السنة: السابعة المجلد: 07 العدد: 02 ص ص:299- 319
EISSN2676-1645 ISSN 2543-375X

تحديات الأمن السيبراني لمواجهة الجريمة الالكترونية

Cyber security challenges to face cybercrime

بن علية بن جدو*، جامعة بومرداس
b.bendjedou@univ-boumerdes.dz

تاريخ الاستلام2022/02/08 تاريخ القبول: 2022/03/01

ملخص:

تهدف هذه الدراسة إلى استكشاف واقع وتحديات الأمن السيبراني على المستوى الدولي والمحلي، خاصة مع التطور التكنولوجي واندماجه في مختلف المجالات السياسية، الاقتصادية والاجتماعية، فتوفير الحماية لمستخدمي التكنولوجيا في الوقت المعاصر أصبح ضرورة يجب أخذها بعين الاعتبار، في ظل توسع استخدام شبكة الانترنت وتنامي ما يعرف بالجريمة الالكترونية والإرهاب السيبراني.

خلصت هذه الدراسة إلى أن هناك جهود دولية للحد من أثار الجريمة الالكترونية على المستوى الدولي من خلال مجموعة من الهيئات والمنظمات الدولية مثل جهود الأمم المتحدة، الاتحاد الأوروبي، من خلال مجموعة من الاتفاقيات والتوصيات الدولية، وكذا على المستوى المحلي من خلال سن قوانين في هذا السياق، وإنشاء هياكل مختصة في محاربة الجريمة الالكترونية في الجزائر.

الكلمات المفتاحية: الأمن السيبراني – الفضاء السيبراني – الإرهاب السيبراني – الجريمة الالكترونية.

*المؤلف المراسل

Abstract:

This study aims to explore the reality of cyber security and the challenges it is facing on the international and local levels, especially with ongoing technological development and its infusion in different political, economic and social domains. Providing cyber security became, therefore, a desperate need, due to the Internet continues widespread use and the consequent growth of cyber crime and cyber terrorism.

The study summed up that international efforts are held, to reduce the effect of cyber crime at international level, by a range of international bodies and organizations such as the U.N and E.U, through a series of conventions and recommendations. At local level, through the enactment of laws in this context, and the establishment of specialized structures to fight cybercrime in Algeria.

Keywords: cyber security, cyber space, cyber terrorism, cyber crime.

مقدمة:

لقد أدى الاستخدام السيئ لمختلف الوسائل التكنولوجية والتقنيات الحديثة من حواسيب وأجهزة هواتف ذكية، وكذا شبكة الانترنت إلى تنامي وتزايد الجريمة الالكترونية، هذه الأخيرة والتي تتميز بمجموعة من الخصائص التي تميزها عن الجرائم التقليدية، من بينها أنها عابرة للحدود والقارات، تطلب ذلك ضرورة إيجاد آليات وحلول على المستوى المحلي والدولي، فالتعاون الدولي أصبح أكثر من ضرورة لمجابهة الجريمة الالكترونية، وتفادي أو التقليل من آثارها.

الإشكالية:

من خلال ما سبق نطرح الإشكالية التالية: ما هي التحديات التي تواجه الأمن السيبراني؟ وما هي الآليات التي تساعد على مواجهة الجريمة الالكترونية على المستوى الدولي وعلى المستوى المحلي؟

أهداف البحث:

يهدف هذا البحث إلى التعرف على المفاهيم المرتبطة بالأمن السيبراني، والتعرف على الآليات التي تساعد على مواجهة الجريمة الالكترونية على المستوى الدولي وعلى المستوى المحلي.

منهج البحث:

ولمعالجة الإشكالية سالفة الذكر، تم إتباع المنهج الوصفي التحليلي بالنسبة لعرض الأدبيات المتعلقة بالأمن السيبراني والجريمة الالكترونية، بالاستعانة بمجموعة من المراجع والدراسات السابقة التي تناولت الموضوع.

خطة البحث:

ولإثراء الموضع تم تقسيم الدراسة إلى أربعة مباحث رئيسية، تم التطرق في المبحث الأول لماهية الأمن السيبراني، بينما تم تخصيص المبحث الثاني لماهية الجريمة الالكترونية، بينما تم في المبحث الثالث التطرق للجهود الدولية لتحقيق الأمن السيبراني بينما تم التطرق في المبحث الرابع لواقع الأمن السيبراني في الجزائر.

1. ماهية الأمن السيبراني

1.1. مفهوم الفضاء السيبراني

الفضاء السيبراني هو بيئة افتراضية تعتمد في بنيتها على التكنولوجية الحديثة في التعامل والتواصل بين العديد من الفواعل سواء كانوا أشخاص أو هيئات حكومية وغير حكومية من خلال شبكة إلكترونية (الحاسوب) له استقلاليتها عن وسائل الاتصال، بمعنى أخر أن كل المعلومات والمعاملات المتداولة بقدر ما تسهل عملية الاندماج بين كل أجهزة الاتصالات والقمار الصناعية، والفضاء الإلكتروني، بقدر ما تفتح المجال لعمليات الاختراق (بوازدية، 2019، صفحة 1265).

2.1. مفهوم الأمن السيبراني

هو النشاط أو العملية والقدرة أو نظم المعلومات واتصالات الدولة، حيث تكون المعلومات الواردة فيه محمية من أي دافع من التلف، والاستخدام غير المصرح به أو التعديل، أو الاستغلال (بارة، 2017، صفحة 257).

سن القوانين السيبرانية وتنفيذها هو من القضايا التي تكتسب مزيداً من الأهمية مع انتشار استخدام تكنولوجيا المعلومات والاتصالات وتطبيقاتها في مختلف القطاعات الاقتصادية، والاجتماعية، والعلمية، والتجارية، وكذلك في الخدمات الحكومية وفي علاقات التفاعل بين الأفراد والمؤسسات. فوجود أطر وضوابط لتنظيم المعاملات الإلكترونية، ولحماية مستخدميها والمتعاملين بها، يولد شعوراً بالأمان لدى جميع المستفيدين من التطبيقات والخدمات الإلكترونية عبر الإنترنت، وتعتبر التشريعات السيبرانية عنصراً أساسياً في توفير البيئة التنظيمية والقانونية اللازمة لتطوير مجتمع المعلومات والمعرفة، ولبناء الثقة بالخدمات الإلكترونية وتأمين الحماية لمستخدمي الإنترنت (الاسكوا، 2012، صفحة 7).

يشمل نطاق عمليات الأمن السيبراني حماية المعلومات والأنظمة من التهديدات السيبرانية الكبرى، تأخذ هذه التهديدات عدة أشكال، نتيجة لذلك، تمثل استراتيجية وعمليات الأمن السيبراني تحديًا يستوجب مواكبة هذه التهديدات، لا سيما في الشبكات الحكومية وشبكات المؤسسات حيث غالبًا ما تستهدف التهديدات الأصول السرية والسياسية والعسكرية للأمة أو لشعبها (P.S.Seemma، S.Nandhini، و M.Sowmiya، November 2018، صفحة 125).

3.1. مفهوم الإرهاب السيبراني

وتعرف كليات الحرب الأمريكية الإرهاب السيبراني، أو كما تسميه "هجمات الشبكات الكمبيوترية"، انطلاقا من تصنيفه تحت بند "العمليات الإلكترونية، وهو يندرج في إطار الحرب الرقمية التي تعرف من خلال الإجراءات التي يتم اتخاذها للتأثير بشكل سلبي على المعلومات ونظم المعلومات، وفي الوقت نفسه الدفاع عن هذه المعلومات والنظم التي تحتويها، والإرهاب الرقمي يستهدف أمن العمليات، العمليات النفسية، الخداع العسكري، الهجمات الفيزيائية، ومهاجمة شبكات الكمبيوتر (غريب، 2018، صفحة 106).

وعرفت هيئة الأمم المتحدة في أكتوبر 2012 بان الإرهاب الالكتروني هو استخدام الانترنت لنشر الأعمال الإرهابية (العشعاش، 2018، صفحة 178).

تقع مهاجمة الدول في المجال السيبراني بالتأكيد ضمن نطاق الحرب الحديثة غير النظامية، التي تكون تكلفة الدخول فيها منخفضة مقارنة بتكلفة الحصول على أنظمة أسلحة تقليدية قادرة على هزيمة القوات العسكرية في حرب نظامية، فالأسلحة والتقنيات السيبرانية تتوفر بسهولة أكبر من أنظمة الأسلحة التقليدية المتقدمة، وتمنح الأسلحة الالكترونية الإرهابيين القدرة على مهاجمة أي دولة معادية، ليس من الصعب تصور إحدى هذه المجموعات التي تجند قراصنة ماهرين لدعم قتالها ضد الدول المعادية (قوادرة، جانفي 2020، صفحة 526).

4.1. مبادئ أساسية للأمن السيبراني:

استناًدا إلى توجيهات الخبراء الإقليميين والأطر الدولية والإقليمية بشأن الأمن السيبراني، فقد حددت جمعية الإنترنت ISOC المبادئ الأساسية التالية لتأمين شبكة الإنترنت (مجتمع الانترنت، مارس 2020، صفحة 2):

-الوعي: يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الإنترنت.

-المسؤولية: يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في إطار أدوارها ومؤسساتها، مع الأخذ في الاعتبار للآثار المترتبة على اتخاذ إجراء ما أو التقاعس عن تنفيذه.

-التعاون: يجب إشراك جميع الجهات المعنية، بما في ذلك الأطراف المعنية خارج الحدود، في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات الجديدة والمستمرة مواجهة فعالة.

وهناك ثلاثة معايير أساسية اتفق عليها الخبراء منذ البداية لضمان المعلومات ويشار إليها بمثلث أو ثلاثي CIA، وهي السرية والأمانة والتوافر (مركز هيدرو، 2017، صفحة 7).

-السرية: ويقصد بها عدم كشف المعلومات لغير أطرافها بما يوفر الخصوصية والسرية للمعلومات المتداولة على الفضاء الرقمي.

- الأمانة: وتعني عدم التلاعب بالمعلومات أو حذفها أو تعديلها بحيث يضمن المستخدم دقة نقل ما يريد من معلومات دون تدخل في أثناء النقل أو التخزين أو المعالجة.

- التوافر: أما فيما يخص فهو استمرار توفر المعلومة للشخص أو الجهة التي يسمح لها المستخدم بالاطلاع عليها عند الحاجة.

2. ماهية الجريمة الالكترونية

سنتطرق في هذا المبحث لمفهوم الجريمة الالكترونية والتعريفات المقدمة لها، وأساليب ارتكاب الجريمة الالكترونية، وخصائصها.

1.2. مفهوم الجريمة الالكترونية

الجريمة الالكترونية نشاط إجرامي تستخدم فيه التقنية الالكترونية (الحاسب الآلي وشبكة الانترنت) بطريقة مباشرة وغير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف (نمديلي، 2017، صفحة 5).

2.2. أساليب ارتكاب الجرائم المعلوماتية

1.2.2. الاختراق: عرف الاختراق في القانون العربي النموذجي الموحد في شأن جرائم إساءة استخدام تقنية المعلومات بأنه: "الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية"، ويعرف الاختراق أيضا على أنه عمليات غير شرعية تتم عن طريق فتحات موجودة في النظام يستطيع المخترق من خلالها الدخول إلى جهاز الضحية من أجل إتمام غرض معين يسعى إليه المخترق (رابحي، 2018/2017، صفحة 112).

2.2.2. الفيروسات المعلوماتية: فالفيروس هو عبارة عن برنامج يحتوي على مجموعة من الأوامر الخاصة بكيفية انتشاره داخل الملفات، ويتم كتابة هذا البرنامج باستخدام إحدى لغات البرمجة منخفضة المستوى، ويحدث أثارا تخريبية، وتختلف الآثار التي يخلفها الفيروس بحسب نوعه (رابحي،

2018/2017)، وهي تتدرج من أقلها ضررا إلى أكبرها كما يلي (رابحي، 2018/2017):

-البطء الشديد في الحاسب بما يجعل التعامل معه مستحيلا؛

-عدم القدرة على تشغيل معظم التطبيقات، وظهور رسائل خطأ كلما تمت محاولة تشغيلها؛

الملفات التنفيذية كالبرامج سواء المثبتة داخل نظام التشغيل أو التي يحتفظ بها داخل الحاسب مما يسبب عدم القدرة على تشغيل هذه التطبيقات؛

-حذف ملفاتFAT مما يعني حذف جميع المعطيات الموجودة داخل القرص الصلب، وهو الأمر الأكثر خطورة؛

-إصابة أحد أجزاء المكونات الصلبة، كما يحدث مع فيروس"تشير نوبل" الذي يصيب نظام الإدخال والإخراج الأساسية، مما يؤدي إلى توقف الحاسب بالكامل، ويمكن حماية نظم المعالجة الآلية للبيانات ضد الإصابة من الفيروس المعلوماتي عن طريق وضع نظم أمنية ضد البرامج والبيانات والنظم الفيروسية، وبالتالي حماية البرامج والبيانات داخل النظام من الاعتداء عليها بهذا الأسلوب.

3.2. خصائص الجريمة الالكترونية

تتميز الجريمة الالكترونية بمجموعة من الخصائص التي تميزها عن الجريمة التقليدية أو العادية، وهي كالتالي (رابحي، 2018/2017، الصفحات 93 - 97):

- أنها ترتكب من مجرم غير تقليدي وهي جرائم ناعمة: يختلف المجرم مرتكب الجريمة المعلوماتية عن المجرم في الجرائم التقليدية ذلك لأن له سمات مختلفة عن غيره كما أن له طوائف وأنماط خاصة به، كما أن العوامل التي تدفعه لارتكاب الجريمة مختلفة عنه أيضا، كما أن هذا المجرم إنسان ذكي ويستغل ذكائه في تنفيذ جريمته ولا يستعين بالقوة الجسدية في ذلك إلا بالقدر اليسير جدا.

- جرائم خفية وعابرة للحدود وصعبة الاكتشاف والإثبات: تتسم الجريمة المعلوماتية بأنها مستترة خفية في أغلبها حيث أن المجني عليه لا يلحظها غالبا

مع أنها قد تقع أثناء وجوده على شبكة الانترنت ولكن لا يكون عالما بها ولا ينتبه إليها إلا بعد فترة من وقوعها وفي بعض الأحيان لا يكتشف أمرها.

- جرائم عابرة للحدود: حيث أن الانترنت وكما يشاهد الجميع ربطت العالم بشبكة الاتصال المتميزة والفعالة، قربت شعوب العالم بأجناسهم وثقافاتهم المختلفة من بعضهم بصورة لم تكن متاحة من قبل بأي وسيلة من وسائل الاتصال حتى كادت أن تلغي الحدود القائمة بين الدول بأن جعلت العالم قرية صغيرة.

- انعدام الآثار التقليدية للجريمة: الجرائم المرتكبة بواسطة الانترنت لا تترك في الأغلب آثارا خارجية أو مادية تدل على الجريمة أو مرتكبها، أغلب البيانات والمعلومات التي يتم تداولها من حاسب آلي إلى آخر عبر الشبكة الانترنت تكون في هيئة رموز مخزنة على وسائط تخزين ممغنطة بحيث لا يمكن للإنسان قراءتها أو إدراكها إلا بواسطة الحاسب الآلي ولا زالت الأجهزة المعنية في سبيل الجمع أو الكشف عن أدلة من هدا النوع لإثبات وقوع الجريمة والتعرف على مرتكبها تعاني الكثير.

- إعاقة الوصول إلى الدليل بوسائل الحماية الفنية: الذين يرتكبون الجرائم الالكترونية أنفسهم بتدابير أمنية واقية تزيد صعوبة من صعوبة التفتيش عن الأدلة التي تؤدي إلى الإدانة ودلك باستخدام كلمات السر، أو دس تعليمات خفية لتصبح بينها كالرمز أو تشفير التعليمات باستخدام طرق وبرامج تشفير البيانات المتطورة مما يجعل الوصول إليها غاية في الصعوبة.

- سهولة إتلاف الدليل المادي وتدميره في زمن قياسي: يسهل غالبا على الجاني في ارتكاب الجرائم الالكترونية محو أدلة الإدانة في زمن قياسي بحيث لا تستغرق أكثر من ثوان معدودة، وذلك بتعريض البيانات المخزنة لديه على وسائط ممغنطة إلى مجال مغناطيسي قوي قادر على محوها في طرفة عين، أو تزويد الحاسب ببرامج من شأنها تدمير وتخريب البيانات في حال استخدامه من قبل شخص غير مرخص له.

- هي جرائم فادحة الأضرار وذات أساليب سريعة التطور: إن الاعتماد على الحاسب الآلي في إدارة مختلفة الأعمال في شتى المجالات ضاعف من

الأضرار والخسائر التي تخلفها الجريمة المعلوماتية الاعتداء على معطيات الحاسب الآلي.

3. التشريعات القانونية والتعاون الدولي للحد من آثار الإرهاب السيبراني وتحقيق الأمن السيبراني

تمتاز الجرائم السيبرانية بخصوصيات تميزها عن الجرائم العادية وتجعل من قوانين العقوبات وقوانين الإجراءات الجزائية غير قادرة على استيعابها لان تطورهما لا يتم بنفس الوتيرة، فالجرائم السيبرانية تقع في بيئة افتراضية ولا تترك أثرا ماديا، وكونها تقع في بيئة افتراضية فهي جريمة لا تعرف مما يتصور معها أن تتأثر عدة أماكن في دول مختلفة في آن واحد (سيدهم و عواشرية، 2020، صفحة 132).

إن الدخول إلى الفضاء الإلكتروني للغير من قبل مؤسسات إنفاذ القانون كان ولا زال يثير جدلاً لدى المشرع وصانع القرار في الكثير من دول العالم. كما أن السؤال حول متى وكيف يتم ذلك، مع الحفاظ على قيم المجتمع ومنها الحق في الخصوصية، لا زال يثير نقاشاً حاداً حتى الآن، خاصة وأن استخدامها في الآونة الأخيرة أصبح أكثر أهمية من أي وقت مضى. ومن أبرز الأمثلة على ذلك حديثاً، الجدل القائم الآن بين الأجهزة العدلية الفدرالية الأمريكية وشركة آبل Apple حيث تطالب الأولى الثانية تمكينها من كشف هوية مستخدمي أجهزة الآيفون IPhone ومعلومات كافية عنهم، فيما ترفض الثانية الطلب بدافع حماية خصوصية وسرية معلومات مالك الجهاز (عبد الباقي، 2018، صفحة 287).

إن وضع نصوص قانونية جنائية لمواجهة الجرائم الالكترونية كان وليد جدل فقهي حول مدى قابلية النصوص الجنائية التقليدية لتشمل على هذا النوع من القيم الجديدة، وحقيقة الأمر أن الاتجاه الفقهي القائل بإمكانية ذلك لم يكتب له النجاح لأن تبني هذه الأفكار سيؤدي إلى تشويه المبادئ المستقرة التي تقوم عليها تلك الجرائم، الأمر الذي سيؤدي بدوره لا محالة إلى وجود ثغرات قانونية، وهو ما يجعل الفكر القانوني يستقر ويقتنع بضرورة وضع

نصوص قانونية خاصة بهذه الجرائم (خضراوي و بوقرين، 2015، صفحة 153).

إن إجراءات التحقيق التي تمر بها الجرائم المعلوماتية تأخذ شكل عناصر التحقيق الجنائي المتكامل، وتمر بذات المراحل الفنية والشكلية، وتعد إجراءات التحقيق الجنائي العام هي الأساس في التحقيق في جرائم الحاسب الآلي إلا أنها تتميز ببعض من الخصوصية في عناصر التحقيق الفرعية كالإجراءات الشكلية المتبعة في تلقي البلاغات، والعناية بمسرح الجريمة وتكوين فرق العمل كأساليب تأمين الأدلة المادية (المصري، 2017، صفحة 53).

1.3. الجهود الدولية لمكافحة الجريمة الالكترونية

تتمثل الجهود الدولية في إطار مكافحة الجريمة الالكترونية في (صغير، 2013، صفحة 93):

1.1.3. جهود منظمة الأمم المتحدة

بذلت منظمة الأمم المتحدة جهودا كبيرة في سبيل العمل على مكافحة الجريمة الالكترونية، وذلك لما تسببه هذه الجرائم من أضرار بالغة وخسائر فادحة بالإنسانية جمعاء، وإيمانا منها بأن منع هذه الجرائم ومكافحتها يتطلبان استجابة دولية في ضوء الطابع والأبعاد الدولية لإساءة استخدام الكمبيوتر والجرائم المتعلقة به، توصلت منظمة الأمم المتحدة في مؤتمرها الثامن حول منع الجريمة ومعاملة المجرمين إلى إصدار قرار خاص بالجرائم المتعلقة بالحاسوب، وأشار القرار إلى أن الإجراء الدولي لمواجهة جرائم الإنترنت يتطلب من الدول الأعضاء اتخاذ عدة إجراءات تتلخص في (صغير، 2013، صفحة 93):

- تحديث القوانين وأغراضها الجنائية بما في ذلك التدابير المتخذة من أجل ضمان إدخال التعديلات تطبيق القوانين الجنائية الراهنة (التحقيق، قبول الأدلة) على نحو ملائم وإذا دعت الضرورة.
- مصادرة العائد والأصول من الأنشطة غير المشروعة.
- اتخاذ تدابير أمن والوقاية مع مراعاة خصوصية الأفراد واحترام حقوق الإنسان.

- رفع الوعي لدى الجماهير والقضاة والأجهزة العاملة على مكافحة هذا النوع من الجرائم بأهمية مكافحة هذه الجرائم ومحاكمة مرتكبيها.

- التعاون مع المنظمات المهتمة بهذا الموضوع، ووضع وتدريس الآداب المتبعة في استخدام الحاسوب ضمن المناهج المدرسية.

- حماية مصالح الدولة وحقوق ضحايا جرائم الإنترنت.

تزايد الجرائم المرتكبة عبر الإنترنت وما تثيره من مشاكل أدى بمنظمة الأمم المتحدة إلى عقد الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية، بالإضافة إلى الدور الذي يمكن أن تقوم به كل من منظمة الأمم المتحدة والمنظمات الإقليمية، عقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل أيام 12، 19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخيرة في استخدام العلم والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية (صغير، 2013، صفحة 94).

2.1.3. منظمة التعاون الاقتصادي والتنمية

بدأت هذه المنظمة الاهتمام بالجرائم المرتكبة عبر الإنترنت منذ عام 1978، حيث وضعت مجموعة أدلة وقواعد إرشادية تتصل بتقنية المعلومات، ويعد الدليل المتعلق بحماية الخصوصية وقواعد نقل البيانات من أول الأدلة التي تم تبنيها من قبل مجلس المنظمة في عام 1980 مع التوصية للأعضاء بالالتزام بها. أصدرت هذه المنظمة تقريرا عام 1983، بعنوان الجرائم المرتبطة بالحاسوب وتحليل السياسة القانونية الجنائية، حيث استعرض التقرير السياسة الجنائية القائمة والمقترحات الخاصة في عدد من الدول الأعضاء (صغير، 2013، الصفحات 96 - 97).

وفي عام 1992 وضعت المنظمة توصيات إرشادية خاصة بأمن أنظمة المعلومات، وقد تمخضت جهود المنظمة من أجل معالجة الجرائم المرتكبة عبر الإنترنت بالتوصية بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء الأفعال التالية (صغير، 2013، صفحة 97):

- التلاعب في البيانات المعالجة آليا بما في ذلك محوها.
- التجسس المعلوماتي ويندرج تحته الحصول، أو الاقتناء، أو الاستعمال غير المشروع للمعطيات.
- التخريب المعلوماتي ويندرج تحته الاستخدام غير المشروع، أو سرقة وقت الحاسب.
- قرصنة البرامج.
- الدخول غير المشروع على البيانات أو نقلها.
- اعتراض استخدام المعطيات أو نقلها.

3.1.3. المنظمة العالمية للملكية الفكرية

اهتمت هذه المنظمة في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، فبعد أن استقر الرأي لديها بعدم إمكانية توفير الحماية لهما في تشريعات براءات الاختراع، تم الاتفاق على توفيرها بواسطة الاتفاقيات العالمية وخاصة "التربس" و"برن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حق المؤلف، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المتعمدة والمرتكبة في إطار تجاري (صغير، 2013، صفحة 98).

2.3. دور الهيئات والمنظمات الإقليمية في مكافحة الجريمة المرتكبة عبر الإنترنت

تتمثل الجهود الإقليمية في مكافحة الجريمة المرتكبة عبر الإنترنت في (صغير، 2013، الصفحات 99 - 102):

1.2.3. الإتحاد الأوروبي

توجت الجهود التي يبذلها الإتحاد الأوروبي والمجلس الأوروبي بصدور اتفاقية بودابست لمكافحة الجرائم الإلكترونية، وتعرف بالاتفاقية الأوروبية لمكافحة جرائم المعلوماتية، وتتلخص أهم أهدافها في السعي لتحقيق وحدة التدابير

التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول الأوروبية والتأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الإنترنت.

تقوم هذه الاتفاقية كذلك بتعريف وتحديد العقوبات من جرائم الإنترنت في إطار قوانينهم المحلية، وباستقراء هذه الاتفاقية نجد في ديباجتها الكثير من الجرائم المرتكبة عبر الإنترنت، منها المتعلقة بالبيانات الشخصية في مجال الخدمات المتعلقة بالاتصالات السلكية واللاسلكية.

وضعت تلك الاتفاقية من قبل مجلس أوروبا بالتعاون مع كندا، واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية وعرضت للتوقيع في بودابست في عام2001 ودخلت حيز التنفيذ في عام 2004، وتعتبر الاتفاقية متاحة لأية دولة من أنحاء العالم تسعى للانضمام إليها، وهناك عدد من البلدان الأخرى من مختلف الأقاليم على وشك طلب الانضمام للاتفاقية، حيث أن في سبتمبر 2006، طلبت الفلبين الانضمام إليها، والجدير بالذكر أيضا أن الكثير من البلدان تعد حاليا تشريعا بشأن جرائم الإنترنت مثل الأرجنتين، والبرازيل، وكولومبيا، والهند، واندونيسيا وغيرها، باستخدام الاتفاقية كنموذج.

2.2.3. على المستوى العربي

نجد من تلك الجهود القرار الصادر عن مجلس وزراء العدل العرب الخاص بإصدار القانون الجزائي الموحد، كقانون عربي نموذجي، أين نجد الباب السابع الخاص بالجرائم ضد الأشخاص، قد احتوى على فصل خاص بالاعتداء على حقوق الأشخاص، الناتج عن المعالجات المعلوماتية، وذلك في المواد 461 -464 التي أشارت على وجوب حماية الحياة الخاصة، وأسرار الأفراد من خطر المعالجة الآلية وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها و العقاب المطبق في حال ارتكاب هذه الجرائم. تم في مجال الملكية الفكرية إبرام الاتفاقية العربية لحماية حقوق المؤلف حيث نصت في مجال المعلوماتية، على توفير الحماية القانونية للبرامج المعلوماتية (برامج الحاسب الآلي).

3.2.3. مجموعة الدول الثمانية

تناولت مجموعة الثمانية في المؤتمر الذي عقدته في باريس في عام2000، موضوع الجريمة السيبرانية وحثت إلى منع الملاذات الرقمية غير الخاضعة للقانون، وكانت مجموعة الثمانية قد ربطت منذ ذلك الوقت محاولاتها الرامية إلى إيجاد حلول دولية باتفاقية مجلس أوروبا بشأن الجريمة السيبرانية، وفي عام 2001 ناقشت مجموعة الثمانية الأدوات الإجرائية لمكافحة الجريمة السيبرانية في ورشة عمل عقدت بطوكيو، ركزت على ما إذا كان ينبغي تنفيذ الالتزامات باحتجاز البيانات أو ما إذا كان حفظ البيانات يعد حلا بديلا.

تطرح الجرائم التي تنطوي على أدلة إثباتية إلكترونية تحديات فريدة أمام السلطات التي يُعهد إليها باتخاذ تدابير التصدي المناسبة لها سواء على الصعيد الداخلي (المشرِّعون والمحقِّقون والمدّعون العامّون والقضاة) أو على مستوى التعاون الدولي (الأمم المتحدة، 2015، صفحة 1).

إنّ للصلاحيات التحقيقية الوطنية دوراً رئيسيا في جمع الأدلة الإثباتية الإلكترونية، وكما جاء في الدراسة التي أعدها مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة بشأن الجريمة السيبرانية، يجوز للدول، في سبيل إجراء تحقيقات فعّالة وجمع الأدلة الإثباتية الإلكترونية، أن تسنّ تشريعات إجرائية تمنح صلاحيات لسلطات إنفاذ القانون ذات الصلة (الأمم المتحدة، 2015، صفحة 2).

4. التشريعات والقوانين والهياكل الخاصة بالأمن السيبراني في الجزائر

بما أنه لا يمكن مواجهة الجريمة الالكترونية بدون توفير حماية كافية للمجال والنطاق الذي تتواجد فيه المعلومات، فقد حاول المشرع الجزائري مكافحة الجرائم الماسة بالأنظمة والبرامج المعلوماتية أو كما يحب أن يسميه المشرع بأنظمة المعالجة الآلية للمعطيات، ومن ثمة حماية المعلومات المتواجدة في هذه الأنظمة (خضراوي و بوقرين، 2015، صفحة 153).

لقد استدرك المشرع الجزائري في السنوات الأخيرة الفراغ القانوني في مجال الجريمة الإلكترونية نسبيا، حيث تمخض عنه إصدار القانون 04 -15

المتضمن تعديل قانون العقوبات، وذلك بتخصيص الفصل السابع مكرر للمساس بأنظمة المعالجة الآلية للمعطيات، وفي عام 2006 أدخل المشرع تعديل بموجب قانون رقم 06 -23 المؤرخ في 20 ديسمبر 2006، ليصدر في 2009 القانون رقم 09 -04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (بوغرارة، سبتمبر 2018، صفحة 110).

1.4. الجهود التشريعية للحد من الجريمة الالكترونية في الجزائر

واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية بما فيها الإنترنت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها، فكانت محاولاته في الحد من هذه الظاهرة المستحدثة على النحو التالي (صغير، 2013، صفحة 103):

1.1.4. مكافحة الجريمة المرتكبة عبر الإنترنت في قوانين الملكية الفكرية من خلال قوانين الملكية الأدبية والفنية

اتجه المشرع الجزائري إلى الاعتراف صراحة بوصف المصنف المحمي لمصنفات الإعلام الآلي، وذلك ما من خلال تعديله للأمر 14 -73 بموجب الأمر 10 -97 والذي يتبين من خلال ما يلي (صغير، 2013، الصفحات 106 - 107):

أن المشرع وسع قائمة المؤلفات المحمية حيث أدمج تطبيقات الإعلام الآلي ضمن المصنفات الأصلية، والتي عبر عنها بمصنفات قواعد البيانات وبرامج الإعلام الآلي التي تمكن من القيام بنشاط علمي، أو أي نشاط من نوع آخر أو الحصول على نتيجة خاصة من المعلومات التي تقرأ بآلة وترجم باندفاعات إلكترونية بالحاسوب، أما قواعد البيانات فهي عبارة عن مجموعة المصنفات والأساليب والقواعد، كما يمكن أن تشمل الوثائق المتعلقة بسير المعطيات. إن الحماية تحدد من 25 سنة إلى 50 سنة بعد وفاة المبدع تماشيا مع اتفاقية برن

التي حددت كمدة دنيا للحماية 50سنة، وبالتالي هذه المدة تشمل حتى مصنفات الإعلام لآلي (صغير، 2013، صفحة 107).

تشديد العقوبات الناجمة عن المساس بحقوق المؤلفين لاسيما مؤلفي المصنفات المعلوماتية، إذ في السابق تجريم الاعتداءات على الملكية الفكرية تناولته المواد 390 -394 من قانون العقوبات، لكنها أخرجت بموجب الأمر10 -97 من مظلة قانون العقوبات وأصبح لها تجريم خاص، حيث أن قانون العقوبات كان يقرر بموجب المادة 393 الغرامة كعقوبة للاعتداء على حق المؤلف، بينما الأمر 10 -97 وكذا الأمر 03 -05 يقرران عقوبتي الحبس والغرامة (صغير، 2013، صفحة 107).

2.1.4. مكافحة الجريمة المرتكبة عبر الإنترنت في قانون العقوبات

تدارك المشرع الجزائري خلال السنوات الأخيرة ولو نسبيا الفراغ القانوني في مجال الإجرام المعلوماتي عموما والإجرام عبر الإنترنت خصوصا بموجب القانون 04 -15 المتضمن تعديل قانون العقوبات، الذي بموجبه جرم المشرع بعض الأفعال المتصلة بالمعالجة الآلية للمعطيات وهي (صغير، 2013، صفحة 108):

1 - جريمة التوصل أو الدخول غير المصرح به: تقوم هذه الجريمة بمجرد ما يتم الدخول غير المرخص به وعن طريق الغش إلى المنظومة المعلوماتية، سواء مس ذلك الدخول أو البقاء كامل المنظومة أو جزء منها فقط، وهو ما أشارت إليه المادة 394 مكرر من قانون العقوبات.

2 - جريمة التزوير المعلوماتي: ولقد أكد المشرع على معاقبة هذه الجرائم في المادة 394 مكرر1.

3 - جريمة الاستيلاء على المعطيات: تعد هذه الجريمة من بين أكثر الجرائم وقوعا في العالم الافتراضي، وهي ما أقرته المادة 394 مكرر2.

4 - جريمة إتلاف وتدمير المعطيات: تطرق إليها المشرع الجزائري بالمادة 394 مكرر1 من قانون العقوبات.

5 -جريمة الاحتيال المعلوماتي: تطرقت إليه فحوى المادة 394 مكرر 1/2.

6 - أنشطة الإنترنت المجسدة لجرائم المحتوى الضار والتصرف غير القانوني: نصت مواد القسم السابع مكرر من قانون العقوبات وخاصة المادة 394 مكرر 2/2 على تجريم أفعال الحيازة، الإفشاء والنشر التي ترد على المعطيات الآلية بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق، وجمع الأفعال غير المشروعة، وذلك بعقوبتي الحبس والغرامة إضافية إلى ما نصت عليه المادة 394 مكرر6 بتوقيع عقوبة تكميلية في غلق المواقع التي تكون محلا لجريمة من الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

3.1.4. مكافحة الجريمة المرتكبة عبر الإنترنت في قانون الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال

دفع القصور الذي عرفه القانون رقم 04 -15 والمعدل لقانون العقوبات الذي نص على حماية جزائية نسبية لأنظمة المعلومات من خلال تجريم مختلف أنواع الاعتداءات الماسة بأنظمة المعالجة الآلية للمعطيات، بالمشرع الجزائري إلى سد الفراغ التشريعي الذي يعرفه مجال الجرائم المتعلقة بوسائل الإعلام والاتصال وخاصة الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الإنترنت. يعتبر القانون رقم 09 -04 المتعلق بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها نطاقا شاملا في مجال مكافحة الجرائم المرتكبة عبر الإنترنت، حيث جاء تجريمه للأفعال المخالفة للقانون والتي ترتكب عبر وسائل الاتصال عاما، وبالتالي فهو يطبق على كل التكنولوجيات الجديدة والقديمة بما فيها شبكة الإنترنت وعلى كل تقنية تظهر مستقبلا (صغير، 2013، الصفحات 112 - 115).

2.4. هياكل تقصي الجريمة السيبرانية في الجزائر

إضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد أنشأت الجزائر هيئات أخرى تضطلع بأدوار جد هامة في مواجهة مختلف الجرائم الالكترونية منها (بن مرزوق و حرشاوي، 2017، صفحة 74):

- مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني؛

- المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني؛
- المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

1.2.4. **مركز الوقاية من جرائم الإعلام الآلي و جرائم المعلوماتية للدرك الوطني**: أنشئ هذا المركز في سنة 2008، أهدافه تأمين منظومة المعلومات لخدمة الأمن العمومي، وهو بمثابة مركز توثيق، ويقوم بتحليل المعطيات والبيانات للجرائم المعلوماتية المرتكبة، ومحاولة تحديد هوية أصحابها، مما يؤمن الأنظمة المعلوماتية للمؤسسات والبنوك والبيوت والشركات ...إلخ، ويعمل على التنسيق الأمني بين الأجهزة الأمنية الأخرى، والجدير بالذكر، أن المركز استطاع معالجة أزيد من 100 جريمة إلكترونية سنة 2014، وما يفوق 500 قضية رقمية خلال سنة 2015، وهذا بفضل التركيبة البشرية المؤهلة التي اكتسبها الجهاز من التكوين المستمر والملتقيات الوطنية والدولية، وتبادل الخبرات مع الدول الأخرى (بوغرارة، سبتمبر 2018، صفحة 111).

2.2.4. **المعهد الوطني للأدلة الجنائية وعلم الإجرام**: يتكون هذا الجهاز من إحدى عشر دائرة متخصصة في عدة مجالات متباينة، تضمن جميعها الخبرة والتكوين والتعليم، وتقديم جميع المساعدات التقنية، تقوم دائرة الإعلام الآلي والإلكتروني المكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد العدالة مع تقديم المساعدة للمحققين، يتكون من عدة تجهيزات تتمثل في محطة ترميم وتصليح الأجهزة والحوامل المعطلة، الشبكات الإعلامية والتجهيزات البيانية، محطة محمولة وثابتة لإجراء خبرات الإعلام الآلي (بوغرارة، سبتمبر 2018، صفحة 111).

3.2.4. **المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة للمديرية العامة للأمن الوطني**: قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية استجابة لمطلب الأمن السيبراني ومكافحة التحديات الأمنية الناجمة عن الجرائم الإلكترونية، والذي أنشئ سنة 2011، وأضيف للهيكل التنظيمي في 2015 (بوغرارة، سبتمبر 2018، صفحة 111).

حيث احتلت الجزائر المرتبة 23 عالميا من أصل 29 في مستوى التأهب في مجال الأمن السيبراني، أما على المستوى العربي فاحتلت المرتبة العاشرة حسب التزامها بتلك التدابير التي يحددها الرقم القياسي العالمي للأمن السيبراني (بن مرزوق و حرشاوي، 2017).

خاتمة:

لقد أدى التطور التكنولوجي إلى مجموعة من النتائج الايجابية التي انعكست على تحسين الحياة العامة للأفراد، كما كان له الأثر الإيجابي على اقتصاديات الدول، ولكن الاستغلال السلبي للتكنولوجيا أفرز مجموعة من المفاهيم، من بينها ما يعرف بالجريمة الالكترونية، حيث أدى استخدام الحاسوب وكذا شبكة الانترنت لأغراض تسبب أضرار للآخرين، تمس بخصوصياتهم، وتحد من حرياتهم في المجال المعلوماتي.

إن التحدي الحالي للدول هو مواجهة الجريمة العابرة للقارات، لتفادي الآثار الكارثية التي قد تسببها، وتحقيق الأمن السيبراني، الذي يحفظ السلامة الالكترونية، ويحقق الأمن الالكتروني، من خلال مختلف الاتفاقيات الدولية أو الإقليمية، أو إطار وإشراف مختلف الهيئات والمنظمات الدولية الرسمية، فجهود الأمم المتحدة والاتحاد الأوروبي، تسعى إلى توحيد الرؤى بين الدول لمواجهة الجريمة الالكترونية والإرهاب السيبراني، وخلق آليات تساعد في التحقيق والمتابعة القانونية للمجرمين الالكترونيين.

النتائج:

من خلال ما سبق تم التوصل إلى النتائج التالية:

-عقدت منظمة الأمم المتحدة إلى الاتفاقية الخاصة بمكافحة إساءة استعمال التكنولوجيا لأغراض إجرامية سنة 2000، أين أكدت على الحاجة إلى تعزيز التنسيق والتعاون بين الدول في مكافحة إساءة استعمال تكنولوجيا المعلومات لأغراض إجرامية.

- عقدت كذلك منظمة الأمم المتحدة المؤتمر الثاني عشر لمنع الجريمة والعدالة الجنائية وذلك بالبرازيل أيام 12، 19 أفريل 2010، حيث ناقشت فيه الدول الأعضاء ببعض التعمق مختلف التطورات الأخيرة في استخدام العلم

والتكنولوجيا من جانب المجرمين والسلطات المختصة في مكافحة الجريمة بما في ذلك الجرائم الحاسوبية.

- في عام 1992 وضعت منظمة التعاون الاقتصادي والتنمية توصيات إرشادية خاصة بأمن أنظمة المعلومات، وقد تمخضت جهود المنظمة من أجل معالجة الجرائم المرتكبة عبر الإنترنت بالتوصية بضرورة أن تعطي التشريعات الجنائية للدول الأعضاء.

- اهتمت هذه المنظمة العالمية للملكية الفكرية في المجال المعلوماتي بتوفير الحماية القانونية للبرامج المعلوماتية وقواعد البيانات، بواسطة الاتفاقيات العالمية وخاصة "التربس" و"برن" اللتان حثتا فيهما الدول الأعضاء على ضرورة تطوير تشريعاتها، وخاصة تشريعات حق المؤلف، وكذلك وضع عقوبات على كل أعمال تزوير في العلامات التجارية والقرصنة المتعمدة والمرتكبة في إطار تجاري.

- توجت الجهود التي يبذلها الإتحاد الأوروبي والمجلس الأوروبي بصدور اتفاقية بودابست لمكافحة الجرائم الإلكترونية، وتعرف بالاتفاقية الأوروبية لمكافحة جرائم المعلوماتية، وتتلخص أهم أهدافها في السعي لتحقيق وحدة التدابير التشريعية بين الدول الأوروبية والدول المنظمة للاتفاقية من غير الدول الأوروبية والتأكيد على أهمية التعاون الإقليمي والدولي في ميدان مكافحة جرائم الإنترنت.

-واكب المشرع الجزائري مختلف التطورات التشريعية التي تم سنها من أجل تنظيم المعاملات التي تتم من خلال الوسائط الإلكترونية بما فيها الإنترنت، خاصة التي تهدف إلى الحد من الاستخدام غير المشروع لها.

-إضافة إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، فقد أنشأت الجزائر هيئات أخرى تضطلع بأدوار جد هامة في مواجهة مختلف الجرائم الالكترونية منها: مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني، المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني، المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني.

قائمة المراجع:

(Overview .November 2018 .(M.Sowmiya، S.Nandhini، و P.S.Seemma of Cyber Security .*International Journal of Advanced Research in Computer and Communication Engineering*.128 ,125 ، *7* ،

اسماعيل العشعاش. (2018). الإرهاب السيبراني وتحديات الدول دراسة مقارنة مع الاتفاقيات الدولية. *مجلة بحوث ، 12* (1)، 173-203.

الاسكوا. (2012). *نشرة تكنولوجيا المعلومات والاتصالات في المنطقة العربية*. اللجنة الاقتصادية والاجتماعية لغربي آسيا.

الأمم المتحدة. (18 أوت, 2015). جمع وتبادل الأدلة الإثباتية الإلكترونية. *مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية* . فيينا.

الهادي خضراوي، و عبد الحليم بوقرين. (2015). تجربة الجزائر في مكافحة الجريمة الالكترونية. *المؤتمر الدولي لمكافحة الجرائم المعلوماتية* (الصفحات 152-173). الرياض، السعودية: جامعة الإمام محمد بن سعود الإسلامية.

جمال بوازدية. (2019). الاستراتيجية الجزائرية في مواجهة الجرائم السيبرانية "التحديات والافاق المستقبلية". *مجلة العلوم القانونية والسياسية ، 10* (1)، 1262- 1293.

حسين قوادرة. (جانفي 2020). الردع السيبراني بين النظرية والتطبيق. *المجلة الجزائرية للأمن والتنمية* (9)، 518-531.

حكيم غريب. (2018). الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة. *المجلة الجزائرية للدراسات السياسية ، 5* (2)، 104-119.

حورية بن سيدهم، و رقية عواشرية. (2020). الأمن الفضائي السيبراني "التحديات والحلول". *المجلة الجزائرية للأمن الإنساني ، 5* (2)، 125-145.

رحيمة نمديلي. (2017). خصوصية الجريمة الالكترونية في القانون الجزائري والقوانين المقارنة. *المؤتمر الدولي الرابع عشر حول الجرائم الالكترونية*. طرابلس، ليبيا.

سمير بارة. (2017). الأمن السيبراني في الجزائر السياسات والمؤسسات. *المجلة الجزائرية للأمن الإنساني ، 4*، 255-280.

عزيزة رابحي. (2018/2017). الأسرار المعلوماتية وحمايتها الجزائية. *أطروحة مقدمة لنيل شهادة الدكتوراه علوم في القانون الخاص* . الجزائر: جامعة أبو بكر بلقايد – تلمسان.

عنترة بن مرزوق، و محيي الدين حرشاوي. (2017). الأمن السيبراني كبعد جديد في السياسة الدفاعية الجزائرية. *الملتقى الدولي حول سياسات الدفاع الوطني*. ورقلة، الجزائر: جامعة ورقلة.

مجتمع الانترنت. (مارس 2020). المبادئ التوجيهية المتعلقة بامن البنية التحتية للانترنت في الدول العربية. *مجتمع الانترنت* .

مركز هيدرو. (2017). *الأمن الرقمي وحماية المعلومات الحق في استخدام شبكة آمنة*. القاهرة، مصر: مركز هيدرو.

مصطفى عبد الباقي. (2018). التحقيق في الجريمة الالكترونية وإثباتها. *مجلة دراسات ، 45* (4).

نداء نائل فداء المصري. (2017). خصوصية الجرائم المعلوماتية. *رسالة ماجستير* . جامعة النجاح الوطنية، فلسطين.

يوسف بوغرارة. (سبتمبر 2018). الأمن السيبراني: الإستراتيجية الجزائرية للأمن و الدفاع في الفضاء السيبيري. *مجلة الدراسات الأفريقية وحوض النيل ، 1* (3).

يوسف صغير. (2013). الجريمة المرتكبة عبر الانترنت. *رسالة ماجستير في القانون الدولي للأعمال* . جامعة تيزي وزو.