

مكافحة الجريمة السيبرانية على المستوى الوطني

Fighting cyber crime at the national level

واجعوط سعاد¹

¹أستاذة محاضرة أ، معهد الحقوق والعلوم السياسية المركز الجامعي تيبازة،

ouadjout.souad@cu-tipaza.dz

القبول: 2024-04-03

الاستلام: 2024-02-01

ملخص: إن تطور التكنولوجيا و اتجاه الجزائر نحوى رقمنة جميع القطاعات يساعد في نشر الجريمة السيبرانية و نظرا لخصائصها التي تتميز و تنفرد بها و أبعادها الخطيرة ، أدى بالمشرع الجزائري إلى وضع آليات قانونية من اجل الوقاية و مكافحة الجريمة السيبرانية و كذلك و تكريس مجموعة من القاعد القانونية التي تعاقب مرتكبيها على المستوى الوطني

تعتبر الجريمة الالكترونية من الجرائم المستحدثة، و التي تطور بتطور الرقمنة ووسائل التكنولوجيا الحديثة، إلا أنها تختلف عن الجرائم التقليدية كونها جرائم عابرة للقارات و يصعب اكتشاف مرتكبيها وأدلة الإثبات فيها، و نظرا لخطورتها على المجتمع اقر لها المشرع الجزائري عقوبات و غرامات نافذة ليحد من هذه الجريمة .

الكلمات المفتاحية : الجريمة السيبرانية ، الآليات ، العقوبات ، الجريمة ، مكافحة .

Abstract:

The technological developments in the different fields leads cyber crime to widespread, since the dangers of this last are numerous the Algerian legislator acknowledged sanction and effective penalties so as to reduce this crime

The Cyber crime is considered as a new crimes' from witch is developed due to technological developments yet it is different from the traditional crimes since it has become transcontinental and it is quite hard to discover the criminals and proves because if its dangers in the society, the Algerian legislator acknowledged sanctions and effective penalties so as to reduce this crime

Keywords: cybercrime/ the crime/ sanctions / mechanisms / combat

المؤلف المراسل: د/ واجعوط سعاد، الإيميل: oaudjaout.souad@gmail.com

1. مقدمة:

تعتبر الجريمة السيبرانية من الجرائم المستحدثة، افرزها التطور التكنولوجي، شبكة الانترنت و مواقع التواصل الاجتماعي ، الرقمنة ، تقنيات الذكاء الاصطناعي، فهي نتيجة الاستخدام السلبي للتكنولوجيا و مهما تعددت أسباب ارتكابها سواء كانت نفسية ، ذاتية،اجتماعية،مالية، عسكرية،قومية وطنية ، إلا أن لها أبعادها خطيرة على المجتمع فقد تمس امن القومي للدولة خاصة اذا كانت الشبكة العسكرية غير مؤمنة او تضرب الاقتصاد الوطني بعدما تم رقمنة البنوك والبورصات او تخلق فوضى في الدولة أو ما بين الدول اذا ما مست الجانب الأمني والأجهزة السيادية في الدولة، و الواقع في الجزائر يثبت ان هذه الجريمة ترتكب بشكل يومي ، لذا المشرع الجزائري كيف هذه الجريمة، ونص عليها في الدستور الجزائري، فخصص الفصل السابع من قانون العقوبات لها و كرس لها ترسانة قانونية خاصة بها واليات ، أجهزة تسهر على الوقاية و مكافحة هذه الجريمة،وقواعد قانونية تعاقب على ارتكاب هذه الجريمة، فالمقصود بالجريمة السيبرانية و ما هي الآليات المكرسة لمكافحتها و العقوبات المقررة لمرتكبي الجريمة الالكترونية؟ مما يجعلنا نطرح الإشكالية التالية :

كيفية مكافحة الجريمة السيبرانية على المستوى الوطني ؟

للإجابة على هذه الإشكالية نتبع الخطة التالية:

معالجة الموضوع تكون من خلال نقطتين:

المبحث الأول: مفهوم الجريمة السيبرانية و خصائصها

المبحث الثاني: آليات مكافحة الجريمة السيبرانية والعقوبات ارتكابها

2. مفهوم الجريمة السيبرانية و خصائصها:

الجريمة السيبرانية الافتراضية أو جريمة فضاء الانترنت أو الجريمة الالكترونية مهما تعددت التسميات إلا أن المعنى يبقى واحد و هو الاستعمال السلبي للتكنولوجيا و الذي يشكل جريمة في نظر القانون يتوجب العقاب عليها، اختلفت التسمية بشأنها إلا أننا سوف نحاول سرد أهم المصطلحات القانونية التي تخصها، وأهم الميزات و الخصائص التي تنفرد بها مقارنة مع الجرائم التقليدية التي نعرفها التي تثبت بالقرائن القانونية و القضائية من ادلة مادية و شهود و بصمة و كميرات مراقبة و غيرها.

1.2 تعريف الجريمة السيبرانية:

تعتبر الجريمة الالكترونية من بين الجرائم المستحدثة و هي كل فعل ضار يقوم به الشخص عبر الوسائط الالكترونية مثل الحواسيب، الهواتف ، شبكة الانترنت (المایل، 2019) يقصد بها الاستعمال السلبي للتكنولوجيا، لم تعرف في الجزائر إلا مؤخرا مع تطور التكنولوجيا و انتشار الهواتف الذكية و استعمال مواقع التواصل الاجتماعي.

يتكون مصطلح الجريمة الالكترونية او الافتراضية من مصطلح **cyber crime**

ويقصد ب **crime** جريمة ، أما **cyber** الكترونية، جرائم ترتكب في الانترنت ، و يستخدم مصطلح الإللكترونية لوصف فكرة تشكل جزء من الحاسوب او فكرة في عصر المعلومات (قط، 2018)

أما الجريمة فهي السلوكيات مادية ومعنوية وكل الأفعال الخارجة على القانون (البدانية، 2018)

الأفعال أو النشاطات غير مشروعة تكون وسيلة تقنية المعلومات محلا لها و أداة للقيام بها" كما جاء في مؤتمر الأمم المتحدة لمنع الجريمة و معاقبة المجرمين على أن الجرائم الالكترونية هي "أي جريمة يمكن ارتكابها بواسطة نظام حاسوب او شبكة حاسوبية فهي تشمل من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في بيئة الكترونية. "

أما المشرع الجزائري لم يتم بتعريف الجريمة الالكترونية بخلاف كل التشريعات و إنما تبنى و اعتمد للدلالة على الجريمة و كتعبير عليها اطل عليها مصطلح المساس بأنظمة المعالجة الآلية للمعطيات معتبرا أن النظام المعلوماتي في حد ذاته و ما يحتويه من مكونات غير مادية محلا للجريمة

و، يمثل نظام المعالجة الآلية للمعطيات الشرط الأول الذي لابد من تحقيقه حتى يتوفر أركان الجريمة ، وفي قانون العقوبات لا نجد تعريف للجريمة الالكترونية بل اكتفى المشرع بذكر الأفعال المجرمة و العقوبات تحت عنوان "الجرائم الماسة بنظام المعالجة الآلية للمعطيات" في القسم السابع منه،تضمن مواد،من المادة 394مكرر لغاية 394مكرر (رشيد، 2019)7

نصت المادة الثانية من قانون رقم 09-04 تعتبر جرائم المساس بأنظمة المعالجة الآلية للمعلومات هي جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية "و نستنتج من خلال هذا التعريف أن المشرع الجزائري اعتمد عدت معايير للجريمة الالكترونية ،هي:

المعيار الأول: يتمثل في وسيلة الجريمة يقصد بيه نظام الاتصالات الالكترونية ، المعيار الثاني : يقصد به موضوع الجريمة و يقصد بيه :المساس بأنظمة المعالجة الآلية للمعطيات المعيار الثالث :والمقصود به القانون الواجب التطبيق أو الركن الشرعي المنصوص عليه في قانون العقوبات ، إضافة إلى أن المشرع الجزائري وسع في نطاق الجريمة الالكترونية فهي الجريمة التي ترتكب في إطار معلوماتي او يسهل ارتكابها عليه، مما يوسع من نطاق الجريمة الالكترونية.

2.2 خصائص الجريمة السيبرانية:

تستهدف هذه الأنواع من الجرائم تحقيق الربح المالي او رغبة المجرم المعلوماتي في إلحاق ضرر بالضحية إلا أن أبعادها أكثر أثرا على أسباب ارتكابها، وكونها جرائم غير مادية ،فهي تمتاز بمجموعة من الخصائص التي جعلتها منفردة عن باقي الجرائم الأخرى بالنظر إلى المعطيات الخاصة بها سواء من حيث أداة ارتكابها ، مرتكبها ، كيفية إثباتها و معاينتها (جيلالي، 2022)، و من بين هذه الخصائص:

1-سرعة التنفيذ و سهولة التنفيذ و التنفيذ عن بعد: بمعنى أنها قد ترتكب في ثواني و تنفيذها سهل جدا بإدخال رموز أو بيانات أو اخذ معلومات لا يتطلب جهد كبير و قد تكون نتيجة ارتكبتها اثر عابر للقارات.

ب- جريمة عابرة للقارات : بمعنى غير مقيدة بمكان او زمان، لان تنفيذها عبر الشبكة المعلوماتية فالجاني يكون في بلد يرتكب فيه الجريمة و المجني عليه يتواجد في بلد آخر و قد يكون الضرر المحتمل في بلد ثالث ، وهنا تطرح إشكالية القانون الواجب التطبيق ؟

ج- جريمة ترتكب بواسطة الأجهزة الالكترونية مثل الحاسوب أو الموبيل أو شبكة الانترنت لأنها من الجرائم المستحدثة التي تحمل في طياتها العديد من الايجابيات و السلبيات ، و تعتبر هذه الأدوات هي أداة و محل لارتكاب الجريمة .

ح- جريمة تخلف عدد كبير من الضحايا و عدة جرائم في وقت سريع: فقد يكون مرتكبها شخص يريد تحقيق هدف بسيط يتفاجئ بوقوع عدد كبير من الضحايا و ارتكب في حقهم عدة جرائم ألحقت بهم ضرر .

خ- جرائم ناعمة ليس فيها عنف :لا تحتاج إلى جهد عضلي أو استخدام آلة أو وسيلة خطيرة لارتكابها، لأنها تعتمد على مجهود ذهني و فني و تقني بالحاسوب و شبكة الانترنت ، ولا تعتبر جرائم عنيفة مثل الجرائم التقليدية التي نعرفها .

هـ- يصعب اكتشاف مرتكبيها إلا بأساليب أمنية و تقنية عالية (ريحان، 2014)

و سهولة إخفاء أثارها، صعوبة اكتشاف و إثبات الجريمة الالكترونية ،لان الجاني لا يترك اثر لإجرامه ،لا لأثار ملموسة ولا لشاهد يمكن الاستدلال بأقواله و لا أدلة مادية يمكن فحصها،لأنها تقع في بيئة افتراضية كإدخال رموز و أرقام أو معلومات غير مرئية .

ز- مرتكب الجريمة الالكترونية يتميز بالذكاء و الدهاء، ليس شخص عادي ، بل يكون إنسان متمكن ذو مهارات تقنية عالية في مجال الحاسب و كيفية تشغيله و كيفية تخزين المعلومات و الحصول عليها، و التي تتطلب من مرتكبيها خبرة و معرفة كبيرة في مجال المعلوماتية.

د- عدم وجود مفهوم مشترك للجريمة الالكترونية:و عدم وجود تعريف قانوني موحد لها نظرا لعدم وجود تنسيق دولي في مجال الجريمة الالكترونية و يرجع ذلك لعدم وجود اتفاقيات دولية و ثنائية أو جماعية لمواجهة الجريمة الالكترونية .

و-وقوع الجريمة المعلوماتية أثناء المعالجة الآلية للمعطيات: وهو شرط لقيام الجريمة الالكترونية سواء كان عند مرحلة بداية إدخال البيانات أو أثناء مرحلة المعالجة أو أثناء مرحلة إخراج المعلومات.

ي-نقص ثقافة الإبلاغ عن الجرائم الالكترونية: أي الأشخاص أو الضحايا أو المجني عليهم لا يبلغون عن وقوع هذه الجريمة خوفا على سمعتهم و مكانتهم في المجتمع، خاصة إذا ما تعلق الأمر بجرائم متعلقة بالاعتداء الجنسي ...

3.آليات مكافحة الجريمة السيبرانية و العقوبات المقررة:

لقد وضعت الجزائر الأمن السيبراني احد أولوياتها من اجل المحافظة على السياسة الأمنية و ذلك بإدراجها مجموعة من الآليات و الميكانيزمات و الأجهزة من اجل مكافحة القضاء على الجريمة السيبرانية ، و كرس لها قواعد قانونية مختصة بها من اجل معاقبة مرتكبيها و هي عقوبات سالبة للحرية و بغرامات مالية نافذة للدولة.

1.3أجهزة مكافحة الجريمة السيبرانية:

رغم أن الجريمة السبرانية إلا أن الجزائر خصصت لها أجهزة و آليات فعالة من اجل اكتشاف مرتكب الجريمة على المستوى الوطني و الدولي ، و تسعى للانضمام إلى الاتفاقيات الدولية لمكافحة الجريمة السيبرانية والانضمام إلى اتفاقيات تسليم المجرمين الدوليين نظرا لخطورة هذا النوع من الجرائم و الذي قد يمتد أثرها إلى عدد كبير من دول العالم ، و من بين الأجهزة الموجودة لمكافحة هذه الجرائم في الجزائر نذكر منها :

ا_مركز الوقاية في جرائم الإعلام الآلي للدرك الوطني لسنة 2008 مقره بئر مراد رابيس : يقوم بتحليل البيانات و المعطيات و الكشف على هوية مرتكب الجريمة السيبرانية سواءا فرد او دول و او منظمة او غيرها ، يقوم بالوقاية و مكافحة الجريمة السيبرانية ، و المقصود بالوقاية وضع حملات تحسيسية من نشر و الإشهار بالجريمة الالكترونية ، و مكافحة يقصد بها التوعية بالاستعمال السلبي للتدترنات ، و من النتائج التي توصل اليها المركز إليها:

-استطاع المركز من معالجة أكثر من 100 جريمة الكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015 منها 300 جريمة تتعلق بمواقع التواصل الاجتماعي " الفيس بوك " و 20 جريمة رقمية تعلقت باختراق مؤسسات عامة و خاصة ، استهدف مجرموها أي الأشخاص الذين استهدفوها أنظمة المعالجة الآلية للمعطيات (سميرة، 2017)

ب- المعهد الوطني للأدلة الجنائية و علم الإجرام وهو معهد تابع للدرك الوطني الذي تم إنشاؤه في 2009 ومقره ببوشاوي، تحت وصاية وزير الدفاع الوطني ، يختص بوضع خبرات للبصمات و الأدلة و أداة الجريمة .

ج- المصلحة المركزية لمكافحة الجريمة المعلوماتية و هي مصلحة تابعة لمدرسة الأمن الوطني و الذي تم إنشاؤه في سنة 2011 مختص بالوقاية و مكافحة الجريمة الالكترونية .

د- الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال : تم إنشاؤها سنة 2015 بموجب قانون رقم 04/09 "عرفت بأنها سلطة إدارية مستقلة ، و تتمتع بالشخصية المعنوية و الاستقلالية المالية تابع لوزير العدل وهي تحت سلطة رئيس الجمهورية (الرسمية، 2009) و هي مختص في الانابات القضائية او الخبرات الدولية و المتعلقة بأمن الدولة و الجرائم الإرهابية، و مهامها:

1-الوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال: دورها هنا وقائي أي قبل وقوع الجريمة وذلك بالتوعية بخطورة هذه الجرائم .

2-مكافحة الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال: كالمساعدة في التحريات و تقديم خبرات القضائية، تبادل المعلومات مع نظيرتها في الخارج.. (اسمهان، 2018)

ف- سلطة ضبط البريد و الاتصالات : استحدثت بموجب القانون رقم 18-04 المؤرخ في 10 ماي 2018 الذي يحدد القواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية وجدت من اجل تجريم انتهاك سرية المراسلات المرسله التي تتم عن طريق البريد أو الاتصالات الالكترونية... أو إفشاء مضمونها أو نشرها أو استعمالها دون ترخيص من المرسل و المرسل إليه أو الإخبار بوجودها و تجريم

محاولة فتح أو تخريب أو تحويل البريد أو المساعدة في ارتكاب هذه الجريمة (الرسمية، قانون 04/18 المتعلق بالقواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية ، عدد 27 في 13 ماي 2018)

ق- سلطة وطنية لحماية المعطيات ذات الطابع الشخصي :استحدثت بموجب قانون رقم 07-18 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي ، تقوم بمهام : _وضع مجموعة التزامات على عاتق المسؤول عن المعالجة الآلية للمعطيات ذات الطابع الشخصي.

-اتخاذ إجراءات إدارية في حالة خرق أحكام القانون من طرف المسؤول عن المعالجة او من ينوبه .
- القيام بالتحريات و معاينة المحلات و الأماكن التي تتم فيها المعالجة .
_تأهيل أعوان الرقابة للقيام بالبحث ومعاينة الجرائم المتعلقة بالمعطيات ذلت الطابع الشخصي تحت إشراف وكيل الجمهورية (الرسمية، قانون 07/18 المتعلق بتحديد قواعد الأشخاص الطبيعيين في معالجة المعطيات ذات الطابع الشخصي، عدد 07/18 سنة 2018)

و- الأقطاب القضائية الجزائية المتخصصة لمكافحة الجرائم الالكترونية، بموجب قانون 14/04 المؤرخ في 10 نوفمبر 2004 المعدل لقانون الإجراءات الجزائية ، تختص الجهات القضائية المتخصصة بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات وفقا للمواد 37،40،329 منه، تتمتع باختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 384/06 المؤرخ في 5 جانفي 2006 حاليا في محكمة مقر المجلس وفقا للمادة 211 مكرر 22 و حاليا متواجد في محكمة دار البيضاء بالجزائر، تختص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال المرتكبة في الخارج حتى و لو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني .

2.3 جزاء ارتكاب الجريمة السيبرانية:

لقد وضع المشرع الجزائري عدت آليات تشريعية لمكافحة الجريمة الالكترونية و الحد منها، ابتداء من الدستور إلى قانون العقوبات ثم إصدار مجموعة قواعد قانونية متخصصة في الجريمة الالكترونية

من خلال تعديله لقانون العقوبات بموجب القانون رقم 15/04 في القسم تحت عنوان "المساس بأنظمة المعالجة الآلية للمعطيات" " الذي حصر الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات من اجل تجريم الأفعال الماسة بأنظمة الحاسب الآلي و التكنولوجيا نظرا لما أفرزت الثورة المعلوماتية و الرقمنة من جهة، ومن جهة أخرى كونها جرائم مستحدثة و خطيرة قد تؤثر على الاقتصاد الوطني و مؤسسات الدولة و بالمجتمع.

أولا: في الدستور الجزائري لسنة 2020 نصت المادة 47 منه على انه " لكل شخص الحماية في حياته الخاصة و شرفه ، تضيف المادة لكل شخص الحق حماية سرية مراسلاته و اتصالاته الخاصة في اي شكل كانت ، وغرض المشرع الجزائري هو حماية الشخص و الحقوق للصيقة بشخصه ، و يستثنى منها اذا اي يكون مسموح بقوة القانون بإضافة عبارة ،إلا بأمر معلل من السلطات القضائية ، حيث تعتبر حماية الأشخاص عند معالجة المعطيات ذات الطابع الشخصي حق أساسي ،يعاقب القانون على انتهاك هذه الحقوق" كما نصت المادة 35 منه على ان " الحريات الأساسية و حقوق المواطن مضمونة."

كما ان الجزائر صادقت على اتفاقية بودابست سنة 2004 من اجل مكافحة الجريمة السيبرانية او المعلوماتية (سليمان، 2022)

ثانيا: قانون العقوبات و في المادة 394 منه ، صنف أنواع الجرائم الالكترونية و العقوبات المقررة لها ،وهي كالتالي:

-جريمتا الدخول و البقاء غير مصرح بهما: نصت المادة 394مكرر من قانون العقوبات " و المقصود من المادة انه :

-بالنسبة لجريمة دخول غير مصرح به و غير مشروع إلى منظومة المعالجة الآلية للمعطيات:القانون الجزائري جرم كل دخول غير مصرح به و غير مشروع إلى منظومة المعالجة الآلية للمعطيات ،مثلا دخول شخص إلى النظام المعلوماتي بدون تصريح من المسؤول أو المالك و ذلك عن

طريق استعمال كلمة المرور أو الشفرة أو الكود سواء تم عن طريق شبكة الاتصالات الهاتفية أو الانترنت.

-أما بالنسبة لجريمة البقاء غير المشروع داخل النظام المعلوماتي فيقصد بها المشرع الجزائري التواجد داخل ذا النظام بالمخالفة لإرادة الشخص صاحب النظام أو من له سيطرة عليه، مثلاً شخص يجد نفس داخل النظام عن طريق الخطأ أو الصدفة إلا أنه قرر البقاء داخل النظام و عدم قطع الاتصال به .

-جريمة الاعتداء على المعطيات: نصت المادة 394 مكرر¹ من قانون العقوبات "يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات كما أضاف المشرع الجزائري إليها عقوبة غرامة، وذلك في العمليات التالية: كل من ادخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزل أو عدل بطريق الغش المعطيات التي يتضمنها" (الرسمية، قانون العقوبات، 1966)

معنى المادة أن المشرع الجزائري وضع ثلاث حالات للمعاقبة على هذه الجريمة:

-الحالة الأولى: إدخال معطيات جديدة غير صحيحة إلى المعطيات الموجودة في النظام .

-الحالة الثانية: أزلت معطيات كانت موجودة في النظام المعلوماتي .

- الحالة الثالثة: تعديل أو تغيير معطيات أو استبدالها بأخرى من خلال برامج معينة تعمل على

إتلاف المعطيات.

-جريمة التعامل في المعلومات غير مشروعة: نصت المادة 394 مكرر² من قانون العقوبات "يعاقب بالحبس من شهرين إلى ثلاث سنوات ، إضافة إلى غرامة ، حسب مفهوم المادة ، كل من يقوم عمداً أو عن طريق الغش بما يلي:

__تصميم أو بحث أو توفير أو نشر أو الاتجار في معطيات وكل العمليات التي تقع على المعطيات و قد تكون هذه المعطيات مخزنة أو معالجة أو مرسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم السابقة .

__حيازة أو إفشاء أو إعلام الغير أو نشر إضافة إلى اي استعمال لآي غرض كان المعطيات المتحصل عليها " (الرسمية، قانون الإجراءات الجزائية ، 1966)

ثالثا:-قانون رقم 04/09 المتعلق بالقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال و مكافحتها: حصرت حالات لمراقبة الاتصالات الالكترونية و تجميع و تسجيل محتواها و القيام بإجراءات التفتيش و الحجز داخل منظومة معلوماتية بإذن من السلطات الأمنية و القضائية و موافقتها و هذه الحالات هي:

__الحالة الأولى: الوقاية من الأفعال الموصوفة بجرائم الإرهاب أو الجرائم الماسة بأمن الدولة .

__الحالة الثانية:توفر معلومات عن احتمال الاعتداء على المنظومة المعلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

__الحالة الثالثة: مقتضيات التحري و التحقيقات القضائية خاصة إذا تطلب التحقيق خبرة في المجال في إطار المساعدة القضائية الدولية من أي دولة في إطار اتفاقية متبادلة .

-كما نصت المادة 5منه:لضباط الشرطة القضائية و السلطات القضائية المختصة الدخول للقيام بالتفتيش و لو عن بعد في منظومة معلوماتية أو جزء منها و كذا المعطيات المعلوماتية التي تكون مخزنة فيها او الدخول إلى أي منظومة معلوماتية في حالتين فقط:

-في إطار أعمال التحقيق الذي تقوم ب السلطة القضائية .

-في إطار أعمال البحث و الاستدلال الذي تقوم به الضبطية القضائية بأمر من السلطة

المختصة.

رابعا: جاء في القانون رقم 04/15 المتعلق بالتوقيع و التصديق الإلكتروني:و نص هذا القانون

على تجريم الأفعال المرتبطة بالبيانات و المعلومات ذات الطابع الشخصي مثل:

جريمة إفشاء البيانات الشخصية أو أساءت استعمالها :نصت المادة 68منه على انه"يعاقب كل

من يقوم بحيازة أو إفشاء أو استعمال بيانات لإنشاء توقيع الكتروني موصوف خاص بالغير يعاقب

بالحبس من ثلاث أشهر إلى ثلاث سنوات وب عقوبة تكميلية غرامة من مليون دج إلى خمسة مليون دج أو بإحدى العقوبتين فقط.

جريمة الإخلال بسرية البيانات: نصت المادة 42 منه "يعاقب بالحبس و الغرامة أو بإحدى العقوبتين، لذا يجب على مؤدي خدمات التصديق الالكتروني أن يحافظوا على سرية البيانات و المعلومات المتعلقة بشهادة التصديق الالكتروني الممنوحة .

جريمة جمع البيانات الشخصية للمعني دون موافقته: نصت المادة 43 منه "لا يمكن لمؤدي خدمات التصديق الالكتروني أن يجمع بيانات الشخصية للمعني إلا بموافقته الصريحة ومتى اخل بهذا الواجب يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 200000 دج إلى مليون دج أو بإحدى العقوبتين (المومن، 2022)

خامسا: القانون رقم 04/18 المتعلق بالقواعد العامة المتعلقة بالبريد و الاتصالات الالكترونية جاء فيه عدم استعمال شبكات و خدمات الاتصال الالكترونية لخرق الحياة الخاصة لأفراد، وفي حالة المخالفة تعتبر جريمة يعاقب عليها القانون، أمثلتها:

انتهاك سرية المراسلات الالكترونية: نصت المادة 164 منه على انه " كل شخص ينتهك سرية المراسلات المرسله الشخصية للإنسان عن طريق البريد أو الاتصالات الالكترونية أو يفشي مضمونها أو نشرها أو استعمالها بدون ترخيص بمفهوم المادة يعاقب بالحبس من سنة الى خمسة سنوات إضافة إلى غرامة من 500000 دج إلى مليون دج ، كما يعاقب بالحبس من سنة إلى خمسة سنوات و غرامة خمس مئة الف دينار ج إلى مليون دج كل شخص قام بتحويل المراسلات الصادرة عن طريق البريد من مليون الخمس ملايين أو بإحدى العقوبتين كل من يحول المراسلات الصادرة أو المرسله أو المستقبله عن طريق الاتصالات الالكترونية .

سادسا: القانون رقم 07/18 المتعلق بتحديد قواعد حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي: جاء من اجل حماية الحياة الخاصة للأفراد

المعطيات ذات الطابع الشخصي "كل معلومة متعلقة بشخص يكون معرف او قابل للتعريف بصفة مباشرة او بصفة غير مباشرة ،عنصر من عناصر هويته البدنية، الفيزيولوجية ،الجينية ،البومترية ،النفسية ، الثقافية ،الاجتماعية" لان الحياة الخاصة نقصد بها :حق الفرد في اختيار أسلوب حياته دون أي تدخل من الغير في حدود النظام العام، و حق الفرد في سرية ما ينتج عن هذه الحرية.(الجبوري، 2022)

و عليه فان : جريمة معالجة المعطيات فهي "كل عملية منجزة بوسائل آلية على المعطيات ذات طابع شخصي،بتسجيل ، الحفظ ، النشر ، التشفير ،المسح أو الإتلاف " والعقوبة عليها تكون على كل عملية:

خرق الحياة الخاصة عند معالجة المعطيات:يعاقب بالحبس و الغرامة.

معالجة المعطيات الشخصية رغم اعتراض الشخص المعني

الاستعمال غير الشرعي للمعطيات الشخصية

جمع المعطيات الشخصية بطريقة غير شرعية

اللوغ غير الشرعي للمعطيات الشخصية :يعاقب بالحبس و الغرامة أو بإحدى العقوبتين

-إفشاء المعلومات الشخصية :يعاقب بمادة 301 من قانون عقوبات بقولها "انه يعاقب من

شهر إلى ستة أشهر و بغرامة عشرين ألف دج إلى مئة ألف دج .

-الاحتفاظ بالمعلومات الشخصية أكثر من المدة القانونية: يعاقب بغرامة مالية.

-نقل المعطيات الشخصية و تقديمها إلى دولة أجنبية: يعاقب بعقوبة سالبة للحرية و عقوبة

تكميلية تتمثل في غرامة.

لقد تم استحداث سلطة وطنية لحماية المعطيات ذات الطابع الشخصي (رضا، 2021)

، من اجل اتخاذ الإجراءات الإدارية في حالة خرق أحكام هذا القانون، و المساعدة على تنفيذ

و تطبيق هذا القانون.

4. خاتمة:

الجريمة السيبرانية او الجريمة الالكترونية هي بين الجرائم المستحدثة و الأشد خطورة على المجتمع الدولي ، لذا لابد من تضافر الجهود من اجل مكافحتها و القضاء عليها و معاقبة مرتكبيها ، و بما إن الجزائر شاركت في المؤتمر الثالث عشر للأمم المتحدة لمنع الجريمة و العدالة الجنائية و رغم ان هذه الجرائم غير معروفة في المجتمع الجزائري و من يرتكبها لا يدرك مخاطرها إلا أنها وضعت قواعد قانونية لمعاقبة على هذه الجرائم و مجموعة من الآليات و الميكانيزمات من اجل تحقيق الأمن السيبراني في البلاد ، خاصة و أنها تتجه نحو رقمته جميع القطاعات مثل العدالة و التعليم و الدفاع الوطني .

أهم النتائج المتوصل إليها من خلال هذه الورقة البحثية:

- الجرائم السيبرانية جرائم يصعب التحكم فيها و التصدي لها
- الجرائم السيبرانية تزداد خطورة في ظل التطور التكنولوجي و الالكتروني الرقمي و الشبكة الانترنت و استخدام مواقع التواصل الاجتماعي
- عدم التوعية و النشر بثقافة الأمن السيبراني و معاقبة المرتكبين لها يؤدي إلى زيادة انتشار هذه الجرائم

أهم التوصيات المقترحة :

- إدراج مادة الأمن السيبراني في الجامعات و المدارس العسكرية و الأمنية و مدرسة القضاء ، وإنشاء مدرسة خاصة بالأمن السيبراني .
- إنشاء أجهزة وطنية تابعة لوزارة الدفاع الوطني مختصة في الأمن السيبراني
- تدريب و تأهيل وحدات عسكرية و أمنية خاصة ، من اجل تأمين المنظومة المعلوماتية من الهجمات السيبرانية خاصة الهجمات الإرهابية
- وضع نظام قانوني للجرائم المستحدثة مع إنشاء محاكم متخصصة في معاقبة على بجميع الجرائم المستحدثة
- وضع اتفاقية دولية أو اتفاقيات إقليمية لمكافحة الجريمة الالكترونية أو السيبرانية

التنسيق و التعاون الدولي بين الحكومات و الدول معاقبة مرتكبي هذه الجرائم.
تبقى رغبة و إرادة الدول هي أساس النجاح من اجل مكافحة و القضاء على هذه الجرائم التي
تهدد العالم ككل، من اجل تحقيق استقرار المجموعة الدولية و الحفاظ على العنصر البشري .

5. قائمة المراجع:

أولاً: النصوص القانونية

أ-القوانين:

-قانون رقم 04/09، المؤرخ في 5 اوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم
لمتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها، الجريدة الرسمية، عدد47، سنة 2009.
-قانون رقم 04/18، المؤرخ في ماي 2028، يحدد القواعد العامة المتعلقة بالبريد و
الاتصالات الالكترونية، الجريدة الرسمية، عدد27، سنة 2018.
- قانون 07/18، المؤرخ في جويلية 2018، يتعلق بتحديد قواعد الأشخاص الطبيعيين في
معالجة المعطيات ذات الطابع الشخصي، الجريدة الرسمية، عدد34، سنة 2018.

ب-الأوامر:

-الأمر رقم 66_156، المؤرخ في 8 جويلية 1966، المتضمن قانون العقوبات، المعدل و
المتمم، الصادر في الجريدة الرسمية، عدد15، سنة 2009.
الأمر رقم 66_156، المؤرخ في 8 جويلية 1966، المتضمن قانون الإجراءات الجزائية، المعدل و
المتمم، الصادر في الجريدة الرسمية، عدد84، سنة 2006.

ثانياً: المؤلفات

-حنان ربحان مبارك، المضحكي، (2014)، الجرائم المعلوماتية دراسة مقارنة، منشورات
الحلبي الحقوقية، الأردن.
- سليم عبد الله، الجبوري، (2022)، الحماية القانونية لمعلومات شبكة الانترنت، الطبعة
الأولى، منشورات الحلبي الحقوقية. الأردن.

ثالثاً: المقالات

-بوضياف أسمهان، (2018)، الجريمة الالكترونية و الإجراءات التشريعية لمواجهتها، مجلة
الإستاد الباحث للدراسات القانونية و السياسية، مجلد3، (عدد3)، ص350.

- بارة سميرة، (2017)، الأمن السيبراني في الجزائر، السياسات و المؤسسات، المجلة الجزائرية للأمن الإنساني، مجلد2، (عدد2)، ص259.
- سي حميدي عبد المؤمن، قيرة سعاد ، (2022)، الجريمة الالكترونية و آليات التصدي لها في القانون الجزائري ، مجلة البيان للدراسات القانونية و السياسية، مجلد7، (عدد1)، ص67.
- قط سمير، كزيز صباح ، (2018)، اثر الجريمة الالكترونية على امن و استقرار الدول :قرصنة الموقع الالكتروني لوكالة الأنباء القطرية نموذجا، مجلة الناقد للدراسات السياسية، مجلد2، (عدد2)، ص121.
- خلوفي رشيد، بوحية شهرزاد، (2019)، تحديات الجريمة الالكترونية في الجزائر، مجلة الاستاد الباحث للدراسات القانونية و السياسية، مجلد4، (عدد2)، ص1997.
- المايل عبد السلام محمد ، الشريجي محمد عادل، (2019)، لجريمة الالكترونية في الفضاء الالكتروني المفهوم والأسباب، سبل مكافحة مع التعرض لحالة ليبيا، مجلة الأفق للبحوث و الدراسات، مجلد2، (عدد2)، ص245.
- مهدي رضا، (2021). الجرائم السيبرانية و آليات مكافحتها في التشريع الجزائري ،مجلة ايليزا للبحوث و الدراسات، مجلد6، (عدد2)، ص125.
- قطاف سليمان، بوقرين عبد الحليم، (2020)، الآليات القانونية الموضوعاتية لمكافحة الجرائم السيبرانية في ظل اتفاقية بودابست و التشريع الجزائري، المجلة الأكاديمية للبحوث القانونية و السياسية، مجلد6، (عدد1)، ص337.
- مينة جيلالي، عروس كوثر، (2022)، الجريمة السيبرانية في صورها المستحدثة ،مجلة القانون و التنمية، مجلد6، (عدد1)، ص55.
- رابعا: المداخلات
- دياب موسى، البدانية، (2004/2003)، الجرائم الالكترونية المفهوم و الأسباب ، الجرائم المستحدثة في ظل المتغيرات و التحولات الإقليمية و الدولية، كلية العلوم الإستراتيجية ،الأردن.