الآليات العقابية لمكافحة الجريمة الالكترونية في التشريع الجزائري

Penal mechanisms to fight cyber-crime in Algerian legislation

الدكتور دمان ذبيح عماد
جامعة عباس لغرور خنشلة
maitreimad040@gmail.com

الدكتورة بهلول سميّة(*)
جامعة محمد لمين دباغين سطيف 2
Soumia.bahloul@hotmail.com

تاريخ الإيداع:2019-05-27 تاريخ المراجعة:2019-12-03 تاريخ القبول:2020-01-05

الملخص

تعتبر الجريمة الالكترونية من أحدث وأخطر الجرائم تواجدا على ساحة العلوم الجنائية اليوم، وذلك لما تشكله هذه الجريمة من تهديد كبير يمس الأفراد والمؤسسات ويتعداهم حتى للمساس بأمن الدول واستقرارها، وهو الأمر الذي جعل العديد من دول العالم وعلى رأسها الجزائر تضع ضرورة التصدي لهذه الجريمة والعمل على كبح مخاطرها أولوية في قائمة حماية الدول ومواطنيها، وهو الأمر الذي ترجمته العديد من النصوص القانونية المستحدثة بهدف الوقاية من الجريمة الالكترونية ومكافحتها والتي عملت في مختلف موادها على وضع العديد من الآليات الردعية والعقابية وتعزيزها بهيئات وطنية ومحلية أنيط بها إلى جانب الهيئات القضائية دور العمل على مكافحة الجريمة الالكترونية والحد من انتشارها، وسنركز من خلال هذا المقال على بيان وتوضيح مختلف الآليات العقابية التي رصدها المشرع الجزائري في سبيل مكافحة الجريمة الالكترونية والوقاية من مخاطرها.

الكلمات المفتاحية: الجريمة الالكترونية، الآليات العقابية، تكنولوجيات الإعلام والاتصال، نظام المعالجة الآلية للبيانات.

Abstract

Electronic crime is one of the latest and most serious crimes in the field of forensic science today, because this crime poses a great threat to individuals and institutions and even affects the security and stability of countries, which has made many countries of the world, especially Algeria, the need to address this crime and work on This is what has been translated into many new legal texts aimed at preventing and combating electronic crime, which has worked in various articles on the development of many deterrent and punitive mechanisms and strengthening them with national bodies and A local body entrusted with the judicial bodies the role of working to combat electronic crime and reduce its spread, And we will focus through this article on the statement and clarify the various penal mechanisms monitored by the Algerian legislator in the fight against electronic crime and the prevention of risk.

Keywords: cybercrime, penal mechanisms, information and communication technologies, data processing system.

(*) المؤلف المُراسِل.

I مقدمة

تعتبر الجريمة الالكترونية من الجرائم الحديثة التي تطورت وانتشرت بوتيرة سريعة لتنقل عالم الجريمة إلى بعد جديد تطور من خلاله كل من مرتكب الجريمة ووسائل ارتكابها لنصبح اليوم أمام مجرمين ذوي درجة عالية من الذكاء، متمرسين وذوي كفاءة كبرى في استعمال التكنولوجيات الحديثة والتحكم فيها، لينتقل الخطر الإجرامي من الأفراد والمجتمعات إلى الدول ومؤسساتها، وهو الأمر الذي أصبح يفرض على التشريعات الوطنية والدولية التجند من أجل مكافحة الجريمة الالكترونية بنصوص قانونية صارمة من شأنها الحفاظ على سلامة الأفراد والمؤسسات والدول من خطر الجريمة الالكترونية بمختلف صورها وأشكالها.

وعلى اعتبار أن العقاب من أقدم أساليب مكافحة الجريمة والحد من انتشارها، لما أثبته من دور في ردع الأفراد عن القيام بالأعمال الاجرامية والتقليل من نسبة انتشارها والتمادي في القيام بها، الأمر الذي جعل النصوص العقابية تحتل قائمة الأساليب المنتهجة من طرف الدول في سياساتها لمكافحة الجريمة، وأمام قصور الآليات العقابية القديمة المبذولة في سبيل مكافحة الجرائم التقليدية أصبح من الواجب على المشرع العمل على بذل آليات عقابية حديثة تتناسب مع طبيعة الجريمة الالكترونية وتكون فعالة وناجعة في مكافحتها والحد من انتشارها وتضييق مخاطرها على كل من الأفراد والمؤسسات والدول، وهو الأمر الذي يضعنا ونحن بصدد إعداد هذا المقال أما إشكالية رئيسية مفادها فيم **تتمثل الآليات العقابية التي وضعها المشرع الجزائري في مجال مكافحة الجريمة الالكترونية والحد من انتشارها؟**

وهو ما سنجيب عنه بانتهاج الخطة التالية:

محور مفاهيمي: الجريمة الالكترونية.

المطلب الأول: نطاق العقوبات المطبقة على الجرائم الالكترونية.

الفرع الأول: العقوبات المقررة للاتفاق الجنائي على ارتكاب الجريمة الالكترونية.

الفرع الثاني: العقوبات المقررة لعملية الشروع في ارتكاب الجريمة الالكترونية.

المطلب الثاني: مضمون العقوبات المقررة للجريمة الالكترونية.

الفرع الأول: مضمون العقوبات المقررة للشخص الطبيعي.

الفرع الثاني: مضمون العقوبات المقررة للشخص المعنوي.

محور مفاهيمي: الجريمة الالكترونية.

أولا-التعريف الفقهي للجريمة الالكترونية: مع بداية ظهور الجريمة الالكترونية وفي غياب تعريف تشريعي لها وقع على عاتق الفقه مسؤولية ضبط تعريف انطلاقا من القواعد العامة واستنادا إلى النقاط المستحدثة في الجريمة الالكترونية، وهو الأمر الذي ترتب عنه ظهور العديد من التعاريف منها التي تضيق من نطاق الجريمة الالكترونية وتركز على محلها ومنها التي تستند إلى الفاعل مرتكب الجريمة كما هناك التي توسعت في تعريف الجريمة الالكترونية لتدخل ضمن نطاقها كافة العمليات والممارسات الغير مشروعة المرتبطة بتكنولوجيات الإعلام والاتصال واستخدام الحاسوب الآلي والوسائل الالكترونية وشبكة الانترنت وعليه انقسم تعريف الجريمة الالكترونية إلى: [1]

1-التعريف الضيق للجريمة الالكترونية: تركز التعاريف الضيقة للجريمة الالكترونية على الوسيلة التي يستخدمها المجرم في سبيل القيام بالجريمة أو على مدى معرفة المجرم بالتقنيات الحديثة للحاسوب وتكنولوجيات الاعلام والاتصال إضافة إلى محل الجريمة ألا وهو المال المعلوماتي المعنوي.

أ-تعريف الجريمة الالكترونية استنادا إلى وسيلة ارتكابها: يذهب الفقه انطلاقا من هذا المعيار إلى التركيز على الحاسب الآلي على اعتباره أساس الجريمة الالكترونية ونقطة التمييز بينها وبين الصور التقليدية وحتى الحديثة للجرائم، مؤكدين أن جهاز الحاسوب ولكونه أصبح وسيلة ضرورية في عصر التكنولوجيا فإن هذا جعله يدخل في العديد من مجالات علم الإجرام [2] وتعرف الجريمة الالكترونية من هذا المنطلق بأنها **"كل نشاط إجرامي تستخدم فيه التقنية الالكترونية المتمثلة في الحاسوب الآلي الرقمي وشبكة الانترنت بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي المستهدف"** [3] **وأيضا "جرائم الشبكة العالمية التي يستخدم فيها الحاسب وشبكاته العالمية كوسيلة مساعدة لارتكاب جريمة، كاستخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب"**[4] وما يسجل أن أنصار هذا الاتجاه أنهم ركزوا بدرجة كبيرة على وسيلة ارتكاب الجريمة في حين أغفلوا في المقابل الفعل أو السلوك الإجرامي ومرتكبه رغم كونهما أهم بكثير من الوسيلة المستخدمة، وهو الأمر الذي ترتب عنه غموض أغلب تعاريفهم وقصورها عن تحديد مفهوم واضح جامع ومانع للجريمة الالكترونية.[5]

---

[1]- بهلول سمية، **دور الإدارة الالكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر**، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص إدارة محلية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، 2017-2018، ص283.

[2]- غنية باطلي، **الجريمة الالكترونية (دراسة مقارنة)**، منشورات الدار الجزائرية، الجزائر، 2015، ص15.

[3]- كحلوش علي، "**جرائم الحاسوب الآلي وأساليب مواجهتها**"، مجلة الشرطة، العدد 84، جويلية 2007، المديرية العامة للأمن الوطني، الجزائر، ص51.

[4]- مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الالكترونية**، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009، ص112.

[5]- للاطلاع على مزيد من تعاريف الجريمة الالكترونية الموضوعة انطلاق من معيار الوسيلة المستخدمة لارتكاب الجريمة راجع:

* عمر بن محمد العتيبي، **الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير الدولية والمحلية**، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010، ص21 وما بعدها.

*Al Azouzi Ali, **La Cybercriminalité au Maroc,** Edition Bishops solution, Casablanca, 2010, P43.

ب-تعريف الجريمة الالكترونية استنادا إلى مستوى معرفة المجرم للتقنيات الحديثة للحاسوب وتكنولوجيات الإعلام والاتصال: إلى جانب تعريف الجريمة الالكترونية انطلاقا من الوسيلة المستخدمة في ارتكابها هناك من يعرفها استنادا إلى مستوى معرفة المجرم للتقنيات الحديثة للحاسوب وتكنولوجيات الاعلام والاتصال على اعتبارها المحل الأساسي لارتكاب هذا النوع من الجرائم وتنفيذها يستحيل دون علم المجرم بهذه التقنيات ومعرفة طريقة استخدامها لارتكاب الفعل الاجرامي، وانطلاقا من هذا المعيار تعرف بأنها **"كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابه من ناحية، ولملاحقته وتحقيقه من ناحية أخرى".** [1]

ج-تعريف الجريمة الالكترونية استنادا إلى محلها أو موضوعها: يذهب جانب ثالث من الفقه إلى تعريف الجريمة الالكترونية بالاستناد إلى محلها أو موضوعها على اعتبار أن وسيلة الجريمة وفاعلها لا يؤديان أي دور في تحديد مفهوم هذا النوع من الجرائم، وبالتالي فإن **"الجرائم الالكترونية هي الجرائم التي ترتكب ضد الأنظمة الالكترونية والشبكات المعلوماتية"** أي أنها بعبارة أخرى **"هي نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الالكتروني أو التي تحول عن طريقه".** [2]

2-التعريف الموسع للجريمة الالكترونية: مع ثبات قصور التعريف الضيق للجريمة الالكترونية عن الإحاطة بأوجه الإجرام الالكتروني خاصة وأن الحاسب الآلي الذي اتخذه البعض قاعدة لا يتعدى مع ظهور وسائل حديثة كالهواتف الذكية عن كونه وسيلة تقليدية، توجه الفقه نحو توسيع معايير تعريف الجريمة الالكترونية فعرفها البعض بأنها **"كل فعل أو امتناع عن فعل يأتيه الانسان إضرارا بمكونات الحاسب الآلي المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التي تمتد تحت مظلة قانون العقوبات لحمايتها"** [3] كما أنها **"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها"** [4] وأيضا **"كل استخدام في صورة فعل أو امتناع من شأنه الاعتداء على أي مصلحة مشروعة، سواء كانت مادية أو معنوية يكون ناتجا بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية ومعاقب عليه قانونا أيا كان غرض الجاني"** [5] وما يمكننا تسجيله أن رواد هذا الاتجاه قد وسعوا من نطاق المعايير المعتمدة لتعريف الجريمة الالكترونية لتستغرق بذلك كل فعل أو امتناعا عن فعل مادي أو معنوي، كما تم التركيز على

---

[1]- نائلة عادل محمد فريد، **جرائم الحاسب الاقتصادية**، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2003، ص21.

[2]- أشرف جمال محمود عبد العاطي، **الإدارة الالكترونية للمرافق العامة**، دار النهضة العربية، القاهرة، 2016، ص359.

[3]- هلالي عبد الله أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم في جرائم المعلومات (دراسة مقارنة)**، دار النهضة العربية، القاهرة، 2000، ص07.

[4]- هشام محمد فريد رستم، **"الجرائم المعلوماتية_ أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية للتدريب التخصصي"**، ورقة بحث مقدمة ضمن فعاليات مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 01 إلى 03 ماي 2000، منشور ضمن مجلة "الشريعة والقانون"، المجلد الثاني، الطبعة الثالثة، 2004، ص407.

[5]- أسماء حسين رويعي، **الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية**، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2013، ص64.

تقنية المعلوماتية وتكنولوجيات الاعلام والاتصال لكونها زاوية التفرقة بين الجريمة الالكترونية وغيرها من الجرائم التقليدية.

3-التعريف المختلط: تعتبر منظمة التعاون والتنمية الاقتصادية(OCDE) من السباقين لوضع تعريف للغش المعلوماتي والجريمة الالكترونية والتي ذهبت إلى القول بأنها:

« Est considéré comme crime informatique tout comportement illégale ou contraire à l'éthique, ou non autorisé qui concerne un traitement automatique de données ou de transmissions de données ». [1]

وانطلاقا من هذا التوجه فإن الجريمة الالكترونية هي **"كل جريمة أو سلوك غير مشروع يستخدم بالحاسب الآلي أو محاولة نسخ أو حذف أو إتلاف لبرامج الحاسب الآلي أو أي جريمة يكون لتنفيذها صلة بالقواعد والعلوم المعلوماتية أو أي سلوك غير مشروع متعلق بالمعالجة الآلية للبيانات".** [2]

ثانيا- التعريف التشريعي: مع انتشار الجرائم الالكترونية واتساع نطاقها أصبح من الضروري التصدي لهذه الظاهرة التي أصبحت تمس بالأمن الوطني الأمر الذي ترتب عنه تعديل الكثير من التشريعات الوطنية والدولية وإدخال هذا النوع من الجرائم ضمن نطاق الأفعال المجرمة التي يعاقب عليها القانون وتخصيص عقوبات تحد من انتشارها واتساعها، وعلى اعتبار أن وضع وضبط تعاريف للمفاهيم القانونية لا يدخل ضمن نطاق اختصاص المشرع فإن المشرع الجزائري وبموجب تعديل قانون العقوبات سنة 2004 [3] عمل على تجريم الجرائم الالكترونية التي أصبحت تنتشر في المجتمع الجزائري مع بداية توجهه نحو المعلوماتية والانفتاح على العالم الرقمي، واستحدث بذلك قسما خاصا بالعقوبات المطبقة على الجرائم المتعلقة بالمساس بأنظمة المعالجة الآلية للمعطيات، ومع انتقال الجزائر نحو انتهاج **استراتيجية الجزائر الالكترونية** وظهور **بوادر التحول الالكتروني** لجميع المؤسسات والهيئات والإدارات العمومية وجد المشرع الجزائري واقعا يفرض استحداث قانون جديد أكثر عمقا لمعالجة الجرائم الالكترونية وما يتعلق بها من تجاوزات تمس الأفراد والمؤسسات فصدر بذلك سنة 2009 أول نص قانوني متعلق بالجرائم الالكترونية ومكافحتها والذي وضع من خلاله المشرع الجزائري تعريفا للجرائم الالكترونية التي اصطلح عليها بمصطلح **الجرائم المتصلة بتكنولوجيات الإعلام والاتصال** وذلك لاستبعاد الغموض والمرونة التي تتميز بها التعاريف الفقهية لهذا النوع من الجرائم ونص بناءا على هذا بأن **"الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: هي جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية".** [4]

---

[1] - Site officiel de L'OCDE www.oecd.org consulté le 22 Mars 2019.

[2] - نايل نبيل عمر، **الحماية الجنائية للعمل الالكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة، القاهرة، 2012، ص23.

[3] - القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71 الصادرة في الصادرة في 10 نوفمبر 2004.

[4] - المادة الثانية (02) الفقرة الأولى من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر العدد 47 الصادرة في 16 أوت 2009.

وبالعودة إلى مختلف التعاريف أعلاه سواء الفقهية أو التشريعية نجد أن التعبير عن الجريمة الالكترونية وتحديد مفهومها تغير وتنوع بحسب الزاوية التي ينطلق منها كل تعريف كما أن هناك من يعتمد مصطلح الجريمة الالكترونية وهناك من يصطلح عليها بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال وآخر يسميها بجرائم التقنية العالية وآخر يربطها بجهاز الحاسوب أو الكمبيوتر إلى جانب جرائم الانترنت أيضا [1] وبالرغم من ذهاب بعض الفقه إلى القول بأن جميع المصطلحات السابقة تصب في نفس الإطار وتحمل نفس المدلول، هناك جانب آخر يقول أنه وحتى تكيف الجريمة بأنها جريمة الكترونية وجب حدوث اتصال بين جهازين الكترونيين، لأنه لا يمكن ارتكاب جريمة الكترونية من خلال العمل على جهاز منفرد مهما كان نوع الجرم المقترف، ذلك أنه يمكن استخدام الكمبيوتر في الكثير من الجرائم لكن ليس بالضرورة أن يتم تكييفها على أنها جريمة الكترونية، على غرار فعل التزوير في المستندات والوثائق، فمثل هذه الأفعال إذا تمت باستخدام جهاز الحاسوب فهي ترد إلى أصل الفعل ويمكن أن تكون جريمة معلوماتية وهي في الوقت ذاته جريمة الكترونية بمجرد ارسالها من جهاز الكتروني إلى جهاز آخر [2] أي أنه وبمفهوم آخر فإن الجريمة الالكترونية لا تختلف عن الجريمة المعلوماتية في كثير من الأحوال باستثناء أنها تتم عن طريق جهازين الكترونيين أو أكثر يمكن الاتصال بينهما بواسطة شبكة انترنت محلية أو دولية أو بواسطة إحدى التقنيات الحديثة المستحدثة في إطار الثورة الرقمية وتطور التكنولوجيات الحديثة [3] وعليه فإنه من الصعب القول بوجود حدود فاصلة بين الجريمة المعلوماتية والجريمة الالكترونية فكلاهما مرتبط بوجود جهاز الكتروني حديث طالما أنه في الوقت الحاضر لم يعد يتم استخدام جهاز الكمبيوتر فقط، إنما ظهرت العديد من الأجهزة الالكترونية التي تسمح بتخزين المعلومات والاتصال فيما بينها كالمفكرات الالكترونية وأجهزة الهواتف النقالة الذكية وغيرها من الاختراعات. [4]

وعموما يلاحظ بأن الجريمة الالكترونية تتكون من مقطعين وهما **"الجريمة"** و **"الالكترونية"** حيث يستخدم مصطلح الالكترونية لوصف جزء من الحاسوب، في حين أن الجريمة هي **"مجموع السلوكيات والأفعال الخارجة عن نطاق القانون"** وبناءا عليه فإن الجريمة الالكترونية هي **"مجموع المخالفات التي ترتكب ضد الأفراد أوالمجموعات من طرف أفراد أو مجموعات أخرى بدافع الجريمة وبقصد إيذاء سمعة الضحية أو القيام بأذى مادي أو عقلي للضحية بطريقة مباشرة أو غير مباشرة باستخدام شبكات الاتصالات مثل الانترنت".** [5]

---

[1]-بهلول سمية، **دور الإدارة الالكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر**، مرجع سابق، ص287.

[2]- حسينة شرون، **"فعالية التشريعات العقابية في مكافحة الجرائم الالكترونية"**، مجلة دراسات وأبحاث، جامعة زيان عاشور_الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009، ص428.

[3]- **المرجع نفسه**، ص428.

[4]- **المرجع نفسه**، ص428. ولتفاصيل راجع: * أحسن رابحي، **"الجريمة الالكترونية: النقطة المظلمة بالنسبة للتكنولوجية المعلوماتية"**، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009، ص ص98-113.

* بلبالي إبراهيم، **"الجريمة الالكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق"**، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009، ص ص133-149.

[5]- مختارية بوزيدي، **"ماهية الجريمة الالكترونية"**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، مركز جيل حقوق الإنسان، الجزائر العاصمة يوم 29 مارس، ص09. ولمزيد من التفاصيل حول مختلف تعاريف الجريمة

II المطلب الأول: نطاق العقوبات المطبقة على الجرائم الالكترونية

إن الجريمة الالكترونية وعلى اختلاف التسميات التي تتخذها على مستوى التشريعات الوطنية والدولية فإنها تشترك في أمر واحد وهي أنها تقوم على وجود نظام آلي معلوماتي لمعالجة المعلومات ويظهر الاختلاف بين صورها ومظاهرها في اختلاف وتنوع صور وأوجه الاعتداء، كما أنه ومن أهم مميزاتها هو نطاق تطبيق هذا العقاب حيث أن المشرع وإدراكا لخطورتها توسع في نطاق الأفعال المجرمة وبالتالي اتسعت هذه العقوبات لتنطلق من مجرد الاتفاق على ارتكاب الجريمة، وفي هذا الإطار يذهب البعض إلى فصل الاتفاق الجنائي على ارتكاب الجريمة الالكترونية كجريمة خاصة وليست مجرد عزم على ارتكاب الجريمة، الأمر الذي يستوجب خصه بعقوبات منفصلة لكونه يظهر العزم الجماعي الجنائي بمظهر خارجي ملموس، لكون كل شخص يعلن عزمه على ارتكاب الجريمة ثم تتحدد إرادة الأفراد لينشأ الاتفاق، علاوة على كون الاتفاق يشكل ظاهرة خطرة تهدد الأمن العام وتخل به الأمر الذي يستوجب ضبطه بأحكام عقابية واضحة ومحددة. [1]

هذا ما سنوضحه من خلال هذا المطلب وذلك من خلال بيان العقاب المقرر للاتفاق الجنائي على ارتكاب الجريمة الالكترونية **(الفرع الأول)** ثم تحديد العقاب المقرر لعملية الشروع في ارتكاب الجريمة الالكترونية **(الفرع الثاني)**.

الفرع الأول: العقاب المقرر للاتفاق الجنائي على ارتكاب الجريمة الالكترونية

يقوم مبدأ العقاب في القانون على الاتفاق الجنائي لارتكاب الجريمة الالكترونية على قيام شخصين أو أكثر بخطوة للبدء في نشاط إجرامي يؤدي مباشرة وفي حالة سير الأمور بوتيرة عادية إلى ارتكاب الجريمة الالكترونية، في حين استقرت أغلب التشريعات العالمية ومن بينها المشرع الجزائري على كون الأعمال التحضيرية التي تسبق عملية البدء في تنفيذ الجريمة غير معاقب عليها كقاعدة عامة إلا إذا توافر نص قانوني خاص يجرمها، من هذا المنطلق وبالعودة إلى المادة 394 مكرر 05 من قانون العقوبات المستحدثة بموجب القانون 04-15 [2] نجد المشرع ينص على أن يعاقب **"كل من شارك في مجموعة أو اتفاق تألف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بنفس العقوبات المقررة للجريمة ذاتها"**، وقد تبنى المشرع هذا التوجه خلافا للقواعد العامة المقررة في إطار قانون العقوبات، والتي تنص على أن العقاب لا يتقرر إلا في الجرائم الواقعة فعلا والتامة المكتملة الأركان أو الجرائم التي تقف عند مرحلة الشروع أو المحاولة، ويعود هذا الاستثناء عن القاعدة العامة في التجريم إلى خطورة الجريمة الالكترونية التي

الالكترونية والفرق في تسميتها في إطار التشريعات المقارنة وصور تجريمها راجع: هروال هبة نبيلة، **جرائم الانترنت (دراسة مقارنة)**، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة أبي بكر بلقايد تلمسان، 2013-2014.

[1]- بهلول سمية، دور الإدارة الالكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر، **مرجع سابق**، ص 322.

[2]-القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71 الصادرة في الصادرة في 10 نوفمبر 2004.

تقتضي التصدي لها بكافة الوسائل الردعية والعقابية، وتقرير نوع من الحماية المتقدمة والوقاية لنظم المعالجة الآلية للمعلومات والمعطيات ضد المخاطر التي تنشأ على النشاط غير المشروع. [1]

بناءا عليه وعلى اعتبار أن الاتفاق الجنائي يعتبر جريمة كاملة معاقبا عليها بموجب القانون فإنه يستوجب لقيامها توافر الركنين المادي والمعنوي حتى تقوم الجريمة وتستوجب العقاب وفقا لما يلي:

أولا-الركن المادي: يقوم الركن المادي على الاتفاق ذاته والذي يترتب عن انعقاد ارادتين أو أكثر واجتماعها على موضوع الجريمة ومحلها مع ضرورة أن يتخذ هذا الاتفاق الطبيعة المادية الملموسة، والذي يفترض تعبير كل طرف عن إرادته ونيته في القيام بالعمل المجرم مع إعلام أطراف الاتفاق، ويتحقق باتجاه إرادتهم نحو هدف وطريق واحد يتلاقى عند موضوع الجريمة، ويقوم سواء استغرق انعقاد الارادات وقت قصيرا أو طويلا وسواء كان اتفاقا منظما أو منفصلا.

ثانيا-الركن المعنوي: على اعتبار أن جريمة الاتفاق الجنائي من الجرائم العمدية فإنه يستوجب لقيامها توافر كل من القصد الجنائي بعنصريه العلم والإرادة، وذلك بعلم كل عضو من أعضاء الاتفاق بماهية الفعل أو الأفعال التي يقدمون على القيام بها والتي تم الاتفاق عليها، وبما لها من خصائص مجرمة من طرف المشرع، وعليه فمن يجهل الغرض من الاتفاق لا يعد القصد الجنائي متوافرا لديه.

وعلاوة على العلم يجب أن تتجه إرادة كل عضو من أعضاء الاتفاق إلى تحقيق نشاط إجرامي يتمثل في التحضير للقيام بالجريمة ولا يشترط في هذه الجريمة أن يكون كل أعضاء الاتفاق عالمين بنشاط بعضهم البعض إلى جانب ضرورة أن يكون لكل أعضاء الاتفاق إرادة الدخول إلى في هذا الاتفاق أي إرادة كل طرف في أن يكون عضوا في الاتفاق وأن تكون الإرادة جادة.

الفرع الثاني: العقاب المقرر لعملية الشروع في ارتكاب الجريمة الالكترونية

يقرر العقاب على أي جريمة انطلاقا من الضرر الذي ترتبه على المصالح الفردية والجماعية محل الحماية القانونية، وعليه فإن العقاب على الشروع بوصفه جريمة لا بد أن يقوم بناءا على الخطر والضرر المقترنين به، حيث ثبت أن خطر الجريمة لا يقتصر على ما تحدثه من ضرر مادي بالفرد بل يتعدى ذلك إلى ما تحدثه من قلق واضطراب في الجماعة، ولكون مجال الشروع في الجنايات هو الأصل بالنظر لخطورتها ولأن جرائم المساس بأنظمة المعالجة الآلية للمعطيات تنطوي على خطورة كبيرة حتى وإن لم تكتمل أركان قيامها وتم الشروع فقط في ارتكابها فإن المشرع قرر إخضاعها عبر قواعد قانون العقوبات إلى نظام الشروع [2] ويعرف الشروع في القانون بأنه **"كل محاولات لارتكاب جناية تبتدئ بالشروع في التنفيذ أو بأفعال لا لبس فيها تؤدي مباشرة إلى ارتكابها تعتبر كالجناية نفسها إذا لم توقف أو لم يخب أثرها إلا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى ولو لم يمكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها"** [3] ويعاقب المشرع الجزائري على محاولة ارتكاب أي

---

[1]- غنية باطلي، **مرجع سابق**، ص197.

[2]- غنية باطلي، **مرجع سابق**، ص ص201-202.

[3]- المادة الثلاثون (30) من قانون العقوبات.

جريمة من جرائم الاعتداء على أنظمة المعالجة الآلية للمعطيات وهو الأمر الذي فسره الفقه برغبته في تغطية أكبر قدر ممكن منها. [1]

ونصت المادة 394 مكرر 07 من قانون العقوبات أن **"يعاقب على الشروع في ارتكاب الجنح المنصوص عليها في هذا القسم بالعقوبات المقررة للجنحة ذاتها"** وفي هذا الإطار انقسم الفقه بين من يذهب إلى أنه لا يوجد شروع في الاتفاق الجنائي لكونه حالة نفسية تتم بتلاقي الإرادات ولا تحتمل لا بداية ولا نهاية وهو لا يقع إلا كاملا ولا يحتمل البدء في التنفيذ، خاصة وأن المشرع لا يعتبر الدعوة إلى الاتفاق شروعا ولكن يعاقب عليها كجريمة قائمة بذاتها، في حين يرى جانب آخر أنه طالما كانت أركان الشروع قائمة ولم يكن القانون يتضمن نصا خاصا يعاقب عليه فلا داعي للأخذ بالرأي السابق لكونه غير صحيح أن الشروع في الاتفاق غير متصور. [2]

III المطلب الثاني: مضمون العقوبات المقررة للجريمة الالكترونية

على اعتبار أن الجريمة الالكترونية واسعة النطاق فإن هذا شكل أول عائق في وجه المشرع لسن عقوبات لها ذلك أن الصور والمظاهر المتطورة التي تتخذها جعلت من واقع تغطيتها مسبقا أمرا صعبا إلى جانب أن تطور التكنولوجيات الحديثة جعل من العقوبات التشريعية تعاني قصورا دائما يستوجب التحيين الدائم والمستمر والسريع، إلى جانب أن مضمون العقوبات المقررة للجرائم الالكترونية أصبحت تفرض سؤالا جوهريا حول **مدى نجاعة هذه العقوبات في تسليط جزاء عادل على المجرم المرتكب للجريمة الالكترونية؟** خاصة وأن الواقع أصبح يثبت مدى تورط الأشخاص المعنوية في هذا النوع من الجرائم التي أصبحت تغري الكثير من الشركات والمؤسسات التي تعمل في مجال التكنولوجيات الحديثة والتي أصبح أصحابها وفي إطار المنافسة الواسعة يتوجهون باسم ولحساب هذه الشركات والمؤسسات للجوء إلى طرق غير قانونية بهدف المنافسة على تملك هذه التكنولوجيات واحتكارها، الأمر الذي استوجب التصدي لهذه الظواهر من خلال بذل عقوبات صارمة للحد من هذه التجاوزات ومكافحتها، بما يتناسب وخطورتها.

هذا ما سنوضحه من خلال هذا المطلب ببيان مضمون العقوبات المقررة للشخص الطبيعي **(الفرع الأول)** ومن ثم العقوبات المقررة للشخص المعنوي **(الفرع الثاني).**

الفرع الأول: مضمون العقوبات المقررة للشخص الطبيعي

نص المشرع الجزائري على مجموعة من العقوبات الأصلية والتكميلية المقررة للشخص الطبيعي والمتمثلة في:

أولا-العقوبات الأصلية: تمثل العقوبات الأصلية المطبقة على الشخص الطبيعي في إطار الجريمة الالكترونية المؤشر الصريح لخطورة هذه الجريمة والتي أقرها المشرع على الأفعال التي يجرمها قانون العقوبات والمتمثلة فيما يلي:

[1]- غنية باطلي، **المرجع السابق**، ص204.

[2]- **المرجع نفسه**، ص205.

1-العقوبات المقررة لجريمة الدخول أو البقاء غير المشروع إلى النظام المعلوماتي: تعتبر هذه الجريمة من أهم الجرائم الالكترونية وأخطرها على المؤسسات والأفراد لكونها تشكل انتهاكا صارخا ومباشرا للحقوق والحريات ويختلف الفقه في طبيعة هذه الجريمة بين من يعتبرها جريمة واحدة تؤدي نفس النتيجة وبين من يقسمها إلى جريمتين بحيث يفصل رواد هذا المذهب بين الدخول إلى النظام المعلوماتي كجريمة أولى والبقاء غير المشروع في النظام كجريمة ثانية.

ويقصد بجريمة الدخول إلى الأنظمة تحقيق فعل الدخول إلى النظام وتشير الكلمة إلى كل **"الأفعال التي تسمح بالولوج إلى النظام المعلوماتي والسيطرة على المعطيات أو المعلومات التي يتكون منها"، كما يقصد به "الدخول إلى محتويات جهاز الكمبيوتر والقيام بأي عملية اتصال بالنظام محل الحماية دون أي ترخيص أو وجه حق".** [1]

أما جريمة البقاء غير المشروع داخل النظام المعلوماتي فتعتبر من الجرائم المستمرة وتبقى قائمة مستوفية أركانها ما دام الجاني لا يزال على اتصال بنظام المعلومات الذي تم الدخول إليه بطريقة غير مشروعة ودون ترخيص.

ويقصد بالبقاء **كفعل "التواجد داخل نظام المعالجة الآلية للمعطيات ضد إرادة من له الحق في السيطرة على هذا النظام والتصرف فيه"** [2] واستقر أغلب الفقه على أن جريمة البقاء غير المشروع داخل النظام المعلوماتي تعتبر بشكل عام من الجرائم التي يصعب تقديم دليل على إثباتها وكثيرا ما تقترن الجريمتان (أي الدخول غير المشروع والبقاء غير المشروع) ببعضهما البعض وهو الأمر الذي جعل الكثير من الفقه المقارن وأغلب التشريعات الجنائية تجمع الصورتين في جريمة واحدة تحت مسمى **الدخول والبقاء غير المشروع في النظام المعلوماتي**، وقد قرر المشرع في إطار قانون العقوبات وبموجب المادة 394 مكرر عقوبتين أصليتين لجريمة الدخول أو البقاء غير المشروع:

- **العقوبة المقررة للجريمة في صورتها البسيطة:** يعاقب القانون على هذه الجريمة في صورتها البسيطة بالحبس من ثلاثة أشهر إلى سنة وبغرامة مالية من خمسين ألف دينار (50.000) إلى مائة ألف دينار (100.000) وفتح في هذا المجال للقاضي السلطة التقديرية بأن جعل له حدا أدنى وحدا أقصى في تقدير العقوبة بالعودة إلى الحيثيات والوقائع، وبالنظر للباعث الذي دفع الشخص لارتكاب الجريمة.
- **العقوبة المقررة للجريمة في صورتها المشددة:** تضاعف عقوبة الجريمة إذا ترتب عنها حذف أو تغيير في المعطيات، بحد أدنى يقدر بستة أشهر بعدما كان ثلاثة أشهر، وحد أقصى يقدر بسنتين

[1]- لتفاصيل حول هذه الجزئية راجع: * نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2008، ص158. *محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر، 2004، ص102.

[2]- أمال قارة، **الحماية الجزائية للمعلومات في التشريع الجزائري**، دار هومة للنشر والتوزيع، الجزائر، الطبعة الأولى، 2006، ص110.

بعدما كان سنة واحدة، ويعاقب على هذه الصورة بغرامة مالية تقدر ب مئة ألف (100.000) دينار إلى مئتين ألف (200.000) دينار وفي حال ما تم القيام بتخريب نظام المعالجة الآلية فيعاقب عليها بالحبس من ستة أشهر إلى سنتين وبغرامة من خمسين ألف (50.000) دينار إلى مئة وخمسين ألف (150.000) دينار.

2-العقوبات المقررة لجريمة إفساد أو تعطيل سير النظام: وتسمى أيضا جريمة **"الاعتداء على سير نظام المعالجة الآلية للمعطيات"** حيث أغفل المشرع الجزائري وضع نص صريح خاص بتجريم الاعتداء على جريمة سير نظام المعالجة الآلية للمعطيات، إلا أنه يمكن استخلاص التجريم من خلال النصوص القانونية المستحدثة في إطار تجريم الاعتداءات الواقعة على أنظمة المعالجة أو على معطيات الأنظمة الداخلية أو الخارجية. [1]

وعلى الرغم من أن هناك من يذهب إلى أن جريمة الاعتداء العمدي على المعطيات مثل جريمة الاعتداء العمدي على نظام المعالجة الآلية للبيانات تهدف إلى القيام بأعمال تخريب وقرصنة، إلا أن هناك من يذهب إلى أن الفرق بينهما يكمن في أن جريمة الاعتداء العمدي على النظام وإن كانت لا تقع بصفة أساسية على البرامج والشبكات إلا أنها تصيب المعطيات كنتيجة لأفعال الإفساد والتوقيف في حين أن الاعتداء على المعطيات الذي تقوم عليه جريمة الاعتداء العمدي على المعطيات قد يؤثر على صلاحية النظام للقيام بوظائفه سواء على البرامج أو شبكات النقل والاتصال، وفي سبيل التفرقة بين الجريمتين تم الاتفاق على أن المعيار الأساسي هو المحل الذي يقع عليه الاعتداء ففي حال وقوع الجرم على العناصر المادية للنظام فإن الجريمة هي جريمة الاعتداء العمدي على نظام المعالجة الآلية للمعطيات، أما إذا كان يقع على العناصر المعنوية فإننا نكون في هذه الحالة أمام جريمة الاعتداء العمدي على المعطيات. [2]

3-العقوبات المقررة لجريمة الاعتداء العمدي على المعطيات: يقصد بالاعتداء على المعطيات **"التجاوز الذي يهدف إلى الإضرار بمعلومات الكمبيوتر أو وظائفه سواء بالمساس بسريتها أو المساس بسلامة محتوياتها وتكاملها أو بتعطيل قدرة وكفاءة الأنظمة بشكل يمنعها من أداء وظيفتها بشكل سليم"** ويتحقق الاعتداء على معطيات النظام عادة بعد تجاوز مرحلة الدخول والبقاء في نظام المعالجة الآلية للمعطيات، ويتخذ وفق ما نص عليه المشرع الجزائري صورتين **"الاعتداء على المعطيات الداخلية للنظام"** أو **"الاعتداء على المعطيات الخارجية للنظام"**. [3]

تنص المادة 394 مكرر1 من قانون العقوبات أنه **"يعاقب بالحبس من ستة (06) أشهر إلى ثلاث (03) سنوات وبغرامة من 500.000 إلى 2.000.000 كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها"** وما يسجل أن عقوبة الاعتداء العمدي على المعطيات تفوق

[1]- براهمي جمال، **"مكافحة الجرائم الالكترونية في التشريع الجزائري"**، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد الثاني (02)، العدد الثاني (02)، ص137.

[2]- غنية باطلي، **مرجع سابق**، ص210.

[3]- براهمي جمال، **مرجع سابق**، ص ص132-133.

عقوبة الدخول أو البقاء غير المشروع سواء في صورتها المشددة أو البسيطة ذلك أن جريمة الدخول أو البقاء غير المشروع في صورتها البسيطة لا تؤدي إلى حدوث أضرار معينة تلحق بالمعطيات أو النظام، أما المشددة وإن أدت إلى نفس النتائج التي تؤدي إليها جريمة الاعتداء العمدي على المعطيات وإن كانت تؤدي إلى نفس النتائج فإن عقوبتها أكبر لأنها جريمة عمدية يجب فيها توافر القصد الجنائي لدى مرتكب جريمة الدخول أو البقاء غير المشروع في صورتها المشددة. [1]

2-العقوبات التكميلية: إلى جانب العقوبات الأصلية المطبقة على مرتكبي جرائم المساس بأنظمة المعالجة الآلية للمعطيات، فقد نص على جملة من العقوبات التكميلية لهذه الجرائم وفي هذا الإطار نصت المادة 394 مكرر6 بأنه **"مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع إغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم، علاوة على إغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها"** وعليه فإن العقوبات التكميلية لهذه الجريمة تتمثل في: [2]

أ-المصادرة: عرف المشرع الجزائري المصادرة بأنها **"الأيلولة النهائية إلى الدولة لمال أو مجموعة أموال معينة أو ما يعادل قيمتها عند الاقتضاء"** [3] وانطلاقا من المادة 394 مكرر6 أعلاه فإنه لا بد لإعمال إجراء المصادرة في مجال الجرائم الالكترونية توافر جملة من الشروط المتمثلة في:

- **أن يحكم على المتهم بعقوبة أصلية في إحدى الجرائم المنصوص عليها في القسم الخاص بالاعتداء على أنظمة المعالجة الآلية للمعطيات.**
- **أن تكون الأشياء التي تمت مصادرتها قد استخدمت في ارتكاب الجريمة الصادر بشأنها الحكم القضائي.**
- **يجب ألا تخل المصادرة بحقوق الغير حسن النية، في حال ما كانت الوسائل المستخدمة في ارتكاب الجريمة ملكا للغير.**
- **وجوب أن يكون الشخص حسن النية جاهلا بكون الوسائل المستخدمة في ارتكاب الجريمة جاهلا بأن هذه الوسائل قد تستخدم في ارتكاب الجريمة.**

ب-الغلق: يعتبر الغلق من ثاني العقوبات التكميلية التي نصت عليها المادة 394 مكرر من قانون العقوبات إلى جانب عقوبة المصادرة، وتشمل عقوبة الغلق في إطار الجرائم الالكترونية غلق المواقع الالكترونية التي تكون محلا للجريمة كما يشمل الغلق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالك المحل.

---

[1]- **المرجع نفسه**، ص212.

[2]- **المرجع نفسه**، ص ص215-217.

[3]- المادة الخامسة عشر (15) من قانون العقوبات.

ويجب الإشارة في هذا المقام بأن المواقع محل الغلق هي المواقع التي تم عن طريقها تنفيذ الجريمة، أو تلك التي تقدم خدمات تسمح بالدخول غير المشروع إلى مختلف الأنظمة أو تسمح بالتلاعب بالمعطيات المعلوماتية في حين أن المواقع التي تعرضت للاعتداء عن طريق هذه الجرائم الالكترونية أو التي تم التلاعب بمعطياتها فإنها تعتبر في مقام الضحية ولا يتصور باي حال من الأحوال أن يتم غلقها وهو الأمر الذي يستوجب في هذا الصدد أن يتحرى الدقة وبدل استخدام عبارة "المواقع محل الجريمة" أن يستخدم عبارة "المواقع المستعملة في ارتكاب الجريمة" وذلك تجنبا للعبارات الغامضة والتي تحتمل أكثر من تأويل، وفي هذا الإطار يجب الإشارة أيضا إلى أن المشرع لم يتعرض بموجب المواد الناظمة لهذه العقوبات لتحديد مدة زمنية للغلق سواء المحلات أو المواقع الالكترونية وهو الأمر الذي يقود إلى احتمال أن غلق المحلات والمواقع الالكترونية التي عن طريقها تم ارتكاب الجريمة الالكترونية قد يكون مؤبدا وقد يكون مؤقتا، وهو الأمر الذي يعود إلى تقدير القاضي مع غياب نص قانوني صريح يحدد هذه الحالات والاحتمالات وذلك نزولا عند أحكام المادة 16 مكرر1 من قانون العقوبات والتي تنص أنه **"يترتب على عقوبة غلق المؤسسة منع المحكوم عليه من أن يمارس فيها النشاط الذي ارتكبت الجريمة بمناسبته.**

ويحكم بهذه العقوبة إما بصفة نهائية أو لمدة لا تزيد عن عشر (10) سنوات في حالة الإدانة لارتكاب جنحة".

الفرع الثاني: مضمون العقوبات المقررة للشخص المعنوي.

جاء في نص المادة 394 مكرر4 من قانون أنه **"يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمسة (05) مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي"** وقد ذهب الفقه إلى أن الجريمة الالكترونية المرتكبة من طرف الشخص المعنوي تنعقد عند قيامه بأحد الجرائم ذات الصلة بالمجال الالكتروني خاصة وأنه مع تزايد قيام الاقتصاد اليوم على المجال الالكتروني فإن العديد من الشركات والمؤسسات أصبحت تسعى إلى البحث عن المعلومات والتكنولوجيا المتصلة بها بأي وسيلة وهو الأمر الذي يترتب عنه اللجوء إلى الدخول والبقاء غير المشروع في النظام المعلوماتي لشركة أو مؤسسة أخرى منافسة، ومن الإشكالات المطروحة في هذا الإطار تلك المتعلقة بحالة قيام جنحة الدخول غير المشروع في حال ما قام بها شخص طبيعي وفي هذا الإطار ذهب البعض إلى الأخذ بمبدأ أن المسؤولية الجنائية للأشخاص المعنوية لا تستبعد الأشخاص الطبيعيين الفاعلين أو المساهمين في نفس الوقائع مع ضرورة تطبيق نظام مستقل للمسؤولية الجنائية للأشخاص المعنوية.

وبالعودة إلى أحكام قانون العقوبات نجد بأن المشرع عمل على تشديد العقوبات المطبقة على الشخص المعنوي لكون الكثير من الأشخاص المعنوية وعلى اعتبار أنها تنشأ بغرض الربح فإن هذا يدفعها إلى اللجوء إلى المنافسة غير المشروعة عن طريق ارتكاب هذا النوع من الجرائم [1] وتخضع العقوبات المقررة للشخص المعنوي في

[1]- غنية باطلي، مرجع سابق، ص220.

حال ارتكاب الجرائم الالكترونية للأحكام العامة المحددة بموجب قانون العقوبات والتي من بينها أحكام المادة 18 مكرر المستحدثة بموجب تعديل قانون العقوبات 04-15 وتتمثل في:

1-الغرامة والتي تساوي من مرة إلى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي والمنصوص عليها في هذا النوع من الجرائم بموجب المادة 394 مكرر4، مع الأخذ بالحد الأقصى لهذه العقوبة فيما يتعلق بجرائم المساس بأنظمة المعالجة الآلية للمعطيات.

2-المنع من ممارسة النشاط المهني الذي وقعت بمناسبته الجريمة مؤبدا أو لمدة لا تتجاوز خمس (5) سنوات.

3-العقوبات المقررة قانونا والمتمثلة في الحل، الحرمان من النشاط، الرقابة القضائية، غلق المنشأة، الاستبعاد من التعامل في الأسواق العامة والحرمان من الاكتتاب العام في الادخار. [1]

وما يجب الإشارة إليه أنه إلى جانب الآليات الرقابية والعقابية المسطرة لمكافحة الجرائم الالكترونية هناك العديد من الوسائل الإدارية الفنية والتقنية التي تبذلها الحكومات في سبيل الوقاية من وقوع الجرائم الالكترونية والتقليل منها وتقوم هذه الوسائل على وضع أسس فنية وتقنية لحماية المعلومات الإدارية الالكترونية ونظم المعلومات الآلية من التجاوزات والانتهاكات المحتمل التعرض لها من طرف المجرمين الالكترونيين، والسعي من خلالها للحفاظ على أنظمة أمن معلومات الإدارة الالكترونية من أي انتهاك واختراق والعمل على التقليل من الاعتداءات التي تهددها.

إن وسائل الوقاية الإدارية الالكترونية تعتبر من أهم صور الحماية الفنية التي تقوم على إيجاد أنظمة أمان لحماية النظم المعلوماتية وتقنية المعلومات المتداولة عن طريق الشركات المنتجة للبرامج الالكترونية، أو تشفير البيانات الإدارية بمعرفة أصحاب الشأن، وتعتبر من أقدم الآليات المبذولة في هذا المجال والتي ظهرت حتى قبل ظهور نظام الإدارة الالكترونية، وتزامن ظهورها مع شبكة الانترنت بحيث كانت في البداية تستخدم على مستوى شخصي من طرف الأفراد في مجال تعاملاتهم الالكترونية الشخصية اليومية، وما زالت اليوم متبعة حيث قامت العديد من الجهات الحكومية بتطويرها وإدخال استعمالها على مستوى الإدارات والحكومات الالكترونية بهدف الوقاية والعمل على حماية الإدارة الالكترونية من مختلف انتهاكات الجرائم الالكترونية قبل وقوعها، وهي عديدة ومتنوعة ومن أهم صورها المستعملة على مستوى الإدارة الالكترونية لحماية المعلومات والأنظمة المعلوماتية نذكر:

1-كلمة السر: تعتبر كلمة السر أقدم وسيلة تامين لأنظمة الحاسوب الآلية، وقد تزامن ظهورها مع بداية ظهور استخدامات الأجهزة الالكترونية وشبكة الانترنت العالمية، وتهدف إلى منع أي شخص غير مصرح له باستخدام الأجهزة الالكترونية للإدارات العمومية من الدخول إلى الجهاز والتعامل مع المعلومات والأنظمة الآلية،

[1]- راجع في هذا الإطار المادة 131 الفقرة 39 من قانون العقوبات.

ويتم استخدام كلمة السر بعدة أساليب ويكون متاحا للمستخدم إمكانية تغييرها في أي وقت يشاء، وتكون خاصة بالجهاز الالكتروني كما تكون خاصة ببرامج أو ملفات معينة. [1]

2-التوقيع الالكتروني: سبق وأشرنا إلى أن الإدارة الالكترونية تقوم على تقديم خدمات والقيام بمعاملات إدارية حكومية للمواطنين عن طريق وثائق ومحررات الكترونية تصدرها الإدارة العمومية الالكترونية ويتم توقيعها من قبل الموظفين العموميين لإضفاء الصفة الرسمية عليها [2] عن طريق توقيع الكتروني له مميزاته وخصوصياته المختلفة عن التوقيع التقليدي.

وقد بذل المشرع الجزائري في سبيل الكشف عن الجرائم الالكترونية ومحاربتها جملة من القواعد الإجرائية التي تم رصدها لمجابهة الجريمة الالكترونية وحدد بناءا عليها جميع المراحل المتعلقة بعملية التحري والتحقيق عن الجرائم الالكترونية إلى جانب بيان وسائل الإثبات المعتد بها في هذا النوع من الجرائم، وتنقسم هذه القواعد الإجرائية على صورتين تقليدية ومستحدثة [3] وهي عديدة ومتنوعة أهمها تلك المحددة بموجب القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها والمتمثلة في:

1-مراقبة الاتصالات الالكترونية: تقوم القاعدة على أن المشرع يعمل وفق مبدأ الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في القانون ألا وهو الدستور وهذا في إطار القواعد العامة التي تعنى بالحماية القانونية للحياة الخاصة للأفراد، وهو ما يفرض ضرورة حماية بياناتهم الشخصية من انتهاكات المعالجة الآلية [4] وهو ما اعترف به المشرع الدستوري في المادة 77 من الدستور التي تنص بأنه **"يمارس كل واحد جميع حرياته في إطار احترام الحقوق المعترف بها للغير في الدستور، لا سيما احترام الحق في الشرف وستر الحياة الخاصة"** وهو الأمر الذي أيدته المادة 46 من دستور سنة 1996 (المعدل والمتمم) [5] التي نصت أنه **"لا يجوز**

---

[1]- أيمن عبد الحفيظ عبد الحميد، **الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية**، دون مكان نشر، 2005، ص144. نقلا عن: أشرف جمال محمود عبد العاطي، **مرجع سابق**، ص441.

[2]- عبد الله أحمد الخضر، منذر عبد العزيز الشمالي، **النظام القانوني للحكومة الالكترونية**، منشأة المعارف، الإسكندرية، 2006، ص27. ولمزيد من التفاصيل حول التوقيع الالكتروني راجع: بهلول سمية، **مرجع سابق**، ص ص180-181.

[3]- لتفاصيل حول مختلف هذه القواعد الإجرائية راجع:

* شيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن**، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2012.

*حاحة عبد العالي، قلات سمية، "**المكافحة الإجرائية للجرائم الالكترونية (دراسة حالة الجزائر)**"، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 16، ديسمبر 2017، ص ص227-243.

[4]- امحمدي بوزينة آمنة، **"إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، مركز جيل البحث العلمي، يوم 29 مارس 2017 بالجزائر العاصمة، ص73

[5]- دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 الموافق عليه من طرف الشعب بموجب استفتاء 28 نوفمبر 1996 والمنشور بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 07 ديسمبر 1996 الجريدة الرسمية العدد 76 الصادرة في 08 ديسمبر 1996. المعدل بموجب: القانون رقم 02-03 المؤرخ في 10 أفريل 2002 الجريدة الرسمية العدد 25 الصادرة في 14 أفريل 2002 / القانون رقم 08-19 المؤرخ في 15 نوفمبر 2008 الجريدة الرسمية العدد 63 الصادرة في 16 نوفمبر 2008.

انتهاك حرمة حياة المواطن الخاصة وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة".

إلا أنه ومع التعديل الدستوري لسنة 2016 [1] حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية من خلال إضافة فقرتين للمادة السابقة تنص بأنه **"لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية. ويعاقب القانون أي انتهاك لهذا الحكم"** وعرف المشرع الجزائري الاتصالات الالكترونية بأنها **"أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة الكترونية"** [2] وحدد على سبيل الحصر الحالات التي تسمح باللجوء إلى المراقبة الالكترونية والمتمثلة في أربع حالات هي: [3]

- **للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.**
- **في حالة توافر معلومات عن احتمال اعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.**
- **لمقتضيات التحريات والتحقيقات القضائية عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء إلى المراقبة الالكترونية.**
- **في إطار تنفيذ طلبات المساعدة القضائية الدولية المتبادلة.**

ونظرا لخطورة هذا الإجراء لما له من انتهاك للحياة الخاصة للأفراد فقد نص المشرع على عدم جواز إجراء عمليات المراقبة الالكترونية إلا بإذن مكتوب من السلطة القضائية المختصة، كما خص الحالة الأولى المتعلقة بالأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة بإجراءات خاصة تدخل ضمن اختصاص النائب العام لدى مجلس قضاء الجزائر وضباط الشرطة القضائية المنتمين للهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال.

2-تفتيش المنظومة المعلوماتية: أجاز المشرع للسلطات القضائية وضباط الشرطة القضائية في سبيل مكافحة الجرائم الالكترونية وفي إطار نصوص قانون الإجراءات الجزائية الدخول بغرض التفتيش ولو عن بعد إلى:[4]

- **منظومة معلوماتية أو جزء منها وكذا المعطيات المعلوماتية المخزنة فيها.**
- **منظومة تخزين معلوماتية.**

---

[1]- القانون 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية العدد 14 الصادرة في 07 مارس 2016.

[2]- المادة الثانية الفقرة "و" من القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، **مرجع سابق.**

[3]- المادة الرابعة (04)، **المرجع نفسه.**

[4]- المادة الخامسة (05) من القانون 09-04، **مرجع سابق.**

وحرص في هذا المجال على فتح باب التعاون الدولي وأشار إلى أهمية فتح مجال المساعدة الدولية في مجال مكافحة الجرائم الالكترونية وفق ما تقتضيه الاتفاقيات الدولية ومبادئ المعاملة بالمثل.

كما نص المشرع بموجب القانون 09-04 على إجراء هام في هذا المجال وهو إجراء **"التسخير"** والذي فتح بموجبه للسلطات المختصة المكلفة بالتفتيش المجال لتسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدة هذه السلطات وتزويدها بكل المعلومات الضرورية لإنجاز مهمتها. [1]

3-حجز المعطيات المعلوماتية: فتح المشرع الجزائري للسلطة التي تباشر التفتيش عندما تكتشف في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم الالكترونية أو مرتكبيها المجال لنسخ المعطيات محل البحث والمعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة قانونا في حال ما لم يكن من الضروري حجز كامل المنظومة. [2]

وأوجب على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية، إلا أنه من جهة أخرى أجاز استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط ألا يؤدي هذا الإجراء إلى المساس بمحتوى المعطيات.

ونص من خلال نصوص القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها أنه: [3]

- **في حالة استحالة إجراء الحجز وفقا لما هو منصوص عليه قانونا لأسباب تقنية يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية أو إلى نسخها والموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.**
- **إمكانية أن تأمر السلطة التي تباشر التفتيش باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة لا سيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.**

---

[1]- المادة الخامسة (05) الفقرة الأخيرة من القانون 09-04، **المرجع نفسه.**

[2]- المادة السادسة (06) من القانون 09-04، **المرجع نفسه.**

[3]- المادتين السابعة (07) والثامنة (08)، **مرجع سابق.** ولمزيد من التفاصيل راجع: * مزيود سليم، **"الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"**، المجلة الجزائرية للاقتصاد والمالية، العدد الأول، أفريل 2014، ص ص94-107.

* امحمدي بوزينة آمنة، **"إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)**، ورقة بحث مقدمة ضمن فعاليات الملتقى الوطني حول "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، المنظم من طرف مركز جيل البحث العلمي، الجزائر العاصمة، 29 مارس 2017، ص ص57-82.

ونظرا لخصوصية الجريمة الالكترونية التي تنطلق من طبيعتها ومن مختلف الوسائل القانونية المبذولة في سبيل محاربتها والوقاية منها والحد من انتشارها علاوة على جملة القواعد الإجرائية المبذولة في سبيل الكشف عنها فقد نص المشرع الجزائري حاله حال أغلب التشريعات الوطنية والدولية على جملة من الآليات القانونية في سبيل البحث والتحقيق في الجرائم الالكترونية وعمل على جعلها تتوافق والطبيعة الخاصة لهذا النوع من الجرائم لتسهيل إثبات وقوعها والعمل على معاقبة مرتكبيها وفق ما ينص عليه القانون، وذلك إلى جانب الوسائل التقليدية للتحقيق والإثبات المتعارف عليها في إطار القانون الجنائي والتي يتم استغلالها بما يخدم الطبيعة الخاصة للجريمة الالكترونية ويساعد على الكشف عنها ومتابعة مرتكبيها وفق ما يقتضيه القانون. [1]

وما يجب التنبيه إليه في هذا الإطار أنه وتحت طائلة التعرض للعقوبات المنصوص عليها في إطار القوانين والتشريعات المعمول بها لا يجوز استعمال أي من المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون إلا في الحدود المسموح بها قانونا والضرورية للتحديات أو التحقيقات القضائية.

IV الخاتمة

مما سبق نخلص إلى أن المشرع الجزائري خطى خطوة هامة في مجال مكافحة الجريمة الالكترونية والحد من انتشارها، وذلك من خلال استحداث العديد من الآليات العقابية بداية بتعديل قانون العقوبات سنة 2004 ومن ثم استحداث القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي وضع من خلاله المشرع آليات عقابية تخص كلا من الأشخاص الطبيعية والأشخاص المعنوية، إلا أن ما يسجل في المقابل أن هذه النصوص القانونية مازالت تعاني العديد من مواضع النقص والقصور التي فرضتها الجريمة الالكترونية في حد ذاتها والتي تتميز بالتطور الدائم والمستمر الأمر الذي يفرض صعوبة القدرة على تغطية كافة جوانبها بنصوص وإجراءات قانونية ردعية دون الحرص على تزويدها بأرضية وقاية مسبقة، من هذا المنطلق حاولنا وضع جملة من الاقتراحات التي من شأنها المساهمة في تدعيم الآليات القانونية عامة والعقابية خاصة لمكافحة الجريمة الالكترونية في الجزائر والتي يمكن حصرها في:

1-فتح مجال التعاون الدولي والحرص على الاستفادة من خبرات الدول الرائدة والسباقة في مجال مكافحة الجريمة الالكترونية والوقاية منها.

2-العمل في مقابل وضع الآليات العقابية على تدعيم برامج مكافحة الجريمة الالكترونية ببرامج تثقيفية يكون الهدف الرئيسي منها نشر ثقافة التعامل الالكتروني ورفع مستوى وعي الأفراد بمخاطر الانترنت للحد من التجاوزات والجرائم التي ترتكب بسبب الجهل في استخدام تكنولوجيات الاعلام والاتصال.

---

[1]- لتفاصيل راجع: * حجازي عبد الفتاح، **الإثبات الجنائي في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، مصر، 2007.

* ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، رسالة مقدمة لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2016.

* محمد علي قطب، **الجرائم المعلوماتية وطرق مواجهتها (الجزء الرابع)**، الأكاديمية الملكية للشرطة، مملكة البحرين، جويلية 2010.

* عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، **"الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية – دراسة تطبيقية مقارنة"**، ورقة بحث مقدمة ضمن فعاليات المؤتمر العربي الأول حول "علوم الأدلة الجنائية والطب الشرعي"، جامعة نايف العربية للعلوم الأمنية، الرياض، من 12 إلى 14 نوفمبر 2007.

3-الحرص على تكوين كفاءات من القطاع الأمني متخصصة في مراقبة التجاوزات والكشف المبكر عن الجرائم الالكترونية خاصة وأنها جرائم غير مادية ولا ملموسة كما سبق ووضحنا، ونادرا ما يتم الكشف عنها في مراحل متقدمة من ارتكابها.

4-التركيز إلى جانب الآليات العقابية على وضع آليات ردعية والحرص من خلالها على فتح المجال لأصحاب الخبرات من خارج القطاع الأمني للمشاركة في هذه البرامج والسياسات والعمل في نفس الوقت على تطوير المؤسسات العمومية والخاصة الناشطة في مجال تكنولوجيات الإعلام والاتصال بصورة تساهم في خلق قاعدة أمنية الكترونية صعبة الاختراق.

5-وفي الأخير ضرورة التفكير جديا في إعادة النظر في أحكام القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها الذي أصبح يثبت قصوره في تغطية الكثير من الجزئيات المتعلقة بالجريمة الالكترونية والتي وضحنا سابقا بأنها جريمة متجددة ودائمة التطور لارتباطها المباشر بتكنولوجيات الاعلام والاتصال التي تعتبر من المجالات سريعة التطور والتقدم وهو الأمر الذي يفرض تطور القانون الناظم للجرائم الالكترونية بنفس الوتيرة لتجنب وقوع أي ثغرات قانونية من شأنها أن تفتح المجال للمجرمين للإفلات من العقاب، هذا فضلا عن ضرورة تفعيل دور الهيئات المستحدثة في مجال مكافحة الجريمة الالكترونية بصورة من شأنها توسيع مساهمتها في مجال مكافحة الجريمة الالكترونية إلى جانب الهيئات الأمنية والقضائية بنجاعة وفعالية عوض أن تكون مجرد هيئات مفرغة من أي محتوى وليس لها أي صلاحية الأمر الذي يجعلها عبء لا فائدة منه.

V قائمة المصادر والمراجع

أولا / قائمة المصادر:

أ-الدساتير:

1-دستور الجمهورية الجزائرية الديمقراطية الشعبية لسنة 1996 الموافق عليه من طرف الشعب بموجب استفتاء 28 نوفمبر 1996 والمنشور بموجب المرسوم الرئاسي رقم 96-438 المؤرخ في 07 ديسمبر 1996 الجريدة الرسمية العدد 76 الصادرة في 08 ديسمبر 1996. المعدل بموجب:

- القانون رقم 02-03 المؤرخ في 10 أفريل 2002 الجريدة الرسمية العدد 25 الصادرة في 14 أفريل 2002
- القانون رقم 08-19 المؤرخ في 15 نوفمبر 2008 الجريدة الرسمية العدد 63 الصادرة في 16 نوفمبر 2008.
- القانون 16-01 المؤرخ في 06 مارس 2016 الجريدة الرسمية العدد 14 الصادرة في 07 مارس 2016.

ب -القوانين:

1-القانون 04-15 المؤرخ في 10 نوفمبر 2004 المعدل والمتمم للأمر 66-156 المؤرخ في 08 جوان 1966 المتضمن قانون العقوبات، ج.ر العدد 71 الصادرة في الصادرة في 10 نوفمبر 2004.

2-القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج.ر العدد 47 الصادرة في 16 أوت 2009.

ثانيا / قائمة المراجع:

أ-الكتب:

1-أمال قارة، **الحماية الجزائية للمعلومات في التشريع الجزائري**، دار هومة للنشر والتوزيع، الجزائر، الطبعة الأولى، 2006.

2-أشرف جمال محمود عبد العاطي، **الإدارة الالكترونية للمرافق العامة**، دار النهضة العربية، القاهرة، 2016.

3-أيمن عبد الحفيظ عبد الحميد، **الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية**، دون مكان نشر، 2005.

4-حجازي عبد الفتاح، **الإثبات الجنائي في جرائم الكمبيوتر والانترنت**، دار الكتب القانونية، مصر، 2007.

5-عبد الله أحمد الخضر، منذر عبد العزيز الشمالي، **النظام القانوني للحكومة الالكترونية**، منشأة المعارف، الإسكندرية، 2006.

6-شيدة بوكر، **جرائم الاعتداء على نظم المعالجة الآلية للمعطيات في التشريع الجزائري والمقارن**، منشورات الحلبي الحقوقية، بيروت، الطبعة الأولى، 2012.

7-غنية باطلي، **الجريمة الالكترونية (دراسة مقارنة)**، منشورات الدار الجزائرية، الجزائر، 2015.

8-محمد أمين الرومي، جرائم الكمبيوتر والانترنت، دار المطبوعات الجامعية، مصر، 2004.

9-محمد علي قطب، **الجرائم المعلوماتية وطرق مواجهتها (الجزء الرابع)**، الأكاديمية الملكية للشرطة، مملكة البحرين، جويلية 2010.

10-مصطفى محمد موسى، **التحقيق الجنائي في الجرائم الالكترونية**، مطابع الشرطة، القاهرة، الطبعة الأولى، 2009.

11-نايل نبيل عمر، **الحماية الجنائية للعمل الالكتروني في جرائم المعلوماتية**، دار الجامعة الجديدة، القاهرة، 2012.

12-نهلا عبد القادر المومني، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، الطبعة الأولى، 2008.

13-هلالي عبد الله أحمد، **تفتيش نظم الحاسب الآلي وضمانات المتهم في جرائم المعلومات (دراسة مقارنة)**، دار النهضة العربية، القاهرة، 2000.

ب-الرسائل الجامعية:

1-أسماء حسين رويعي، **الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية**، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2013.

2-بهلول سمية، **دور الإدارة الالكترونية في تفعيل أداء الجماعات الإقليمية في الجزائر**، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، تخصص إدارة محلية، كلية الحقوق والعلوم السياسية، جامعة باتنة 1 الحاج لخضر، 2017-2018.

3-عمر بن محمد العتيبي، **الأمن المعلوماتي في المواقع الالكترونية ومدى توافقه مع المعايير الدولية والمحلية**، أطروحة مقدمة استكمالا لمتطلبات الحصول على درجة دكتوراه الفلسفة في العلوم الأمنية، كلية الدراسات العليا، جامعة نايف العربية للعلوم الأمنية، الرياض، 2010.

4-نائلة عادل محمد فريد، **جرائم الحاسب الاقتصادية**، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق، كلية الحقوق، جامعة القاهرة، 2003.

5-هروال هبة نبيلة، **جرائم الانترنت (دراسة مقارنة)**، أطروحة مقدمة لنيل شهادة الدكتوراه في العلوم القانونية، جامعة أبي بكر بلقايد تلمسان، 2013-2014.

6-ربيعي حسين، **آليات البحث والتحقيق في الجرائم المعلوماتية**، رسالة مقدمة لنيل شهادة الدكتوراه في القانون، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر باتنة، 2016.

ج-المقالات في المجلات:

1-أحسن رابحي، **"الجريمة الالكترونية: النقطة المظلمة بالنسبة للتكنولوجية المعلوماتية"**، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009.

2-بلبالي إبراهيم، **"الجريمة الالكترونية بين وضوح معالم وأهداف التجريم وصعوبة التصنيف والتطبيق"**، مجلة دراسات وأبحاث، جامعة زيان عاشور، الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009.

3-براهمي جمال، **"مكافحة الجرائم الالكترونية في التشريع الجزائري**، المجلة النقدية للقانون والعلوم السياسية، جامعة مولود معمري تيزي وزو، المجلد الثاني (02)، العدد الثاني (02).

4-حسينة شرون، **"فعالية التشريعات العقابية في مكافحة الجرائم الالكترونية"**، مجلة دراسات وأبحاث، جامعة زيان عاشور_الجلفة، المجلد الأول، العدد الأول، سبتمبر 2009.

5-كحلوش علي، "**جرائم الحاسوب الآلي وأساليب مواجهتها"**، مجلة الشرطة، العدد 84، جويلية 2007، المديرية العامة للأمن الوطني، الجزائر.

6-مزيود سليم، **"الجرائم المعلوماتية واقعها في الجزائر وآليات مكافحتها"**، المجلة الجزائرية للاقتصاد والمالية، العدد الأول، أفريل 2014.

د-المقالات في الملتقيات والندوات:

1-امحمدي بوزينة آمنة، **"إجراءات التحري الخاصة في مجال مكافحة الجرائم المعلوماتية (دراسة تحليلية لأحكام قانون الإجراءات الجزائية وقانون الوقاية من جرائم الإعلام)**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول "آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، مركز جيل البحث العلمي، يوم 29 مارس 2017 بالجزائر العاصمة.

2-حاحة عبد العالي، قلات سمية، **"المكافحة الإجرائية للجرائم الالكترونية (دراسة حالة الجزائر)"**، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، العدد 16، ديسمبر 2017.

3-عبد الناصر محمد محمود فرغلي، محمد عبيد سيف سعيد المسماري، **"الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية –دراسة تطبيقية مقارنة"**، ورقة بحث مقدمة ضمن فعاليات المؤتمر العربي الأول حول "علوم الأدلة الجنائية والطب الشرعي"، جامعة نايف العربية للعلوم الأمنية، الرياض، من 12 إلى 14 نوفمبر 2007.

4-مختارية بوزيدي، **"ماهية الجريمة الالكترونية"**، مداخلة مقدمة ضمن فعاليات الملتقى الوطني حول آليات مكافحة الجرائم الالكترونية في التشريع الجزائري"، مركز جيل حقوق الإنسان، الجزائر العاصمة يوم 29 مارس.

5-هشام محمد فريد رستم، **"الجرائم المعلوماتية_ أصول التحقيق الجنائي الفني واقتراح إنشاء آلية عربية للتدريب التخصصي"**، ورقة بحث مقدمة ضمن فعاليات مؤتمر القانون والكمبيوتر والانترنت، كلية الشريعة والقانون، جامعة الإمارات العربية المتحدة، من 01 إلى 03 ماي 2000، منشور ضمن مجلة "الشريعة والقانون"، المجلد الثاني، الطبعة الثالثة، 2004.

هـ-مواقع الانترنت:

1- Site officiel de L'OCDE www.oecd.org consulté le 22 Mars 2019.