المواجهة التشريعية للجرائم السيبرانية في الجزائر - بين النص و الواقع-

The legislative confrontation of cybercrimes in Algeria - between text and reality-

أ.د القينعي بن يوسف*

كلية الحقوق و العلوم السياسية – جامعة المدية (الجزائر)

تاريخ الاستلام: 2025/02/08 تاريخ القبول: 2025/04/15 تاريخ النشر: 2025 /12/04

ملخص:

إن التطور التكنولوجي و ثورة المعلومات التي عرفتها البشرية مع بروز العالم الافتراضي بفضل استعمال تكنولوجيات الإعلام و الإتصال ظهرت الجرائم السيبرانية كنمط جديد للإجرام، و للحد منها كان لابد من التصدي لها من الناحية التشريعية خاصة الجنائية منها، نظرا لما تحمله القاعدة الجنائية لخاصية الردع.

و عليه سنحاول من خلال هذه الورقة البحثية تسليط الضوء على هذه المواجهة التشريعية من منظور التشريع الجزائري و إبراز الثغرات القانونية المتعلقة بها إن وجدت.

كلمات مفتاحية: الجريمة السيبرانية، الحماية الموضوعية، الحماية الإجرائية، الدليل الإلكتروني.

Abstract:

The technological development and information revolution that humanity has known, with the emergence of the virtual world thanks to the use of information and communication technologies, cybercrimes have emerged as a new type of crime, and to limit them, it was necessary to address them from the legislative aspect, especially the criminal ones, given the criminal rule's deterrence feature.

Therefore through this research paper, we will attempt to shed light on this legislative confrontation from the perspective of Algerian legislation and highlight the legal gaps related to it if any.

Keywords:

Cyber crime, Substantive protection,Procedural protection,Electronic guide

المؤلف المرسل*

1. مقدمة:

يعتبر القرن العشرين عصر الثورة المعلوماتية فأصبح العالم عالما رقميا، و البيئة بيئة رقمية، أين بات استخدام الحاسوب أو الكمبيوتر مسيطر على كل مجالات الحياة، فظهرت أنماط جديدة للجرائم و المعروفة بالجرائم المعلوماتية أو السيبرانية، و الذي زاد من انتشارها الإستعمال السيء لهذه التكنولوجيا.

و بظهور هذه الجرائم المستحدثة كان لابد من مواجهتها على المستوى التشريعي بتجريم الأفعال التي تهدد المصالح المحمية قانونا إما بضرر أو خطر بواسطتها، و هو ما سارت عليه التشريعات الجنائية بما فيها المشرع الجزائري.

و عليه سنحاول و دون إطالات مملة أو اختصارات مخلة الإجابة عن الإشكالية التالية: فيما تمثلت أساليب تصدي المشرع الجزائري للجرائم السيبرانية؟ و ما مدى كان صائبا في ذلك؟

و بغية الوصول إلى ذلك اتبعنا الخطة التالية:

المبحث الأول: المواجهة الموضوعية للجرائم السيبرانية

المطلب الأول: مفهوم الجريمة السيبرانية و صورها.

المطلب الثاني: مظاهر المواجهة الموضوعية للجرائم السيبرانية.

المبحث الثاني: المواجهة الإجرائية للجرائم السيبرانية.

المطلب الأول: مظاهر المواجهة الإجرائية للجرائم السيبرانية.

المطلب الثاني: مشكلة إثبات الجرائم السيبرانية .

الخاتمة.

2. المواجهة الموضوعية للجرائم السيبرانية

تمثلت المواجهة الموضوعية للجرائم السيبرانية بتجريم العديد من الأفعال و تقرير عقوبات جزائية ضد مرتكبيها، و قبل ذلك ينبغي تحديد مدلول الجريمة السيبرانية و معرفة خصائصها و أهم صورها، وصولا على أوجه الحماية الموضوعية.

1.2. مفهوم الجريمة السيبرانية و صورها

أولا– تعريف الجريمة السيبرانية:

أستعمل مصطلح الجرائم السيبرانية أول مرة من طرف وليام جيبسون عام 1982، و منذ ذلك استعت دائرة استعماله، حتى أصبح العديد من العلماء و المنظمات يفضلون مصطلح جرائم الكومبيوتر بالمعنى الضيق للجريمة السيبرانية، فهي جزء من الجرائم المعلوماتية كونها ترتكب باستعمال تكنولوجيات الإعلام و الإتصال (ماينو و كوثر، جويلية 2022، صفحة 53).

عُرِّفت الجريم المعلوماتية بأنها" كل فعل إيجابي أو سلبي عمدي يهدف إلى الإعتداء على تقنية المعلوماتية أية كان غرض الجاني" (العريان، 2004، صفحة 45).

و عرفها جانب آخر بأنها "مجموعة الأعمال أو الأفعال غير القانونية التي تتم عبر شبكة الأنترنيت أو تبث عبر محتوياتها، و يكون الغرض منها المساس بحرمة الأفراد و حرياتهم الشخصية، و ذلك بالاستعانة بالحاسب الآلي" (محمودي، 2018، صفحة 168).

و منه فالجريمة الإلكترونية ظاهرة إجرامية فريدة، فهي جريمة إفتراضية في عالم إفتراضي و بآليات إفتراضية (ديار، 2018، صفحة 102).

يمكن من خلال هذه التعاريف أن نعرف الجريمة المعلوماتية بأنها كل فعل أو امتناع عن فعل يحضره القانون، و تكون النظم المعلوماتية إما موضوع الجريمة أو وسيلة فيها.

و بالرجوع إلى التشريع الجزائري فقد نظم المشرع الجريمة المعلوماتية تحت تسمية المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى غاية 394 مكرر8 و المستحدثة بموجب القانون رقم: 04-15 المؤرخ في: 10 نوفمبر 2004 المعدل و المتمم لقانون العقوبات، و المعدلة بموجب القانون رقم 24-06 المؤرخ في: 28 أفريل 2024 المعدل و المتمم لقانون العقوبات.

و تجسيدا لمكافحة هذا النوع من الجرائم و التي أضحت من أخطر الجرائم المستحدثة في هذا العصر للاستعمال المفرط للمعلوماتية قام المشرع الجزائري و على غرار باقي التشريعات بإصدار قانون خاص بها و هو القانون 09-04 المؤرخ في: 5 غشت 2009 المتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال و مكافحتها.

من خلال هذه النصوص لم يضع المشرع الجزائري تعريفا للجريمة المعلوماتية و حسن ما فعل بل نص على صورها لما أحالنا للجرائم الماسة بالمعالجة الآلية للمعطيات الواردة في قانون العقوبات، غير أنه حدد بعض المصطلحات ذات الصلة و هذا طبقا لنص المادة الثانية من هذا القانون.

إلا أنه عرف المنظومة المعلوماتية في الفقرة ب من المادة الثانية منه بأنها أي «نظام منفصل أو مجموعة من الأنظمة المتصلة ببعضها البعض أو المرتبطة، يقوم واحد منها أو أكثر بالمعالجة آلية للمعطيات تنفيذا لبرنامج معين».

كما عرف المعطيات المعلوماتية في الفقرة ج من ذات المادة بأنها « أي عرض للوقائع أو المعلومات أو المفاهيم في شكل جاهز للمعالجة داخل منظومة معلوماتية، بما في ذلك البرامج المناسبة التي من شأنها جعل منظومة معلوماتية تؤدي وظيفتها».

غير أنه باستعمال المشرع لمصطلح المساس بأنظمة المعالجة الآلية للمعطيات ضيق في نظر البعض في تعبيره عن الجريمة المعلوماتية، حيث حصر الجرائم التي يستعمل في ارتكابها الكمبيوتر دون الأنترنيت، أما مضمون النصوص التجريمية تشمل في نفس الوقت الأنترنيت كون هذه الأخيرة تتطلب أجهزة كومبيوتر.

ما يُعاب على المشرع الجزائري التأخر الكبير في تفعيل القانون 09-04 على أرض الواقع، حيث أن التجريم جاء 2004 ثم بقانون خاص في 2009، في حين تنظيم عمل الهيئة المجسدة له جاء بمقتضى المرسوم الرئاسي رقم: 19-172 المؤرخ في: 06 يونيو 2019 الذي يحدد تشكيلة الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الاتصال و مكافحتها و تنظيمها و كيفيات سيرها أي عشر سنوات من صدور القانون.

يتضح من خلال تعريف الجريمة السيبرانية أنها تتميز بعدة خصائص تميزها غن غيرها من الجرائم، نذكر أهمها:

– هي من الجرائم المستحدثة و المستجدة، و هي تلك الجرائم التي أفرزتها التطورات و المتغيرات التي تحدث في إطار المجتمع الذي ترتكب فيه، فهي تتميز بخصائص معينة و مخاطر متعددة، و التي تستخدم فيها التكنولوجيا الحديثة (صادق، 2009، صفحة 24).

– هي من الجرائم العابرة للحدود الوطنية، و المعروفة بالجريمة المنظمة عبر الوطنية، حيث تتعدى حدود الدولة الواحدة أين ترتكب عن طريق شبكات إجرامية دولية.

– تعتبر من الجرائم التي لا يتم التبليغ عنها في معظم الأحيان خاصة إذا تعلق الأمر بالمؤسسات و الشركات التجارية تجنبا الإساءة للسمعة أو اهتزاز ثقة العملاء (المهدي، 2021، صفحة 114).

–إضافة إلى أنها من الجرائم التي يصعب فيها معرفة مرتكب الجريمة، و الدليل ايضا كونها مرتبطة بعالم إفتراضي و ليس حقيقي أو واقعي.

ثانيا– صور الجرائم السيبرانية

تتخذ الجريمة السيبرانية عدة مظاهر نبرز أخطرها على سبيل المثال و ليس الحصر.

أ– الإرهاب الإلكتروني:

عُرِّف الإرهاب الإلكتروني بأنه " خدام التقنيات الرقمية ومهاجمة نظم المعلومات لإخافة وإخضاع الآخرين بدوافع سياسية أو عرقية أو دينية" (خميخم، 2020، صفحة 33).

أما المشرع الجزائري فلم يضع تعريفا له، غير أن نص المادة 87 مكرر 11 قانون عقوبات جرمت ارتكاب الأفعال أو تدبيرها أو الإعداد لها أو المشاركة فيها باستخدام تكنولوجيات الإعلام و الإتصال.

كما جرم المشرع من خلال نص المادة 87 مكرر 12 و المستحدثة بموجب القانون 16– 02، المؤرخ في 08/ 2016/06، المتمم لقانون العقوبات كل من يستخدم تكنولوجيات الإعلام والاتصال لتجنيد الأشخاص لصالح إرهابي أو جمعية أو تنظيم أو جماعة منظمة يكون غرضها تحت طائلة أحكام القسم المتضمن الأفعال الإرهابية والتخريبية، أو عند قيام الجاني بنشر أفكار الكيانات الإرهابية عبر وسائل الاتصال الالكترونية أو تمجيدها أو الإشادة بها.

ب– الجرائم المتعلقة بالذكاء الإصطناعي:

يعتبر الذكاء الإصطناعي آخر ما توصلت إليه ثورة المعلومات و التكنولوجيا الحديثة، عُرف الذكاء الإصطناعي بأنه أحد فروع علوم الكمبيوتر المعنية بكيفية محاكاة الآلات لسلوك البشر، فهو علم إنشاء أجهزة و برامج كمبيوتر قادرة على التفكير بالطريقة نفسها التي يعمل به الدماغ البشري، تتعلم مثلما نتعلم، تتصرف مثلما نتصرف، و تقرر مثلما نقرر (مراد، 2022، صفحة 199).

و استعمل الذكاء الإصطناعي في ارتكاب العديد من الجرائم منها جرائم السيارات ذاتية القيادة، جرائم الروبوتات، و كذا الطائرات المسيرة عن بُعد.

تعتبر تقنية التزييف العميق أهم استخداماته و هي تقنية تعمل على صنع فيديوهات مزيفة عبر برامج الحاسوب، ثم تقوم هذه التقنية على محاولة دمج العديد من الصور و مقاطع الفيديو لشخصية ما من أجل إنتاج فيديو جديد باستخدام تقنية التعلم الآلي مثلما حدث عام 2018 اين استبدل وجه الرئيس الأرجنتيني ماوريسيو ماكري بوجه أودولف هتلر (ماينو و كوثر، الجريمة السبيرانية في صورها المستحدثة،، 2022، صفحة 59).

ت–جرائم تمس الحياة الخاصة و مختلف المصالح الجديرة بالحماية

و هنا إنتقلت الجريمة من طابعها التقليدي إلى طابعها الحديث باستخدام الكمبيوتر و المعلوماتية، و من بين هذه الجرائم نجد:

- جرائم التزوير و النصب الإلكترونيين؛
- الجرائم الأخلاقية عبر الأنترنيت، و أخطرها الاستغلال الجنسي للأطفال؛
- جرائم الإعتداء على البيانات الشخصية الخاصة بالأفراد.

2.2 مظاهر المواجهة الموضوعية للجرائم السيبرانية

بالرجوع إلى النصوص القانونية ذات الصلة تتخذ الجريمة السيبرانية واجه المشرع الجزائري هذه الجريمة بعدة أوجه، و ذلك سواء في قانون العقوبات بوصفه قانونا عاما، و كذا في القوانين الخاصة، و تتجلى الحماية الموضوعية في شقي للتجريم و العقاب، حيث جرم العديد من الأفعال التي تكون الركن المادي لكل صورة منها، و اقر بعض الأحكام فيما يخص العقاب عليها، نورد أهمها.

أولا– جريمة الدخول أو البقاء غير المشروع في النظام المعلوماتي

سبق و أن أشرنا أن المشرع نظم الجرائم المعلوماتية في قانون العقوبات تحت تسمية المساس بالمعالجة الآلية للمعطيات في المواد 394 مكرر إلى غاية 394 مكرر7 و فق تعديل 24-06.

نصت عليها المادة 394 مكرر " يعاقب بالحبس من ستة (6) أشهر إلى سنتين (2) وبغرامة من 60.000 دج إلى 200.000 دج، كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة. و إذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من سنة (1) إلى ثلاث (3)سنوات و الغرامة من 100.000 دج الى 300.000 دج".

و الملاحظ أن المشرع لم يُعرِّف الدخول ول م يحدد وسيلته التي يمكن لمرتكب الفعل القيام بها من أجل الولوج إلى النظام المعلوماتي فقد تكون باستخدام كلمة مرور حقيقية، أو برنامج أو شفرة خاصة، فالمهم أن يكون هذا الدخول مخالفا لإرادة صاحب النظام.

أما فعل البقاء فهو التواجد ضمن النظام المعلوماتي دون موافقة من له حق السيطرة على النظام والحق في إدارته ويتحقق فعل البقاء باقترانه بفعل الدخول سواء كان غير المشروع أو حتى مشروعا.

و عليه فهي من جرائم الخطر، فبمجرد إتيان الفعل تقوم الجريمة ويسأل الجاني عنها، كما يعاقب على الشروع فيها بالعقوبة المقررة للجريمة ذاتها طبقا للمادة 394 مكرر7، و بعقوبات تكميلية و تتمثل في مصادرة الأجهزة و البرامج و الوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لإحدى جرائم المساس بالأنظمة المعلوماتية بالإضافة إلى إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها طبقا لنص المادة 394 مكرر6 من ذات القانون.

ثانيا– جريمة التلاعب بمعطيات النظام المعلوماتي

نصت عليها المادة 394 مكرر2 " يعاقب بالحبس من سنة (1) أشهر إلى خمس (5) سنوات وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

و لقد حددت المادة 394 مكرر1 سلوكها المجرم المكون للركن المادي في الإدخال بطريق الغش للمعطيات داخل نظام المعالجة الآلية للمعطيات، أو إزالتها عن طريق محوها أو تعديلها عن طريق الغش.

تعد هذه الجريمة من جرائم الضرر و المتمثل في إتلاف أو تغيير في النظام، على عكس جريمة الدخول أو البقاء غير المشروع التي هي من جرائم الخطر، كما أن صورها ذكرت على سبيل الحصر (نبيلة، 2014، صفحة 278).

و تضاعف العقوبة المقررة للجريمة في حال استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد و الواردة في 394 مكرر3، كما يعاقب على الشروع فيها بالعقوبة المقررة للجريمة ذاتها حسب نص المادة 394 مكرر7.

ثالثا– جريمة التعامل في معطيات غير مشروعة

نصت عليها المادة 394 مكرر2 " يعاقب من بالحبس من سنة (1) إلى خمس (5) سنوات، وبغرامة من 1.000.000 دج إلى 5.000.000 دج، كل من يقوم عمدا و عن طريق الغش بما يأتي:

1– تصميم أو بحث أو تجميع أو توفير أو نشر أو الإتجار في معطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.

2– حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم".

و تضاعف العقوبة المقررة للجريمة في حال استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام، دون الاخلال بتطبيق عقوبات أشد طبقا للمادة 394 مكرر3، كما يعاقب على الشروع فيها بالعقوبة المقررة للجريمة ذاتها حسب المادة 394 مكرر7.

رابعا– جريمة معالجة المعطيات ذات الطابع الشخصي دون موافقة المعني بالمعالجة

نصت عليها المادة 55 من القانون رقم: 18- 07 المتعلق بحماية الاشخاص الطبيعيين في مجال المعطيات ذات الطابع الشخصي "يعاقب بالحبس من سنة (1) إلى ثلاث (3) سنوات وبغرامة من 100.000 دج إلى 300.000 دج، كل من قام بمعالجة المعطيات ذات الطابع الشخصي خرقا لأحكام المادة 7 من هذا القانون، و يعاقب بنفس العقوبة على كل من يقوم بمعالجة المعطيات ذات الطابع الشخصي رغم اعتراض الشخص المعني.

و تشدد العقوبة إذ تصبح الحبس من سنتين (2) إلى خمس (5) سنوات و الغرامة من 200.000 دج إلى 500.000 دج عند ارتكاب الجريمة بمعالجة معطيات حساسة دون الموافقة الصريحة للشخص المعني طبقا للمادة 57 من ذات القانون، كما يعاقب على الشروع فيها بالعقوبة المقررة للجريمة التامة عملا بنص المادة 73 منه.

كما اعتبر المشرع إستعمال المعلوماتية أو تكنولوجيات الإعلام و الإتصال بوجه عام ظرفا مشددا لبعض الجرائم منها:

- جرائم التمييز و خطاب الكراهية طبقا لنص المادة 31 من القانون 20-05 المؤرخ في 28 أفريل 2020 و المتعلق بالوقاية من التمييز و خطاب الكراهية.
- جرائم الإرهاب الإلكتروني طبقا لنص المادة 87 مكرر11 قانون عقوبات.
- جرائم القذف و السب عبر شبكات التواصل الإجتماعي طبقا لنص المادة 333 مكرر6 المستحدثة في القانون 24-06 السالف الذكر.

تقرير المسؤولية الجزائية للشخص المعنوي عن الجرائم السيبرانية

نص المشرع الجزائري كغيره من التشريعات الجنائية على المسؤولية الجزائية للشخص المعنوي صراحة في نص المادة 51 مكرر قانون عقوبات، إلا أنها مسؤولية خاصة و متميزة حيث قيدها بشروط محددة يجب توفرها و إلا فلا تقوم هذه المسؤولية.

و الجرائم السيبرانية بوجه عام سواء المنصوص عليها في قانون العقوبات أو القوانين الخاصة فهي من الجرائم التي يسأل عنها الشخص المعنوي مهما كانت صورة الجريمة.

و العقوبات المقررة عليها هي الغرامة كعقوبة أصلية، بالإضافة إلى تطبيق عقوبات تكميلية أيضا تخضع للسلطة التقديرية لقاضي الحكم طبقا للمواد من 18 مكرر إلى 18 مكرر3 قانون عقوبات.

3. المواجهة الإجرائية للجرائم السيبرانية و مشكلة إثباتها

نظرا لخطورة هذا النوع من الجرائم و تداعياتها الخطيرة على المجتمع و الدولة ككل، قام المشرع الجزائري بالنص على ابتاع إجراءات خرج بمقتضاها عن القواعد العامة من جهة، و من جهة أخرى نص على إجراءات لها طابع الوقائي منها، يعني مكافحتها حتى قبل وقوعها.

1.3 . مظاهر المواجهة الإجرائية للجرائم السيبرانية:

بالرجوع إلى النصوص القانونية ذات الصلة فإن هذه الإجراءات منها ما هو ذو طابع وقائي من هذه الجرائم، و منها ما يدخل ضمن إجراءات البحث و التحري أو التحقيق أي بعد وقوع الجريمة، و يمكن إجمالها فيما يلي:

أولا– إستحداث هيئة وطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام و الإتصال ومكافحته طبقا لنص المادة 13 من القانون 09-04.

ثانيا– تمديد الإختصاص الإقليمي:

الأصل في تحديد الإختصاص الإقليمي يكون بمكان وقع الجريمة أو إقامة المشتبه فيه أو مكان إلقاء القبض عليه، إلا أنه بالنسبة للجرائم المعلوماتية بوجه عام فالإختصاص فيها وطنيا طبقا لنص المادة 7/16 قانون الإجراءات الجزائية.

كما قام المشرع في ذات السياق بالنص على القطب الجزائي المتخصص في الجرائم المعلوماتية بمقتضى المواد 211 مكرر22 إلى غاية المادة 211 مكرر29 من ذات القانون و المستحدثة بموجب الأمر 21-11 المؤرخ في: 25 غشت 2021، المعدل و المتمم لقانون الإجراءات الجزائية، و يمكن أيضا تمديد الإختصاص حتى خارج الوطن وفق مبدأي شخصية و عينية النص الجنائي.

ثالثا– إستحداث أيضا سلطة وطنية لحماية المعطيات ذات الطابع الشخصي طبقا لنص المادة 22 من القانون 18-07 و المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.

رابعا– تمديد مدة التوقيف للنظر في مثل هذه الجرائم، حيث أن الأصل أنه لا يفوق 48 ساعة إلا أنه في هذه الحالة يمكن تمديده مرة واحدة طبقا للمادة 48 و ما بعدها قانون إجراءات جزائية.

خامسا– إجراء التفتيش المعلوماتي و حجز المنظومة المعلوماتية:

التفتيش المعلوماتي هو ذلك الإجراء القانوني الذي تقوم به جهات التحقيق كقاعدة عامة يستهدف ضبط الدليل في المنظومة المعلوماتية، جراء ارتكاب إحدى الجرائم المعلوماتية، أو هو البحث عن الدليل الموجود أو المخزن في شكل إلكتروني.

نظم المشرع أحكام التفتيش بوجه عام في المواد من 44 إلى غاية 47 من قانون الإجراءات الجزائية، و من المادة 79 إلى غاية المادة 86 من ذات القانون، أما التفتيش المعلوماتي فقد نص عليه في الفصل الثالث من القانون 09-04 المادة 05 منه.

و نظرا لخصوصيته و بما أنه يتعلق بالجرائم الماسة بالمعالجة الآلية للمعطيات فقد استثنى المشرع هذه الجرائم من تحديد مدته، حيث يمكن إجرائه في أي وقت من أوقات الليل أو النهار شريطة الحصول على إذن مكتوب من السيد وكيل الجمهورية إعمالا بنص المادة 3/47 قانون الإجراءات الجزائية، كما أن القائم به التفتيش المعلوماتي يُشترط فيه العلم و الدراية بتقنية المعلومات.

غير أنه يُؤخذ على المشرع استعماله عبارة "يمكن" في القانون 09-04 مما يعني أن المسألة جوازية للسلطة المختصة و هذا في نظرنا غير صائب، فمن جهة التفتيش المعلوماتي يحتاج إلى ذوي الخبرة و بالتالي الإستعانة بهم ضرورية، و من جهة أخرى اللجوء إليهم مسألة جوازية.

سادسا– إتباع أساليب التحري الخاصة:

خروجا عن القواعد العامة سمح المشرع للضبطية القضائية و جهات التحقيق إجراء المراقبة الإلكترونية عن طريق إعتراض المراسلات و تسجيل المكالمات و إلتقاط الصور و كذا إجراء التسرب إذا تعلق الامر بالجرائم المعلوماتية على العموم بما فيها السيبرانية طبقا لنص المواد 65 مكرر 5 إلى غاية المادة 65 مكرر 18 قانون إجراءات جزائية، و حتى لا يتعارض مع حرمة الحياة الخاصة و التي الإعتداء عليها يشكل جريمة طبقا لنص المادة 303 مكرر قانون عقوبات قيده المشرع بشروط شكلية و أخرى موضوعية يجب احترامها.

سابعا– إضافة إلى هذا و في إطار مكافحة هذا النوع من الجرائم و ملاحقة المجرمين نص المشرع على التنسيق الدولي في مجال مكافحتها عن طريق تبادل المعلومات و المساعدة القضائية الدولية، بالتعاون مع المؤسسات الدولية الأمنية و على رأسها الأنتربول تطبيقا لنص المادة 15 و ما بعدها من القانون 09-04.

3 2.مشكلة الإثبات في الجرائم السيبرانية:

إن هذا النوع من الجرائم تقع في عالم الإفتراضي مما يخلق مشكلة للجهات القضائية تتعلق بالإثبات و إقامة الدليل عليها، حيث أنه يخرج من طابعة المادي إلى الإفتراضي و الذي يسمى بالدليل الإلكتروني أو الرقمي، و هذا الأخير يخلق إشكالات عديدة و متنوعة تحول أحيانا دون الوصول إلى الحقيقة سواء تعلقت بالبراءة أو الإدانة.

أولا– تعريف الدليل الإلكتروني:

عُرِّف الدليل الإلكتروني بأنه" الدليل الذي يتضمن بيانات إلكترونية مخزنة في الحاسب الآلي و لها وجود في الوسط الإفتراضي و التي من خلالها يتم الكشف عن الجريمة أو إثبات العلاقة بينها و بين الفاعل" (بلهادي، 2019، صفحة 17).

و منه يمكن تعريفه بأنه كل ما يتوصل إله القاضي الجنائي في تكوين قناعته الشخصية بسبب ارتكاب جريمة إلكترونية، الذي يكون مصدرة تقني أو معلوماتي.

و تجدر الإشارة في هذه المسألة أن الدليل الإلكتروني يمكن الإستعانة به حتى في إثبات بعض الجرائم التقليدية رغم صعوباته، حيث سمح المشرع في بعض الجرائم استعمال التكنولوجيا قصد كشف الجرائم على غرار الترصد الإلكتروني بكل أنواعه و غيرها و المعروفة بالأدلة العلمية الحديثة.

ثانيا– مشكلة الدليل الإلكتروني (القينعي، 2022، صفحة 24):

يمكن إجمال الصعوبات المتعلقة بالدليل الإلكتروني فيما يلي:

- الدليل الإلكتروني دليل غير ظاهر؛
- الدليل الإلكتروني ذو طبيعة ديناميكية؛
- صعوبة فهم الدليل الإلكتروني و سهولة التخلص منه؛
- ضعف الخبرة الفنية لأجهزة العدالة الجنائية
- صعوبة مرتبطة بالتحقيق؛
- مشكلة تنازع القوانين الإجرائية؛
- صعوبة الوصول إلى الفاعلين.

4. خاتمة:

نخلص إلى ما تقدم إلى أن المشرع الجزائري كغيره من التشريعات الجنائية المقارنة تصدى للجرائم السبيرانية بترسانة قانونية قصد مواجهتها و التقليل منها على الأقل، و خلصنا غلى مجموعة من النتائج من بينها ما يلي:

- الجرائم السبيرانية أكبر تحدي تواجهه الدول في ظل البيئة الرقمية؛
- لم يضع المشرع الجزائري تعريفا للجريمة السبيرانية بل نص على أهم و أخطر صورها؛
- تجلت المواجهة من ناحيتين موضوعية و أخرى إجرائية؛
- للجرائم السبيرانية مشكلة تواجه القضاة و تتعلق بطبيعة الدليل فيها الذي يعد إلكترونيا بالدرجة الأولى مما سعب إثباتها.

و في الأخير و على ضوء هذه الدراسة نقدم بعض الاقتراحات لعلها تسد الثغرات القانونية المتعلقة بالجرائم محل الدراسة و من بينها:

أ– الاهتمام أكثر بالتأهيل البشري و تكوين المتخصصين في مكافحة الجرائم المعلوماتية بدء من الضبطية القضائية وصولا إلى جهات الحكم و مرورا بالمحققين.

ب–نظرا للطابع الخفي و صعوبة الحصول على الدليل حبذا لو ينص المشرع على تجريم عدم التبليغ عن الجرائم المتعلقة بتكنولوجيات الإعلام و الاتصال لمن لا يبلغ عنها بحكم مهنته أو وظيفته، وذلك بإضافة نص قانوني إما في القانون 09-04 أو قانون العقوبات تكريسا لفكرة التجريم الوقائي، فلا نصل للتفتيش المعلوماتي الذي هو أصلا من مشكلات الإجرائية التي تعترض الجهات.

ت–تشديد العقوبة أكثر على مثل هذه الجرائم و جعلها من قبيل الجنح المشددة على الأقل و ليست بسيطة.

5. قائمة المراجع:

القانون 24-06، المعدل و المتمم لقانون العقوبات. *الجريدة الرسمية العدد 30، المؤرخة في: 30 أبريل 2024.*

بن عودة حسكر مراد. (2022). إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي. *مجلة الحقوق والعلوم الإنسانية، المجلد الخامس عشر، العدد الأول، جامعة الجلفة، الجزائر.*

بن يوسف القينعي. (2022). الإشكالات التي تعترض القاضي الجزائي في قبول الدليل الإلكتروني. تأليف عدة مؤلفين، *الإثبات الإلكتروني في المواد المدنية و الجزائية.* جامعة الوادي، الجزائر.

جيلالي ماينو، و عروس كوثر. (جويلية, 2022). الجريمة السبيرانية في صورها المستحدثة، *مجلة القانون و التنمية، المجلد الرابع، العدد الأول، جامعة طاهري محمد، بشار، الجزائر.*

جيلالي ماينو، و عروس كوثر. (جويلية 2022). الجريمة السبيرانية في صورها المستحدثة. *مجلة القانون و التنمية، المجلد الرابع، العدد الأول، جامعة طاهري محمد، بشار، الجزائر.*

حسين صادق. (22-23 أكتوبر 2009). علم النفس الجنائي و علاقته بالجرائم المستحدثة، *مجلة أصداء الأمانة، عدد خاص، مجلس وزراء الداخلية العرب، الدورة 26، بيروت.*

حميد بلهادي. (ديسمبر 2019). حجية الدليل الرقمي في الإثبات الجنائي، . *مجلة البحوث و الدراسات القانونية و السياسية، المجلد التاسع، العدد الأول، كلية الحقوق و العلوم السياسية، جامعة البليدة2، الجزائر.*

رضا المهدي. (2021). الجرائم السبيرانية و آليات مكافحتها في التشريع الجزائري. *مجلة إيليز للبحوث و الدراسات، المجلد السادس، العدد الثاني.*

محمد خميخم. (جوان, 2020). موقف المشرع الجزائري من جريمة الإرهاب الالكتروني. *مجلة حوليات جامعة الجزائر 1، المجلد 34، العدد الثاني، الجزائر.*

محمد علي العريان. (2004). *الجرائم المعلوماتية.* الإسكندرية: دار الجامعة الجديدة للنشر.

مليكة أبو ديار. (2018). الإثبات الجنائي في الجرائم الإلكترونية . *المجلة الإلكترونية للأبحاث القانونية، العدد الثاني، المملكة المغربية*.

نور الهدى محمودي. (جوان, 2018). مشروعية الوسائل العلمية الحديثة في الإثبات الجنائي (دراسة تحليلية) . *أطروحة دكتوراه في علم الإجرام و العقاب* . جامعة الحاج لخضر، باتنة1، الجزائر: كلية الحقوق و العلوم السياسية.

هروال هبة نبيلة. (2014). جرائم الانترنت (دراسة مقارنة). *أطروحة دكتوراه*. جامعة أبي بكر بلقايد، تلمسان، ،كلية الحقوق و العلوم السياسية، الجزائر.