الحماية الدولية من جرائم التقليد والقرصنة الإلكترونية وموقف المشرع الجزائري منها

International protection from counterfeiting and electronic piracy crimes and the position of the Algerian legislator towards it

* د.كريمة خنوسي

[1]جامعة الجيلالي بونعامة خميس مليانة (الجزائر

ملخص:

مع النمو المستمر للثورة المعلوماتية الذي يعيشه عصرنا، ويشهده حاضرنا، أصبحنا نواجه العديد من الأخطار والمشاكل التي تنشأ بشكل تلقائي مع أي تطور حضاري وتقني، فدخول الأنترنت في عالمنا وتمكن الصغير والكبير من استخدامه دون أي قيود أو رقابة أدى إلى زيادة الأخطار وتفشي السرقات الالكترونية عبر جرائم التقليد والقرصنة، ومن شأن ذلك أين يخلق تابعات كبيرة جدا على اقتصاديات الدول وعلى سلامة وصحة المستهلكين، بالإضافة إلى أن هناك بعدا جوهريا مهما وهو أن الغش والتقليد من شأنهما أن يعوقا نمو الابداع والابتكار عن طريق استغلال حقوق الآخرين؛ مما يدفعنا إلى طرح اشكالية ما موقف كل من المجتمع الدولي والمشرع الجزائري من جرائم التقليد والقرصنة الالكترونية؟ وتوصلنا إلى ضرورة بلورة شراكة عالمية لمواجهة خطر هذه الظاهرة، وأهمية وضع تشريعات دولية وقوانين ملزمة لمكافحة هذا الخطر.

الكلمات المفتاحية:

حماية؛ دولية؛ تقليد؛ قرصنة؛ الكترونية.

Abstract :

With the continuous growth of the information revolution that our time is experiencing, and our present is witnessing it, we are facing many dangers and problems that arise automatically with any civilizational and technical development. Counterfeiting and piracy crimes, and this would create very significant dependencies on the economies of countries and on the safety and health of consumers, in addition to that there is an important fundamental dimension, which is that fraud and counterfeiting hinder the growth of creativity and innovation by exploiting the rights of others; Which leads us to raise a problem: What is the position of the international community and the Algerian legislator on these crimes? We reached the need to develop a global partnership to confront the threat of this phenomenon, and the importance of developing international legislation and binding laws to combat this danger.

Keywords :

protection; International; Counterfeiting; piracy ; Electronic.

.

*د. كريمة خنوسي.

تمهيد :

إن حقوق الملكية الفكرية تؤدي دورا حاسما في تعزيز التطورات الفكرية والتكنولوجيا كما في أنشطة البحث والتنمية، وحماية حقوق الملكية الفكرية أمر محوري أيضا نظرا للانعكاسات السلبية الجمة التي تخلفها تجارة السلع المقلدة والمقرصنة على الاقتصاد وعلى صحة المستهلكين وسلامتهم.

ولايزال التقليد والقرصنة مشكلتين كبيرتين في جميع أنحاء العالم تغذيهما المتغيرات الاجتماعية والاقتصادية، كالفقر وسلوك المستهلكين الملتبس إزاء حقوق الملكية الفكرية، ومشاركة شبكات إجرامية وسهولة الوصول إلى السلع غير الشرعية، لاسيما بواسطة الوسائط الرقمية؛ ورغم توفر أطر قانونية ومؤسستيه متينة ينبغي بذل المزيد من الجهود لتحقيق الامتثال لنظم الملكية الفكرية القائمة وضمان أداء هذه النظم لدورها كمحرك للابتكار والابداع.

وعلى ذلك فهناك أبعاد خطيرة لانتشار عمليات التزييف والقرصنة، حيث يمتد تأثيرها ليشمل الفرد والمجتمع ويؤثر على الاقتصاديات الوطنية خاصة في الدول الناشئة ويعرقل مسيرة نمو وازدهار الاقتصاد بها، لافتين النظر إلى أن للظاهرة بعد آخر يرتبط بسلامة وصحة المستهلكين بحيث امتدت لمجالات في غاية الخطورة مثل تزييف الدم البشري في الصين وتقليد الادوية.

وبما أن الجزائر عنصر فاعل في المجتمع الدولي باعتبارها من أعضائه، فأنها تناولت موضوع جريمة التقليد والقرصنة في القوانين ذات الصلة كقانون العقوبات، وذلك حماية للملكية الفكرية ولضحايا مثل تلك الجرائم، وتجسيدا للاتفاقيات الدولية التي صدقت عليها وتفعيلا الالتزامات الناتجة عنها.

وهذا ما دفعنا إلى طرح الإشكالية المتمثلة في: ما موقف كل من المجتمع الدولي والمشرع الجزائري من جرائم التقليد والقرصنة الالكترونية؟

وتوصلنا إلى فكرة ضرورة بلورة شراكة عالمية لمواجهة خطر هذه الظاهرة، وأهمية وضع تشريعات دولية وقوانين ملزمة لمكافحة هذا الخطر.

I. مفهوم الجريمة الإلكترونية :

يعود تاريخ الانترنت لعام 1960 عندما بدأت أبحاث علمية في هذا المجال بتكليف من حكومة الولايات المتحدة الأمريكية بالتعاون مع شركات تجارية من القطاع الخاص، وهكذا بدأ تسويق الانترنت لتصبح شبكة عالمية تطال تقريبا كل جانب من جوانب الحياة البشرية المعاصرة؛ ومنه عام 2000 أضحى أكثر من ربع سكان العالم موصولا على الشبكة العنكبوتية، والارقام في ارتفاع مستمر (جورج لبكي، 2013).

وتعرف الجريمة الإلكترونية بأنها "الارتكاب المتعمد لفعل ضار من الناحية الاجتماعية أو فعل خطير محظور يعاقب عليه القانون"، وتمثل الجرائم الالكترونية مجموعة الأفعال والأعمال غير القانونية التي تتم عبر معدات أو أجهزة الكترونية أو شبكة الانترنت،

أو تبث عبرها محتوياتها، وهي ذلك النوع من الجرائم التي تتطلب الإلمام الخاص بتقنيات الحاسب الآلي ونظم المعلومات لارتكابها أو التحقيق فيها ومقاضاة فاعليها(ذياب موسى البداينة، 2014).

ويعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الحاسوبية، والبرامج المعلوماتية دورا رئيسيا" (محمد عبيد الكعبي، 2009).

وقد اتجه جانب كبير من الفقهاء إلى اعتماد التعريف الذي تبنته منظمة التعاون الاقتصادي والتنمية للجريمة المعلوماتية في اجتماع باريس عام 1983 من أنها "كل سلوك غير مشروع، أو غير أخلاقي، أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو نقلها" (يونس عرب، 2002).

وتبنى المشرع الجزائري للدلالة على الجريمة مصطلح المساس بأنظمة المعالجة الآلية للمعطيات، معتبرا أن النظام المعلوماتي في حد ذاته وما يحتويه من مكونات غير مادية محلا للجريمة، حيث أنه عرفها من خلال المادة 02 من القانون رقم 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها مسميا إياه "المنظومة المعلوماتية"؛ وهي "أي نظام منفصل أو مجموعة من الأنظمة المتصلة مع بعضها البعض أو مترابطة، يقوم واحد منها أو أكثر المعالجة الآلية للمعطيات تنفيذا لبرنامج معين" (يعرة سعيدة، 2016).

وتعد جرائم المعلوماتية إفرازا ونتاجا لتقنية المعلومات، فهي ترتبط بها وتقوم عليها، وهذا ما أكسبها لونا وطابعا قانونيا خاصا يميزها عن الجرائم التقليدية أو المستحدثة بمجموعة من السمات؛ قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى فإن اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الاجرامية أكسبها خصوصية غير عادية.

وأن متابعة جرائم الحاسب الآلي والانترنت والكشف عنها من الصعوبة بما كان، حيث أن هذه الجرائم لا تترك أثرا، فهي أرقام تتغير في السجلات ومعظمها تم اكتشافها بالصدفة وبعد وقت طويل من ارتكابها (رصاع فتيحة، 2012)؛ ومن خصائص الجريمة الالكترونية أنها:

1-من الجرائم العابرة للحدود؛ فمسرح الجريمة لم يعد محليا بل أصبح عالميا.

2-صعوبة اكتشاف واثبات الجرائم الالكترونية، فهي لا تترك آثار ملموسة وبذلك لا تترك شهودا يمكن الاستدلال بأقوالهم، ولا أدلة مادية يمكن فحصها لأنها تقع في بيئة افتراضية.

3-تحتاج إلى وسائل خاصة؛ اذ تستلزم لقيامها توفر الحاسب الآلي، ومعرفة تقنية.

4-تتطلب خبرة وتحكما في تكنولوجيا المعلومات؛ لذلك لابد أن يكون المحقق متخصص في الجريمة الالكترونية حتى لا يتسبب في إتلاف الدليل الالكتروني (جميل عبد الباقي الصغير، 1992).

إن الانترنت اختراع بشري يحمل في طياته بذور الخير والشر معا، ولم يكن منذ الوهلة الأولى موضوع الحماية المعلوماتية مطروحا، حيث كان استعماله محتكرا من طرف فئة معينة، إلا أن انتشار استعمال الانترنت أظهر عيوبا، فسجل أول اختراق للشبكة سنة 1988، حيث توقف عملها لمدة ثلاث أيام ولذلك كان لابد من إيجاد برامج أمنية وقواعد قانونية للحماية من الجرائم الإلكترونية.

والحماية تعني إبعاد الخطر عن الوجود الانساني أو عن أي شيء موضوع الحماية (باسكال ودا، 2014)؛ وحتى وقت قريب كان للحكومات مقاربات مختلفة بشأن التشريعات الخاصة بالأنترنت، فمعظم الدول تنظم الأنترنت ضمن حدود قيمتها السياسية، والقانونية، والثقافية، لكن بما أن تطور تكنولوجيا الاتصالات والمعلومات يجري على مستوى دولي خارجا على نطاق سيطرة تلك الدول، فإن اعتماد تشريعات فعالة وتنفيذها لمكافحة جرائم الانترنت يشكل تحديا كبيرا للحكومات والأجهزة القانونية في كل البلدان المتقدمة منها أو النامية، بالإضافة إلى ذلك أن عملية التشريع تستغرق وقتا طويلا يمنع مكافحة الجرائم الالكترونية بسرعة.

ومن ناحية أخرى، أن الانتشار خارج حدود الدولة يطرح تحديات قانونية تتعلق بسيادة الدول وصلاحية محاكمتها التي تمتد فقط على مساحتها الجغرافية (الاختصاص الاقليمي)، ولكن بما أن جرائم الانترنت ظاهرة عالمية تمتد خارج نطاق الحدود الوطنية، فإن ذلك يستلزم لنجاح مكافحة تلك الجرائم تنسيقا كبيرا بين القوانين الداخلية والمعاهدات الدولية، والتعاون بين مختلف البلدان.

II. مكافحة الجرائم الالكترونية في القانون الدولي :

وأبرز المجموعات والمنظمات الدولية التي عملت في موضوع جرائم شبكة الانترنت نذكر:

أ.الآليات المقررة في مجموعة الدول الثمانيG8

اعتمد وزراء العدل والداخلية التابعين لبلدان الـ G8 في اجتماعاتهم المختلفة سياسات لمكافحة العديد من جرائم الإنترنت تستند إلى المبادئ التالية: عدم السماح بفرار المعتدين على تكنولوجيا المعلومات؛ التنسيق بين جميع الدول المعنية في ملاحقة مرتكبي جرائم الإنترنت ومحاكمتهم بغض النظر عن مكان حدوث الضرر؛ تدريب الموظّفين المكلفين بتنفيذ القوانين، وتجهيزهم بالمعدات الضرورية للتعامل مع الجرائم ذات التقنية العالية.

بالإضافة إلى ذلك، دعت دول الـ G8 إلى مواصلة العمل حتى التوصّل إلى حلول دولية ناجحة، من خلال عقد اتفاقات دولية، لمعالجة الجريمة ذات التقنية العالية والاستفادة من عمل المنظمات الدولية المختلفة ومن تثمير الدراسات العديدة التي وضعتها دول ومن بينها: وضع خطة عمل بشأن الجريمة ذات التكنولوجيا العالية وجرائم الكمبيوتر سنة 1997، ومبادئ بشأن الحصول على المعلومات المخزّنة على الكمبيوتر خارج حدود الدول لسنة 1999، وتوصيات لتعقّب الاتصالات على الشبكة خارج الحدود الوطنية في التحقيقات الإرهابية والإجرامية ومبادئ توافر البيانات الأساسية لحماية السلامة العامة لعام 2002، وإعلان بيان دول G8 على نظم حماية المعلومات الذي اعتمد في نفس السنة.

وترى دول الـ G8 أن الحماية الفعالة ضد الجرائم ذات التقنية العالية تتطلّب الاتصال والتنسيق والتعاون داخليًا ودوليًا بين جميع أصحاب المصلحة في القطاع الخاص والأوساط الأكاديمية، والمؤسسات الحكومية. وبناءً على ذلك، فإن دول الـ G8 التزمت بتدريب جميع العاملين في مجال تطبيق القانون وتجهيزهم بالمعدات الضرورية لمكافحة جرائم الإنترنت؛ كما تعهّدت بمساعدة جميع البلدان الأعضاء على إقامة مراكز اتصال تعمل على مدار 24 ساعة سبعة أيام في الأسبوع (جبران خليل ناصر، 2018).

إن وجود جرائم تعتمد التكنولوجيا المتقدّمة تطرح تحديات كبيرة على الأجهزة القضائية، فغالبًا ما يكون من الصعب على المحققين ذوي المهارة العالية العمل بسرعة فائقة لحماية البيانات الالكترونية وتحديد المتهمين بخرق القانون، من هنا تأتي أهمية الشبكة التي طرحت دول الـ G8 إنشاءها لأنها ستمكّن من الاستجابة بسرعة كبيرة لطلبات السلطات الرسمية أو مستخدمي شبكات الانترنت.

إن توصيات الـ G8 بالنسبة لجرائم التكنولوجيا المتقدمة والجرائم ذات الصلة بالكمبيوتر موجودة في إطار الباب D من المعاهدة وتتلخص بما يلي:

– يتعيّن على الدول أن تُجرِّم الانتهاكات على حقوق الغير الموجودة في الشبكة العنكبوتية التي تستوجب العقوبات الجزائية، وأن تعالج المشاكل المتعلقة بالتحقيقات القضائية بالتدريب الفعال لمنع الجريمة، وإقامة تعاون دولي فيما يتعلّق بمكافحة هذه الانتهاكات.

– ينبغي للدول أن تتخذ خطوات رادعة لمنع الجريمة ذات التقنية العالية، ويشمل ذلك:

- التعاون مع القطاع الصناعي لضمان أمن شبكات الكمبيوتر ونظم الاتصالات، وإيجاد الآليات المناسبة عند تعرّض المواقع الالكترونية للهجمات.
- سن قوانين وتدابير أخرى وتنفيذها لضمان حماية ملائمة لحقوق الملكية الفكرية ضد التزوير والقرصنة.
- تحديد المشاكل المحتملة ومعالجتها في المستقبل التي قد تنتج عن التطورات في مجال تكنولوجيا المعلومات.
- نشر الوعي العام فيما يتعلق بموضوع الجريمة ذات التقنية العالية.

– يتوجب على الدول العمل المستمر على اقتناء التكنولوجيات الملائمة والتطوير المستمر للخبرات والقدرات في مجال التحقيق والادعاء العام، من أجل ملاحقة المجرمين الذين يستخدمون تكنولوجيا الكمبيوتر لارتكاب جرائمهم، ويتوجّب على الدول تشجيع قيام المزيد من الأبحاث من أجل زيادة فعالية تقنيات تطبيق القانون.

– ينبغي تحسين التواصل بين الموظفين المكلّفين بتطبيق القوانين في مختلف الدول، بما في ذلك تبادل الخبرات في معالجة هذه المشاكل.

– يتوجب على الدول الحفاظ على التوازن المناسب بين حماية الحق في الخصوصية، ولا سيما بالنظر إلى الخطر الذي تخلقه التكنولوجيات المستجدة، والحفاظ على قدرة تطبيق القانون لحماية السلامة العامة والقيم الاجتماعية الأخرى.

وأخيرًا، على الدول أن تشجّع التعاون في مجال تطوير الاستراتيجيات المناسبة لرفع الوعي العام في هذا الشأن، وكذلك التقييم المستمر لبرامج المكافحة والوسائل القانونية المتبعة.

ب. قرارات الجمعية العامة للأمم المتحدة:

عملت الأمم المتحدة منذ فترة طويلة في مجال تأمين سلامة استخدام التكنولوجيا وشبكات المعلوماتية (الانترنت)، عبر مشاركة وكالاتها المختلفة في مختلف المفاوضات لإيجاد ووضع معايير توفير الحماية لشبكات الانترنت؛ ومن أبرز القرارات تلك التي أصدرتها الجمعية العامة للأمم المتحدة في هذا المجال نذكر منها:

– القرار 121/45 العام 1990، مع نشر دليل منع الجرائم المتصلة بأجهزة الكمبيوتر ومكافحتها لعام 1994.

– القرارات 70/53 في 4 ديسمبر 1998، و49/54 في 1 ديسمبر 1999، 28/55 في 20 نوفمبر 2000 و19/56 في 29 نوفمبر 2001 و53/57 في 22 نوفمبر 2002 و32/58 في 18 ديسمبر 2003 حول موضوع "التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي"

– القرارات 63/55 في 4 ديسمبر 2000، و121/56 في 19 ديسمبر 2001 بشأن "مكافحة استخدام نظم المعلومات الإدارية الجنائية لتقنية المعلومات" أين دعت من خلالهما الدول الأعضاء، عند وضع التشريعات الوطنية لمكافحة إساءة استعمال تكنولوجيا المعلومات الأخذ بعين الاعتبار عمل لجنة منع الجريمة والعدالة الجنائية.

– القرارات رقم: 239/57 الصادر بتاريخ 20 ديسمبر 2002، 57/ 239 في 31 جانفي 2003 و199/58 في 30 جانفي 2004 بشأن "إنشاء ثقافة عالمية للأمن السيبراني".

أما عن القرارات الصادرة عن باقي هيئات الأمم المتحدة فيمكن ذكر:

• قرار المجلس الاقتصادي والاجتماعي رقم E/2007/20 الصادر بتاريخ 26 جويلية 2007 الخاص بـ "التعاون الدولي من أجل منع وتحري ومقاضاة ومعاقبة جرائم الاحتيال الاقتصادي والجرائم المتصلة بالهوية".

• توصيات مؤتمر ورشة العمل على "التدابير الرامية إلى مكافحة الجريمة المتصلة بأجهزة الكمبيوتر"، الذي عقد في بانكوك في 22 أفريل 2005 كجزء من مؤتمر الأمم المتحدة الحادي عشر لمنع الجريمة والعدالة الجنائية. الفقرة 2 من قرار الجمعية العامة 177/60 التي دعت الحكومات لتنفيذ جميع التوصيات التي اعتمدها المؤتمر الحادي عشر.

• قرار لجنة مكافحة المخدرات رقم 5/48 حول "تعزيز التعاون الدولي من أجل منع استخدام شبكة الإنترنت لارتكاب الجرائم المتصلة بالمخدرات".

• قرار لجنة مكافحة المخدرات 8/43 في 15 آذار/مارس 2000 عبر الإنترنت.

• قرار المجلس الاقتصادي والاجتماعي رقم 42/2004 بشأن "بيع المخدرات المشروعة الخاضعة للمراقبة الدولية إلى الأفراد عن طريق الإنترنت".

ج. الاتحاد الدولي للاتصالات:

يوفّر الاتحاد الدولي للاتصالات الذي يضم 192 دولة و700 شركة من القطاع الخاص والمؤسسات الأكاديمية منبرًا «استراتيجيا» للتعاون بين أعضائه، باعتباره وكالة متخصصة داخل الأمم المتحدة.

ويعمل الاتحاد على مساعدة الحكومات في الاتفاق على مبادئ مشتركة تفيد الصناعات التي تعتمد على تكنولوجيا المعلومات والبنية التحتية للاتصالات. وقد وضع الاتحاد الدولي للاتصالات مخططًا لتعزيز الأمن السيبراني العالمي يتكوّن من سبعة أهداف رئيسة المتمثلة في (إدوارد كريستيان عيد، 2009):

– وضع استراتيجيات لتطوير نموذج التشريعات الخاصة بالمجال الالكتروني يكون قابلاً للتطبيق محليًا وعالميًا بالتوازي مع التدابير القانونية الوطنية والدولية المعتمدة.

– وضع استراتيجيات لتهيئة الأرضية الوطنية والإقليمية المناسبة لوضع الهيكليات التنظيمية والسياسات المتعلّقة بجرائم الانترنت.

– وضع استراتيجية لتحديد الحد الأدنى المقبول عالميًا في موضوع معايير الأمن ونظم تطبيقات البرامج والأنظمة.

– وضع استراتيجيات لوضع آلية عالمية للمراقبة والإنذار والرد المبكر مع ضمان قيام التنسيق عبر الحدود.

– وضع استراتيجيات لإنشاء نظام هوية رقمي عالمي وتطبيقه، وتحديد الهيكليات التنظيمية اللازمة لضمان الاعتراف بالوثائق الرقمية للأفراد عبر الحدود الجغرافية.

– تطوير استراتيجية عالمية لتسهيل بناء القدرات البشرية والمؤسسية لتعزيز المعرفة والدراية في مختلف القطاعات وفي جميع المجالات المعلوماتية.

– تقديم المشورة بشأن إمكانية اعتماد إطار استراتيجي عالمي لأصحاب المصلحة من أجل التعاون الدولي والحوار والتعاون والتنسيق في جميع المجالات التي سبق ذكرها.

د. اتفاقية المجلس الأوروبي بشأن جرائم الإنترنت:

في العام 1996 أنشأت اللجنة الأوروبية لمشاكل الجريمة (CDPC) لجنة خبراء للتعامل مع مشكلة الجريمة الالكترونية، أين عملت ما بين العامين 1997 و2000 على إعداد مشروع الاتفاقية التي اعتمدها البرلمان الأوروبي في الجزء الثاني من جلسته العامة في شهر أفريل 2001؛ تهدف الاتفاقية إلى:

– توحيد عناصر القانون الجزائي المحلي مع الأحكام المتعلقة بالجرائم الإلكترونية.

– توفير الاجراءات القانونية اللازمة للتحري وملاحقة الجرائم المرتكبة الكترونيًا بواسطة الكمبيوتر.

– تعيين نظام سريع وفعال للتعاون الدولي.

– الحفاظ بشكل سريع على البيانات المخزّنة على أجهزة الكمبيوتر وحفظها والإفصاح الجزئي عن حركة هذه البيانات المخزنة على الكمبيوتر.

– جمع معلومات عن حركة البيانات وعن إمكان وجود تدخّل في محتواها.

– تتضمن أيضًا الاتفاقية المبادئ العامة المتعلّقة بالتعاون الدولي في المواضيع التالية: تسليم المجرمين، المساعدة الدولية المتبادلة، إعطاء المعلومات بصورة آلية، وإنشاء الولاية القضائية على أي جريمة.

– المساعدة المتبادلة في جمع حركة المعلومات واعتراضها.

– الإجراءات المتعلقة بطلبات المساعدة المتبادلة في غياب الاتفاقات الدولية.

III. الحماية من جريمة التقليد والقرصنة الالكترونيتين :

1– الحماية من جريمة التقليد الالكترونية:

مصطلح الملكية الفكرية هو مصطلح قانوني في المقام الأول، ويراد به حق الانسان في انتاجه العلمي والادبي والفني والتجاري، ليستفيد من ثماره وآثاره المادية والمعنوية، وحرية التصرف فيه، والتنازل عنه واستثثاره؛ وسوف نركز دراستنا هنا على الحماية المقررة للمصنفات الرقمية وفق ما قرره المشرع الجزائري، وذلك عبر دراسة وتحليل النقاط الموالية:

أ–تحديد مفهوم لمصنفات الرقمية:

عرف الفقه المصنفات الرقمية بأنها تعتبر "الوسيلة التقنية التي تسمح بنقل المعلومة من ظاهرة محسوسة إلى ظاهرة تدرك بواسطة أرقام وفق الترقيم المزدوج (0–1)" (العربي بن حجار ميلود، 2011).
كما عرف بأنه "مصنف إبداعي عقلي ينتمي إلى بيئة تقنية المعلومات، والتي يتم التعامل معها بشكل رقمي؛ أو أنه أي إبداع من بيئة تكنولوجيا المعلومات" (طه عيساني، 2013).

أما عن المشرع الجزائري؛ فلم يتطرق إلى تعريف المصنفات الرقمية، وإنما اعتبرها كنوع من المصنفات الأدبية والفنية، حيث نصت المادة 5 من الأمر 03–05 المتعلق بحقوق المؤلف والحقوق المجاورة على حماية برامج الحاسوب والمادة 4 على حماية قواعد البيانات إذا توفرت فيها شروط الاصالة.

ب–المصنفات الرقمية المشمولة بالحماية القانونية:

وتتمثل في برامج الحاسوب، قواعد البيانات، المصنف المتعدد الوسائط.

-برامج الحاسوب: عرفته الجمعية الدولية لحقوق المؤلف على أنه "برنامج الاعلام الآلي يشمل كل البرامج والطرق، وحتى الوثائق المتعلقة
بسير مجموع المعطيات، وبرامج الإعلام الآلي يمكن أن يعتبر كمجموع غير قابل للتجزئة ومحمي كما هو" (كوثر مازوني، 2008).

وتنقسم برامج الحاسوب من الزاوية التقنية إلى: برمجيات التشغيل؛ التي يقصد بها مجموعة البرامج التي تعد خصيصا لتنظيم أجهزة الحاسوب منذ بدء تشغيلها حتى إغلاقها كالكتابة. وبرامج التطبيق؛ وهي تلك البرامج التي يكون غرضها تنفيذ مهام إدارية أو وظيفية معينة كقائمة الطلبة وأرقام تسجيلهم في الجامعة (أحمزيورادية، 2014).

أما عن موقف المشرع الجزائري، كما أسلفنا الذكر، فقد قرر لها حماية بموجب نص المادة 4 من الأمر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة واعتبرها كمصنفات أدبية مكتوبة سواء أكانت بلغة المصدر أو بلغة الآلة، واستبعدها من الحماية بصفتها كبراءة اختراع بموجب قانون براءة الاختراع في الأمر 07/03 عبر نص المادة 6/7 التي نصت على عدم اعتبار برامج الحاسوب من قبيل الاختراعات المحمية بموجب هذا الأمر (الأمر 07/03، 2003).

-قواعد البيانات: وتعرف بأنها "معلومات مجمعة وتتعلق بموضوع ما يتم تخزينها على دعامة مادية متصلة بالحاسب الآلي، يتوفر فيه عنصر الابتكار أو الترتيب، وأي مجهود شخصي يستحق الحماية، ويكون مخزنا بواسطة الحاسوب ويمكن استرجاعه بواسطته أيضا" (شحاتة غريب شلقامي، 2008).

وهذا ما أخذ به المشرع الجزائري بصفة ضمنية في المادة 2/5 من الأمر رقم 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة، بأنها تلك قواعد البيانات سواء كانت مستنسخة على دعامة قابلة للاستغلال بواسطة آلة أو بأي شكل من الأشكال الأخرى، والتي تتأتى أصالتها في انتقاء موادها أو في كيفية ترتيبها (بوزيدي أحمد تجاني، 2009).

-المصنف المتعدد الوسائط: يقصد بها وسائل تمثيل المعلومات باستخدام أكثر من نوع من الوسائط مثل الصور والأصوات والنصوص وكذا النص المترابط، ويتميز هذا النوع من المصنفات بدمج عدة عناصر وتفاعلها معا عن طريق برامج الحاسوب.

وقد أورد المشرع الجزائري في المرسوم التنفيذي رقم 98-257 المؤرخ في 25 أوت 1998 الذي يضبط شروط وكيفيات اقامة خدمات الانترنت واستغلالها باعتبار صفحة (الواب) هي صفحة متعددة الوسائط تتكون من نصوص، رسوم بيانية، صور موصولة بينها عن طريق وصلات تسمى نصوص متعددة (حواس فتيحة، 2004).

ج_ أركان جنحة تقليد المصنفات الرقمية:

تقوم جنحة تقليد المصنفات الرقمية عبر القيام بالاعتداء بصفة مباشرة أو غير مباشرة.

1-قيام جنحة تقليد المصنفات الرقمية عبر الاعتداء المباشر:

الملاحظ على المشرع الجزائري أنه لم يعرف جنحة تقليد المصنفات الرقمية وإنما اكتفى ببيان صوره في المواد 151 و155 من الأمر 05/03 المتعلق بحقوق المؤلف والحقوق المجاورة ويكون ذلك عبر انتهاج الوسائل التالية:

_الكشف غير المشروع للمصنف: ويقصد به عملية الكشف التي تقع دون إذن صاحب الحق، ويعد من قبيل الحق المعنوي والادبي في نفس الوقت وإلا يعد مرتكبا لجنحة التقليد.

–المساس بسلامة المصنف: يجوز للمؤلف دفع كل اعتداء يمس بسلامة مصنفه، وذلك بمنع أي تشويه أو تعديل لمصنفه بدون إذنه، وهذا ما أكده المشرع الجزائري؛ والمساس بسلامة المصنفات الرقمية يظهر بقيام أصحاب المواقع بنشر مصنفات محمية بموجب حق المؤلف على مواقعهم بدون إذن من أصحابها (شريفي نسرين، ص 2014).

–استنساخ مصنف في شكل نسخ مقلدة: يقصد به اعادة نسخ المصنف لعدة نسخ مقلدة بأساليب متعددة لإبلاغه للجمهور، ويتم التقليد باستعمال عدة وسائل والمتمثلة في استنساخ المصنف كله أو جزء منه في نظام إعلام آلي.

وقد يكون المؤلف ذاته مرتكبا لجنحة التقليد في حالة قيامه ببيع مصنفه للغير ثم أعاد بيع حقوق النسخ لشخص آخر دون الرجوع إلى الشخص الذي تم التصرف إليه كليا (عبد الرحمان خلفي، 2010).

2–قيام جنحة التقليد للمصنف الرقمي عبر الاعتداء غير المباشر:

ويكون ذلك عند ارتكاب السلوكيات المشكلة للركن المادي للجنحة والمتمثلة في:

–استيراد أو تصدير نسخ مقلدة من المصنف: حيث منع المشرع الجزائري استيراد المصنفات المنشورة في الخارج حماية للمؤلفين الأجانب.

–بيع النسخ المقلدة للمصنف: يقصد به الاستغلال التجاري للنسخ المقلدة، وذلك ببيعها مثلا أو عن طريق عرضها للتداول بين الجمهور.

–تأجير أو وضع رهن التداول لنسخ مقلدة لمصنف: ويشترط في عملية التأجير أن يكون المصنف المؤجر مقلدا، ولا يشترط أن تكون العملية منظمة في شكل رسمي.

د–آليات حماية المصنفات الرقمية من جنحة التقليد:

تنوعت هذه الآليات التي تعطي لمالك المصنف الحق في العديد من الخيارات لمواجهة الاعتداء فله الحق في اتباع:

–التدابير الاحترازية: حيث يحق بموجب هذه الحماية للمؤلف المتضرر أن يطلب من الجهة القضائية المختصة اتخاذ التدابير التحفظية التي تحول دون المساس الوشيك بحقوقه.

وذلك عبر تقديم طلب لرئيس المحكمة المختصة قضائيا من أجل ايقاف أي عملية استنساخ للمؤلف غير المشروع، وحجز النسخ المقلدة وما ترتب عنها من ايرادات إذا تم نشرها وتوزيعها ولو خارج الأوقات القانونية؛ حيث يأمر ضباط الشرطة القضائية أو الأعوان المحلفون التابعون للديوان الوطني لحقوق المؤلف والحقوق المجاورة بالقيام بعملية الحجز بناء على رخصة من رئيس المحكمة من أجل الفصل في طلب الحجز في أجل ثلاثة أيام من تاريخ الاخطار (نرجس صفوة، 2016) عملا بنص المادة 144–145 من القانون 05/03 الخاص بحقوق المؤلف والحقوق المجاورة.

–الدعاوى القضائية: قصد توقيع عقوبات صارمة تتضمن الحبس أو الغرامات المالية، أو المصادرة أو الإتلاف؛ حيث قرر المشرع الجزائري على مرتكب جريمة التقليد الحبس من 6 أشهر إلى 3 سنوات، وبغرامة مالية من 500.000 دج إلى 1000000 دج

سواء تمت عملية النشر في الجزائر أو في الخارج؛ وشدد العقوبة في حالة العود مع تقرير الإغلاق المؤقت للمؤسسة التي يستغلها المقلد أو الشريك مدة لا تتعدى 6 أشهر وللجهة القضائية أن تقرر الغلق النهائي عند الاقتضاء.

IV. الحماية من جريمة القرصنة الإلكترونية :

بدأت ظاهرة القرصنة والاختراق مع بداية الحاسوب الإلكتروني، وازدادت بشكل كبير مع استخدام تقنية الشبكات؛ حيث يشمل الاختراق الهجوم على شبكات الحاسوب من قبل مخترقي الانظمة الإلكترونية ومنهكي القوانين.

ففي سنة 1986 قام شخص يدعى (روبيرتو سوتو) و هو كولومبي الجنسية، بسرقة خط تليكس حكومي ليرسل مجموعة رسائل عبره إلى مصارف في المملكة المتحدة، ومنها إلى دول أخرى والذي نتج عنها نقل الملايين من الدولارات من أرصدة الحكومة الكولومبية (الزوهري أيوب، 2018)؛ لتليه مجموعة من هجمات قراصنة المعلومات التي مست الأفراد و/أو المؤسسات العامة والخاصة.

هذا ما دفع بالمجتمع الدولي في العقود الأخيرة إلى تقديم جهود دولية استثنائية لمحاربتها، وذلك بغية تقديم الحماية للأفراد والمؤسسات من مخاطر هذه الجرائم عبر مجموعة من الاتفاقيات، والمؤتمرات، والبرتوكولات. ومنه سعت الشركات المختصة في صناعة البرامج إلى الاتحاد وانشاء منظمة خاصة لمراقبة وتحليل سوق البرمجيات، ومن ذلك منظمة اتحاد برمجيات الأعمال أو ما يعرف اختصارا (ASA)، والتي أجرت دراسة تبين منها أن القرصنة على الأنترنت ستطغى على أنواع القرصنة الأخرى، ودق هذا التقرير ناقوس الخطر للشركات المعنية فبدأت طرح الحلول المختلفة لتفادي القرصنة على الأنترنت (مكي يوسف، 2018).

أ- تعريف القرصنة الالكترونية:

تعددت التعاريف المرتبطة بالقرصنة الالكترونية لما لها من ارتباط بالجانب التقني للحاسب الآلي وشبكة الأنترنت من جهة، ومن جهة أخرى فهي تشكل فعلا أو عملا غير قانوني يدخل ضمن الجريمة الإلكترونية، كل من زاوية تكوينه الخاص ومنهجه في دراسة مفهوم القرصنة الإلكترونية.

حيث تم تعريف القرصنة الإلكترونية أو المعلوماتية؛ على أنها عملية اختراق لأجهزة الحاسوب تتم عبر شبكة الانترنت غالبا، لأن أغلب حواسيب العالم مرتبطة عبر هذه الشبكة، أو حتى عبر شبكات داخلية يرتبط فيها أكثر من جهاز حاسوب. يقوم بهذه العملية شخص أو عدة أشخاص متمكنين في برامج الحاسوب، بالإضافة إلى تمكنهم من اختراق حاسوب معين ، والتعرف على محتوياته بواسطة برامج مساعدة، ومن خلالها يتم اختراق باقي الأجهزة المرتبطة معها في نفس الشبكة (سامي علي حامد عياد، 2007).

وقد عرفت القرصنة الإلكترونية على أنها الاستيلاء على ملك الغير عن طريق النهب أو السرقة، دون اللجوء إلى العنف أو الترهيب أو التهويل أو القتل، وهي مختلفة عن القرصنة التي كان يمارسها الأقدمون عن طريق البر والبحر.

ولا يدخل في نطاق القرصنة الإلكترونية استيلاء الفاعل على المكونات المادية المستخدمة في الحاسب الآلي، والتي قد تحتوي تلك البرامج والبيانات كاستيلائه على الأقراص المدمجة مثلا أو الأشرطة أو الأقراص اللينة، فلا يكاد ذلك يخرج عن اعتباره غصبا في مجال الفعل الضار والعادي الذي يقع على الأشياء المادية.

و لعل ما تتميز به القرصنة الإلكترونية، أن الفاعل رغم حصوله على البرامج والبيانات الإلكترونية المملوكة للغير، إلا أنه لا يخرجها في الوقت ذاته من حيازة ذلك الغير ولا يحول بالتالي بينه وبين الانتفاع بها. ويقوم الفاعل في قرصنة البرامج والبيانات الإلكترونية إما إعادة إنتاجها أو نسخها للاستفادة منها أو لبيعها، والحصول على منفعة مادية منها (عبد الرزاق السالمي، 2007).

ب–أنواع مجرمي المعلومات:

وفقا لما توصلت إليه الدراسات والأبحاث في مجال مجرمي المعلومات، يمكن أن نبين أنماط وتصرفات هؤلاء من خلال تصنيفهم، وإن كان لابد من الإشارة إلى أنه لا يعني ذلك أن كل مجرم معلوماتي يندرج تحت فئة معينة دون غيرها، بل يمكن أن يكون المجرم الواحد مزيجا من أكثر من فئة؛ وهنا سوف نركز على نوع واحد وهم القراصنة التي يمكن تصنيفهم إلى الأنواع التالية:

القراصنة الهواة (الهاكرز)؛ وهذا النوع من المجرمين يرون في اختراق الأنظمة المعلوماتية تحديا لقدراتهم الذاتية، وغالبا ما تكون هذه الفئة من هواة الحاسوب، فيقومون بأعمالهم لمجرد إظهار أنهم قادرون على اقتحام المواقع الأمنية أحيانا، أو بمجرد ترك بصماتهم التي تثبت وصولهم إلى تلك المواقع، وهم يدعون أنه لا توجد هناك دوافع تخريبية وراء أعمالهم، بل قد يكون الفضول وحب المعرفة والتعمق في عمل الأنظمة المعلوماتية هو دافعهم الأول (نهلا عبد القادر المومي، 2010).

وفي الحقيقة هناك سمة مميزة لهذه الفئة من القراصنة، ألا وهي تبادلهم للمعلومات فيما بينهم، وتحديدا التشارك في وسائل الاختراق وآليات نجاحها في مواطن الضعف في نظم الحاسوب والشبكات، خاصة عن طريق النشرات الإعلامية الإلكترونية.

القراصنة المحترفون (الكاركز)؛ هذه الفئة تعكس اعتداءاتهم ميولا اجرامية خطيرة، ناتجة عن رغبتها في إحداث التخريب، ويتميز هؤلاء بقدراتهم التقنية الواسعة وخبرتهم في مجال أنظمة الحاسوب والشبكات، وهم أكثر خطورة من الصنف الأول السالف الذكر. وعادة ما يعود المجرم المخترق إلى إعادة ارتكاب الجريمة مرة أخرى وهو يعيش لسنوات طويلة من عائده الاجرامي (يونس عرب، 2002).

ج– موقف المشرع الجزائري من جريمة القرصنة الإلكترونية:

قد تناول المشرع الجزائري جريمة القرصنة الإلكترونية في المادة 394 مكرر 2 من قانون العقوبات في الشق المتعلق بالجرائم المتعلقة بالمعطيات المعلوماتية المقرصنة، وذلك وفق الأشكال التالية:

–جريمة تصميم معطيات معلوماتية مقرصنة؛ وتتمثل جريمة التصميم لمعطيات معلوماتية مقرصنة في برمجتها بواسطة الحاسب الآلي، من ذلك الفيروسات المعلوماتية، وبرامج القرصنة في حد ذاتها.

أما المعطيات المعلوماتية المقرصنة؛ فهي تشمل جميع أنواعها سواء كانت معطيات أو بيانات أو مستندات وبرامج...بحيث يكون دورها الأساسي هو القيام بالإضرار بالأنظمة المعلوماتية (دردور نسيم، 2013).

والملاحظ أن المشرع الجزائري لم يشترط طريقة معينة لتصميم المعطيات المقرصنة، كما أنه لم يشترط استعمال هذه المعطيات في جرائم أخرى، ولكن اشترط أن تكون الوسيلة بإمكانها المساس سواء بالأنظمة وفقا لنص المادة 394 مكرر من قانون العقوبات، أو بالمعطيات المعلوماتية السليمة ،عملا بنص المادة 394 مكرر 1.

وفي حالة ارتكاب مثل تلك الأفعال، فإن المجرم يتعرض لعقوبة الحبس من شهرين إلى 3 سنوات، وغرامة مالية تتراوح بين مليون دينار جزائري إلى خمسة ملايين دينار جزائري وفق ما نصت عليه المادة 394 مكرر 2.

-جريمة بحث أو تجميع معطيات معلوماتية مقرصنة؛ ويقصد بها قيام المجرم بعملية بحث أو تحميل عبر شبكات الاتصال المعلوماتية أو أي مصدر آخر، وكذا تجميع المعطيات المعلوماتية المقرصنة، قصد استعمالها للمساس بالأنظمة و/أو المعطيات المعلوماتية السليمة، وذلك تطبيقا لما ورد النص عليه في المادة 394 مكرر 1/2 من قانون العقوبات.

-جريمة توفير أو نشر معطيات معلوماتية مقرصنة المادة 394 مكرر 2؛ويكون ذلك عبر قيام المجرم بتوفير أو نشر معطيات معلوماتية مقرصنة من الممكن استعمالها للمساس بالأنظمة أو المعطيات المعلوماتية السليمة؛ وأنه غالبا ما تتم العملية-التوفير والنشر- عبر شبكة الانترنت، وذلك عبر عرض على جمهور الأنترنت هذه المعطيات المجرمة، سواء من خلال تثبيتها في مواقع صفحات الانترنت قابلة للاستنساخ أو نشرها عن طريق البريد الإلكتروني، أو عن طريق برامج الاستنساخ بين الخواص.

وفي جميع الأحوال فإنه مهما كانت طبيعة السلوكيات الإجرامية التي وضعها المشرع الجزائري، فإنه يشترط في جميعها توفر الركن المعنوي، المتمثل في توفر النية الإجرامية أي ارتكاب الجريمة عمدا مع العلم بأن ذلك غير مسموح به، ولا يشترط توافر القصد الجنائي الخاص لقيامها.

الخلاصة :

كان للتطور التكنولوجي الأثر الكبير على حياة الإنسان، عبر تحويل العالم الكبير إلى قرية صغيرة، من خلال السرعة الكبيرة التي توفرها الانترنت في تداول المعلومات والافكار.

لا مناص من الاعتراف بأن ظاهرة الجرائم الإلكترونية التي باتت تتخذ أنماطا جديدة وضربا من ضروب الذكاء الإجرامي، تمثل بلا شك تحديا جديا وجديدا في الوقت الحاضر، تجاوزه يتطلب التعرف على هذه التحديات وإبراز جوانبها، بما يعني التشخيص الأمثل للظاهرة ومكافحتها على صعيد التجريم والعقاب من ناحية، وعلى صعيد الملاحقة الإجرائية من ناحية أخرى، وهذا أمر يستلزم:

أولا -الانطلاق من الاقتناع بخطورة هذه الظاهرة، ومحاولة التوفيق بين احترام مبدأ السيادة الوطنية لكل دولة في صورته التقليدية، والنزول ولو بقدر أمام ضرورات ومقتضيات التعاون القضائي الدولي الذي بقدر نجاحه تتحقق فعالية كل الجهود والإمكانيات المسخرة للتصدي لظاهرة الجرائم الإلكترونية ومكافحتها؛

وثانيا – تطوير البنية التشريعية الجنائية بذكاء تشريعي متواصل ودؤوب يسد ثغرات الأنظمة الجنائية على نحو يجعلها قادرة على إخضاع هذه الجرائم لأوصافها ونصوصها، ومواكبة التطورات التي يتوسل بها مرتكبو هذه الجرائم، على أن يتم هذا التطور في إطار القانون وكفالة احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وأن يتكامل هذا التطور في الدور والهدف مع المعاهدات الدولية.

غير أنه كأي ظاهرة اجتماعية، فإن وجود العناصر الايجابية لا يعني ذلك عدم وجود سلبيات، بل بالعكس هناك العديد منها وذلك راجع إلى سوء استعمال تلك الوسيلة من أجل تحقيق الأطماع الشخصية والذاتية، بخرق مجموع القواعد القانونية المقررة لحماية أصحاب الحقوق في العالم الالكتروني؛ وعلى هذا ندعو إلى:

-تكريس الحماية الفعالة للحقوق في العالم الافتراضي.
-تعديل التشريعات الوطنية تماشيا مع الاتفاقيات الدولية.

الإحالات والمراجع:

1-جورج لبكي، (2013)،**المعاهدات الدولية للأنترنت –حقائق وتحديات–**، مجلة الدفاع الوطني الصادرة عن وزارة الدفاع الوطنية اللبنانية، العدد (83)، كانون الثاني، ص.33.

2-ذياب موسى البداينة، (2014)،**الجرائم الالكترونية: المفهوم والاسباب**، ورقة علمية مقدمة في الملتقى: الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، خلال فترة من 02-04 سبتمبر، الأردن: كلية العلوم الاستراتيجية، ص.05.

3-محمد عبيد الكعبي، (2009)،**الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت**، القاهرة: دار النهضة العربية، ص.33.

4-يونس عرب، (2002)،**جرائم الكمبيوتر والانترنت–ايجاز في المفهوم والنطاق والخصائص والصور والقواعد الاجرائية للملاحقة والاثبات**، ورقة عمل مقدمة إلى مؤتمر الأمن العربي خلال 10-12 فيفري، أبو ضبي: المركز العربي للدراسات والبحوث الجنائية، ص.8

5-يعرة سعيدة، (2016)، **الجريمة الالكترونية في التشريع الجزائري دراسة مقارنة**، مذكرة الماستر قانون جنائي، كلية الحقوق، الجزائر: جامعة محمد خيضر بسكرة، ص.31.

6-رصاع فتيحة، (2012)، **الحماية الجنائية للمعلومات على شبكة الأنترنت**، رسائل ماجستير في القانون العام، كلية الحقوق والعلوم السياسية، الجزائر: جامعة أبو بكر بلقايد تلمسان، ص.43.

7-جميل عبد الباقي الصغير، (1992)،**القانون الجنائي والتكنولوجيا الحديثة**، القاهرة: دار النهضة العربية، ص.62.

8-باسكال وردا، (2014)،**الحماية: السبب الأساسي في انعدام الحماية هو الأحزاب السياسية**، محاضرة ملقاة في مؤتمر الأمم المتحدة عن حماية الأقليات في 26/25 تشرين الثاني، ص.01.

9-جبران خليل ناصر، (2018)،**حماية الملكية الفكرية: حقوق المؤلف في ظل التشريعات الوطنية والاتفاقيات الدولية**، أطروحة دكتوراه في علم المكتبات والعلوم الثقافية، كلية العلوم الإنسانية والعلوم الإسلامية، الجزائر: جامعة وهران 1 أحمد بن بلة، ص.108.

10-إدوارد كريستيان عيد، (2009)،**حق المؤلف والحقوق المجاورة في القانون اللبناني والقوانين العربية والأجنبية**، بيروت: منشورات صادر الحقوقية، ص.366.

11-العربي بن حجار ميلود، (2011)"**تشريعات الملكية الفكرية في حقل حماية البرمجيات في الجزائر**"، مجلة المنتدى، (26)، الجزائر: جامعة وهران، ص02.

12-طه عيساني، (2008)،**الاعتداء على المصنفات الرقمية وآليات حمايتها**، مذكرة ماجستير، كلية الحقوق، الجزائر: جامعة الجزائر، ص.8.

13-كوثر مازوني، (2008)،**الشبكة الرقمية وعلاقتها بالملكية الفكرية**، الجزائر: دار هومة للطباعة والنشر والتوزيع،ص92.

14-احمزيو رادية، سلامي حميدة، (2014)، **الحماية القانونية للمصنفات الرقمية**، مذكرة الماستر في الحقوق، كلية الحقوق والعلوم السياسية، الجزائر: جامعة عبد الرحمان ميرة بجاية، ص.9.

15-الأمر رقم 07/03 المؤرخ في 19 يوليو 2003 **المتعلق ببراءات الاختراع**، الجريدة الرسمية الجزائرية (44)، المؤرخة في 23 يوليو 2003.

16-شحاتة غريب شلقامي، (2008)،**الملكية الفكرية في القوانين العربية، دراسة لحقوق المؤلف والحقوق المجاورة ولخصوصية حماية برامج الحاسب الآلي**، الاسكندرية: دار الجامعة الجديدة للنشر، ص.50 .

17-بوزيدي أحمد تجاني، (2009)، **حق المؤلف والكتاب الرقمي**، مذكرة ماجستير في الملكية الفكرية، الجزائر: جامعة الجزائر، ص.33.

18-حواس فتيحة، (2004)،**حماية المصنفات المنشورة على الانترنت**، مذكرة ماجستير، كلية الحقوق، الجزائر: جامعة الجزائر، ص.16.

19-شريفي نسرين، (2014)،**حقوق الملكية الفكرية، حقوق المؤلف والحقوق المجاورة، حقوق الملكية الصناعية**، الجزائر: دار بلقيس للنشر، ص.45.

20-عبد الرحمان خلفي، (2010)،**محاضرات في القانون الجنائي العام**، الجزائر: دار الهدى، ص.89.

21-نرجس صفوة، (2016)، **الحماية القانونية للملكية الفكرية في البيئة الرقمية**، مداخلة في أعمال المؤتمر الدولي الحادي عشر، حول التعلم في عصر التكنولوجيا الرقمية خلال 22-24 أفريل، طرابلس، ص.293.

22-الزوهري ايوب، القرعى علي، (2018)،**الحماية الجنائية من القرصنة الالكترونية**، ماستر تشريع ومنازعات المعلومات والاتصالات الرقمية، كلية العلوم القانونية والاقتصادية والاجتماعية، الرباط: جامعة محمد الخامس، ص.2.

23-مكي يوسف، دوار محمد، (2018)، **واقع القرصنة الالكترونية في الجزائر، دراسة ميدانية على عينة من ضحايا القرصنة الالكترونية بلدية عمي موسى ولاية غليزان**، مذكرة الماستر علوم الاعلام والاتصال، كلية العلوم الاجتماعية، الجزائر: جامعة عبد الحميد ابن باديس مستغانم، ص10.

24-سامي علي حامد عياد، (2007)،**الجريمة المعلوماتية واجرام الأنترنت**، الإسكندرية: دار الفكر الجامعي، ص.78.

25-عبد الرزاق السالمي، (2007)، **تكنولوجيا المعلومات**، عمان: دار المناهج، ص.432.

26-نهلا عبد القادر المومي، (2010)،**الجرائم المعلوماتية**، عمان: دار الثقافة للنشر والتوزيع، ص.82.

27-يونس عرب، (2002)، **دليل أمن المعلومات والخصوصية، جرائم الكمبيوتر والأنترنت**، القاهرة: منشورات اتحاد المصارف العربية، ص.286.

28-دردور نسيم، (2013)،**جرائم المعلوماتية على ضوء القانون الجزائري والمقارن**، مذكرة ماجستير القانون الجنائي، كلية الحقوق، الجزائر:جامعة منتوري قسنطينة،ص.42.