التشفير كآلية لحماية المصنفات الرقمية من القرصنة الإلكترونية

Encryption as a mechanism to protect digital business from Electronic piracy

مرابط حمزة *
جامعة تيارت ابن خلدون/ الجزائر
University of tiart.algeria
كلية الحقوق والعلوم السياسية
عضو مخبر البحث في تشريعات حماية النظام البيئي
hamza.mrabet@univ-tiaret.dz

داودي منصور
جامعة تيارت ابن خلدون/ الجزائر
University of tiart.algeria
كلية الحقوق والعلوم السياسية
MANSOUR.DAOUIDI@univ-tiaret.dz

تاريخ الإيداع: 2022/05/15	تاريخ المراجعة:2022/11/02	تاريخ القبول:2022/11/02

ملخص:

في ظل التطور التقني والمعلوماتي للملكية الفكرية أصبح الإنتاج الفكري للإنسان خاصة ما تعلق بحقوق المؤلف المنشورة على شبكة الأنترنت محلا للقرصنة الإلكترونية كممارسة سيئة للثورة التكنولوجية الحاصلة والمستمرة، التي تهدف لاستغلال غير المشروع للمصنف الرقمي بدون دفع مقابل مالي، فكان لزاما إيجاد تدابير تقنية وقائية لمواجهتها، وظهر التشفير الإلكتروني كآلية يضعها أصحاب الحقوق بشكل مكمل للحماية القانونية.

وقد توصلنا إلى أن القرصنة الإلكترونية تشكل تهديد مستحدثا لصاحب حق الاستئثار للمصنف الرقمي، وأن التشفير الإلكتروني يمثل أهم التدابير التكنولوجية الفعالة لحمايته، مع ضمان أنه لا يشكل عائق للمستخدم لاستعمال حقه في النسخة الخاصة للمصنف المنصوص عليه قانونا.

الكلمات المفتاحية: المصنفات الرقمية؛ التشفير؛ التدابير التكنولوجية؛ القرصنة؛ أمن المعلومات.

Abstract:

With the technical and Informational evolution of the intellectual property, the human's intellectual production became vulnerable to Electronic piracy especially those relating to authors' rights published on the internet. As a malpractice of the technological revolution that aim to the illegal exploitation of the digital work without making any payements It had to find preventive technical measure To face it so the electronical Encryption appeared as a mechanism puts by rights holders to devote the protection supplementary to the legal protection.

And the electronical encryption represents most important of the efficient technological mechanisms to protect it while ensuring that it won't be an obstacle to the user to use his right in the digital works' special edition as it is required by law.

Keywords: digital business; Encryption; Technological Precautions; piracy; Information Security

* المُؤلف المُراسِل.

مقدمة:

تلعب حقوق الملكية الفكرية دورا كبيرا في تعزيز التطورات المعرفية مثل أنشطة البحثية والعلمية، وتأثيرها جليا على حقل المعلوماتية وظهور ما يعرف بالمصنفات الرقمية أو الإلكترونية كأبرز المنتجات المستحدثة بسبب الثورة التكنولوجية، والتي أضحت تشكل أهم مكونات البيئة الإلكترونية لما تقدمه من ميزات بالغة أهمية من ناحية نشر الوعي الثقافي والعلمي في المجتمع، وكذا المقابل الزهيد لنشرها عبر شبكة الأنترنت مما صاحبه سرعة في الانتشار، غير أن هذه المصنفات الرقمية تتعرض لعديد من الاعتداءات المستحدثة في الفضاء الرقمي والتي يبرز منها القرصنة الإلكترونية كأخطر الجرائم المعلوماتية على حقوق المؤلف والحقوق المجاورة.

وكان لزاما على أصحاب الحقوق إيجاد أساليب حديثة لحماية إنتاجاتهم الفكرية، فظهرت التدابير التكنولوجية كأحد الحلول المنصوص عليها في الاتفاقيات والمعاهدات الدولية وكذا التشريعات المقارنة، حيث أكد عليها التوجيه الأوروبي بشأن حق المؤلف في المجتمع المعلوماتي الصادر 2001 في المادة (3/06) باعتبارها ترمي في إطار التشغيل المعتاد لها إلى الحد أو منع الأعمال غير المأذون بها من طرف صاحب حق المؤلف والتي تقع على المصنفات الرقمية أو غيرها من المحتويات المحمية، وما يميز هذه التدابير أنها متعددة ومتنوعة ومتطورة لضمان حماية متكاملة لحق المؤلف والحقوق المجاورة المنشورة على شبكة الأنترنت، نذكر منها على سبيل المثال: التوقيع الإلكتروني، نظام التعرف على المصنفات الرقمية "IDDN"، نظام كلمات المرور، تقنية منع النسخ "Anti-copie"، تقنية تنقية المواقع في شبكة الانترنت. نظام التسيير الإلكتروني لحقوق المؤلف" ECMS"، الإيداع الإلكتروني القانوني للمصنفات الرقمية المنشورة إلكترونيا...إلخ.

لكن أخذ التشفير الإلكتروني مكانة بارزة من بين آليات أنواع الحماية التقنية لأمن المعلومات، يرتكز في عمله على الثقة والأمان، وهو ما يعكس استعماله بكثافة كوسيلة تأمين المراسلات والبيانات العسكرية في وقتنا الحالي.

يكتسب موضوع البحث أهمية متزايدة بسبب استغلال وسائل الاتصال الحديثة في ممارسة نشاطات القرصنة الالكترونية التي تتطور بشكل كبير تعجز معه النصوص الحماية القانونية التقليدية على ضمان الحماية الكافية للمصنف الرقمي، كما يبرز أيضا أهمية الموضوع في تسليط الضوء على التشفير الإلكتروني من الناحية القانونية والتقنية باعتباره الآلية الأساسية المعتمدة لحماية أمن المعلومات.

ومن خلال ما سبق تتمحور الإشكالية التي يمكن طرحها فيما يلي:

ما مدى تكريس التشفير كآلية قانونية مستحدثة لضمان حماية المصنفات الرقمية من القرصنة الإلكترونية؟

ومن أجل تحقيق الأهداف المرجوة من هذه الدراسة فإننا ارتأينا الإعتماد على المنهج الوصفي التحليلي من خلال تحليل النصوص المتعلقة بالقرصنة والتشفير والمفاهيم وأبعادها والوقوف على مواطن النقد والاعتراض، كما اعتمدنا أيضا على المنهج المقارن في تناولنا للاتفاقيات والمعاهدات الدولية والتشريعات الأجنبية المنظمة لها.

وللإجابة على الإشكالية المطروحة، فقد تم تقسيم البحث إلى مبحثين رئيسين هما:

المبحث الأول: القرصنة الإلكترونية كصورة مستحدثة للإعتداء على المصنفات الرقمية.

المبحث الثاني: دور التشفير الإلكتروني في حماية المصنفات الرقمية.

المبحث الأول: القرصنة الإلكترونية كصورة مستحدثة للإعتداء على المصنفات الرقمية

منذ ظهرو شبكة الإنترنت نتيجة لمشروع «أربانت» الذي انطلق عام 1969 من قبل وزارة الدفاع الأمريكية، قامت بتطويره مؤسسة العلوم القومية عن طريق تمويل شبكة (NSF) مما جعل العالم قرية صغيرة، وقد أتاح تزايد نفاذ الأشخاص لشبكة الأنترنت بواسطة الأساليب التقليدية (الحواسيب) أو الأساليب الحديثة (الهواتف المحمولة، اللوح الرقمي ...إلخ)، هذاما رافقه بروز النشر الإلكتروني كأحد روافد حقوق المؤلف والحقوق المجاورة من خلال تبسيط آليات نشر خاصة من ناحية التكلفة والسرعة، مما جعله مكان خصب لقرصنة المصنفات الرقمية التي تمتاز بمحيطها الرقمي وبنائه التقني واشكالها المختلفة.

المطلب الأول: مفهوم القرصنة الإلكترونية للمصنفات الرقمية

كثر الحديث في عصرنا الحاضر عن القرصنة فأصبح من الطبيعي سماع هذا المصطلح الشائع نظير استعماله في عدة مجالات منها البيولوجية أو البحرية، لكن تبرز منها القرصنة المرتكبة في البيئة الرقمية كأحد سلبيات هذا العصر مما شكل هدم للإنتاج الفكري البشري، وسبب مشكلة عالمية وحقيقية للدول حتى تلك أكثرها تقدما.

الفرع الأول: تعريف القرصنة الإلكترونية للمصنفات الرقمية

تعددت التعريفات التي تناولته، ما بين التعاريف اللغوية والتعاريف الاصطلاحي وذلك كما يلي:

أولا/ تعريف اللغوي:

القرصنة لغة هي: الاسم من القرصان، وهم لصوص البحر، ويجعلها بعض الكتاب لفظة مفردة يجمعونها على قراصنة وهي كلمة إيطالية[1]، كما عرف أيضا لغة: "سطو على حقوق الملكية الفكرية أو الأدبية أو الفنية قرصنة حقوق المؤلفين-القرصنة في مجال التسجيلات الموسيقية"[2].

ثانيا/ التعريف الاصطلاحي:

سوف نتناول في التعريف الاصطلاحي ما يلي:

1- التعريف الفقهي:

تعددت تعاريف الفقهية وهذا ما سوف نتناوله فيما يلي:

إن لفظ القرصنة الإلكترونية في وقتنا الحالي أصبح وصفيا، يشير إلى النهب والاستيلاء على المصنفات الرقمية المنشورة للغير من خلال الحصول على نسخة منها دون مقابل مالي أو موافقة مالكها [3].

عرف الفقهاء القرصنة الإلكترونية في مجال الملكية الفكرية على أنها: "الاستلاء أو النسخ غير المشروع على ملك الغير بدون ترخيص من المالك ومن دون أي سند قانوني، فهي اختراق للتدابير التقنية عبر شبكة الأنترنيت من خلال اشخاص أو أطراف قراصنة متمكنين في هذا المجال عن طريق استخدام التقنيات الحديثة للتحايل على التدابير التقنية

---

(1) سعاد جواهرة، حماية الملكية الفكرية في البيئة الرقمية من خلال التشريع الجزائري والقانون الدولي دراسة وصفية تحليلية، أطروحة دكتوراه، كلية علوم الإعلام والاتصال، جامعة الجزائر -3-، 2017/2016، ص 149.

(2) أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، 2008، ص 1798.

(3) مليكة عطوي، الحماية القانونية لحقوق الملكية الفكرية على شبكة الأنترنت دراسة وصفية تحليلية، أطروحة دكتوراه، كلية علوم الإعلام والاتصال، جامعة دالي براهيم الجزائر -3-، 2010/2009، ص 232.

أو عن طريق الغش، أو يمكن ان تنفذ الى المصنفات عن طريق استعمال كلمة سر بواسطة برامج معدة لهذا الغرض من اجل اختراق الاعمال الفكرية والإبداعية والنفاذ اليها ونسخها بصورة غير مشروعة"[1].

كما تعرف أيضا بأنها: "الانتهاك العمدي لحقوق المؤلف بغرض الحصول على المصنفات والبرمجيات أو البيانات معالجة آليا بشكل غير المشروع ذلك أن القرصان المعلوماتي الذي يسمى اصطلاحا " بالهاكر أو الكراكر" يمارس اعتداءاته في هدوء تام مستخدما التقنيات التكنولوجية التي تتيح له الحصول على المنتجات الرقمية دون التسبب في تلفها تحسبا لإعادة الانتفاع بها تجاريا بإعادة نسخها أو نشرها إلكترونيا"[2].

وعليه يمكننا تعريفها أنها: عملية غير قانونية تتم من قبل شخص يسمى القرصان باستخدام وسائل تكنولوجية حديثة للسطو على المصنف الرقمي، بقصد الانتفاع دون دفع مقابل أو الاستغلال التجاري له.

ومنه يمكن استنتاج شروط القيام بالقرصنة الإلكترونية على المصنفات الرقمية:

- أن تكون القرصنة الإلكترونية منصبة على مصنف رقمي يتمتع بالحماية قانونية[3]، لأن العلة في القرصنة هي اشتماله على الحماية[4].
- استعمال الوسائل التقنية والتكنولوجية الحديثة.
- حصول قرصان على مبلغ من المال من أصحاب الحقوق، أو جراء عرض للبيع.

لكن التساؤل المثار هنا، هل المصنف الرقمي الغير محمي قانونا ومقترن بتدابير تكنولوجية يمكن أن يكون محل للقرصنة الإلكترونية؟

في الأصل أن المصنف الرقمي الغير المشمول بالحماية قانونا وأصبح من الملك العام لا يمكن أن يكون محل للقرصنة الإلكترونية وبالتالي نصبح أمام الاستعمال المشروع له حتى ولو لم يدفع مقابل استخدامه ، لكن عند وضع المؤلف أو أصحاب الحقوق لتدابير تكنولوجية (التوقيع الإلكتروني، التشفير، نظام التعرف على المصنفات الرقمية...إلخ) تصبح هذه التدابير التكنولوجية في حد ذاتها محل للقرصنة وبالتالي نكون أمام جريمة التحايل على التدابير الحماية التكنولوجية التي تم النص عليها في المعاهدات الدولية( ) والتشريعات الوطنية المقارنة( )، حتى ولو كانت هذه التدابير وضعت على المصنف فقد الحماية القانونية لسبب من الأسباب، أو أنه غير محمي بالأصل، لكن تجب الملاحظة أن استمرار وضع هذه التدابير بعد انتهاء مدة الحماية القانونية يتعارض مع الاستعمال العادل للمصنف.

2- تعريف المنظمات الدولية:

[1] نور حسين علي الفهداوي، الآثار القانونية الناتجة عن انتهاك الوسائل التقنية لحماية المصنفات الرقمية "دراسة مقارنة"، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة بجاية، المجلد 12، العدد 02، 2021، ص75 و76.

[2] طه عيساني، القرصنة الالكترونية الضرر الاقتصادية والفكرية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي الجزائر، العدد 5، يوليو 2016، ص 107.

[3] تنص المادة 03 الفقرة الثانية أمر رقم 05-03 على أنه: " ...تمنح الحماية مهما يكن نوع المصنف ونمط تعبيريه ودرجة استحقاقه ووجهته، بمجرد إيداع المصنف سواء كان المصنف مثبتا أم لا بأية دعامة تسمح بإبلاغه إلى الجمهور"، الأمر رقم 03-05، مؤرخ في 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر، عدد 44، صادر في 23 يوليو 2003.

[4] اختلف الفقه والقضاء في بيان الشروط الواجب توفرها في المصنف ليكون جديرا بالحماية القانونية، لكنه عموما يتطلب شرطين هما الأصالة والتجسيد المادي المحسوس للمصنف المادة 03 و07 من الأمر 03-05 المتعلق بحق المؤلف والحقوق المجاورة.

عرفت المنظمة العالمية للملكية الفكرية (WIPO) القرصنة بقولها أنه: "استنساخ المصنفات المنشورة أو الفوتوغرافيات بأية طريقة مناسبة من أجل توزيعها على الجمهور وإعادة إذاعة البرامج الإذاعية دون أي تصريح"[(1)].

كما تناول مركز التجارة الدولية الأونكتاد[2] تعريف السلع المقرصنة بقولها أنها: " تلك التي يعتدى فيها على حقوق المؤلف، وما يتصل بها من حقوق، وأن ناشري الكتب ومنتجي الأسطوانات والأفلام هم ضحايا هذا الاعتداء نظرا للتقدم التقني الذي لعب دورا جوهريا في تسهيل النسخ"[(3)].

3- التعريف القانوني:

أ- على المستوى الدولي:

منذ بدء ظهور القرصنة الإلكترونية اتجهت الجهود الدولية لتعريفها من خلال الاتفاقيات والمعاهدات الدولية وذلك على النحو التالي:

عرفت اتفاقية تريبس (TRIPS) القرصنة بقولها أنها: " السلع أو المواد المقرصنة هي كل سلعة تشكل نسخة نسخت من دون الحصول على موافقة صاحب الحق، سواء تصنيف بصورة مباشرة أو غير مباشرة"[(4)].

كما نصت الاتفاقية العربية لمكافحة الجرائم التقنية للمعلومات على تعريف جريمة الدخول الغير مشروع في المادة 06 بقولها أنه: "الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به"[(5)].

أما المادة 7 من الاتفاقية السالفة فعرفت جريمة الاعتراض غير المشروع بقولها: "الاعتراض التعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات".

ب- على مستوى التشريعات الأجنبية:

تناول المشرع المصري تعريف الاعتراض والاختراق كصور للقرصنة وذلك من خلال قانون رقم 175 لسنة 2018 المتعلق بمكافحة جرائم تقنية المعلومات المصري في المادة 01 والتي نصت: "الاعتراض: مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل أو التخزين أو النسخ أو التسجيل أو تغيير المحتوى أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه، وذلك لأسباب غير مشروعة ودون وجه حق.

الاختراق: الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأي طريقة غير مشروعة على نظام معلوماتي أو حاسب إلى أو شبكة معلوماتية وما في حكمها"[(6)].

---

(1) نادية زواني، حماية الملكية الفكرية من التقليد والقرصنة -دراسة مقارنة-، أطروحة الدكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة –الجزائر-، 2013 -2012، ص132.

22 هي وكالة للتعاون التقني لمؤتمر الأمم المتحدة للتجارة والتنمية ومنظمة التجارة العالمية وتسمى اختصارا "ITC"

(3) نادية زواني، المرجع نفسه، ص 130 و131.

(4) طه عيساني، الاعتداء على المصنفات الرقمية وآليات حمايتها، رسالة ماجستير، كلية الحقوق، جامعة يوسف بن خدة الجزائر1، 2013/2012، ص61.

(5) الاتفاقية العربية لمكافحة الجرائم التقنية للمعلومات، الصادرة بالقاهرة بتاريخ 21 ديسمبر 2010، صادقت عليها الجزائر بموجب المرسوم الرئاسيّ رقم 14-252، مؤرّخ في 8 سبتمبر 2014، ج ر، عدد 57، الصادرة في 28 سبتمبر 2014.

(6) القانون المتعلق بمكافحة جرائم تقنية المعلومات المصري، رقم 175 لسنة 2018، الجريدة الرسمية لجمهورية مصر العربية، العدد 32 مكرر(ج)، 14 أوت 2018.

بينما تناول قانون الملكية الفكرية المصري في المادة 181 في القانون رقم 82 لسنة 2002[1]، على تجريم القرصنة الإلكترونية على المصنفات الرقمية.

كما لم يورد المشرع الفرنسي تعريفا للقرصنة الإلكترونية، لكنه في المقابل جرمها في قانون العقوبات الفرنسي في المادة L3-223، اضافة إلى تجريمه بعض الاعتداءات التي تستهدف البيانات والمعلومات المعالجة إلكترونيا وتمس بالمصالح العليا للدولة من المادة L6-411 إلى المادة L1- 411.

ت- على مستوى التشريع الجزائري:

المشرع الجزائري وعلى غرار التشريعات المقارنة لم يعرفه أيضا، ولكن بالرجوع إلى قانون العقوبات الجزائري[2] فقد نص على تجريم القرصنة الإلكترونية في القسم السابع مكرر المعنون بالمساس بأنظمة المعالجة الآلية للمعطيات حيث نصت المادة 394 مكرر "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنة (1) وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة، ...".

كما استحدث المشرع الجزائري نص تشريعي جديد متخصص في الجرائم المرتكبة في بيئة رقمية، من خلال القانون رقم 09-04 المتضمن قواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها[3].

وعليه من خلال التشريعات الأجنبية وقانون الجزائري يمكن القول إنه من وجهة نظرنا قد أصابت التشريعات بعدم تعريف القرصنة، باعتباره أن التعاريف هي من مهام الفقه والقضاء، وهذا راجع لكون التعريفات تختلف باختلاف المحدد الزمني والمكاني وحتى بنية الدولة الاجتماعية والاقتصادية والتكنولوجية.

الفرع الثاني: خصائص جريمة القرصنة الإلكترونية

تتميز القرصنة ببعض الخصائص تتشابه إلى حد بعيد مع خصائص الجريمة المعلوماتية:

1- ترتكب بأجهزة الكمبيوتر.

2- أنها سهلة الارتكاب أي أنها جرائم ناعمة، أي أنها لا تعتمد في ارتكابها على أية أعمال عنف أو استخدام أسلحة سواء نارية أو بيضاء مثل جريمة الضرب والجرح أو جريمة السرقة، فالقرصان الإلكتروني يتسم بالهدوء والاعنف ويستعمل الحاسوب الآلي فقط للقيام بهذه الأفعال وغالبا ما ترتكب من منزله.

3- الضرر الناجم من الجرائم الإلكترونية غير قابل للقياس.

4- السطو على المؤلفات والأعمال الفكرية للغير واستخدامها بغير ترخيص.

5- صعوبة اكتشاف الجريمة المعلوماتية وإثباتها: تتميز القرصنة الإلكترونية بأنها مستترة وخفية في أغلبها لتمتعها بقدرات فنية تمكنها من تنفيذه بدقة، وفي غالب الأحيان لا تترك أثرا لها بعد ارتكابها.

---

(1) القانون المتعلق بحماية حقوق الملكية الفكرية المصري، رقم 82 لسنة 2002، الجريدة الرسمية، العدد 22 (مكرر)، 2002/06/02.

(2) القانون رقم 04-15، المؤرخ 10 نوفمبر 2004، المعدل والمتمم للأمر رقم 66-156 المتضمن قانون العقوبات، ج ر، عدد 71، الصادرة في 10 نوفمبر 2004.

(3) القانون رقم 09-04، المؤرخ 5 غشت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ج ر العدد 47، الصادرة في 15 غشت 2009.

6- الجريمة المعلوماتية المتعدية للحدود (عابرة للوطنية): ومعنى ذلك أن هذا القرصنة الإلكترونية غير محصورة بالحدود الجغرافية أو المكانية للدول.

المطلب الثاني: أدوات القرصنة الإلكترونية للمصنفات الرقمية

تتنوع أدوات القرصنة الإلكترونية للمصنفات الرقمية سواء من حيث الأشخاص الذين يقمون منها، أو من حيث طرقها أو حتى من حيث وسائلها، وهذا ما سوف نتطرق إليه فيما يلي:

الفرع الثاني: أشخاص القرصنة الإلكترونية

إن أفضل التصنيفات للقراصنة الالكترونيين هو ذلك التصنيف الذي قسم قراصنة الانترنت إلى فئتين هما: القراصنة الهواة (الهاكرز)، القراصنة المحترفون (الكراكرز) [1].

أولا/ القراصنة الهواة (الهاكرز)

الهاكر هو اللفظ العربي للكلمة الإنجليزية **"HAKERS"**، يمكن أن ننعتهم بالمبتدئين أو الهواة الذي يكون الهدف من وراء اختراقهم للأنظمة الالكترونية للتعلم والتسلية على الأغلب، وهي تحمل عدة معان، إلا أننا في هذه الدراسة نحن معنيون بمعنى واحد وهو المخترق أو الهاتك [2].

وعادة ما يرى هذه الفئة من المجرمين في اختراق الأنظمة الإلكترونية تحديا لقدراتهم الذاتية، وغالبا ما يكون هذا النوع من هواة الحاسوب أن قيامهم بهذه الأعمال لمجرد ترك توقيعهم الذي يثبت الولوج إلى تلك المواقع ، أو بمجرد تبيان أنهم قادرون على اختراق المواقع الأمنية أحيانا، وهم يدعون أن فضول وحب المعرفة في عمل الأنظمة الإلكترونية هو دافعهم الحقيقي، كما يتميزون بالتعاون والتشارك في وسائل الاختراق وآليات نجاحها في مكامن الضعف في نظم الشبكات والحاسوب وبتبادلهم المعلومات والبيانات فيما بينهم ، خاصة عن طريق المعلومات الإعلامية الإلكترونية، مع العلم أنهم لا يملكون دوافع تخريبية وراء أعمالهم[3].

---

[1] ووفقا لخبراء علم الإجرام المعلوماتي فإن قرصان يتميز عن المجرم التقليدي بمجموعة من المزايا منها:

1- الذكاء والفطنة ولديه معرفة تقنية عالية.

2- الهدوء كونه يستعمل العقل ولا يحتاج إلى العنف.

3- يرتكب الفعل بغرض إظهار ذكائه وقدرته التقنية، أنظر طه عيساني، الاعتداء على المصنفات الرقمية وآليات حمايتها، المرجع السابق، ص 67.

[2] عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2018/2017، ص 106.

[3] كريمة خنوسي، الحماية الدولية من جرائم التقليد والقرصنة الإلكترونية وموقف المشرع الجزائري منها، مجلة مصداقية، المدرسة العليا العسكرية للإعلام والاتصال، المجلد 02، العدد 02، 2020، ص70.

ومع ذلك فإن علينا أن نعترف بخطورة الهاكرز [1] الذين تربوا في أجواء التفاخر بإبداعاتهم وتحديات الاختراق في هذا الحقل والذين يتم استعمالهم من قبل مجموعات الجريمة المنظمة الدولية لارتكاب نشاطات المخطط لها، فالتحدي القائم عندهم لا يترك لديهم طريق للتراجع ولا يتيح لهم تقليب الأمور أو التمييز، وليس لديهم ضوابط وشروط بشأن أفعالهم الذي يقوم به النظام الذي يخترقونه [2].

ثانيا/ القراصنة المحترفون (الكراكرز)

الكراكرز هو اللفظ العربي للكلمة الإنجليزية "CRACKERS"، وهم المخترقون المحترفون والذين يكون دخولهم الى الحواسيب من أجل هدف معين يسعون إليه، وهي تحمل عدة معان، ويطلق على هذا النوع أيضا إسم القراصنة المخادعين وغالبا ما يحدثون أضرارا كبيرة على أنظمة المعلومات وعلى الصناعات لأنهم يؤلفون مجموعات لتبادل المعلومات فيما بينهم، وهم يقسمون أيضا على أساس جرائمهم إلى مخادعون وجواسيس [3].

1- المخادعون:

وهم أشخاص يمتلكون بقدرات فائقة باعتبارهم من المتخصصين وأصحاب الكفاءات في أنظمة المعلوماتية، وتنصب نشاطاتهم على جرائمهم في أغلبها على الأموال والتلاعب في المؤسسات المالية والاقتصادية وحسابات المصارف ولديهم القدرة عالية على إخفاء الأدلة التي تشير إليهم [4].

2- الجواسيس:

ويعرف الجاسوس "بأنه الشخص الذي يقوم بمجموعة من الأعمال المنجزة لصالح بلد أجنبي تهدف إلى إيقاع الضرر بسلامة بلد آخر، وتكون غالبا معلومات سرية عن الجيوش أو أجهزة المخابرات وسواها، وذلك بطرق ملتوية ومخالفة للقانون، مما يعرضه لعقوبات قاسية [5].

الفرع الثاني: طرق القرصنة الإلكترونية

عادة ما تتم القرصنة الإلكترونية بطرق عديدة، ولعلى أشهرها الآتية:

---

[1] صنفت إحدى أهم شركات تأمين أمن المعلومات في أمريكا الهاكرز بأنهم:
1- المتشردون وهم عادة ما يكونون كالأطفال في أعمالهم.
2- ذو القبعة السوداء أو المستغلون وهم الذين يعملون من أجل الربح الشخصي أومن أجل الثأر وتأكيد مواقف سياسية.
3- ذو القبعات البيضاء وهم الذين يعملون من أجل أغراض.
4- ذو القبعات الزرقاء وهو الذي يعمل لصالح شركات العالمية في مجال الأمن السيبراني.
5- المبتدئ أو قليل الخبرة في مجال القرصنة الإلكترونية.
6- الصالح ذو الأخلاق وهم الذين يعملون من أجل هدف يهم المجتمع.
الهاكرز الذي يعمل لدى الهيئات الاستخبارية التابع لدول، أنظر عبد الكريم نعمان، المرجع السابق، ص 112.

[2] اعمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة -دراسة وصفية تحليلية-، أطروحة دكتوراه، كلية العلوم السياسية والإعلام، جامعة بن يوسف بن خدة الجزائر -1-، 2009/2008، ص 129.

[3] عزيزة رابحي، المرجع نفسه، ص 107.

[4] عبد الكريم نعمان، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر-1-، 2016-2017، ص107.

[5] عزيزة رابحي، المرجع السابق، ص 108.

أولا/الاختلاس والتضليل

وتتمثل هذه الطريقة في نسخ العناصر التي يتكون منها الموقع ومحتوياته دون وجه حق، فالمعطيات والبيانات موجودة عليه من رسوم وصور وعناصر ونصوص صوتية، يمكن بيسر نسخها وإعادة عرضها على موقع آخر دون موافقة صاحب الموقع الأصلي [1].

ثانيا/ الاختراق

تتمثل هذه العملية في القدرة على الوصول لهدف محدد بطريقة غير مشروعة، بواسطة ثغرات في نظام الحماية الخاص بالحاسب الآلي المستهدف، وقد استخدم المشرع الجزائري عبارة جريمة الدخول والبقاء عن طريق الغش إلى النظام المعلوماتي للإشارة إلى عملية الاختراق وذلك في نص المادة 394 مكرر من قانون العقوبات [2].

ثالثا/ البقاء غير المصرح به في النظام المعلوماتي

قد لا يكتفي القرصان الرقمي بمجرد الاختراق والدخول إلى النظم المعلوماتية، بل يمكث داخل هذا النظام بالرغم من علمه بعدم أحقيته في الدخول إليه وهو ما يستنتج من خلال عبارة " عن طريق الغش" الواردة في المدة السالفة الذكر، كما قد يقوم الجاني بإحداث تغييرات في معطيات المنظومة أو القيام بحذف البيانات والمعلومات الخاصة [3].

رابعا/ التعطيل (العرقلة)

يقوم التعطيل أو ما يسمى بالعرقلة على أساس افترض وجود عمل ايجابي، ولم يشترط القانون أن يتمّ التعطيل بواسطة طريقة معينة، فقد تكون تلك الطريقة معنوية أو مادية، تكون آلية التعطيل معنوية إذا حصلت على الكيانات المنطقية للنظام مثل المعطيات والبرامج، وتكون آلية التعطيل ماديّة إذا حصلت على الأجهزة الماديّة للنظام أو عطلت من الوصول إليها مثل تخزينها وذلك بقطع شبكات الاتصال أو كسارها أو تحكيم أسطوانة أو وقف وصول العاملين على الأنظمة [4].

خامسا/لاعتداء على أمن حماية التقنية:

يعرف التحايل على تدابير الحماية التقنية بأنه: "إبطال مفعول التدابير التكنولوجية التي أبدعها أصحاب الحقوق لحماية مصنفاتهم في البيئة الرقمية أو التحايل عليها أو تغيير المعلومات الضرورية لإدارة الحقوق، وذلك باستحداث آليات وأساليب تكنولوجية مضادة من شأنها المساس بحقوق المؤلفين وتعريض مصالحهم للخطر لأنه يتيح للغير

---

[1] جميلة سليماني، حق المؤلف في البيئة الرقمية بين الاعتداء والحماية، مجلة معارف للعلوم القانونية والاقتصادية، المركز الجامعي بريكة، المجلد 01، العدد 01، 2020، ص 70.

[2] إكرام مزراوي، القرصنة الرقمية كعائق تقني لنظام التقاضي الإلكتروني، مجلة البصائر للدراسات القانونية والاقتصادية، جامعة بوشعيب بلحاج عين تموشنت، المجلد 01، عدد خاص، ديسمبر 2021، ص 316.

[3] المرجع نفسه، ص 316.

[4] فوزية عبد الله، الآفاق المستقبلية لحقوق المؤلّف، رسالة ماجستير، جامعة بن يوسف بن خدة الجزائر -1-، كلية الحقوق، 2012/2013، ص 67.

الحصول على المصنفات الرقمية والاستفادة منها بدون دفع أي مقابل مالي لأصحاب الحقوق"[1]، وتتمثل صور الاعتداء على التدابير التقنية، فيما يلي[2]:

1. تصميم برامج حاسوب لغرض التحايل أو التعطيل أو الإبطال.
2. أعمال التوزيع أو الاستيراد لأغراض التوزيع أو الإذاعة أو النقل إلى الجمهور مصنفات أو نسخ من مصنفات.
3. تعطيل دون وجه حق لأي حماية تقنية أو معلومات إلكترونية تستهدف تنظيم وإدارة الحقوق المقررة قانونا.
4. أعمال الصنع أو الاستيراد أو عرض لغايات البيع أو التأجير أو حاز لأي غاية تجارية اخرى تم تصميمها أو انتاجها أو استعمالها لغايات التحايل على التدابير التقنية الفعالة أو ابطال أو تعطيل أي منها[3].

الفرع الثالث: وسائل القرصنة الإلكترونية

تطورت وسائل القرصنة الإلكترونية للمصنفات الرقمية بشكل مخيف وهذا ما يجعل من الصعب علينا تحديد جميع الوسائل، لكن سوف نبرز أهمها من خلال:

أولا/ حصان الطروادة Trojan horse

يعتبر حصان الطروادة[4] برنامجا يضعه القرصان مخبأ داخل البرامج العادية لمنشأة ما. ويعمل الكمبيوتر بصورة عادية، ويصبح البرنامج مخبأ للبيانات التي جمعها، ويجري تعديلات سرية في الملفات والبرامج، ويدمر أو يمحو البيانات أو حتى يسبب إغلاقا كاملا. ويمكن أن تبرمج أحصنة الطروادة لتدمير كل آثار وجودها بعد التنفيذ [5].

ثانيا/ البرامج الخبيثة Malware

تسمى البرامج الخبيثة ببرامج ضارة أو البرمجيات الماكرة وهي اختصار لكلمتين (Software) و (Malicious)، برزت البرامج الخبيثة إلى العلن بعد الشروع في استعمال الحاسبات بفترة قصيرة وتستهدف أهداف مختلفة فمنها ما يهادف إلى الاستيلاء والاحتيال عن طريق الحاسبات على المال، ومنها ما يسعى لتمييز ومن أخطرها البرامج الذي يسعى لإدخال أوامر إلى الحاسوب لتحقيق أهداف الإجرامية [6].

ثالثا/ الفيروسات virus

---

(1) مقابلة نبيل زايد، حماية حقوق النشر الالكتروني وفقا للقانون الأردني دراسة المقارنة، المؤتمر الدولي الأول: المكتبات ومراكز المعلومات في بيئة رقمية متغيرة، جمعية المكتبات والمعلومات الأردنية بالتعاون مع جامعة البلقاء التطبيقية، الأردن، 2013، ص 260.

(2) عبد الكريم صالح عبد الكريم، تدابير الحماية التكنولوجية ودورها في حماية المصنفات الرقمية دراسة تحليلية مقارنة، مجلة الحق، جمعية الإمارات للمحامين والقانونيين إدارة البحوث والدراسات، العدد 17، سنة 2013. ص 123.

(3) أنظر المادة 54 من قانون حماية حق المؤلف الأردني والمادة 181 من القانون حماية حقوق الملكية الفكرية المصري.

(4) أعده روبرت موريس (طالب دكتوراه في علم الكمبيوتر) بجامعة كورنيل سنة 1988، الذي أطلق عليه اسم (Internet) نسبة إلى شبكة الأنترنت وأسماه آخرون باسم دودة موريس حيث أراد أن يثبت فعالية الإجراءات الأمنية القائمة لحماية الكمبيوتر.

(5) هداية بوعزة، النظام القانوني للدفع الالكتروني دراسة مقارنة، أطروحة الدكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد –تلمسان- 2019/2018، ص 375.

(6) فوزية عبد الله، المرجع السابق، ص 68.

تستعمل كلمة فيروس في مجال المعلوماتية، تسبب إتلافا لأنظمة المعالجة الآلية للمعلومات والمعطيات وهي تتسبب في تعطيل أجهزة الكمبيوتر أو إتلاف المكونات المنظمة للحاسب الآلي، أو تعطيل الشبكات عن تأدية عملها [1] وتعرف من الناحية التقنية بأنها "عبارة عن مجموعة من التعليمات التي تتكاثر بمعدل سريع جداً وتصيب النظام المعلوماتي بالشلل، ويعد الفيروس خلية مغنطيسية قائمة ومبرمجة تنشط في وقت محدد لتخريب البرنامج الأصلي وتنتشر في الأجهزة الأخرى التي تتضمنها الشبكة بحيث تفسر ما تحتويه من معلومات"[2].

رابعا/ القنبلة المعلوماتية Bomb informatic

هي برامج يتم إعداده وتثبيته داخل النظام المعلوماتي بغرض تدمير أو تعطيل البيانات التي يحتويها ويشمل على قنابل المنطقة وقنابل الزمنية تبقى ساكنة لمدة زمنية طويلة وقد يشمل البرنامج تاريخ معين بحيث يفعل البرنامج عند حلوله، وهذه المدة يحددها عادة مؤشر زمني مهامه التهديم وقد لا يرتبط مؤشر التفجير بالزمن، وإنما بشروط منطقية معينة داخل نظام التشغيل أو داخل برنامج أو ملف وذلك حسبما يحدده مبرمج القنبلة [3]، وعليه يمكن تحديد نوعين من القنبلة المعلوماتية هما:

1- القنبلة المنطقة bomb Logique: هي برنامج أو جزء منه ينفذ في لحظة محددة، يتم وضعه في شبكة المعلومات بهدف تحديد ظروف أو حالة أو فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع [4].

2- القنبلة الزمنية time bomb: وهي قريبة من القنبلة المنطقية وتسمح بتحريك أحداث مستقبلية في تاريخ محدد أو لوقوع أحداث معينة [5].

المبحث الثاني: دور التشفير الإلكتروني في حماية المصنفات الرقمية

يعد التشفير علم قائم بذاته ولد منذ القدم كان يستعمل في الأمور العسكرية لضمان سرية الرسائل والمعلومات المرسلة، وأصبح يشكل وسيلة حديثة لحماية أمن المعلومات، ويستعمل أيضا حاليا كتدبير تكنولوجي لمجابهة القرصنة نظرا لخصائصه وفاعليته العالية الكفيلة بضمان حماية المصنف الرقمي، وعليه سوف نتطرق في هذا المبحث إلى ما يلي:

المطلب الأول: مفهوم التشفير الإلكتروني

هي كلمة يونانية (إغريقية) وتسمى بالترميز تعني باللغة بالإنجليزية Encryptions، ويقصد بها الكتابة السرية وقد تعددت التعريفات الممنوحة للتشفير سواء من الناحية الفقهية أو من الناحية القانونية.

الفرع الأول: التعريف الفقهي

---

[1] هداية بوعزة، المرجع السابق، ص 374.

[2] عبد الكريم فوزي القدومي، أثر قانون المعاملات الإلكترونية الأردني على عمليات البنوك، أطروحة دكتوراه، كلية الدارسات العليا، جامعة عمان العربية للدراسات القانونية العليا، للأردن، 2005، ص 254.

[3] أمال قارة، الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر -1-، 2001-2002، ص49.

[4] عبير بعقيقي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي –دراسة مقارنة-، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2018/2017، ص 35.

[5] المرجع نفسه، ص35.

على الصعيد الفقهي يعرف التشفير على أنه:" أي تغيير أو تحويل أو تعديل في البيانات و/أو المعلومات و/أو الرسائل عبر استخدام رموز أو إشارات غير متداولة ولا تكون معلومة إلا لمن يملك فك الرمز بحيث تصبح المعلومات عند تشفيرها غير مفهومة أو غير مقروءة لحين القيام بعملية عكس التشفير من خلال البرامج والأجهزة المعدة لهذه الغاية، بحيث تشكل التقنية وسيلة لحماية المعلومات أثناء انتقالها عبر الشبكة المعلوماتية، ولا يتحقق فهمها أو قراءتها إلا بعد فك رموزها من خلال منظومة أو برامج خاصة لدى مستقبل هذه المعلومات بحيث يضمن التشفير سلامة المعلومة وموثوقيتها"[1].

كما عرفه الأستاذ ليونال بوشرباغ بأنه: "مجموعة من التقنيات التي تهدف إلى حماية المعلومات، عن طريق استعمال بروتوكولات سرية، تجعل البيانات مشفرة غير مفهومة لدى الغير، بواسطة البرامج المخصصة لذلك"[2].

وعليه يمكن تعريف التشفير في مجال حماية المصنفات الرقمية من القرصنة الإلكترونية أنه: هو تدبير تكنولوجي يهدف لحماية المصنفات الرقمية من القرصنة، عن طريق استخدام رموز وإشارات وأرقام وحروف تجعل البيانات مشفرة غير مفهومة للغير، تكبح الاستعمال غير المشروع للمصنف إلا لمن يملك فك الشفرة بناء على ترخيص أصحاب الحقوق، وغالبا ما تكون بناء على مقابل مادي.

ومن التعريف السابق نستنتج ما يلي

1- أن التشفير يقوم على أساس خوارزميات معقدة وآمنة، باستخدام رموز أو إشارات غير متداولة ولا تكون معلومة إلا لمن يملك فك الرمز.

2- تحويل المصنف الرقمي المحمي الواضح إلى مصنف رقمي غير واضح.

الفرع الثاني: التعريف القانوني

تناول الاتحاد الأوروبي التشفير الإلكتروني في توجيهه رقم 1993/1999 بشأن الإطار الأوروبي للتوقيع الالكتروني، فعرف الشخص الذي يتولى عملية التشفير بأنه: " كل شخص طبيعي أو اعتباري يقدم شهادات الصحة والتوثيق والخدمات الأخرى المتعلقة بالتوقيع الالكتروني"[3].

أما المشرع الفرنسي فقد عرف التشفير الإلكتروني في نص المادة 22 من قانون 90-1170[4] "يفهم من خدمات التشفير كل الخدمات التي تهدف الى تغيير البيانات أو الإشارات الواضحة الى بيانات أو إشارات غير مفهومة من طرف الغير بفضل برامج ومعدات مخصصة لهذا الغرض".

أما المشرع الجزائري فقد استعمل مصطلح الترميز بدل مصطلح التشفير، وذلك في نص المادة 14 من المرسوم التنفيذي رقم 98-257، المتعلق باستغلال خدمات الانترنت المعدل والمتمم دون ذكر تعريف له.

---

[1] عبد الكريم فوزي القدومي، المرجع السابق، ص 276.

[2] Lionel BOCHURBERG, Internet et commerce électronique ,2 éd., DELMAS, paris, 2001, p 155et 156.

[3] Directive CE/93/1999 Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, N° : o.j l013 du 01-19-2000.

[4] Loi N° 90-1170 du 29/12/1990 sur la réglementation de la télécommunication, J.O. de la République Française, N° 303, du 30/12/1990.

وتجدر الإشارة أيضا أن المشرع الجزائري لم يأت بتعريف للتشفير الإلكتروني، لكنه عرف مفتاح التشفير الخاص والعام في القانون المتعلق بالتوقيع والتصديق الإلكترونيين[1] في المادة الثانية ف 08 و09 على التوالي، وكان من الأجدر على المشرع معالجة التشفير بشكل أكثر تفصيل من خلال تناول جوانبه القانونية وأحكامه لضمان أمن وسلامة المعلومات المشفرة في ظل التطور التكنولوجية الكبير وما صاحبها من تزايد الاعتداءات في الفضاء الرقمي.

الفرع الثالث: طرق ومستويات التشفير الإلكتروني

تعتمد قوة وفعالية التشفير[2] على عاملين أساسيين هما الخوارزمية وطول المفتاح، ويعد فك التشفير عبر إعادة تحويل البيانات إلى صياغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشفرة.

أولا/ طرق التشفير الإلكتروني

1. التشفير باستخدام المفتاح المتماثل

عرف التشفير المتماثل بأنه: "التشفير الذي يستعمل فيه صاحب الرسالة المفتاح الخاص ذاته لإنشاء الترميز ولفكه بعد الاتفاق المسبق مع المرسل إليه على كلمة السر بينهما"[3].

كما عرفه أيضا المشرع الجزائري في القانون المتعلق بالتوقيع والتصديق الإلكترونيين في نص المادة 2 ف 9 بقوله: "مفتاح التشفير الخاص: هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا المفتاح بمفتاح التشفير العمومي".

هذا النوع من أشهر الأنواع التشفير الإلكتروني استعمالا في تشفير البيانات والمعلومات، فهي تكفل تحقيق الأمان والتصدي لأي اعتداء على البيانات المشفرة إلكترونيا، ذلك أنها ترتكز المعادلات الخوارزمية متنوعة ذات مستوى عالي مما أكسبها صيتا عالميا، فأصبحت من أشهر طرق تشفير البيانات والمعلومات المستعمل في المجال الالكترونية [4].

2. النظام التشفير غير المتماثل

تسمى هذه الطريقة بالهندسة العكسية أو بالمفتاح العام، وعرف أيضا المشرع الجزائري في نص المادة 2 ف 9 من القانون المتعلق بالتوقيع والتصديق الإلكترونيين بقوله أنه: "المفتاح التشفير العمومي: هو عبارة عن سلسلة من

---

[1] القانون رقم 15-04، المؤرخ في 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، العدد 06، الصادر في 10 فبراير 2015.

[2] يخضع التشفير إلى مجموعة من ضوابط تنظمه تمثل فيما يلي:

1- احترام سرية البيانات المشفرة.
2- الحق في خصوصية البيانات المشفرة المرسلة عبر الانترنت واحترام سريتها.
3- مشروعية تشفير البيانات والمعلومات.
4- اعتبار النص المشفر محرر إلكترونيا.
5- تحديد الجهات المختصة باستخدام التشفير.

[3] عبد الرحمان بليلة، الإثبات والتوقيع الإلكتروني وسيلة لحماية العقد التجاري الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج البويرة، 2017، ص88.

[4] اسيا بوعمرة، النظام القانوني للتجارة الالكترونية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر 1، الجزائر، 2013/2012. ص197.

الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني".

هذه الطريقة من التشفير تعتمد على مفتاحين، فالأول عبارة عن مفتاح عام متاح للجميع يتم استعماله في عملية التشفير، أما الثاني فهو مفتاح خاص غير متاح أي سري لا يعلمه إلا شخص مرسل الرسالة، فرغم تباين المفتاح الخاص عن العام كونه متاح ومعروف إلكترونيا لأكثر من جهة إلا أنهما متكاملان ومترابطان في عملهما، فإذا استخدم المفتاح الخاص لتشفير الرسالة فلا يمكن فتحها إلا بالمفتاح العام، كما أنه لو أحد المفتاحين عرف فلا يحتمل معرفة المفتاح الثاني حسابيا [1].

3. **التشفير المزدوج:**

معناه "استعمال نظام خليط بين نظام التشفير المتماثل وغير المتماثل من طرف المرسل والمرسل إليه، وفيه يتم تشفير المفتاح الخاص بمفتاح عام، وإرسال كل من الرسالة المشفرة والمفتاح الخاص المشفر إلى المرسل إليه باستخدام أية شبكة اتصالات"[2]، وتقوم على الخطوات التالية [3]:

- تشفر الرسالة الأصلية المبعوثة من المرسل الى المرسل اليه بالمفتاح الخاص.
- يشفر المفتاح المتماثل أيضا عن طريق المفتاح العام للمرسل اليه ثم يتم بعث الرسالة المشفرة.
- بعد تلقي المفتاح المتماثل بالمفتاح العام الذي يملكه المرسل عليه يعمل بفك شفرة المفتاح المتماثل المشفر باستعمال المفتاح الخاص ومنه يمتلك المفتاح المتماثل الذي تم استخدامه والذي شفرت به الرسالة الأصلية.
- وأخيرا يعمل المرسل اليه بعد فك شفرة المفتاح المتماثل باستعمال هذا الأخير في فك الرسالة المشفرة.

ثانيا/ مستويات التشفير الإلكتروني

1- **نظام الشبكة الافتراضية:** تعتبر شبكة الأنترنت وسيط لتحويل البيانات والمعلومات من نقطة الإرسال إلى نقطة الموجهة لها، ويكن القول أنه وسيلة آمنة لتبادل تلك المعلومات والبيانات على جزء من هذه الشبكة[4].

2- **التشفير على مستوى الإرسال:** في هذا المستوى يتم تشفير جميع البيانات والمعلومات وذلك من نقطة الإرسال إلى غاية نقطة الاستقبال، ويعمل هذا المستوى بواسطة الشبكات الافتراضية الخاصة [5].

3- **التطبيق المستخدم في تنفيذ:** يستخدم للتشفير الجزئي من أهم نماذجه نظام "SET" وهو نظام خاص لتشفير البيانات والمعلومات وتأمين المعاملات الالكترونية[6].

---

[1] علي نابت أعمر، الملكية الفكرية في إطار التجارة الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري -تيزي وزو-، 2014، ص 64.

[2] المرجع نفسه ص 64 و65.

[3] اسيا بوعمرة، المرجع السابق، ص199.

[4] عثمان بقنيش، التحكيم الإلكتروني في تسوية منازعات التجارية الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس مستغانم، 2016-2017، ص 189.

[5] علي نابت أعمر، المرجع نفسه ص65.

[6] عثمان بقنيش، المرجع نفسه، ص 190.

4- **التشفير على مستوى التصفح أو التنقل:** من أجل حماية البيانات والمعلومات أثناء تحويلها عبر الشبكة يتم تشفير جميع الاتصالات في هذا المستوى سواء تلك التي تتم بين فتحات الشبكة، أو برامج المواقع أو التصفح الموجودة عليها، مما يؤدي إلى حماية المعلومات والبيانات أثناء انتقالها[1].

5- **التطبيق المستخدم في تنفيذ:** يستخدم للتشفير الجزئي من أهم نماذجه نظام "SET" وهو نظام خاص لتشفير البيانات والمعلومات وتأمين المعاملات الالكترونية[2].

المطلب الثاني: أثر التشفير الإلكتروني على المصنفات الرقمية

رغم أن التشفير يقوم بتوفير الحماية التقنية إلا أنه ينتج أثار، وهو ما سوف نتناوله فيما يلي

الفرع الأول: أثر التشفير الإلكتروني على استثناء النسخة الخاصة:

إن التطورات التكنولوجية الهائلة والتنامي المتزايد لوسائل النسخ الحديثة، ورغم فرض مقابل مالي لنسخة الاستعمال الشخصي [3]، إلا أن التشفير الإلكتروني لم يحقق حماية ناجعة وفعالة للمصالح المادية لأصحاب الحقوق والمؤلفين في البيئة الرقمية، ومن ثمة إن قيام مستخدمي الفضاء الرقمي بنسخ العديد من المصنفات أثناء إبحارهم في شبكة الأنترنت مستندين في ذلك إلى استثناء النسخة الخاصة في تبرير عمليات النسخ الهائلة، دفعت أصحاب الحقوق إلى المبادرة باتخاذ التشفير لحماية إبداعاتهم، والتي من خلالها لا يمكن استخدام المصنف لتحقيق فعل النسخ عليها [4].

وهو الإتجاه الذي نادى بيه تيار من الفقه والذي اتبعته القانون المصري والقوانين الوطنية المقارنة وكذا الاتفاقيات الدولية كوسيلة وحيدة للتحكم في عدم الامكانية في تحقيق عمليات النسخ المتكررة، كما يرى جانب أخرى من الفقه في هذا الصدد أن حماية المصنفات عن طريق التشفير الإلكتروني من شأنه أن يلغي الحق في النسخة الخاصة وهو ما يتنافى والاستعمال العادل للمصنف [5]، كما أنه يخدم بالدرجة الأكبر منتجي المصنفات الرقمية ولا علاقة له بحماية الملكية الأدبية والفنية"[6].

---

[1] علي نابت أعمر، المرجع السابق، ص66.

[2] عثمان بقنيش، المرجع السابق، ص 190.

[3] يقصد بالنسخة الخاصة الرقمية تلك النسخة الوحيدة التي تؤخذ عن المصنف المحمي، ويتم تخزينها رقمياً على جهاز الحاسب الآلي لشخص الناسخ

1- أن يكون المصنف المراد عمل نسخة منه قد سبق نشره.
2- أن يكون الاستنساخ للاستعمال الشخصي البحت للناسخ.
3- عدم الإضرار بالمصالح المشروعة للمؤلف.

أنظر عبد الكريم صالح عبد الكريم، المرجع السابق، 136.

[4] خديجة يحيى باي، النسخة الخاصة في نظام حق المؤلف والحقوق المجاورة دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة وهران، 2019، ص64.

[5] ساند القضاء الفرنسي هذا الاتجاه في قضية مولولوند درايفر (Mulholland Drive) والتي تتلخص وقائعها في قيام شخص يدعى ستيفان بشراء فيلم مولولوند درايفر مثبت على قرص فيديو رقمي، ثم أراد أن يعمل نسخة خاصة منه لمشاهدته على جهاز الفيديو، ونتيجة لوجود التدابير التكنولوجية على قرص فيديو لم يتمكن من إنجاز هذه النسخة خاصة بيه، وهو ما اعتبره اعتداء على حقه في عمل النسخة المخصصة للاستعمال الخاص المقررة له بموجب المادة L122-5 من قانون الملكية الفكرية، رحبت محكمة الإستئناف في قرارها الصادر بتاريخ 22/ 2005/04 بطلبات المتضررين وحظرت على الشركات المدعى عليها استخدام التدابير التكنولوجية لمنع عمل نسخة من DVD خاصة و أنا المستهلك قد وصل إلى المصنف بطريقة مشروعة. أنظر أسماء بن لشهب، وسائل الحماية القانونية لحق المؤلف والحقوق المجاورة على شبكة الإنترنت، أطروحة دكتوراه، جامعة الإخوة قسنطينة، كلية الحقوق، 2019/2018، ص 302.

[6] خديجة يحيى باي، المرجع نفسه، ص 64و65.

وعموما يمكن القول إن وضع التدابير التكنولوجية المتمثلة في التشفير الإلكتروني وإن كان أمر جائز كوسيلة قانونية لحماية المصنفات الرقمية من القرصنة فإنه يجب ألا يعرقل الاستفادة من النسخة الخاصة المقررة قانونا، وهذا الاتجاه الذي تبناه المشرع الجزائري بموجب نص المادة 41 من الأمر 05-03 "يمكن استنساخ أو ترجمة أو اقتباس أو تحوير نسخة واحدة من مصنف بهدف الاستعمال الشخصي أو العائلي ...".

الفرع الأول: أثر التشفير الإلكتروني على الطبيعة الحقوقية لحق المؤلف

إن صاحب الحق بلجوئه إلى التشفير الإلكتروني يهدف إلى إنشاء رابطة فردية مع كل مستعمل، يصبح فيها كل استغلال للمصنف الرقمي تحت تحكم الكامل لصاحب الحق. فتحكمه لم يعد محددا على التصرفات المتعلقة بنشر المصنف الرقمي للجمهور عامة، بل أصبح يتحكم بوصول المصنف لأفراد محددين من الجمهور. فعلى سبيل المثال المحطة التلفزيونية غير مشفرة التي تشمل البث لجمهور بحيث يمكن لجميع لأفراد الجمهور الاستمتاع بها، أما بث المحطات التلفزيونية المشفرة فيشمل فقط الأفراد المشتركين مع هذه المحطة فقط [(1)].

ويعني هذا أن إرادة المشرع وإرادة أصحاب الحقوق مشتركة هم الذين يقررون وضع أو عدم وضع التشفير الإلكتروني على المصنف، فيكون هؤلاء هم من يقررون عدم وجود أو وجود الاستثناءات، وهم من يقررون طرق انتفاع الجمهور بالمصنف وإن تخطى الحدود التي رسمها المشرع لهذه الحماية، وهذا الفعل يطلق عليه الفقه بالتنظيم الذاتي لحق المؤلف، فالمشرع إنما يؤكد إرادة أصحاب الحقوق بمنعه التحايل على التشفير الذي تستخدم للمنع أو الحد من القيام بأعمال غير مرخص بها [(2)].

الخاتمة:

من خلال الورقة البحثية، يمكن القول إنه في ظل التطور التكنولوجية وما صاحبه من ظهور القرصنة الإلكترونية كأحد أبرز تجليات السلبية للعصر الحديث والتي تمتاز بتطور أساليب ممارستها خاصة مع صعوبة ترك أثر لها أو اكتشافها، مما شكل صعوبة للدول حتى أشدها تقدما ولعل أبرز مثال في وقتنا الحالي قضية برنامج بيغاسوس الذي استهدف قرصنة هواتف رؤساء دول العالم أبرزهم الرئيس الفرنسي دون استطاعة على كشفه.

ولما باتت القرصنة تشكله خطر داهما على الملكية الفكرية في البيئة الرقمية والتي تمتاز أصلا بانتشار الجريمة المعلوماتية، خاصة في ظل قصور الحماية القانونية التقليدية (الحماية القضائية، والحماية المؤسساتية) عن ضمان الحماية الفعالة والكاملة، وهو ما كبد أصحاب الحقوق خسائر مالية كبيرة نتيجة لاستغلال المصنفات الرقمية بطريقة غير شرعية دون دفع مقابل مالي لهم (الاستعمال الشخصي، عرضه للبيع)، وهو ما أثر بشكل كبير على الإنتاج الفكري.

وعليه كان لزاما على المؤلفين أخذ المبادرة بأنفسهم عن طريق استعمال آليات حديثة تكبح القرصنة الإلكترونية لتضمن حقوقهم وتقيد استعمال المصنف الرقمي بشكل غير مشروع، فبرز التشفير الإلكتروني كآلية فعالة، من خلال استعمال حروف ورموز المعقدة التي يصعب على القرصان حلها، بما يضمن الأمان والثقة لدى المؤلفين وأصحاب الحقوق وتجعلهم يتحكمون بالمصنف بتحديد مدة ووسيلة الاطلاع، بحيث تسعى هذه التقنية إلى تحقيق مجموعة من وظائف

(1) سوفالو أمال، حماية الملكية الفكرية في البيئة الرقمية، أطروحة دكتوراه، كلية حقوق، جامعة يوسف بن خدة الجزائر -1-، 2017 ص 315

(2) المرجع نفسه، ص 316.

تتمثل في التكاملية وتوفير البيانات والسرية، مما يجعلها وسيلة هادفة إلى ضمان حفظ الخصوصيات وتكرس أمن المعلومات.

ورغم المكانة البارزة للتشفير الإلكتروني كتدبير تكنولوجي أثبت فاعليته، إلا أننا سجلنا بعض النقائص تتمثل في:

1- أن للتشفير الإلكتروني لم يحظى بالتنظيم القانوني اللازم، حيث لا يملك إطار تشريعي خاص سواء المستوى الوطني أو الدولية الذي يعكس أهميته في مجال حماية المصنفات الرقمية

2- أنه يقيد الحق في النسخة الخاصة للاستعمال الشخصي والعائلي.

3- أن المصنف الرقمي الذي سقط حمايته القانونية لسبب من الأسباب (انتهاء مدة الحماية) وبالتالي أصبح من الملك العام، يمكن لأصحاب الحقوق أن يواصلوا أو يضعوا التشفير الإلكتروني للمصنف لتقيد الوصول إليه، وهو ما يشكل خرق لحق الجمهور في استعماله.

4- كما يحتاج باستمرارية إلى تحديث مستمر من الناحية التقنية، مع التطور المتزايد لأساليب وطرق القرصنة.

إزاء هذه النتائج وتداعياتها فإننا نوصي بما يلي:

1- تكثيف الجهود الدولية لمكافحة القرصنة الإلكترونية للمصنفات الرقمية، من خلال استحداث اتفاقيات ومعاهدات دولية تضمن توحيد الجهود وتكثيف العمل المشترك الدولي لمجابهتها.

2- يتعين إضفاء الحماية القانونية من خلال تجريم القرصنة الإلكترونية عبر تعديل القانون 03-05 المتعلق بحق المؤلف والحقوق المجاورة، نظرا لخصوصيتها التي تميزها عن الجرائم المعلوماتية المنصوص عليها في قانون العقوبات، ولضمان تنفيذ التزامات معاهدتي الويبو الأولى (المادة 11) والثانية (المادة 18) التي صادقت عليهما الجزائر.

3- لا بد من وضع سياسية وطنية للتشفير الإلكتروني، من خلال استحداث تشريعات لتبيان أحكامه وتنظيمه في ظل الفراغ التشريعي الحالي، وتدعيم الأبحاث التقنية والقانونية الرامية لتطويره قصد ضمان فاعليته.

4- كما يجب وضع آليات قانونية وتقنية تضمن حق المستهلك الإلكتروني في نسخة خاصة للاستعمال الشخصي أو العائلي، بما يتماشى مع القاعدة العامة الواردة في المادة 41 من قانون 03-05 المتعلق بحق المؤلف والحقوق المجاورة.

5- لا بد من وجود آليات قانونية تفرض على أصحاب الحقوق أن يكون وضع أو استمرار وضع التشفير مقترن بوجود الحماية القانونية، لكي يتمكن الجمهور من استعمال العادي للمصنف دون حاجز يمنعه من ذلك.

6- استحداث هيئة وطنية تعنى بتنظيم التشفير الإلكتروني لضمان أمن المعلومات في الجزائر.

قائمة المراجع والمصادر:

1- التشريعات:

- **المعاهدات:**

1. معاهدة المنظمة العالمية للملكية الفكرية (الويبو) بشأن حق المؤلف، الموقعة بجنيف، في 20 ديسمبر 1996، صادقت عليها الجزائر بموجب المرسوم الرئاسي رقم 13 -123، المؤرخ في 3 أبريل 2013، ج ر، عدد 27، الصادرة في 22 مايو 2013.

2. الاتفاقية العربية لمكافحة جرائم تقنية المعلومات المحرّرة بالقاهرة بتاريخ 21 ديسمبر 2010، صادقت عليها الجزائر بموجب مرسوم رئاسيّ رقم 252-14، مؤرّخ في 8 سبتمبر 2014، ج ر، عدد 57، الصادرة في 28 سبتمبر 2014.

- **القوانين:**

1. القانون المتعلق بحماية حقوق الملكية الفكرية المصري، رقم 82 لسنة 2002، الجريدة الرسمية، العدد: 22 (مكرر)، 2002/06/02.

2. الأمر رقم 03-05، مؤرخ في 19 يوليو سنة 2003، يتعلق بحقوق المؤلف والحقوق المجاورة، ج ر، عدد 44، صادر في 23 يوليو سنة 2003.

3. القانون رقم 09-04 المؤرخ 5 غشت 2009، المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها ج ر، عدد 47، الصادرة في 15 غشت 2009.

4. القانون رقم 15-04، المؤرخ في 01 فبراير سنة 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج ر، العدد 06، الصادر في 10 فبراير 2015.

5. القانون المتعلق بمكافحة جرائم تقنية المعلومات المصري، رقم 175 لسنة 2018، الجريدة الرسمية لجمهورية مصر العربية، العدد 32 مكرر(ج)، 14 أوت 2018.

2- الكتب:

1. أحمد مختار عمر، معجم اللغة العربية المعاصرة، عالم الكتب، القاهرة، 2008.

3- الأطروحات والمذكرات:

❖ **أطروحات:**

1. أسماء بن لشهب، وسائل الحماية القانونية لحق المؤلف والحقوق المجاورة على شبكة الإنترنت، أطروحة دكتوراه، جامعة الإخوة قسنطينة، كلية الحقوق، 2019/2018، ص 302.

2. اسيا بوعمرة، النظام القانوني للتجارة الالكترونية دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر 1، الجزائر، 2013/2012.

3. اعمر يوسفي، التكنولوجيا الرقمية وحقوق المؤلف والحقوق المجاورة –دراسة وصفية تحليلية-، أطروحة دكتوراه، كلية العلوم السياسية والإعلام، جامعة بن يوسف بن خدة الجزائر -1-، 2009/2008.

4. أمال سوفالو، حماية الملكية الفكرية في البيئة الرقمية، أطروحة دكتوراه، كلية حقوق، جامعة يوسف بن خدة الجزائر -1-، 2017.

5. خديجة يحي باي، النسخة الخاصة في نظام حق المؤلف والحقوق المجاورة دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة وهران، 2019.

6. سعاد جواهرة، حماية الملكية الفكرية في البيئة الرقمية من خلال التشريع الجزائري والقانون الدولي دراسة وصفية تحليلية، أطروحة دكتوراه، كلية علوم الإعلام والاتصال، جامعة الجزائر -3-، 2017/2016.

7. عبد الكريم فوزي القدومي، أثر قانون المعاملات الإلكترونية الأردني على عمليات البنوك، أطروحة دكتوراه، كلية الدارسات العليا، جامعة عمان العربية للدراسات القانونية العليا، للأردن، 2005.

8. عبير بعقيقي، مكافحة الجريمة المعلوماتية في التشريعين الجزائري والإماراتي –دراسة مقارنة-، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2018/2017.

9. عزيزة رابحي، الأسرار المعلوماتية وحمايتها الجزائية، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد تلمسان، 2018/2017.

10. مليكة عطوي، الحماية القانونية لحقوق الملكية الفكرية على شبكة الأنترنت دراسة وصفية تحليلية، أطروحة دكتوراه، كلية علوم الإعلام والاتصال، جامعة دالي براهيم الجزائر -3-، 2010/2009.

11. نادية زواني، حماية الملكية الفكرية من التقليد والقرصنة -دراسة مقارنة-، أطروحة دكتوراه، كلية الحقوق، جامعة بن يوسف بن خدة – الجزائر-، 2013 -2012.

12. هداية بوعزة، النظام القانوني للدفع الالكتروني دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة أبو بكر بلقايد – تلمسان-، 2019/2018.

❖ **مذكرات:**

1. أمال قارة، الجريمة المعلوماتية، رسالة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر -1-، 2002-2001.

2. طه عيساني، الاعتداء على المصنفات الرقمية وآليات حمايتها، رسالة ماجستير، كلية الحقوق، جامعة يوسف بن خدة الجزائر 1، 2013/2012.

3. عبد الرحمان بليلة، الإثبات والتوقيع الإلكتروني وسيلة لحماية العقد التجاري الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة أكلي محند أولحاج البويرة، 2017.

4. عبد الكريم نعمان، الجرائم الإلكترونية وموقف المشرع الجزائري منها، رسالة ماجستير، كلية الحقوق، جامعة بن يوسف بن خدة الجزائر 1، 2017-2016.

5. عثمان بقنيش، التحكيم الإلكتروني في تسوية منازعات التجارية الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس مستغانم، 2016-2017.

6. علي نابت أعمر، نابت أعمر علي، الملكية الفكرية في إطار التجارة الإلكترونية، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري -تيزي وزو-، 2014،

7. فوزية عبد الله، الآفاق المستقبلية لحقوق المؤلّف رسالة ماجستير، جامعة بن يوسف بن خدة الجزائر -1-، كلية الحقوق، 2012/2013.

4- المقالات والمداخلات:

1. إكرام مزراوي، القرصنة الرقمية كعائق تقني لنظام التقاضي الإلكتروني، مجلة البصائر للدراسات القانونية والاقتصادية، لجامعة بوشعيب بلحاج عين تموشنت، المجلد 01، العدد الخاص، ديسمبر 2021.

2. جميلة سليماني، حق المؤلف في البيئة الرقمية بين الاعتداء والحماية، مجلة معارف للعلوم القانونية والاقتصادية، المركز الجامعي بريكة، المجلد 01، العدد 01، 2020.

3. طه عيساني، القرصنة الالكترونية الضرر الاقتصادية والفكرية، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي الجزائر، العدد 5، يوليو 2016.

4. عبد الكريم صالح عبد الكريم، تدابير الحماية التكنولوجية ودورها في حماية المصنفات الرقمية دراسة تحليلية مقارنة، مجلة الحق، جمعية الإمارات للمحامين والقانونيين إدارة البحوث والدراسات، العدد 17، سنة 2013.

5. كريمة خنوسي، الحماية الدولية من جرائم التقليد والقرصنة الإلكترونية وموقف المشرع الجزائري منها، مجلة مصداقية، المدرسة العليا العسكرية للإعلام والاتصال، المجلد 02، العدد 02، 2020.

6. مقابلة نبيل زايد، حماية حقوق النشر الالكتروني وفقا للقانون الأردني دراسة المقارنة، المؤتمر الدولي الأول: المكتبات ومراكز المعلومات في بيئة رقمية متغيرة، جمعية المكتبات والمعلومات الأردنية بالتعاون مع جامعة البلقاء التطبيقية، الأردن، 2013.

7. نور حسين علي الفهداوي، الآثار القانونية الناتجة عن انتهاك الوسائل التقنية لحماية المصنفات الرقمية "دراسة مقارنة"، المجلة الأكاديمية للبحث القانوني، جامعة عبد الرحمان ميرة بجاية، المجلد 12، العدد 02، 2021.

❖ **التشريعات باللغة الفرنسية:**

1. Directive CE/93/1999 Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques, N° : o.j l013 du 01-19-2000.

2. Loi n° 2006-961 du 1er Aout 2006 relative au droit d’auteur et aux droits voisins dans la société de l’information, JORF n° 178 du 03 aout 2006.

3. Loi n° 90-1170 du 29-12-1990 sur la réglementation des télécommunications, J.O.R.F N° 303 du 30-12-1990.

❖ **الكتب باللغة الفرنسية:**

1. Lionel BOCHURBERG, Internet et commerce électronique ,2 éd., DELMAS, Paris, 2001 .