "**معوقات مكافحة الجريمة المعلوماتية**"، مجلة العلوم الإنسانية، المجلد أ، العدد 50، كلية الحقوق، جامعة الجزائر 01، ص ص 85- 97.

6. بن عودة صليحة، "**الشروع في الجرائم المعلوماتية بين الوقاية والردع**"، مجلة دفاتر الحقوق والعلوم السياسة، المجلد 01، العدد 02، جامعة أبوبكر بلقايد تلمسان، ص 71-85.

7. بن نقي سفيان، "**جريمة غسل الأموال بين الوسائط الإلكترونية والنصوص التجريمية**"، مجلة الأبحاث القانونية والسياسية، المجلد 03، العد02، جامعة طاهري محمد، الجزائر، 2021، ص ص 149-166.

8. بواب بن عامر، لخضر إدريس خوجة، "**المواجهة التشريعية للإرهاب الإلكتروني في الجزائر**"، مجلة البحوث القانونية والسياسية، جامعة مولاي الطاهر، سعيدة، الجزائر، العدد 09، ديسمبر 2017، ص ص 274-309.

9. جمال زين العابدين أمين أحمد، "**الإختصاص القضائي وإجراءات التحقيق في الجرائم الإلكترونية**، "دراسة مقارنة""، مجلة مستقبل العلوم الإجتماعية، العدد 04، جامعة عبد الملك السعدي، المغرب،2021، ص ص 76-135.

10. جمال محمد خلفان محمد النقبي، سلطان محمد سالم عوض هيسان المصعبي، "**التعاون الوطني والدولي في الجرائم الإلكترونية المشكلات والحلول**"، مجلة المعهد العالي للدراسات القانونية، المجلد 3، العدد 16، 2023، ص ص 5449-5550.

11. حاتم أحمد محمد بطيخ، "**تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات**"، مجلة الدراسات القانونية والإقتصادية، المجلد 07، العدد 01، جامعة عين شمس مصر، 2021، ص ص 1-143.

12. حوالف حليمة، مهاجي فاطمة الزهراء، "**معالم الجريمة المعلوماتية في القانون الجزائري**"، مجلة البحوث القانونية والسياسية، مجلد 03، العدد 16، 2021، ص ص 140-155.

13. خلوفي رشيد، بولحية شهرزاد، "**تحديات الجريمة الإلكترونية في الجزائر**"، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، المجلد 04، العدد 02، جامعة الجزائر، 2019، ص ص 1974-2003.

14. سليماني مباركة، "**الإرهاب الإلكتروني وطرق مكافحته**"، مجلة الحقوق والعلوم السياسية، العدد 08، الجزء 01، جامعة عباس لغرور خنشلة، 2017 ص ص 340-355.

15. صهيب ياسر محمد شاهين، بشرى محمد حسن أبو ترابي، "**الجريمة الإلكترونية وبعدها القانوني** (دراسة مقارنة بين التشريع الجزائري والفلسطيني)"، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الأول، جامعة عباس لغرور، خنشلة، الجزائر، 2021، ص ص 150-169.

16. عبد المومن بن صغير، "**تطبيق النص الجنائي بين الإقليمية والعالمية في ظل عولمة مكافحة الجرائم المستحدثة**"، مجلة العلوم القانونية و السياسية، المجلد 10، العدد03، جامعة سعيدة، الجزائر، ص ص 58-87.

17. عراب مريم، "**الإختصاص القضائي في الجرائم المعلوماتية**"، مجلة حوليات كلية الحقوق والعلوم السياسية، المجلد07، العدد 03 كلية الحقوق والعلوم السياسية، جامعة محمد بن أحمد، وهران، 2015، ص ص 268-294.

18. عزيزة شبري، "**تفعيل مبدأ عالمية النص الجنائي في التصدي للجريمة المعلوماتية**"، مجلة الإجتهاد القضائي، العدد15، جامعة محمد خيضر بسكرة، 2017، ص ص 92-102

19. لموسخ محمد، "**تنازع الإختصاص في الجرائم المعلوماتية**"، مجلة دفاتر السياسة والقانون، المجلد 07، العدد 02، 2009، ص ص 151-167.

20. محمد عبد المحسن بن طريف، "**جريمة السرقة المعلوماتية**"، مجلة الدراسات والبحوث القانونية، المجلد 07، العدد 02، جامعة عمان العربية، الأردن، 2022، ص ص 13-27.

21. مخلد إبراهيم الزغبي، "**فاعلية القوانين والتشريعات العربية في مكافحة الجرائم الإلكترونية** "دراسة مقارنة""، المجلة العربية للنشر العلمي، العدد 37،2021 ، ص ص 275-294.

22. مونة مقلاتي، راضية مشري، "**الجريمة الإلكترونية (دلالة المفهوم وفعالية المعالجة القانونية)**"، مجلة أبحاث قانونية وسياسية، المجلد 6 ، العدد 01، جامعة 0 ماي 1945 قالمة، 2021، ص ص 491-510.

23. نبيلة كردي، "**الإتجار بالبشر عبر الأنترنت**"، مجلة الأبحاث، المجلد 7، العدد 2، جامعة العربي التبسي، الجزائر،2022، ص ص 521-532.

24. نعيمة داودي، "**الجريمة الإلكترونية(خصائصها ومجالات إستخدامها، وأهم سبل مكافحتها)**"، مجلة مهد اللغات، المجلد 2، العدد1، كلية لغات الاجنبية، جامعة حسيبة بن بوعلي، الشلف، 2020، ص ص 45-53.

**04 الملتقيات**

01 -حمالي سمير، "التحديات القانونية لمواجهة الجرائم السيبرانية"، مداخلة منشورة في المسطرة الإجرائية لأشغال الملتقى الوطني الإفتراضي حول "الجرائم الإلكترونية في المجتمع الجزائري"، كلية العلوم الإنسانية و الإجتماعية، جامعة يحي فارس، المدية، 15 مارس 2022، منشور على الموقع الإلكتروني https://www.univ-medea.dz .

02 -شفيقة خنيفر، الإجرام الإلكتروني، كفاءات ضائعة في عالم التقنية، مداخلة منشورة في المسطرة الإجرائية للمؤتمر العلمي الافتراضي الأول: الجريمة الإلكترونية (الواقع والتداعيات)، كلية العلوم الإنسانية والاجتماعية ،جامعة محمد الشريف مساعدية –سوق أهراس، 2022، منشور على الموقع الإلكتروني https://www.univ-soukahras.dz .

03 –موسى مسعود أرحومة، الإشكاليات الإجرائية التي تثيرها الجريمة المعلوماتية عبر الوطنية، ورقة بحثية مقدمة إلى المؤتمر المغاربي حول (المعلوماتية والقانون)،أكاديمية الدراسات العليا، طرابلس، ليبيا، يومي 28 و 2009/10/29، منشور على الموقع الإلكتروني https://iefpedia.com .

**05 المواقع الإلكترونية**

01 –محمد عدنان علي الزير، الجرائم الإلكترونية (المحاضرة الأولى): مفهومها وخصائصها و أركانها والمصلحة المحمية فيها، المدونة القانونية، فيديو منشور على الموقع www.youtube.com/@DrMohammedAadnan، تم الإطلاع عليه بتاريخ 2024 /04/24 على الساعة 14.36.

02 –نادية شريف، الجرائم المعلوماتية، مقال متوفر على الموقع الإلكتروني https://www.aps.dz ، تم الإطلاع عليه بتاريخ 2024 /04/23 على الساعة 17.20.

03 –يعقوب عبد العزيز الصانع، التلبس في الجرائم الإلكترونية، منصة القبس، مقال متوفر على الموقع الإلكتروني، https://www.alqabas.com ، تم الإطلاع عليه يوم 2024/05/05 على الساعة 14.20.

04 –يوسف قجاج، إشكالية الإختصاص في الجريمة الإلكترونية، مقال متوفر على منبر هسبريس، https://www.hespress.com، تم الإطلاع عليه بتاريخ يوم 2024/04/28، على الساعة 17.10..

05 –يوسف قجاج، الجريمة الإلكترونية و إشكالية الإختصاص القضائي _مكان إرتكاب الجريمة نموذجا _ المفهوم الجديد لمكان إرتكاب الجريمة الإلكترونية– مقال متوفر على الموقع الإلكتروني https://www.mrlatalib.com، تم الاطلاع عليه بتاريخ 2024/04/22 على الساعة 16:05.

- **باللغة الأجنبية**

**ARTICLE**

01- Prévention de la criminalité et sécurité quotidienne: prévenir la cybercriminalité, 6 eme rapport international, centre international pour prévention de la criminalité, page 90-91.

**فهرس الموضوعات**

**فهرس الموضوعات**

**فهرس الموضوعات**