الجريمة السيبرانية وآليات مكافحتها - مواجهة تحديات الأمن السيبراني -

Cybercrime and mechanisms to combat it - Facing cyber security challenges –

قادري نورالهدى

مخبر المرافق العمومية والتنمية، جامعة جيلالي اليابس، سيدي بلعباس(الجزائر)

Inasse223@gmail.com

تاريخ الإرسال: 2023/03/07 تاريخ القبول: 2023/05/11 تاريخ النشر: 2023/06/01

****

ملخص:

تهدف هذه الورقة البحثية إلى دارسة موضوع الجريمة السيبرانية باعتبارها من بين المواضيع القانونية الحديثة التي ظهرت تزامنا مع ظهور وانتشار الثورة التكنولوجية التي أثرت وبدرجة كبيرة على جميع مناحي الحياة الاقتصادية والاجتماعية والإدارية.

ونظرا لطابع الخصوصية التي تتميز بها الجرائم السيبرانية باعتبارها أنها من بين الجرائم التي يصعب اكتشافها وإثباتها أمام القضاء ،إضافة إلى أنها تعد من الجرائم العابرة للحدود، فلقد عمل المشرع الجزائري على غرار مختلف التشريعات المقارنة على إتخاذ مجموعة من التدابير والآليات القانونية لمكافحتها وردع مرتكبيها بهدف تحقيق الأمن السيبراني على مختلف المعاملات والمواقع الإلكترونية، وهو ما نستشفه من القانون رقم 04/09 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال .

الكلمات المفتاحية:

التطور التكنولوجي، الجريمة السيبرانية ، المجرم السيبراني ، القانون رقم 04/09 ، الأمن السيبراني .

Abstract:

This research paper aims to study the issue of cybercrime as one of the modern legal topics that appeared synchronically with the emergence and spread of the technological revolution, which greatly affected all aspects of life, and with which traditional transactions turned into transactions that take place through cyberspace.

Given the nature of privacy that characterizes cybercrime, as it is among the crimes that are difficult to detected and proved before the judiciary, in addition to being considered as one of the border crime, the Algerian legislator has worked, along the lines of various comparative legislations, to take a set of legal measures and mechanisms to combat it and deter its perpetrators in order to achieve Cyber security on various transactions and websites, the latter we learn from Law No. 09/04 concerning crimes related to information and communication technology.

Key words:

technological development , cyber crime , cyber criminal , Law No. 09/04 , Cyber security.

مقدمة:

لقد شهدت الألفية الأخيرة من الزمن تطورا إلكترونيا مذهلا صاحبه تطور وتبادل المعلومات والتقنيات العلمية ووسائل الاتصال الفوري وظهور شبكة المعلومات التي أدت إلى فتح أبواب عالمية لتسهيل التعاملات والتبادلات ما بين الأفراد التي تحولت من تعاملات تقليدية إلى تعاملات إلكترونية تبرم عبر فضاء رقمي .

غير أنه في ذات الوقت يعد التطور التكنولوجي المذهل الذي يعيشه العالم سلاحا ذو حدين ، فبالرغم من الإيجابيات التي حققتها،إلا أن هذا لا ينفي انعكاساتها السلبية التي تولدت عنها وأثرت وبدرجة كبيرة على المجتمع، وقد ظهرت ملامحها في استخدام واستغلال مختلف التقنيات التكنولوجية الحديثة بصورة غير مشروعة، مما أدى إلى تنامي وتزايد انتشار نوع من الجرائم لم تكن معروفة سابقا ألا وهي الجرائم السيبرانية أو ما يطلق عليها بالجرائم الإلكترونية التي تهدف إلى إضرار بمصالح الأفراد وكذا الجماعات والدول .

وفي هذا الصدد أصبحت تشكل الجرائم السيبرانية الشغل الشاغل للدول والمنظمات الدولية خاصة في السنوات الأخيرة لاتخاذ كافة الإجراءات و التدابير اللازمة للتصدي لهذه الأخيرة ووضع حد لمرتكبيها، فالجزائر كغيرها من الدول لم تكن في منأى من تداعيات هذه الظاهرة وهو ما تطلب بالضرورة تدخل المشرع الجزائري على غرار مختلف التشريعات المقارنة إلى تكريس مجموعة من الآليات وكذا الإجراءات القانونية والتقنية على حد سواء لمكافحة هذه الجرائم.

ويكتسي موضوع مكافحة الجريمة السيبرانية أهمية ومكانة كبيرة في مختلف التشريعات الدولية منها والعربية بما فيها التشريع الجزائري، والتي عملا على مكافحة هذه الأخيرة والتصدي لها بهدف تحقيق وتفعيل الأمن السيبراني لمختلف المعاملات الإلكترونية .

وعليه تتمحور إشكالية الدراسة في البحث عن طابع الخصوصية التي تتميز بها الجرائم السيبرانية ؟ ومدى نجاعة الآليات الإجرائية و كذا التقنية في مكافحتها ؟.

وللإجابة عن هاته **الإشكالية** ارتأينا تقسيم موضوع دراستنا إلى **محورين** أساسين هما:

- **المبحث الأول:** مفهوم الجريمة السيبرانية
- **المبحث الثاني:** فتم التطرق فيه إلى الآليات الإجرائية والتقنية لمكافحة الجريمة السيبرانية في ظل التشريع الجزائري.

وسيتم إتباع المنهج التحليلي الوصفي من خلال التطرق إلى مفهوم الجريمة السيبرانية عن طريق التعرف عليه وعلى أهم الخصائص التي تميزها عن غيرها من الجرائم التقليدية إضافة إلى التعرف على الآليات الإجرائية

و كذا التقنية المكرسة في ظل التشريع الجزائري لمكافحتها و ردع مرتكبيها ، ولقد تم الاستناد إلى المنهج الاستقرائي من خلال استقراءنا لبعض النصوص القانونية ذات الصلة بموضوع الدراسة.

المبحث الأول

مفهوم الجريمة السيبرانية

لقد تطورت أساليب ارتكاب الجرائم عن ما هو معروف سابقا ، فلم تعد الاعتداءات تهدف النفس والمال فقط ، بل تعدتها إلى المعلومات والبيانات الخاصة بمتعاملي البيئة الرقمية، إذ أصبح بإمكان المجرمين إرتكاب أبشع الجرائم في هدوء تام دون إراقة للدماء ، وذلك بسبب ظهور نوع جديد من الجرائم لم تكن معروفة سابقا، يطلق عليها بالجرائم السيبرانية.

وبناء على ذلك سنخصص المبحث الأول للتعرف على هذا النوع الجديد من الجرائم من خلال التطرق إلى تعريفها و إلى الخصائص التي تميزها عن الجرائم التقليدية وذلك في (**المطلب الأول**) وإلى إطارها القانوني (**المطلب الثاني**) .

المطلب الأول: تعريف الجريمة السيبرانية وخصائصها

سوف نحاول من خلال هذا المطلب التطرق إلى تعريف الجريمة السيبرانية وإلى أهم الخصائص التي تميزها عن الجريمة التقليدية .

الفرع الأول : تعريف الجريمة السيبرانية

لم يعرف المشرع الجزائري شأنه شأن جل التشريعات العقابية المقارنة الجريمة السيبرانية، ولعل سبب يرجع في كون أن وضع التعاريفات للمفاهيم القانونية العامة هو عمل فقهي وليس من عمل المشرع .

لذلك يعرف الفقه القانوني الجريمة بصفة عامة على أنها " فعل غير مشروع صادر عن إرادة جرمية يقرر له القانون العقوبة أو التدبير إحترازيا."[1] ، كما تعرف على أنها " كل تصرف جرمه القانون سواء كان إيجابيا أو سلبيا كالإمتناع ما لم يرد نص على خلاف ذلك ".[2]

أما بالنسبة لمفهوم الجريمة السيبرانية فلم يتفق الفقهاء والباحثون على تعريف موحد لهذه الأخيرة، فمنهم من ينظر إلى موضوع الجريمة في حد ذاتها،وهناك من ينظر إلى الوسيلة المستعملة في إرتكابها ، هذا على غرار أنهم لم يتفقوا على تسمية موحد لهذا النوع الجديد من الجرائم التي تباينت تسمياتها عبر مراحل زمنية ارتبطت بتقنية المعلومات[3]، فهناك من يطلق عليها بتسمية الجرائم السيبرانية "cybre crime"وهناك من يطلق

---

(1)- فريد روابح ، محاضرات في القانون الجنائي العام ، مطبوعة الدروس لسنة الثانية ليسانس ، قسم الحقوق ، كلية الحقوق والعلوم السياسية ، جامعة محمد لمين دباغين ، سطيف ، 2019/2018 ، ص 29 .

(2)–مرجع نفسه ، ص 29 .

(3)- رامي متول القاضي ، مكافحة الجرائم المعلوماتية ، دون طبعة ، دار النهضة العربية ، مصر ، 2011 ، ص 17 .

عليها بتسمية الجرائم الإلكترونية وجانب أخر من الفقه يطلق عليها بتسمية إساءة إستخدام تكنولوجيا المعلومات والإتصال ،كما يطلق عليها أيضا بجرائم الكومبيوتر والأنترنت .

وعلى العموم يتراوح تعريف الجريمة السيبرانية بين الجرائم التي ترتكب عبر الحاسب الآلي وبين الجرائم الني ترتكب عبر مختلف المعدات الرقمية ، غير انه يمكن تعريفها على أنها " نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسب الآلي وشبكة الأنترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي.[1]

كما يمكن تعريفها على أنها " سلوك غير قانوني يتم بإستخدام الأجهزة الإلكترونية ، ينتج عنها حصول المجرم الرقمي على فوائد مادية ومعنوية، وغالبا ترتكب هذه الجرائم عبر القرصنة أو الإختراق للأنظمة المعلوماتية" .[2]

وتعرف أيضا على أنها " السلوك غير المشروع و المنافي للأخلاق أو غير المسموح به المرتبطة بالشبكات المعلوماتية العالمية فهي تعد من الجرائم العصر الرقمي التي تطال بالمال والمعرفة والثقة والسمعة وهي كلها تنفذ عن طريق التقنية ." [3]

أما بالنسبة للمشرع الجزائري نجده أنه لم يستقر على استخدام مصطلح واحد للدلالة على هذه الجرائم حيث أطلق عليها تسمية " الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات " و ذلك بموجب القانون رقم 15/04 المتعلق بقانون العقوبات[4] ، كما أن استخدم مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال[5] ، وتعتبر هذه التسميات التي اعتمد عليها المشرع الجزائري دلالة على الجرائم السيبرانية حيث عرفها على أنها" جرائم الماسة بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الإتصال الإلكترونية ."[6]

---

(1)- جدو بن علية ، تحديات الأمن السيبراني في مواجهة الجريمة السيبرانية ، المجلة الجزائرية للأمن الإنساني ، جامعة الحاج لخضر ، باتنة ، المجلد 07 ، العدد 02 ، جويلية 2022 ، ص 304 .

(2) -علي قويدري ، أمال العيش ، الجريمة السيبرانية مفهومها و سبل الوقاية منها ، مجلة نوميرس الاقتصادية ، المجلد الثالث ، العدد 01 ، 2022 ، ص 194 .

(3)- روان بنت عطية الله الصحفي. الجرائم السيبرانية ، المجلة الإلكترونية الشاملة متعددة التخصصات ، العدد 24، ماي2020 ، ص 08 .

(4) - القانون رقم 15/04 ، المؤرخ في 2004/11/10 ، المعدل و المتمم للقانون رقم 156/66 ، المتضمن قانون العقوبات ، الجريدة الرسمية ، العدد 71 ، لسنة 2004 .

(5)- القانون رقم 04/09، المؤرخ في 2009/08/05 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته ، الجريدة الرسمية ، العدد 47 ، الصادر بتاريخ 2009/08/16.

(6) -المادة 01 من القانون رقم 04/09 ، السابق ذكره.

الفرع الثاني : خصائص الجريمة السيبرانية

إن طبيعة الخاصة التي تتميز بها الجرائم السيبرانية جعلها تنفرد بمجموعة من الخصائص والمميزات التي تميزها عن غيرها من الجرائم التقليدية ، ويرجع ذلك إلى الوسط التي ترتكب فيه هذه الجريمة ، وكذا الأداة أو الوسيلة المجرم الرقمي في إرتكابها ، وتتمثل هذه الخصائص في :

- بأنها جرائم تتم عبر التقنيات التكنولوجية الحديثة، وعلى رأسها شبكة الأنترنت التي تعتبر كوسيلة لارتكابها .

- **من حيث الهدف** : تستهدف الجريمة السيبرانية الأنظمة المعلوماتية من خلال قرصنتها بهدف إحداث تغيير أو تحريف في المعلومات والبيانات الخاصة بمتعاملي البيئة الرقمية على غرار الجرائم التقليدية .

- **جريمة ناعمة** : تتميز الجرائم السيبرانية بأنها جريمة ناعمة ، وذلك لخفتها لكونها متسترة في أغلبها ، فقد لا يلاحظ الضحية إرتكابها رغم أنها قد تقع أثناء وجوده على الشبكة، فالجاني يتمتع بقدرات فنية فائقة تمكنه من إرتكابها بمهارات عالية دون ملاحظة ذلك[1] مثل سرقة الأموال ، أو إرسال الفيروسات المدمرة على البرامج والحاسوب الآلي .

- **صعوبة اكتشافها** : تعتبر الجريمة السيبرانية من الجرائم التي يصعب إكتشافها ولذلك لعدم تركها لآثار مادية يمكن من خلالها كشف مرتكب هذه الأخيرة[2]، مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق، فداخل هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية ، مما يجعل أمر طمس هذا الدليل الإلكتروني ومحوه كليا من قبل الفاعل أمر في غاية السهولة .[3]

-**جريمة ذات بعد دولي** : تعد الجرائم السيبرانية جرائم عابرة للحدود لا تعترف بعنصر الزمان والمكان ، فهي تتميز بالتباعد الجغرافي واختلاف التواقيت بين الجاني والمجني عليه[4]، وهذا راجع إلى مجتمع المعلومات الذي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح على شبكات تخترق الزمان والمكان دون أن تخضع لحرس الحدود.

- تعتبر الجرائم السيبرانية من بين الجرائم التي يتطلب إلمام مرتكبيها بالجوانب التقنية وكذا الخبرة الفائق في استخدام الحاسب الآلي .

---

(1)-يوسف الصغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة ماجستير ، قسم الحقوق ، كلية الحقوق والعلوم السياسية، جامعة مولود معمر ، تيزي وزو ، 2013/2012 ، ص ص 15.14 .

(2) -رضا مهدي ، المرجع السابق ، ص 114 .

(3)-عبد المؤمن الصغير ، الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن ، مجلة الحقوق والحريات ، جامعة محمد خيضر – بسكرة -المجلد 02 العدد 02 ، 2014 ، ص 08 .

(4)-علي قويدري ، أمال العيش ، المرجع السابق ، ص 201 .

- **إمتناع المجني عليه عن التبليغ** : لا يتم في الغالب الأعم الإبلاغ عن جرائم الأنترنت إما لعدم اكتشاف الضحية لها وإما خشية من التشهير ، لذا نجد أن معظم الجرائم التي تتم عبر الأنترنت تم اكتشافها بالمصادفة بل وبعد وقت طويل من إرتكابها .[1]

- **تعتبر الجرائم السيبرانية أقل عنفا في التنفيذ** : فهي تمتاز بعدم استخدام القوة الجسدية لتحقيق الهدف ، فهي تعد من بين الجرائم التي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من الجهد العضلي الذي يكون في صورة ممارسة العنف والإيذاء كما هو الحال في جريمة القتل والإغتصاب[2] على عكس الجرائم الأنترنت التي تتميز بأنها جرائم هادئة بطبيعتها فكل ما تحتاج إليه هو القدرة على التعامل مع جهاز الحاسوب بمستوى تقني يوظف في ارتكاب الأفعال الغير المشروعة .

- **صعوبة ضبط وتوصيف الجرائم السيبرانية** : أن من بين الصعوبات التي تواجه ضباط الشرطة القضائية والمحققين وكذا القضاة خاصة فيما يتعلق بإجراءات ضبط الجرائم المعلوماتية وإضفاء الوصف القانوني المناسب لها، ولعل مرد ذلك إلى الطبيعة الخاصة التي تتميز بها هذه الأخيرة . [3]

المطلب الثاني: الإطار القانوني للجريمة السيبرانية

إن دراسة الجريمة السيبرانية وحدها أمر غير كافي ما لم يتم دارسة المجرم السيبراني والأساليب التي يعتمد عليها في إرتكابه هذا النوع من الجرائم . وهو ما سنتطرق إليه في المطلب الثاني .

الفرع الأول : المجرم السيبراني

لقد تعددت التسميات التي أطلقت على هذه الطائفة من المجرمين بين " قراصنة المعلوماتية " أو " المجرم المعلوماتي " وهناك من أطلق عليهم تسمية " مجرم الأنترنت " أو " مجرم التقنية " .

ويعرف المجرم السيبراني هو ذلك المجرم الذي له القدرة على تحويل لغته إلى لغة رقمية وتخزينها واسترجاعها باستخدام الحاسوب الإلكتروني في ملحقاته ووسائل الإتصال الرقمي، وذلك بأداء فعل والإمتناع عنه ، مما يحدث عنه إحداث اضطراب في المجتمع الدولي والمحلي .[4]

كما يعد المجرم السيبراني ذلك الشخص الذي يتمتع بمجموعة من المميزات التي لا نجدها عند كل الأشخاص[5]، إذ يتميز بقدرة فائقة من الذكاء الذي يقوم باستغلاله واستغلال مهارته الفائقة في مجال استخدام

---

(1) -عبد المؤمن الصغير ، المرجع السابق ، ص 75 .

(2) -صالح بن محمد المسند ، عبد الرحمان بن راشد المهيني ، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية و التدريب ، المجلد 15 ، العدد 29 ، أفريل 2000 ، ص 20 .

(3) -عبد المؤمن الصغير ، المرجع السابق ، ص 75 .

(4) -سهام خليل ، خصوصية المجرم السيبراني ، مجلة المفكر ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر ، بسكرة ، المجلد 17 ، العدد 15 ، 2017 ، ص 401 .

(5) - روان بنت عطاء الله الصحفي ، المرجع السابق ، ص 14 .

الحاسب الآلي والتقنيات التكنولوجية الحديثة في الاختراق والقرصنة الإلكترونية للأنظمة المعلوماتية وكذا التلاعب بالبيانات والمعلومات الشخصية لمتعاملي البيئة الافتراضية .

ولقد أثبتت الدراسات النفسية أن المجرم السيبراني ليس لديه أي شعور بعدم مشروعية الأفعال التي يقوم بها واستحقاقهم للعقاب ، كما تغيب لديه مشاعر الإحساس بالذنب[1] ، ولقد تعددت أنماط المجرمين في إرتكابهم للجرائم السيبرانية وهما :

- **النمط الأول يطلق عليهم بالهاكارز** : يقصد به الشاب البالغ المفتون بالمعلوماتية حيث يطلق عليهم إسم صغار نوابغ المعلوماتية ، فهم قراصنة محترفون الذين يستغلون خبراتهم وإمكانياتهم في مجال تقنية المعلومات للحصول على معلومات سرية معينة أو تغييرها و تحريفها أو من اجل قرصنة الأنظمة المعلوماتية معينة وإلحاق الضرر بصاحبه بقصد الانتقام أو الإبتزاز[2].
- **النمط الثاني يطلق عليهم بالكراكرز**: كما يطلق عليهم بالمخترفن الذي يتميزون بالقدرات التقنية العالية في اختراق الأنظمة المعلوماتية والأجهزة الإلكترونية تحقيقا لأهداف غير مشروعة كالتلاعب بالبيانات والمعلومات قصد تغييرها و تحريفها[3]وتعد هذه الطائفة أكثر خطورة من الصنف الأول .
- **النمط الثالث يطلق عليهم بالحاقدين** : غالبا ما يطلق على هذه الفئة بالمنتقمين لأن صفة الانتقام والثأر هي ما تتميز بها عن الطوائف الأخرى ، فهي فئة لا تهدف إلى إثبات قدراتها أو تحقيق مكاسب مادية ، وإنما تسعى إلى تخريب الأنظمة المعلوماتية عن طريق زراعة الفيروسات والبرامج المضارة .[4]

و يتميز **المجرم السيبراني** بمجموعة من **السمات** يمكن استخلاصها فيما يلي :

- شخص محترف يتمتع بقدرات ومهارات عالية لا يستهان بها في مجال التعامل بالتقنيات الحاسوب والأنترنت .[5]
- أنه شخص عائد إلى الإجرام يوظف مهاراته في إختراق وإحداث تغييرات في المعلومات والبيانات الإلكترونية .
- أنه مجرم غير عنيف نظرا لطبيعة الجريمة التي تتميز بلا عنف .

---

(1) - روان بنت عطاء الله الصحفي ، المرجع السابق ، ص 14 .

(2) - نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة و التوزيع ، الأردن 2008 ، ص 08 .

(3)- مرجع نفسه ، ص 08 .

(4) - نوال قادة عبد الله ، محمد بن حمو ، الجريمة الإلكترونية قراءة سوسيولوجية لأهم النظريات المفسرة لسلوك الإجرامي ، مجلة الروافد للدراسات والأبحاث العلمية في العلوم الإجتماعية الإنسانية ، جامعة عين تموشنت . المجلد06 ، العدد 03 ، ديسمبر 2022 ، ص 668 .

(5) - فتيحة رصاع ، الحماية الجنائية للمعلومات عبر شبكة الأنترنت ، مذكرة مقدمة لنيل شهادة الماجستير في القانون قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة أبي بكر بلقايد – تلمسان – 2012/2011 ، ص 51 .

- يتميز المجرم السيبراني بأنه مجرم ذكي ، يتمتع بالذكاء المعلوماتي الذي يمكنه من التعديل والتطوير من الأنظمة الأمنية، حتى لا يكون من الممكن ملاحقته وتتبع أعماله الإجرامية عبر الشبكات وداخل أجهزة الحواسيب مما يجعل من الصعب تصنيفه حسب التصنيف الإجرامي المعتاد .

الفرع الثاني : أنواع الجرائم السيبرانية التي يرتكبها المجرم السيبراني

يعتمد المجرم السيبراني في ارتكابه للجرائم السيبرانية على مجموعة من الطرق والأساليب في إرتكابها التي تتمثل أبرزها في :

– **تخريب المعلومات و إساءة استخدامها** : ويشمل ذلك قواعد المعلومات ، والمكتبات، تمزيق الكتب ، تحريف المعلومات ... إلخ [1].

– **التزوير المعلوماتي** : عرفه المشرع الفرنسي على انه " كل تغيير بطريق الغش للحقيقة في مكتوب أو في أي دعامة أخرى تحتوي تعبير فن الفكرة . " [2] أما بالنسبة للمشرع الجزائري فنلاحظ لم يعرف جريمة التزوير المعلوماتي وبالضبط في قانون العقوبات .

- **القرصنة الإلكترونية**[3]: تعد القرصنة الإلكترونية ليست سوى عملية دخول غير مصرح به إلى أجهزة الغير وشبكاتهم الإلكترونية[4]، وتأخذ القرصنة الإلكترونية صورتين هما :

* **جريمة الدخول الغير المرخص به للأنظمة المعلوماتية** : ويكون بمجرد الولوج إلى النظام المعلوماتي دون علم صاحبه و دون رضاه .

* **جريمة البقاء الغير المرخص به النظام الآلي للمعالجة للمعطيات**[5]: أحيانا لا يكتفي المجرم السيبراني بمجرد الدخول إلى النظام المعلوماتي دون علم ورضا صاحبه بل يذهب إلى أكثر من ذلك من خلال بقائه داخل النظام و يقوم بالتلاعب بالبيانات والمعلومات الشخصية والسرية بدافع الإنتقام والإبتزاز وغالبا ما يقوم بهذه الجريمة **بالقراصنة** الحاقدون .

ولقد تناول المشرع الجزائري هذا النوع من الجرائم السيبرانية (الإلكترونية) من المواد 394 مكرر إلى المادة 394 مكرر07 جرم من خلالها الأفعال المتصلة بالمعالجة الآلية للمعطيات6، حيث إدراكا منه بضرورة تعزيز

---

(1)-علي قويدري ، أمال العيش، المرجع السابق ، ص 203 .

(2)- المادة 441 /01 من قانون العقوبات الفرنسي ، المعدل بموجب القانون رقم 1336/92 ، المؤرخ في 16 ديسمبر 1966 .

(3) - كما تعرف على أنها " ليست سوى عملية اختراق لأجهزة الحاسوب أو المواقع التي تتم عبر شبكة الأنترنت ، يقوم بها شخص أو مجموعة من الأشخاص متمكنين في اختراق برامج الحاسوب ".

(4) -أشرف سعيد أحمد ، القرصنة الإلكترونية ، د ط ، د د ن ، د ب ن ، 2013 ،ص ص 62 ، 63 .

(5)- المادة 394 مكرر من القانون رقم 23/06 ، المؤرخ في 2006/12/20 ، المتضمن تعديل قانون العقوبات ، الجريدة الرسمية ، العدد 84 ، الصادرة بتاريخ 2006/12/24 .

(6) -القانون رقم 15/04 ، المؤرخ في 2004/11/10 ، المعدل و المتمم للقانون رقم 156/66 ، المتضمن قانون العقوبات ، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية ، العدد 71 ، لسنة 2004 .

الحماية الجنائية لنظم المعالجة الآلية للمعطيات قام بتعديل قانون الإجراءات الجزائية بموجب قانون رقم 23/06 الذي مس بموجبه القسم المتعلق بالجرائم المعلوماتية في جانب من العقوبة[1]

– التنصت السيبراني: وهو إستخدام برنامج في جهاز الشخص المعتدي عليه يمكن من خلاله الإطلاع والإستماع إلى جميع المحادثات والمراسلات الصادرة ، ويتم إدخال هذا الملف إلى جهاز المعتدي عليه عن طريق البريد الإلكتروني أو عن طريق مواقع مغرية يزورها المعتدي عليه فيقوم بتنزيل بعض البرامج منها برنامج التنصت .[2]

المبحث الثاني

الآليات الإجرائية والتقنية لمكافحة الجريمة السيبرانية في ظل التشريع الجزائري

تعتبر الجرائم السيبرانية من بين الأكثر الجرائم التي أصبحت تشكل هاجس تؤرق المواطن في حياته الشخصية ، والدول في سيادتها وأمنها ، باعتبار أن التطور التكنولوجي والرقمي الهائل وما صاحبه من تأثيرات مست كافة المستويات من جهة، ومن جهة أخرى أصبحت تداعيات هذه الثورة التكنولوجية تمس بحرمة وخصوصية المواطن[3]، ما هو ما دفع بالتشريعات المقارنة بما فيها التشريع الجزائري العمل جاهدة على مكافحتها سعيا منها إلى تحقيق الأمن السيبراني من خلال إتخاذ مجموعة من الآليات سواء كان ذلك من الجانب الإجرائي أو التقني لتصدي لها. وهو ما سوف نتطرق إليه ضمن هذا المبحث .

المطلب الأول :الآليات الإجرائية لمكافحة الجريمة السيبرانية

سنتطرق من خلال هذا المطلب إلى الآليات و الأساليب الإجرائية التي تبنها المشرع الجزائري وكرسها في النظام القانوني الجزائري لمكافحة الجريمة السيبرانية من خلال :

الفرع الأول : الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصال

نظرا لخطورة الجرائم السيبرانية استحدث المشرع الجزائري بموجب القانون رقم 04/09 السابق ذكره الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ليحدد تنظيمها وتشكيلتها عن طريق التنظيم .[4]

حيث تعرف أنها " سلطة إدارية مستقلة تتمتع بالشخصية المعنوية والاستقلال المالي توضع تحت تصرف رئيس الجمهورية ، يحدد مقرها بالجزائر العاصمة ويمكن نقله إلى أي مكان من التراب الوطني بموجب مرسوم

---

(1)-القانون رقم 23/06 ، المؤرخ في 2006/12/20 ، المعدل و المتمم للأمر رقم 66/ 155 ، المتعلق بقانون العقوبات ، الجريدة الرسمية ، العدد رقم 84 ، الصادر بتاريخ 2006/12/24 ، المعدل و المتمم . .

(2)- روان بنت عطاء الله الصحفي ، المرجع السابق ، ص 19 .

(3) -رضا مهدي ، الجرائم السيبرانية و آليات مكافحتها ، مجلة إيليزا للبحوث و الدراسات ، المجلد 06 ، العدد 02 ، 2022 .

(4) - المادة 13 من القانون رقم 04/09 ، السابق ذكره .

رئاسي[1]، وتتكون الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الاتصال من مجلس توجيه ومديرية عامة يوضعان تحت السلطة المباشرة لرئيس الجمهورية ويقدمان له عرضا لنشاطاتهما[2].

تكلف الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في إطار مكافحتها للجرائم السيبرانية بمجموعة من الصلاحيات التي تتمثل فيا يلي :

- اقتراح عناصر استراتيجية للوقاية من جرائم تكنولوجيا الإعلام والاتصال .
- تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام الاتصال.
- مساعدة السلطة القضائية وضباط الشرطة القضائية في مكافحة الجرائم السيبرانية لاسيما ما يتعلق بجمع المعلومات والتزويد بها.[3].
- ضمان المراقبة الوقائية للاتصالات الإلكترونية قصد الكشف عن الجرائم التي تتصف بالأفعال الإرهابية والمساس بأمن الدولة .
- إضافة إلى ذلك تكلف الهيئة بتسجيل وحفظ المعطيات الرقمية للأنظمة المعلوماتية وتحديد مصدرها ومسارها من أجل استعمالها في الإجراءات القضائية.[4]

وفي إطار مكافحة الجرائم السيبرانية تكلف الهيئة الوطنية بمراقبة الإلكترونية وتجميع وتسجيل محتواها في حينها ، وكذا القيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية وفقا لأحكام المادة 04 من نفس القانون السابق ذكره ، كما أنها تكلف بتطوير التعاون مع المؤسسات والهيئة المعنية بهذه الجرائم .

وعليه يمكننا القول أن إتجاه المشرع الجزائري نحو إنشاء الهيئة الوطنية للوقاية من الجرائم السيبرانية تعد خطوة مهمة وإيجابية، إلا هذا لا يكفي لمواجهة هذه الأخيرة ، خاصة في عصر المعلوماتية التي تطورت معه الأساليب التي يتبعوها المجرمين في ارتكابهم للجرائم الإلكترونية .

هذا ولقد استحدث المشرع الجزائري على غرار الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال المعهد الوطني الوطني للأدلة الجنائية على الإجرام والذي يتكون من إحدى (11) عشر دائرة متخصصة في مجالات مختلفة جميعها تتضمن الخبرة وكذا التكوين والتعليم وتقديم المساعدات التقنية ومن بين هذه الدوائر توجد دائرة الإعلام الإلكتروني التي تتولى معالجة وتحليل وتقديم كل دليل رقمي يهدف إلى

---

(1)- المادة 02 ، من المرسوم الرئاسي رقم 183/20 ، المؤرخ في 13 يوليو 2020 ، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الاتصال و مكافحتها ، الجريدة الرسمية ، العدد 40 ، الصادرة بتاريخ 18يوليو 2020 .

(2) -المادة 02 من المرسوم الرئاسي رقم 183/20 .

(3) -المادة 14 من القانون رقم 04/09 ، السابق ذكره .

(4) -المادة 04 من المرسوم الرئاسي 183/20 .

الكشف عن الحقيقة، وكشف عن مرتكبي الجرائم المعلوماتية ، كما أنها تتولى بتقديم المساعدة التقنية للمحققين في المعاينات .[1]

الفرع الثاني : التفتيش و الحجز المنظومة المعلوماتية :

عرف المشرع الجزائري المنظومة المعلوماتية ضمن نص المادة الثانية الفقرة الثانية من القانون رقم 04/09 السابق ذكره على أنها" نظام منفصل أو مجموعة من الأنظمة المتصلة يبعضها البعض ، يقوم واحد منها أو أكثر بمعالجة الآلية للمعطيات تنفيذا لبرنامج معين ."[2]

ولمقتضيات الحفاظ على النظام العام ومستلزمات التحريات وكذا التحقيقات الجارية في إطار مكافحة الجريمة السيبرانية، تم اتخاذ مجموعة من التدابير الإجرائية والترتيبات التقنية لمراقبة الاتصالات الإلكترونية ، وتجميع وتسجيل محتواها في حينها والقيام بإجراءات الحجز والتفتيش ولو عن بعد داخل المنظومة المعلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها3،

وفي حالة كشف السلطات المختصة التي تباشر إجراء تفتيش بوجود معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل منظومة ، ففي هذه الحالة يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على كل دعامة تخزين إلكترونية تكون قابلة للحجز يتم وضعها في أحراز وفقا للقواعد الإجرائية المنصوص عليه في قانون إجراءات الجزائية[4]، وإذا إستحالة إجراء الحجز لأسباب تقنية فإنه يتعين على السلطات التي تقوم بإجراء التفتيش إستعمال تقنيات مناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة .

كما يمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها قصد مساعدتها وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها .

الفرع الثالث : تبادل المساعدة القضائية الدولية

---

(1) - حنان مهداوي ، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري ، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي ، الأغواط ، المجلد السادس ، العدد 02 ، 2022 ، ص 1073 .

(2)- المادة 02 /02 من القانون رقم 04/09 ، السابق ذكره .

(3)- رضا مهدي ، المرجع السابق ، ص 120 .

(4) -المادة 06 من القانون رقم 04/09 ، السابق ذكره .

لقد أقر المشرع الجزائري بموجب القانون رقم 04/09 اختصاص المحاكم الجزائية بالنظر في الجرائم المتصلة بتكنولوجيا الإعلام الاتصال المرتكبة خارج إقليم التراب الوطني عندما يكون مرتكبها أجنبيا وتستهدف مؤسسات الدولة الجزائرية أو الدفاع الوطني أو المصالح الاستراتيجية للاقتصاد الوطني .[1]

غير انه في إطار التحقيقات القضائية والمعاينات للجرائم السيبرانية وكشف عن مرتكبيها يمكن للسلطات المختصة تبادل المساعدة القضائية الدولية لجمع الأدلة الخاصة بالجريمة في شكلها الإلكتروني[2]، ومن الممكن الإستجابة لطلبات المساعدة الرامية إلى تبادل المعلومات أو اتخاذ أي إجراء تحفظي وفقا للإتفاقيات دولية تطبيقا لمبدأ المعاملة بالمثل .[3]

المطلب الثاني: الآليات التقنية لمكافحة الجريمة السيبرانية:

لقد سعى المشرع الجزائري بموجب القانون رقم 04/09 المتعلق بقانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال جاهدا على تكريس مجموعة من الآليات التقنية الكفيلة لتصدي للجرائم السيبرانية، وعلى العموم تتجسد هذه الآليات في:

-الفرع الأول : المر اقبة الإلكترونية

تعرف الرقابة الإلكترونية على أنها استخدام الحاسوب الآلي في العملية الرقابية وفق برامج حاسوبية تعد خصيصا لهذا الغرض بما يحقق الاقتصاد في الجهد والوقت والتكلفة في الوصول إلى النتائج المطلوبة بأقل خسائر ممكنة[4].

وبالرجوع إلى القانون رقم 04/09 السابق ذكره نلاحظ أن المشرع الجزائري لم يعرف المراقبة الإلكترونية أو مراقبة الاتصالات الإلكترونية[5] وإنما اكتفى فقط بتحديد مفهوم الإتصالات الإلكترونية .

ولقد حددت المادة 04 من القانون رقم 04/09 الحالات التي تسمح باللجوء إلى المراقبة الإلكترونية:

- الوقاية من الأفعال الإرهابية أو التخريبية أو الجرائم الماسة بأمن الدولة .

---

(1)- المادة 15 من القانون رقم 04/09 ، السابق ذكره .

(2)- المادة 16 من القانون رقم 04/09 ، السابق ذكره .

(3)- رضا مهدي ، المرجع السابق ، ص 120.

(4)- عدنان مصطفى البار ، الخصوصية و سعي الدولة للرقابة الإلكتروني الشاملة ، مركز هردو لدعم التعبير الرقمي القاهر ، 2018 ، مقال منشور عبر موقع

تم الإطلاع عليه يوم 2022/11/05 على الساعة 02:12 http://www.arab-cio.org

(5)-كما تعرف على أنها العمل الذي يقوم به المراقب لجمع البيانات والمعلومات عن المشتبه فيه سواء أمان شخصا أو مكانا أو شيئا حسب طبيعته بالزمن لتحقيق غرض آمني أو أي غرض أخر مصطفى محمد موسى ، المراقبة الإلكترونية عبر شبكة الأنترنت ، دراسة مقارنة بين المراقبة الأمنية التقليدية و الإلكترونية ، الكتاب الخامس ، دار الكتب والوثائق القومية المصرية ، 2003 ، ص 192 .

- في حالة توفر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو الذي يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.

- لمقتضيات البحث والتحري عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى هذا الإجراء يمكن الاستعانة بالمراقبة الإلكترونية.

- في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.[1]

غير أن اللجوء إلى إجراء عمليات المراقبة الإلكترونية لا يجب أن يكون إلا بموجب إذن مكتوب صادر من طرف السلطات القضائية المختصة .

الفرع الثاني : الاستعانة بمزودي خدمات للوقاية من الجرائم السيبرانية

لقد عرف المشرع الجزائري مقدمي الخدمات على أنها " أي كيان عام أو خاص يقدم لمستعملي خدماته ، القدرة على الاتصال بواسطة منظومة معلوماتية ،أو أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها ." [2]

يتولى مزودي خدمات في إطار مكافحة الجرائم المعلوماتية بتقديم المساعدة للسلطات المكلفة بالتحريات القضائية بهدف جمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها توضع المعطيات تحت تصرف السلطات[3]، زيادة على ذلك منح المشرع الجزائري لمقدمي الخدمات الأنترنت مجموعة من الالتزامات التي تشمل التدخل الفوري لسحب المحتويات التي يتيح الإطلاع عليها بمجرد العلم بها بطريقة مباشرة أو غير مباشرة بمخالفتها للقوانين وتخزينها أو حضر الدخول إليها ، إضافة إلى إلتزامها بوضع ترتيبات تقنية تحضر إمكانية الدخول الموزعات التي تحتوي على معلومات مخالفة للنظام العام أو الأداب العامة وإخبار المشتركين لديهم بوجودها.4

ومن خلال قراءتنا لنص المادة 03/10 من القانون رقم 04/09 السابق ذكره نلاحظ أن المشرع الجزائري فرض على مزودي الخدمات بمناسبة عند قيامها بالتزاماتها المحددة سابقا بكتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها تحت طائلة تطبيق العقوبات المتعلقة بإفشاء أسرار التحري والتحقيق ، وتتجسد هذه المعطيات في :

- المعطيات التي تسمح بالتعرف على مستعملي الخدمة .
- المعطيات المتعلقة بالتجهيزات الظرفية للإتصال .

---

(1) - المادة 04 من القانون رقم 04/09 ، السابق ذكره .

(2)- المادة 04/02 من القانون رقم 04/09 ، السابق ذكره .

(3)- المادة 10 من القانون رقم 04/09 ، السابق ذكره .

(4)- المادة 12 من القانون رقم 04/09 ، السابق ذكره.

- الخصائص التقنية و كذا تاريخ ووقت ومدة كل إتصال .
- المعطيات المتعلقة بالخدمات التكميلية المطلوبة أو المستعملة و مقدميها .
- المعطيات التي تسمح بالتعرف على المرسل إليه أو المرسل إليهم الإتصال و كذا عناوين المواقع المطلع عليها .[1]

خاتمة:

وختاما لموضوع دراستنا يمكننا القول ،انه تعد الجريمة السيبرانية من بين الجرائم التي عرفها العالم خاصة في الأونة الأخيرة من الزمن ، فهي تعتبر من الجرائم الخطيرة التي لا تمس بالحياة الخاصة للفرد فقط ، وإنما تعدتها بأن تمس بسلامة وامن واستقرار الدول ويرجع سبب ذلك إلى طابع الخصوصية التي تتميز بها الأمر الذي دفع بالمشرع الجزائري إلى تكريس ترسانة وأسس قانونية عمل من خلالها جاهدا على مكافحة الجريمة السيبرانية سعيا بذلك إلى تحقيق الأمن السيبراني .

ومن خلال من تم دراسته لقد توجت هذه الدراسة بمجموعة من **النتائج** يمكن أن نستخلصها فيما يلي :

-تعتبر الجريمة السيبرانية من الآثار السلبية التي خلفتها الثورة التكنولوجية الهائلة التي يشهدها العالم .

- يلاحظ عدم الاستقرار سواء على مستوى الفقه القانوني أو على المستوى مختلف التشريعات حول تسمية موحدة للجريمة السيبرانية، فهناك من أطلق عليها تسمية " الجريمة الإلكترونية " وجانب أخر أطلق عليها " بالجريمة التي تتم عبر الأنترنت " ،ويعود سبب ذلك في إمكانية ظهور جرائم جديدة متصلة بالتكنولوجيات الحديثة .

- تتميز الجريمة السيبرانية في أنها من جرائم التي يصعب اكتشافها وإثباتها أمام القضاء ، كما تعد من الجرائم عابرة للحدود لا تعترف بالحدود الزمانية والمكانية.

- لقد عمل المشرع الجزائري على مكافحة الجريمة السيبرانية ، من خلال استحداثه قسم خاص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات.

- لقد منح المشرع الجزائري لسلطات المختصة في إطار مكافحة الجريمة السيبرانية مجموعة من صلاحيات الواسعة كالمراقبة الإلكترونية والتفتيش الأنظمة المعلوماتية وحجزها ، ومع ذلك يمكن القول أنها غير كافية في ظل ظهور جرائم جديدة تتماشى والتطورات التكنولوجية الحديثة.

ومن خلال النتائج التي تم التوصل إليها نقترح مجموعة من **التوصيات** التي تتجسد فيما يلي:

---

(1)- المادة 11 من القانون رقم 09/ 04 ، السابق ذكره .

-ضرورة إصدار نصوص قانونية عقابية خاصة تعني بمكافحة الجرائم السيبرانية ، مع أخذ بعين الاعتبار الخصوصية التي تتميز بها لاسيما ما يتعلق بالإثبات هذا النوع من الجرائم .

- العمل على تجسيد الفعلي لمختلف الآليات التقنية وكذا الإجرائية التي كرسها المشرع الجزائري لمكافحة الجرائم السيبرانية .

- العمل على تنظيم دورات تكوينية لضباط الشرطة القضائية حول كيفية إستخدام التقنيات التكنولوجية الحديثة حتى يسهل عليهم التعامل مع هذا النوع الجديد من الجرائم، وكذا كيفية الحفاظ على الدليل الإلكتروني ليتسنى لهم تقديمه كوسيلة إثبات أمام القضاء .

- ضرورة العمل على تعزيز عنصر التعاون الدولي قضائيا أو إجرائيا في مجال مكافحة الجرائم المعلوماتية .

- ضرورة نشر الوعي داخل المجتمع لاسيما الشباب من خلال تنظيم ندوات وحملات تحسيسية حول مخاطر التعامل بالوسائل التكنولوجية والمواقع السيئة الموجودة على شبكة الأنترنت ، مع العمل على تحفيزهم للإستفادة من إيجابياتها.

قائمة المصادروالمراجع

أولا : المصادر

أ / النصوص القانونية

01 - قانون العقوبات الفرنسي ، المعدل بموجب القانون رقم 1336/92 ، المؤرخ في 16 ديسمبر 1966

02 - القانون رقم 15/04 ، المؤرخ في 2004/11/10 ، المعدل و المتمم للقانون رقم 156/66 ، المتضمن قانون العقوبات ، الجريدة الرسمية ، العدد 71 ، لسنة 2004 .

03 - القانون رقم 23/06 ، المؤرخ في 2006/12/20 ، المعدل و المتمم للأمر رقم 66/ 155 ، المتعلق بقانون العقوبات ، الجريدة الرسمية ، العدد رقم 84 ، الصادر بتاريخ 2006/12/24 ، المعدل و المتمم .

04 - القانون رقم 04/09، المؤرخ في 2009/08/05 ، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال و مكافحته ، الجريدة الرسمية ، العدد 47 ، الصادر بتاريخ 2009/08/16.

ب / المراسيم الرئاسية

01 - المرسوم الرئاسي رقم 183/20 ، المؤرخ في 13 يوليو 2020 ، المتضمن إعادة تنظيم الهيئة الوطنية للوقاية من جرائم المتصلة بتكنولوجيا الإعلام و الإتصال و مكافحتها ، الجريدة الرسمية ، العدد 40 ، الصادرة بتاريخ 18يوليو 2020 .

ثانيا : المراجع

أ / الكتب

01 - أشرف سعيد أحمد ، القرصنة الإلكترونية ، د ط ، د د ن ، د ب ن ، 2013 .

02 - رامي متول القاضي ، مكافحة الجرائم المعلوماتية ، دون طبعة ، دار النهضة العربية ، مصر ، 2011 .

03 - مصطفى محمد موسى ، المراقبة الإلكترونية عبر شبكة الأنترنت ، دراسة مقارنة بين المراقبة الأمنية التقليدية و الإلكترونية ، الكتاب الخامس ، دار الكتب والوثائق القومية المصرية ، 2003 .

04 - نهلا عبد القادر المومني ، الجرائم المعلوماتية ، الطبعة الأولى ، دار الثقافة و التوزيع ، الأردن 2008 .

ب مذكرات الماجستيرولأطروحات الدكتوراه

1 / مذكرات الماجستير

01 - فتيحة رصاع ، الحماية الجنائية للمعلومات عبر شبكة الأنترنت ، مذكرة مقدمة لنيل شهادة الماجستير في القانون قسم الحقوق ، كلية الحقوق و العلوم السياسية ، جامعة أبي بكر بلقايد – تلمسان – 2012/2011 .

02 - يوسف الصغير ، الجريمة المرتكبة عبر الأنترنت ، مذكرة ماجستير ، قسم الحقوق ، كلية الحقوق والعلوم السياسية، جامعة مولود معمر ، تيزي وزو ، 2013/2012 .

ج/ المقالات العلمية

01- حنان مهداوي ، التنظيم القانوني للجريمة الإلكترونية في التشريع الجزائري ، مجلة الفكر القانوني والسياسي، جامعة عمار ثليجي ، الأغواط ، المجلد السادس ، العدد 02 ، 2022 .

02 - جدو بن علية ، تحديات الأمن السيبراني في مواجهة الجريمة السيبرانية ، المجلة الجزائرية للأمن الإنساني ، جامعة الحاج لخضر ، باتنة ، المجلد 07 ، العدد 02 ، جويلية 2022 .

03 - عبد المؤمن الصغير ، الطبيعة الخاصة للجريمة الإلكترونية المرتكبة عبر الأنترنت في التشريع الجزائري والتشريع المقارن ، مجلة الحقوق والحريات ، جامعة محمد خيضر – بسكرة -المجلد 02 ، العدد 02 ، 2014 .

04 - سهام خليل ، خصوصية المجرم السيبراني ، مجلة المفكر ، كلية الحقوق والعلوم السياسية ، جامعة محمد خيضر ، بسكرة ،المجلد 17 ، العدد 15 ، 2017 .

05 - علي قويدري ، أمال العيش ، الجريمة السيبرانية مفهومها و سبل الوقاية منها ، مجلة نوميرس الإقتصادية ، المجلد الثالث ، العدد 01 ، 2022.

06 - صالح بن محمد المسند ، عبد الرحمان بن راشد المهيني ، جرائم الحاسب الآلي الخطر الحقيقي في عصر المعلومات، المجلة العربية للدراسات الأمنية و التدريب ، المجلد 15 ، العدد 29 ، أفريل 2000 .

07 - رضا مهدي ، الجرائم السيبرانية و آليات مكافحتها ، مجلة إيليزا للبحوث و الدراسات ، المجلد 06 ، العدد 02 ، 2022 .

08 - روان بنت عطية الله الصحفي .الجرائم السيبرانية ، المجلة الإلكترونية الشاملة متعددة التخصصات ، العدد 24، ماي2020.

09 - نوال قادة عبد الله ، محمد بن حمو ، الجريمة الإلكترونية قراءة سوسيولوجية لأهم النظريات المفسرة لسلوك الإجرامي ، مجلة الروافد للدراسات والأبحاث العلمية في العلوم الإجتماعية الإنسانية ، جامعة عين تموشنت. المجلد06 ، العدد 03 ، ديسمبر 2022 .

د / المحاضرات

01 - فريد روابح ، محاضرات في القانون الجنائي العام ، مطبوعة الدروس لسنة الثانية ليسانس ، قسم الحقوق كلية الحقوق و العلوم السياسية ، جامعة محمد لمين دباغين ، سطيف ، 2019/2018.

هـ / المواقع الإلكترونية

01 - عدنان مصطفى البار ، الخصوصية و سعي الدولة للرقابة الإلكتروني الشاملة ، مركز هردو لدعم التعبير الرقمي القاهر ، 2018 ، مقال منشور عبر موقع

تم الإطلاع عليه يوم 2022/11/05 على الساعة 02:12 http://www.arab-cio.org