

دور التشفير الإلكتروني في حماية النظام القضائي من الجرائم السيبرانية

*The role of electronic encryption in protecting
the judicial system from cybercrimes*



دحماني كمال^{1*}، قادري نور الهدى²

¹ جامعة تيسمسيلت- أحمد بن يحيى الونشريسي - ، الجزائر،

profdahmani@gmail.com

² جامعة جيلالي اليابس - سيدي بلعباس، الجزائر،

lnasse223@gmail.com

تاريخ الإرسال: 2024/09/15 تاريخ القبول: 2024/10/23 تاريخ النشر: 2024/12/01

ملخص: تعتبر تكنولوجيا الإعلام و الاتصال سلاحا ذو حدين ، فبرغم من آثارها الإيجابية التي مست مختلف القطاعات بما فيها قطاع العدالة ، وذلك من خلال طرح فكرة النزاع القضائي الإلكتروني عن طريق خلق ما يعرف بالمحاكم الإلكترونية ، إلا أنها في ذات الوقت تولدت عنها العديد من النتائج السلبية التي من شأنها تؤدي بالمساس بسلامة وأمن النظام المعلوماتي الخاص بهذه الأخيرة ، وذلك بسبب انتشار نوع جديد من الجرائم ألا وهي الجرائم السيبرانية ، الأمر الذي توجب على المشرع الجزائري على غرار باقي التشريعات على مساهمة التطورات التكنولوجية ، وذلك باتخاذ كافة الإجراءات والتدابير الكفيلة لحماية النظام المعلوماتي القضائي عن طريق تبنيه لفكرة النظام التشفير الإلكتروني نظرا للدور الرائد والفعال الذي يلعبه في التصدي ومكافحة الجرائم السيبرانية .

الكلمات المفتاحية: التشفير الإلكتروني؛ النظام القضائي؛ الحماية المعلوماتية؛ الجرائم السيبرانية.

Abstract: Information and communication technology is considered a double-edged sword. Despite its positive effects that have affected various sectors, including the justice sector, through the introduction of the idea of electronic judicial disputes by creating what is known as electronic courts, it has at the same time generated many negative results that may lead to harming the safety and security of the information system of the latter, due to the spread of a new type of crime, namely cybercrimes, which required the Algerian legislator, like other legislations, to keep pace with technological developments, by taking all measures and procedures to protect the judicial information system by adopting the idea of the electronic encryption system due to the leading and effective role it plays in confronting and combating cybercrimes.

Key words: electronic encryption; The judicial system ; information protection; Cyber crimes

مقدمة:

إن التطور العلمي والتكنولوجي المذهل الذي شهده العالم في الأونة الأخيرة من الزمن الذي أثر على المجتمع بصفة عامة وعلى المشرعين في القانون الداخلي والدولي بصفة خاصة، الأمر الذي دفع بالعديد من الدول العالم إلى التسابق لمواكبة هذه الموجة التكنولوجية الحديثة وتكنولوجيا المعلومات وتوظيفها للرقى في مختلف القطاعات خاصة في مجال تطوير المنظومة القضائية وذلك من خلال طرح فكرة النزاع القضائي الإلكتروني عن طريق خلق المحاكم الإلكترونية وإتباع كافة إجراءات التقاضي الإلكترونية.

إلا أنه يمكن اعتبار أن هذه التكنولوجيا تعد سلاحا ذو حدين، فهي بالإضافة إلى المزايا والوظائف المتعددة التي حققتها في تطوير وورقي بمختلف القطاعات والمجالات بما فيها المنظومة القضائية، فقد فتولدت عنها العديد من الآثار السلبية التي مست بأمن وسلامة البيانات والمعلومات الخاصة بالمتقاضين وكذا مختلف الملفات والمرسلات القضائية، وذلك بسبب ظهور وانتشار نوع جديد من الجرائم لم تكن معروفة سابقا ألا وهي الجرائم السيبرانية أو ما يطلق عليها بالجرائم المعلوماتية، وهو ما دفع بالمشرع الجزائري على غرار باقي المشرعين سواء على المستوى الوطني أو على المستوى الدولي إلى التدخل السريع لاتخاذ كافة الإجراءات والتدابير القانونية وكذا التقنية التي من شأنها التصدي لهذا النوع من الأفعال الإجرامية، عن طريق تبني ما يعرف بنظام التشفير الإلكتروني باعتباره آلية تقنية تهدف إلى توفير الحماية المعلوماتية للبيانات والمعلومات الخاصة بمتعاملي البيئة الرقمية بما فيها النظام المعلوماتي للجهاز القضائي.

وعليه يكتسي موضوع دور التشفير الإلكتروني في حماية النظام القضائي خاصة في ظل الظروف الراهنة بالغ الأهمية ذلك أن حماية البيانات والمعلومات الخاصة بالمتقاضين وكذا مختلف المراسلات القضائية تتميز بطابع السرية والخصوصية، وهو ما دفع الفضول لمعرفة أهميته ودوره في حماية هذه الأخيرة.

ونتيجة مما سبق؛ يطرح موضوع دراستنا العديد من الإشكاليات سواء كانت من الجانب القانوني أو الجانب التقني؛ وهو ما أثارنا إلى طرح الإشكال الآتي: فيما يتمثل دور التشفير الإلكتروني في حماية النظام القضائي خاصة في ظل عصر عرف بانتشار الجرائم السيبرانية؟

وللإجابة عن هاته الإشكالية ارتأينا تقسيم موضوع دراستنا إلى المبحثين الآتين هما:

- المبحث الأول: مفهوم التشفير الإلكتروني.

- المبحث الثاني: تقنية التشفير الإلكتروني كآلية حيمائية من الجرائم السيبرانية.

وسيتبع إتباع المنهج التحليلي الوصفي وذلك لمعرفة النظام القانوني للتشفير الإلكتروني ودوره في حماية النظام القضائي من مختلف الجرائم التي قد تمس بصحته وسلامته، كما تم الاستناد إلى المنهج الاستقرائي من خلال استقراءنا لبعض النصوص القانونية ذات صلة بموضوع الدراسة.

المبحث الأول

مفهوم التشفير الإلكتروني

إن مفهوم التشفير بصفة عامة ليس حديثاً فالكتابة المشفرة واستخدام الشيفرات في المراسلات موجودة منذ زمن طويل، إذ كانت تستعمل للأغراض العسكرية والاستخباراتية وغيرها من الأغراض التي كانت تقدرها الدول، بالنظر إلى أهمية المعلومات المتبادلة¹، ظهر التشفير كإجراء من إجراءات الأمان للحفاظ على أمن وسرية هذه الأخيرة.

ونظراً لأهمية التشفير الإلكتروني باعتباره من أنجع التقنيات التكنولوجية الحديثة لحماية مختلف التعاملات الإلكترونية وتأمين الأنظمة الإلكترونية بما فيها النظام القضائي الإلكتروني وحمايته من أي تلاعب أو اختراق إلكتروني، فإنه لبيان حقيقة هذه التقنية المستحدثة فإنه لا بد في البداية وقبل كل شيء التعرف على هذه التقنية وذلك من خلال:

المطلب الأول: تعريف التشفير الإلكتروني وضوابط استخدامه

يعتبر التشفير الإلكتروني في مقدمة الوسائل والأدوات الإلكترونية الحديثة والمستعملة لحماية مختلف التعاملات الإلكترونية خاصة في ظل انتشار التجارة الإلكترونية كما أصبحت من بين الوسائل التقنية التي أصبح يُعتمد عليها لحماية البيانات والمعلومات الخاصة بمتعاملي البيئة الافتراضية بما فيها البيانات الخاصة بالمتقاضين وملفاتهم الخاصة.

الفرع الأول: تعريف التشفير الإلكتروني

لقد تباينت التعريفات التي أعطيت للتشفير الإلكتروني بين ما هو فقهي وما هو تشريعي وذلك من خلال:

¹ - موسى حسن فضالة، التنظيم القانوني للإثبات الإلكتروني - دراسة مقارنة - الطبعة الأولى، دار السنهوري، لبنان، 2016، ص 232.

أولاً: التعريف الفقهي للتشفير الإلكتروني

لقد اتجه الفقه إلى تعريف التشفير على أنه "تحويل المعلومات إلى رموز وإشارات غير مفهومة لمنع الأشخاص غير المرخص لهم من الاطلاع عليها أو فهمها"¹.

كما يعرف على أنه "عبارة عن تقنية تعتمد على المعادلات الرياضية التي تسمح لمن يمتلك مفتاحاً سرياً أن يحول الرسالة من رسالة مقروءة إلى رسالة غير مقروءة"².

كما عرف جانب آخر من الفقه التشفير الإلكتروني على أنه: "عملية تمويه الرسالة بطريقة تخفي محتواها وتجعلها رموزاً غير مقروءة، أو أنه علم الكتابة السرية وعدم فتح شفرة هذه الكتابة من قبل غير المخولين"³.

كما يعرفه البعض على أنه: "مجموعة من التقنيات التي تسمح بحماية المعلومات من أيّ تعديل غير مرغوب فيه أو الحفاظ على خصوصيتها من أيّ اختراق بفضل الاستعانة برموز خاصة يطلق عليها تسمية المفاتيح"⁴.

وعليه يمكننا القول من خلال التعاريف السابقة؛ أن التشفير الإلكتروني آلية تقنية حديثة تقوم على تحويل البيانات والمعلومات الخاصة بالمتقاضين من بيانات مقروءة مفهومة إلى رموز وإشارات غير مقروءة التي تجعل من عملية إطلاع عليها أو التلاعب بها من طرف الغير مستحيلاً.

ثانياً: التعريف التشريعي للتشفير الإلكتروني:

أجازت أغلبية التشريعات استعمال التشفير في مجال المعاملات الإلكترونية عبر شبكة الانترنت ولقد نظمتها نصوص قانونية خاصة بالمعاملات الإلكترونية.

لقد أشار قانون الأونسترال بشأن التوقيعات الإلكترونية إلى أن التشفير هو "فرع الرياضيات التطبيقية الذي يعني بتحويل الرسالة إلى أشكال تبدو غير مفهومة ثم إعادتها إلى أشكالها الأصلية"⁵.

¹ - آزد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني - دراسة مقارنة -، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2016، ص 82.

² - موسى حسن فضالة، المرجع السابق، ص 232.

³ - زينب غريب، إشكالية التوقيع الإلكتروني وحجته في الإثبات، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد الخامس، السويسي، الرباط، 2010/2009، ص 68.

⁴ - عمير حسن المؤمني، التوقيع الإلكتروني وقانون التجارة الإلكترونية، دار وائل، عمان الأردن، دون طبعة، 2003، ص 54.

⁵ - البند 32 من دليل الإشتراع قانون الأونسترال بشأن التوقيعات الإلكترونية، الصادر عن لجنة الأمم المتحدة للقانون التجاري الدولي لعام 2001.

حيث عرّف المشرع الفرنسي ضمن نص المادة 28 من القانون رقم 1170/90 المؤرخ في 1990/12/29 بشأن تنظيم الاتصالات عن بعد، أدوات التشفير بأنها "التقديرات التي تهدف إلى تحويل معلومات مقروءة إلى معلومات وإشارات غير قابلة للقراءة والفهم". ولقد سمح هذا القانون للمشروعات الصغيرة، والأفراد باستخدام التشفير بعد أن كان قاصراً على المجالات العسكرية والحكومية فقط،¹ وفي 24 فبراير 1998 صدر المرسوم رقم 98 / 101 المحدد لضوابط استخدام التشفير.

كما عرف المشرع المصري التشفير الإلكتروني ضمن قانون التجارة الإلكتروني المصري بأنه: "تغيير في شكل البيانات عن طريق تحويلها إلى رموز أو إشارات لحماية هذه البيانات من الإطلاع الغير عليها أو من تعديلها أو تغييرها"²، كما عرفه ضمن لائحة قانون التوقيع الإلكتروني المصري على أنه: "منظومة تقنية حسابية تستخدم مفاتيح خاصة لمعالجة وتحويل البيانات والمعلومات المقروءة إلكترونياً بحيث تمنع استخلاص هذه البيانات والمعلومات إلا عن طريق استخدام مفتاح أو مفاتيح فك الشفرة".

أما بالنسبة للمشرع الجزائري فنلاحظ أنه قد سار بنفس مسار ما ذهبت إليه مختلف التشريعات الدولية منها والوطنية في الأخذ بفكرة التشفير الإلكتروني خاصة بعد تبني فكرة التجارة الإلكترونية³ وفكرة التقاضي الإلكتروني من خلال عمله على عصرنه قطاع العدالة⁴ الأمر الذي كان لا بد له من اتخاذ كافة الإجراءات والتدابير القانونية والتقنية التي تكفل حماية المراسلات والملفات الخاصة بالمتقاضين، غير أنه لم يعرفه بصفة عامة في ظل القانون رقم: 04/15 المحدد للقواعد المطبقة على التوقيع والتصديق الإلكترونيين وإنما تطرق إلى تعريف مفتاحي التشفير العام والخاص، حيث عرف مفتاح التشفير الخاص على أنه: "عبارة عن سلسلة من الأعداد يحوزها حصرياً الموقع، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير خاص"⁵ أما بالنسبة لمفتاح

¹ - المادة 28 من القانون الفرنسي رقم 1170/90، الخاص بتنظيم الاتصالات عن بعد.

هذا وتجدر الإشارة إليه، أن المشرع الفرنسي لقد أصدر مرسوماً عن التكامل بوسيلة التشفير في 18 فبراير 1986 حيث اعتبر التشفير الإلكتروني على أنه صياغة معلومات للتعبير عنها في شكل غير مفهوم للغير.

² - المادة الأولى من مشروع قانون التجارة المصري لسنة 1999.

³ - القانون رقم 05/18، المؤرخ في 24 شعبان عام 1439 الموافق لـ 10 مايو 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 28، الصادرة بتاريخ 16 مايو 2018.

⁴ - القانون رقم 03/15، المؤرخ في 20 ربيع الثاني عام 1436 الموافق لـ 10 فبراير 2015، المتعلق بعصرنه العدالة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 06، الصادرة بتاريخ 10 فبراير 2015.

⁵ - المادة 08 / 02 من القانون رقم: 04/15، المؤرخ في 20 ربيع الثاني عام 1436 الموافق 10 فبراير 2015، المحدد للقواعد العامة المطبقة على التوقيع والتصديق الإلكترونيين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 06، الصادرة بتاريخ 10 فبراير 2015.

التشفير العمومي فقد عرف على انه " سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني".¹

وعليه يتضح مما تقدم أن عملية التشفير تتألف من ثلاثة عناصر مترابطة مع بعضها البعض وهي:

- المعلومات التي سيتم تشفيرها: قد تكون رسالة نصية أو ملفات مهمة أو إشارات إلكترونية مشفرة ومنها في مجال التعاملات الإلكترونية، والتعاقد عن بعد، أو المفاوضات السرية التي تسبق التعاقد.²

- خوارزمية التشفير: التي ستطبق على المعلومات وذلك لتحويلها إلى بيانات مهمة وخوارزمية فك التشفير التي تعيد هذه البيانات إلى حالتها الأصلية المفهومة.³

- المفاتيح: وهي سلسلة أو أكثر من الرموز التي تستند إلى صيغ رياضية معقدة في شكل خوارزميات وتستخدم هذه المفاتيح في " تشفير " النصوص المرسل والمرسل فك التشفير من قبل المرسل إليه المسموح له بتسليمها.⁴

الفرع الثاني: ضوابط استخدام التشفير الإلكتروني:

استلزم استخدام التشفير قواعد تشريعية في ميدان المعايير المقبولة التي لا تحد فائدته من الإيجابيات، وتنعكس إلى سلبيات في مجال انسياب المعلومات ونشرها، وهو ما جعله مقيداً بضوابط يجب احترامها والتي تتجسد في:

أولاً: إباحة تشفير البيانات والمعلومات:

ويقصد به أن القانون أباح استخدام تقنية التشفير، وذلك لترميز السندات والمحركات الإلكترونية وكذا التوقيعات الإلكترونية الخاصة بالمتقاضين وكذا المراسلات الخاصة التي ترسل بين موظفي قطاع العدالة من أمناء الضبط وكذا وكلاء الجمهورية والمحامين.

إذ أنّ غالبية التشريعات المقارنة وضعت قواعد ونصوص قانونية تتعامل مع تشفير البيانات والمعلومات والتوقيعات الإلكترونية مؤكدة على أهميتها حمايتها من الجرائم السيبرانية⁵ (التزوير

¹ - المادة 09/02 من القانون رقم 04/15.

² - محمد حسين عبد العليم، إثبات العقد الإداري الإلكتروني، دون طبعة، دار الجامعة للنشر، الإسكندرية، 2019، ص 253.

³ - مرجع نفسه، ص 253.

⁴ - مرجع نفسه، ص 253.

⁵ - لم يتفق الفقهاء والباحثون على تعريف موحد للجريمة السيبرانية ، فمنهم من ينظر إلى موضوع الجريمة في حد ذاتها، وهناك من ينظر إلى الوسيلة المستعملة في ارتكابها، هذا على غرار أنهم لم يتفقوا على تسمية موحد لهذا النوع

الإلكتروني أو اختراق إلكتروني أو القرصنة الإلكترونية) سواء باستخدام عناصر التشفير الشخصية الخاصة بالتوقيع من غير طرفي العلاقة لاستخدام التشفير هذه الأخيرة أو سرقة مفاتيح التشفير أو فك التشفير التي تقوم بفك النص المشفرة وإرجاعه إلى النص الأصلي، وذلك باستخدام مفاتيح التشفير الخاص.

ثانيا: الحق في خصوصية البيانات المشفرة

ويقصد به الحفاظ على سرية البيانات والمعلومات الخاصة بمتعاملي البيئة الإلكترونية (بما فيها الملفات الخاصة بالمتقاضين وكذا المراسلات الخاصة التي تتم بين موظفي جهاز العدالة) وتجريم الاعتداء عليها، وهو الأمر الذي يتطلب الاعتراف بحق في الخصوصية في الحفاظ على سرية البيانات والمعلومات وتجريم الإطلاع والاعتداء عليها من غير أصحابها دون إذن.

وعليه وفي هذا الصدد، لقد اعتزقت جل التشريعات المقارنة بخصوصية البيانات المرسلّة واعتبرت التشفير الإلكتروني كوسيلة من الوسائل التقنية التي يمكن من خلالها تحقيق هذه الخصوصية، كما لقد اعتبر المشرع الجزائري بموجب القانون رقم 04/15 المحدد القواعد الخاصة بالتوقيع والتصديق الإلكترونيين السابق ذكره أنه وجب ضمان سرية البيانات والمعلومات المرسلّة عبر الفضاء الإلكتروني ومنع الاعتداء عليها.

الجديد من الجرائم التي تباينت تسمياتها عبر مراحل زمنية ارتبطت بتقنية المعلومات، فهناك من يطلق عليها بتسمية الجرائم السيبرانية "cyber crime" وهناك من يطلق عليها بتسمية الجرائم الإلكترونية وجانب آخر من الفقه يطلق عليها بتسمية إساءة استخدام تكنولوجيا المعلومات والاتصال، كما يطلق عليها أيضا بجرائم الكومبيوتر والانترنت . وعلى العموم يتراوح تعريف الجريمة السيبرانية بين الجرائم التي ترتكب عبر الحاسب الآلي وبين الجرائم التي ترتكب عبر مختلف المعدات الرقمية، غير أنه يمكن تعريفها على أنها " نشاط إجرامي تستخدم فيه التقنية الإلكترونية (الحاسب الآلي وشبكة الانترنت) بطريقة مباشرة أو غير مباشرة كوسيلة لتنفيذ الفعل الإجرامي، جدو بن عليه، تحديات الأمن السيبراني في مواجهة الجريمة السيبرانية، المجلة الجزائرية للأمن الإنساني، جامعة الحاج لخضر، باتنة، المجلد 07، العدد 02، جويلية 2022، ص 304.

أما بالنسبة للمشرع الجزائري نجده أنه لم يستقر على استخدام مصطلح واحد للدلالة على هذه الجرائم حيث أطلق عليها تسمية " الجرائم الماسة بالأنظمة المعالجة الآلية للمعطيات " وذلك بموجب القانون رقم 15/04 المتعلق بقانون العقوبات، كما أن استخدم مصطلح الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بموجب القانون رقم 04/09 المتعلق بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، وتعتبر هذه التسميات التي اعتمد عليها المشرع الجزائري دلالة على الجرائم السيبرانية حيث عرفها على أنها " جرائم الماسة بالأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظم الاتصال الإلكترونية ."، القانون رقم 04/09، المؤرخ في 05/08/2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحته، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 47، الصادرة بتاريخ 2009/08/16.

ثالثاً: اعتبار استخدام التشفير الإلكتروني بالتصريح المسبق

كأثر لإقرار المشرع للنص المشفروحيته في الإثبات التصرفات القانونية، وبالتالي فإنه يعتبر من المحررات الإلكترونية، حيث يمكن تحويل الإشارات والرموز إلى نصوص مقروءة ومفهومة تكون حجة على من قام بمخالفة العقد¹.

حيث أن التشفير يمكن أن ينصب على العقد أو المحرر الإلكتروني أو على التوقيع الإلكتروني، في حالة ما إذا كان العقد الكترونياً والموقع عليه الكترونياً يمكن أن تشفر بيانات العقد، وفي حالات أخرى تكون البيانات غير مشفرة على الرغم من أن التوقيع على العقد، أي أن بيانات العقد الإلكتروني يمكن الاطلاع عليها وفهم محتوى العقد وبنوده مشفرة ناحية أخرى لا يمكن لمن اطلع عليه أن يكشف هوية الموقع على العقد ذلك أن التوقيع المشفر².

المطلب الثاني: أنظمة العمل بالتشفير الإلكتروني

يسعى معظم الباحثين إلى الحصول على عدة طرق مختلفة للتشفير تناسب مع حجم المعلومات حتى تكون أكثر فاعلية في حفظها، والوصول إليها بمستوى عالي من السرية والأمان، لذلك تختلف طرق التشفير التي تستخدم في مجال تقنيات الإعلام والاتصال، والتي تنقسم إلى قسمين التشفير المتماثل والتشفير غير المتماثل وهناك من يقوم بالمزج بينهما:

الفرع الأول: التشفير المتماثل

ويطلق على هذا النوع من التشفير "التشفير السيمتري" ويستعمل هذا الأخير مفتاح سري واحد يتبادل بين المرسل والمستقبل، وغالباً ما يكون عبارة عن عملية رياضية يستعمل فيها مفتاح سري واحد يمتلكه كل من المرسل والسند والمرسل إليه والذي يتم بموجبه تشفير السندات وفك رموزها³. وتتم آلية إرسال السند في هذا النظام بتشفير السند والتوقيع عليه عبر الرموز التشفيرية المتفق عليها في المفتاح الخاص، ثم يرسل عبر وسيلة الاتصال الحديثة إلى المرسل إليه، إذ يقوم بتسليمه من حاسبه الآلي، الذي بدوره يقوم بفك الرموز التشفيرية بالمفتاح الخاص المتماثل⁴.

¹ - عبيدات يوسف محمد، داركة لافي محمد، وسائل حماية التوقيع الرقمي التي جعلته عنصراً مهماً في زيادة العمل عبر الأنترنت "دائرة تحليلية في قانون المعاملات الإلكترونية الأردني، مؤتمر للبحوث والدراسات "سلسلة العلوم الإنسانية"، جامعة مؤتة، الأردن، مجلد 24، العدد 01، 2009، ص 138.

² - إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون الكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الإمارات، مجلد 02، الجزء الثالث، 2000، ص 10.

³ - موسى حسن فضالة، المرجع السابق، ص 234.

⁴ - مرجع نفسه، ص 234.

وغالباً ما تستعمل هذه الطريقة في البنوك لتشغيل آلات الصراف الآلي. هذا وتجدر الإشارة إلى أن هذا الأسلوب لا يخلو من مخاطر الاختراق والقرصنة، إذ تبدو عملية تبادل المفتاح السري بين شخصين عرضة للدخول غير المشروع من طرف الغير.

الفرع الثاني: التشفير غير المتماثل

يقصد بهذا التشفير استخدام مفتاح أو رمز مختلفة في تشفير السندات الإلكترونية نفسها، حيث يتم استخدام مفتاحين أو رمزين مختلفين لفك تشفير السند الإلكتروني، ويكون الأول خصوصي يعرفه مستخدم معين ويبقى سرياً وخاصاً به، أما المفتاح الثاني فهو عمومي يوزعه ويبلغه إلى المستخدمين الآخرين الذين يتعامل معهم من خلال توجيه الرسائل الإلكترونية الموقعة بالمفتاح الخاص.¹

أي أنه يتم الاستعانة بمفتاحين مرتبطين بشكل حسابي لإنشاء التوقيع الإلكتروني وذلك لتحويل البيانات والمعلومات، ثم يتم تثبيتها بنظام التشفير غير المتماثل، حيث لا يمكن للغير اكتشاف المفتاح الخاص بالموقع واستعماله في التعرف على محتوى الرسالة المرسل، حتى لو تمكنوا من معرفة مفتاح العام، والمفتاح الخاص يكون معروفاً لدى جهة واحدة فقط وهو المرسل ويستعمل لتشفير الرسالة أو فك تشفيرها، بخلاف المفتاح الذي عادة ما يكون معروفاً لدى أكثر من جهة أو شخص.²

ولقد تطرق المشرع الجزائري لأنواع التشفير من خلال نص المادة 09.08/02 من القانون رقم 04/15 المتعلقة بالتوقيع والتصديق الإلكترونيين، بإعطاء تعريف لكل نوع منها معتبرا أنها جزء تتضمنه شهادة التصديق الإلكتروني، حيث تنص المادة السابقة الذكر " يقصد بما يأتي ... مفتاح التشفير الخاص: هو عبارة عن سلسلة الأعداد التي يحوزها الموقع فقط وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي، مفتاح التشفير العمومي: هو عبارة عن سلسلة الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني.³

¹ - عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، دراسة مقارنة، الطبعة الأولى، منشورات الحلبي الحقوقية، بيروت لبنان، 2010، ص 233.

² - محمد عقوني، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة المفكر، كلية الحقوق والعلوم السياسية جامعة محمد خيضر، بسكرة الجزائر، عدد 18، فيفري 2018، ص ص 304-305.

³ - المادة 09.08/02 من القانون رقم 04/15، المحدد للقواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، السابق ذكره.

الفرع الثالث: المزج بين التشفير المتماثل والتشفير غير المتماثل:

يتميز هذا النظام بتجاوزه لسلبات الأنظمة السابقة، وذلك للتغلب على مشكلة إرسال المفتاح المتماثل بطرق آمنة لحل شفرة الرسالة، واقتصار الوقت باستخدام المفتاح العام من جهة أخرى¹، إذ يمكن للمرسل والمرسل إليه أن يستخدموا كلاً من النظامين في التشفير، وهذا بتشفير الرسالة المرسل بها بالمفتاح المتماثل (المفتاح السري) ثم بعدها يتم تشفير المفتاح المتماثل بالمفتاح غير المتماثل للشخص المرسل إليه الرسالة ويرسل المفتاح المشفر والرسالة المشفرة إلى المرسل إليه الذي يقوم بفك الشفرة بمفتاحه الخاص².

تشفير الرسالة بالمفتاحين يكون عبر عدة مراحل تتمثل فيما يلي:

- كتابة النص الأصلي وتشفيره بالمفتاح العام للمرسل إليه.
- تشفير ذات الرسالة مرة أخرى باستخدام المفتاح الخاص للمرسل وهذا بغرض التأكد من مرسلها وقابلية فكها باستخدام المفتاح العام للمرسل.
- إرسال الرسالة إلى المرسل إليه عبر الوسائل الإلكترونية.
- وصول الرسالة إلى المرسل إليه المشفرة بالمفتاح المتماثل والمفتاح المشفر³.
- يقوم المرسل إليه بفك تشفير المفتاح العام للمرسل فيحصل على رسالة مشفرة بمفتاحه العام فيقوم بفكها باستخدام المفتاح السري الخاص به الذي يكون معلوما لديه. وتعتبر هذه الطريقة أكثرها أماناً نظراً لدورها الفعال في تحقيق سرية البيانات الخاصة بالرسالة وإمكانية التحقق من صاحبها.

المبحث الثاني

تقنية التشفير الإلكتروني كآلية حماية من الجرائم السيبرانية

تعتبر تقنيات تشفير الرسائل الإلكترونية من أحدث الوسائل في مجال توفير الأمن وسرية المعلومات والمعاملات المتبادلة عبر شبكة الأنترنت، كما لها دور في تدعيم وسائل الإثبات الإلكتروني من

¹ - آزد دزه بي، المرجع السابق، ص 101.

² - سراح حليتم، خصوصية التوقيع الرقمي، مجلة الباحث للدراسات الأكاديمية، العدد الثالث عشر، باتنة، جويلية، 2018، ص 743.

³ - الأنصاري حسن النيداني، القاضي و الوسائل الإلكترونية الحديثة، دار الجامعة الجديدة، الإسكندرية، 2009، ص. ص 20 - 21.

خلال التحقق من هوية مرسل المحررات أو السندات القضائية ومضمونها وتجاوز مختلف الصعوبات التي تعيقه. وهو ما سوف نتناوله من خلال هذا ضمن المطلبين الآتين:

المطلب الأول: حماية النظام المعلوماتي القضائي من الجرائم السيبرانية

لقد فرض العمل في بيئة افتراضية التي أصبحت اليوم لا تكاد تخلو من الجرائم الإلكترونية اتخاذ مجموعة من الإجراءات والتدابير التقنية والقانونية التي تلعب دورا رائدا وفعالا في توفير الحماية اللازمة للأنظمة المعلوماتية بما فيها النظام المعلوماتي للجهاز القضائي¹ وذلك عن طريق:

الفرع الأول: تجسيد بيئة تحتية آمنة

إن توجه نحو رقمنة قطاع العدالة من خلال طرح فكرة النزاع القضائي الإلكتروني عن طريق إنشاء محاكم إلكترونية يعتمد بالدرجة الأولى على إنشاء بنية تحتية رقمية آمنة يتم فيها تسجيل فيها مختلف البيانات والمعلومات الخاصة بمتعاملي البيئة الإلكترونية داخل مرفق القضاء.

لذلك يكمن الهدف الأساسي الذي يسعى إليه التشفير الإلكتروني في تجسيد بنية تحية آمنة ومشفرة يصعب اختراقها خاصة في ظل الانتشار الواسع للتعاملات الإلكترونية، ذلك أن هذا النوع من التعاملات يرتبط بأمور فنية بالغة الدقة² عن طريق اعتمادها على آلية التشفير الإلكتروني، الذي يعتبر نتاج لمقتضيات الحفاظ على سرية والأمن البيانات والمعلومات الخاصة بجلّ التعاملات الإلكترونية، التي اقتضتها طبيعة البيئة الرقمية³.

وهذا ما يتطلب بالضرورة وجود متخصصين في هذا المجال ملمين بالجانب القانوني وكذا التقني المرتبطين بهذا النوع من التعاملات الإلكترونية، مما يؤدي إلى إبرام عقود تتسم بالثبات والصحة والوضوح والثقة بين جميع الأطراف فيها⁴ وذلك نظرا لما يحققه التشفير الإلكتروني من سلامة وسرية المعلومات والبيانات الخاصة بالمعاملات الإلكترونية.

¹ - نور الهدى قادري، الحماية المعلوماتية والجنائية لبيانات المحكمة الإلكترونية ودورها في مكافحة ظاهرة الفساد داخل مرفق القضاء، بحث منشور في كتاب جماعي حول المحكمة الإلكترونية كوسيلة لتقريب مرفق القضاء من المواطن، المركز المغربي - شرق أدني للدراسات الإستراتيجية - المملكة المتحدة - بريطانيا - سبتمبر 2022، ص 270.

² - مصطفى محمد الحسبان، النظام القانوني لتقنية البلوك تشين في ظل تشريعات التجارة الإلكترونية، مجلة الحقوق والعلوم الإنسانية، المجلد الثاني عشر، العدد 03، نوفمبر 2019، ص 141.

³ - يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2007، ص 98.

⁴ - مصطفى محمد الحسبان، المرجع السابق، ص 142.

وبالتالي يلعب التشفير الإلكتروني دوراً هاماً وأساسياً في حماية النظام المعلوماتي القضائي الذي يتم من خلاله تسجيل الملفات القضائية وكذا مختلف المراسلات والمعلومات التي ترسل عبر مختلف الوسائط الإلكترونية بين مستخدمي قطاع العدالة من أمناء الضبط وكلاء الجمهورية والمحامين كتلك البيانات والمعلومات ؛ وكذا المحررات الإلكترونية الخاصة التي ترسل بين الضبطية القضائية ووكيل الجمهورية أو بين قاضي التحقيق أو قاضي الحكم وأمانة ضبط المحكمة أو المحادثات المرئية عن بعد التي تتم داخل المحكمة يتم من خلالها سماع أقول الشهود، هذا وتجدر الإشارة أن المشرع الجزائري اعتمد بموجب القانون رقم 03/15 على المحادثات المرئية عن بعد لسماع واستجواب أطراف الخصومة .

الفرع الثاني: تأمين البيانات والمعلومات

مما لا شك فيه أن التشفير عبارة عن عملية يتم من خلاله الحفاظ على سرية المعلومات والبيانات باستخدام برامج لها القدرة على تحويل وترجمة الكتابة القابلة للقراءة إلى عبارة عن إشارات ورموز غير قابلة للقراءة، بحيث إذا ما تم الوصول إليها من قبل أشخاص ليس لهم الحق في الإطلاع عليها لا يمكنهم من فهمها، لأن ما يظهر لهم ما هو عبارة عن أرقام وإشارات ورموز غير مفهومة ولا يمكن فك تشفيرها إلا من يملك مفتاح فك الشفرة.

إذ أن أهم ما يميز تقنية التشفير الإلكتروني يتمثل في أنها تقوم بتخزين البيانات والمعلومات في شكل كتل مشفرة، فإذا ما أدخلت تلك البيانات وتم إضافتها فعلاً إلى سلسلة الكتل بعد التحقق منها من خلال " عقد الشبكة " فإنه لا يمكن تعديلها أو تغييرها، مما يجعلها غير قابل للتغيير¹. والسبب في ذلك هو اعتماده على آلية التشفير عن طريق ما يطلق عليه بدالة التجزئة أو آلية الهاش وهي عبارة عن خوارزميات معينة للتشفير تحول البيانات التي تم إدخالها في الكتلة، مهما كان حجمها، إلى مجموعة فريدة من الأرقام والحروف والرموز ذات طول ثابت يطلق عليها بالهاش. فهو بمثابة بصمة مميزة للبيانات يتغير بتغير محتوى هذه الأخيرة².

وعليه فإن تأمين البيانات والمعلومات خاصة بأي نظام معلوماتي وبالأخص النظام القضائي يتم ضمن بنية تحتية آمنة ومشفرة، يتم من خلالها تحقيق وحدة البيانات والمعلومات عبر التقنيات التكنولوجية الحديثة، وذلك بفضل تقنية التوقيع الإلكتروني الذي يعتبر بمثابة بصمة مميزة لصاحب المحرر الإلكتروني إذ بموجبه لا يستطيع أي شخص معرفة فك رموز التوقيع الخاص به أو الدخول

¹ - هيثم السيد أحمد عيسى، نشأة العقود الذكية في عصر البلوك تشين، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع، القاهرة، 2021، ص 22.

² - مرجع نفسه، ص 22.

عليه سواء عند استعماله لهذا التوقيع أو عند إنشائه هذا من ناحية، وكذا بفضل المفتاح الشفرة العام أو كود خاص الذي يكون تحت السيطرة الكلية لصاحبه¹ وهذا من ناحية أخرى، وبالتالي فوجود التوقيع والتشفير الإلكترونيين يشكل مخرجاً من كافة الجرائم السيبرانية على مختلف المحررات الإلكترونية وكذا الأنظمة المعلوماتية مما يوفر الأمن المعلوماتي من خلال توفير قاعدة بيانات آمنة وذاتية الصيانة.

ذلك أنّ نجاح تطبيق عصنة قطاع العدالة متوقفاً على ضمان درجة من تأمين مناسبة عند التعامل بالبيانات والمعلومات التخزين أو في التداول، بما يحقق عدم إجراء أيّ تغيير أو تعديل أو فقدان البيانات والمعلومات كلها أو جزء منها، وتأسيساً على ذلك تحظى تقنيات وسياسات التشفير باهتمام في ميدان أمن المعلومات، ومرد ذلك أن حماية التشفير الإلكتروني يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة: السرية والتكاملية وتوفير المعلومات، فالتشفير تقنيات تدخل في مختلف وسائل التقنية المنصبة على تحقيق هذه العناصر.

إذ أن ضمان سرية المعلومات أصبح يعتمد على ما يعتمد عليه التشفير الإلكتروني للملفات والمعلومات، بل تشفير وسائل التثبيت وكذا كلمات السرّ، وفي هذا الصدد لقد عمل المشرع التونسي على حماية البيانات المشفرة ومختلف العناصر المستخدمة في عملية التشفير وفكها من أيّ اعتداء، سواء باستخدام عناصر التشفير الشخصية المتعلقة بتوقيع من غير طرفي العلاقة، لاستخدام التشفير في أساليب احتيالية أو سرقة مفاتيح التشفير، حيث قضى قانون المبادلات التجارية الإلكترونية التونسي في الفصل 48 بأنه يعاقب كل من استعمل بصفة غير مشروعة عناصر التشفير شخصية متعلقة بإمضاء غيره بالسجن لمدة تتراوح بين 06 أشهر إلى عامين وبخطية تتراوح من 1000 إلى 10.000 دينار أو بإحدى هاتين العقوبتين.

الفرع الثالث: إثبات هوية وإرادة المتراسلين:

يعتبر التوقيع الرقمي مميّزة شخصية تعكس معلومات وبيانات الموقع من خلال توقيعه للعقد المبرم إلكترونياً، الذي يكشف عن اسم ولقب وتوقيع الموقع على المعاملة الإلكترونية من خلال خوارزميات التشفير الإلكتروني التي تأخذ شكل الرموز أو الأرقام أو الحروف والمنظمة في شهادات

¹ - يمينه حوحو، عقد البيع الإلكتروني في القانون الجزائري، الطبعة الأولى، دار بلقيس للنشر، الجزائر، 2016، ص

التصديق الإلكتروني، فهو بذلك يعبر عن شخصية الموقع وهويته، ما يرتب عنه صعوبة تزوير أو تقليد أو استعمال التوقيع الرقمي من دون أو غير صاحبه الأصلي.¹

فمن خلال توقيع السند الإلكتروني باستخدام تقنيات التشفير بواسطة الدعامة الإلكترونية يتم إبرام العقد والذي هو حجة على إرادة وموافقة الموقع على ما ورد في السند من التزامات وحقوق، وهو ما نستشف ضمن نص المادة 02/02 من القانون رقم 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين.²

وعليه يلعب التشفير الإلكتروني دور كبير في تحقيق درجة عالية من الأمن التقني التي تحول دون إحداث أيّ تغيير أو تحريف بالبيانات، كون أنها عبارة عن خوارزميات يتم من خلالها تشفير المعلومات والبيانات الخاصة بالملفات المتقاضيين. مما يجعل من فرض إمكانية الإخلال بسلامة البيانات أمر صعب المنال.

المطلب الثاني: مستويات التشفير الإلكتروني

إن حماية البيانات والمعلومات الخاصة بالنظام القضائي يعد أمر في بالغ الأهمية، وللقيام بعملية التأمين هذه الأخيرة لا يكون إلا عن طريق تشفيرها الذي يأخذ عدة مستويات وهي:

الفرع الأول: على مستوى الإرسال

في هذا المستوى يتم التشفير جميع البيانات والمعلومات بين نقطة الإرسال ونقطة والاستقبال ويتم ذلك عن طريق الشبكات الافتراضية الخاصة وهي شبكات جزئية من شبكة الانترنت، تقوم فيه إحدى المشروعات بتخصيصه وذلك عن طريق إحاطته بالاحتياطات التأمينية المطلوبة لإرسال واستقبال المعلومات من خلاله ويكون بشكل آمن، وبالتالي أيّ تبادل المعلومات والمراسلات الخاصة بقطاع العدالة أو الخاصة بالمتقاضيين يكون بشكل آمن، نظرا لما يحققه التشفير الإلكتروني من أمن وسرية هذه الأخيرة والذي يكون من نقطة الإرسال إلى نقطة الاستقبال الرسالة .

الفرع الثاني: التشفير على مستوى التصفح أو التنقل

على مستوى التصفح يتم التشفير جميع الاتصالات بين نوافذ الشبكة أو أحد البرامج التصفح أو أحد المواقع الموجودة عليها، مما يؤدي إلى حماية البيانات أثناء انتقالها، حيث لقد أعلنت شركة Netscape أحد البرتوكولات التأمينية عام 1995 وهو البرتوكول securesochatlayer، وتنصرف وظيفة

¹ - سراح حليتم، خصوصية التوقيع الرقمي، مجلة الباحث للدراسات الأكاديمية، العدد الثالث عشر، باتنة، جويلية، 2018، ص 747.

² - تنص المادة 02/ 02 من القانون رقم 04/15 على أنه " الموقع هو شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله."

هذا البرتوكول في تشفير جميع الاتصالات مما يقلل من فرصة نسخ البيانات أو وصولها إلى شخص غير مرغوب فيه وقصر وصولها للمستقبل النهائي فيعطي هذا الأمر شكلاً من أشكال الثقة والأمان للعملاء، لأن المعلومات والبيانات الخاصة بهم بما فيها بطاقة الائتمان لن تكون متاحة سوى للتاجر، أو المنشأة أو المؤسسة المراد التعامل معها عن طريق هذه الشبكة دون غيرها .

الفرع الثالث: التشفير على مستوى التطبيق أو التنفيذ

يرتبط ظهور هذا النوع من التشفير بظهور التجارة الإلكترونية، فهو عبارة عن نظام يتم من خلاله تشفير عملية طلب الشراء والدفع عبر شبكة online، ويعتبر هذا الأخير من أهم البرتوكولات المتعلقة بنواحي التي ظهرت في مجال المعاملات الإلكترونية¹.

يتطلب العمل بنظام set فتح حساب بنكي لكل من بائع والمشتري بأحد البنوك المستخدمة له، واستخدام المشتري لأحد برامج التصفح - نوافذ شبكة المعلومات - المدعم لنظام set واستخدام البائع لمقر معلومات server يدعم هو الآخر ذلك النظام.

الفرع الرابع: التشفير على مستوى الملفات

يتم التشفير على مستوى الرسائل الإلكترونية والملفات التي يتم مداولتها، فوفقاً للبرنامج التأميني الذي وضعه Philip Zimmerman لحماية الرسائل الإلكترونية عام 1995، والذي يطلق عليه باختصار PGP، يتم تشفير البيانات التي تحتويها الرسائل باستخدام مفتاح العام Public Key، ويتميز هذا النظام بسهولة استخدام وصعوبة اختراقه والهجوم عليه².

ويعتمد نظام PGP في حل الشفرة الخاصة بالرسالة المشفرة باستخدام المفتاح الملائم لحل الشفرة، وبالتالي فإن أي تجربة لأي مفتاح آخر غير المفتاح المطلوب لحل الشفرة يعتبر من المهام المستحيلة التي لا يمكن أن تنجح³.

وعليه يمكننا القول أنه نظراً لطابع السرية التي يتميز به النظام القضائي من السرية فإنه توجب على المنظومة القضائية خاصة في ظل عصرة قطاع العدالة فإنه كان لا بد من تبني آلية قانونية من جهة وتقنية من جهة أخرى تهدف إلى منع الغير من مستخدمي شبكات الانترنت من الدخول إلى النظام القضائي المعلوماتي والإطلاع على مختلف البيانات والمعلومات الخاصة بالمتقاضين

¹ - وهو اختصار لـ Secure Electronic Transaction بروتوكول الإخفاء المزدوج والدفين الأمن،

لا لوش راضية، امن التوقيع الإلكتروني مذكرة مقدمة لنيل شهادة الماجستير في القانون، تخصص قانون الدولي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.

² - لالوش راضية، نفس المرجع، ص 103.

³ - مرجع نفسه، ص 103.

ومختلف الملفات الخاصة بهم نظرا لخصوصيتها، وكذا مختلف المراسلات التي يتم إرسالها بين موظفي قطاع العدالة، لذلك نجد أن أغلب التشريعات الدولية منها والوطنية بما فيها التشريع الجزائري أقر بضرورة استخدام تقنية التشفير الإلكتروني في التوقيع الإلكتروني بهدف تحقيق الأمن المعلوماتي في مختلف التصرفات القضائية.

وعلى العموم ومن خلال ما سبق يمكن القول ان التشفير الإلكتروني يحقق مجموعة من الأهداف تتمثل فيما يلي:

- الخصوصية أو السرية: ويكون عن طريق التأكد من عدم إمكانية الإطلاع والكشف عن المعلومات والبيانات من قبل أشخاص غير مسموح لهم بذلك.
- تكاملية البيانات: وذلك من خلال التأكد من صحة البيانات والمعلومات بأنها لم يطرأ عليها أي تغيير ولم يتم تعديلها أو تحريفها، خاصة أنه لن يتم تدمير التوقيع الإلكتروني لأحد طرفي النزاع خلال مرحلة من مراحل المعالجة أو التبادل المعلومات والرسائل.
- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به: أي ضمان عدم إنكار الشخص الذي قام بتصرف ما "متصل بالمعلومات أو مواقعها".
- التحقق من هوية صاحب التوقيع: أي يجب أن تكون المعلومات المستلمة مطابقة شخصيا للمعلومات الأصلية التي أرسلت وكذلك تاريخ إرسال المعلومات ومحتواها ووقت الإرسال.¹

خاتمة:

وختاما لموضوع الدراسة يمكن القول، أنه يعد موضوع حماية النظام القضائي الإلكتروني يعد من المواضيع القانونية وكذا القضائية التي حظيت ومازالت تحظى باهتمام المشرع من أجل حمايته وحماية مختلف المعلومات والبيانات الخاصة بالمتقاضين.

وعليه يُعد نظام التشفير الإلكتروني من بين التقنيات التكنولوجية الحديثة التي أفرزها التطور العلمي المذهل الذي يشهده العالم في وقتنا الحاضر، وذلك نظرا للدور الذي يلعبه في توفير الأمن المعلوماتي للنظام القضائي من خلال توفير أمن وسلامة البيانات الخاصة بطرفي النزاع، مما يجعل دور هذه التقنية لا يقتصر فقط في أداء وظائف الحماية فقط، وإنما يمتد دوره كذلك في المساهمة في تدعيم وسائل الإثبات الإلكتروني من خلال حمايتها من كافة المخاطر والجرائم الإلكترونية التي تعترضها.

¹ - على محمد دهب، التشفير وأمن المعلومات، كلية الدراسات والحاسوب الإحصاء، جامعة كردفان، السودان،

وعليه لقد توجت هذه الدراسة بمجموعة من النتائج يمكن أن نستخلصها فيما يلي:

* يعتبر التشفير الإلكتروني عبارة عن خوارزميات تحول البيانات المفهومة إلى بيانات غير مفهومة تأخذ شكل أرقام أو حروف أو إشارات.

* يلعب التشفير الإلكتروني دورا هاما في توفير الأمان عند عملية نقل وحفظ الدليل الإلكتروني كما له دورا في ضمان سرية المعلومات من خلال منع الغير من الإطلاع عليه.

* يعد التشفير الإلكتروني من أهم الوسائل والآليات التقنية الحديثة التي تلعب دورا هاما في حماية مختلف المعاملات وكذا التصرفات الحديثة وكذا حماية الأنظمة المعلوماتية بما فيها النظام القضائي نظرا لطابع الخصوصية والسرية التي يتميز بها بما يضمن توفير الأمن السيبراني لهذه الأخيرة.

* يشكل التشفير الإلكتروني من بين الضمانات القانونية وكذا التقنية التي تؤدي إلى حماية مختلف البيانات والمعلومات الخاصة بالمتقاضيين وكذا مختلف الملفات والوثائق القضائية وضمان عدم المساس بها أو تحريفها أو تغييرها.

ومن النتائج السابقة توصلنا إلى مجموعة من الاقتراحات يمكن إجمالها في:

* ضرورة العمل على إنشاء قاعدة بيانات رقمية آمنة ومشفرة يتم من خلالها تسجيل مختلف البيانات والمعلومات التي تخص المتقاضيين نظرا لطبيعة السرية التي تفرضها.

* ضرورة سن نظام قانوني خاص ينظم أحكام التشفير الإلكتروني وكيفية العمل به.

* العمل على وضع برامج مضادة لمختلف أشكال القرصنة الإلكترونية والسعي لتكثيف الجهود لمجابهة كافة أشكال الجرائم الإلكترونية ومواجهة مرتكبيها.

* العمل على جعل من التشفير الإلكتروني أحد السياسات العامة للحفاظ على أمن المعلومات والبيانات المتعلقة بالدولة أو الخاصة بالأفراد سواء كان ذلك على المستوى الوطني أو الدولي.

* تنظيم دورات تدريبية لتكوين موظفي الهيئة القضائية من القضاة وأعضاء النيابة العامة وكذا المحامين وأمناء الضبط على كيفية استخدام تكنولوجيا الإعلام والاتصال والاستفادة منها في المجال خدمة العدالة.

قائمة المصادر والمراجع:

أولاً: قائمة المصادر

أ – النصوص القانونية

• على مستوى الدولي:

- دليل الإشتراع قانون الأونسترال بشأن التوقيعات الإلكترونية، الصادر عن لجنة الأمم المتحدة للقانون التجاري الدولي لعام 2001.

• على مستوى الداخلي:

1- التشريع الفرنسي:

- القانون الفرنسي رقم 1170/90، الخاص بتنظيم الاتصالات عن بعد.

2 – التشريع المصري:

- مشروع قانون التجارة المصري لسنة 1999.

3-التشريع الجزائري:

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

- القانون رقم 03/15، المؤرخ في 20 ربيع الثاني عام 1436 الموافق لـ 10 فبراير 2015، المتعلق بعصنة العدالة، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 06، الصادرة بتاريخ 10 فبراير 2015.

- القانون رقم 04/15، المؤرخ في 20 ربيع الثاني عام 1436 الموافق 10 فبراير 2015، المحدّد للقواعد العامة المطبقة على التوقيع والتصديق الإلكترونيّين، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد رقم 06، الصادرة بتاريخ 10 فبراير 2015.

- القانون رقم 05/18، المؤرخ في 24 شعبان عام 1439 الموافق لـ 10 مايو 2018، المتعلق بالتجارة الإلكترونية، الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية، العدد 28، الصادرة بتاريخ 16 مايو 2018.

أ- الكتب

- آزد دزه يي، النظام القانوني للمصادقة على التوقيع الإلكتروني – دراسة مقارنة -، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2016.

- موسى حسن فضالة، التنظيم القانوني للإثباتات الإلكترونية – دراسة مقارنة – الطبعة الأولى، دار السنهوري، لبنان، 2016.

- عمير حسن المؤمني، التوقيع الإلكتروني وقانون التجارة الإلكترونية، دون طبعة، دار وائل، عمان الأردن، 2003.

- عباس العبودي، تحديات الإثبات بالسندات الإلكترونية ومتطلبات النظام القانوني لتجاوزها، دراسة مقارنة، الطبعة الأولى منشورات الحلبي الحقوقية، بيروت لبنان، 2010.

دور التشفير الإلكتروني في حماية النظام القضائي من الجرائم السيبرانية

- الأنصاري حسن النيداني، القاضي والوسائل الإلكترونية الحديثة، دار الجامعة الجديدة، الإسكندرية، 2009.
- يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2007.
- هيثم السيد أحمد عيسى، نشأة العقود الذكية في عصر البلوك تشين، الطبعة الأولى، دار النهضة العربية للنشر والتوزيع القاهرة، 2021.
- يوسف أحمد النوافلة، حجية المحررات الإلكترونية في الإثبات، دار وائل للنشر والتوزيع، الأردن، الطبعة الأولى، 2007.
- يمينه حوحو، عقد البيع الإلكتروني في القانون الجزائري، دار بلقيس للنشر، الجزائر، الطبعة الأولى، 2016.

ب -مذكرات الماجستير وأطروحات الدكتوراه

1 -مذكرات الماستر

- زينب غريب، إشكالية التوقيع الإلكتروني وحجته في الإثبات، مذكرة مقدمة لنيل شهادة الماستر في الحقوق، تخصص القانون الخاص، كلية الحقوق والعلوم السياسية، جامعة محمد الخامس، السويسي، الرباط، 2010./2009

2-أطروحات الدكتوراه:

- لالوش راضية، امن التوقيع الإلكتروني مذكرة مقدمة لنيل شهادة الماجستير في القانون، تخصص قانون الدولي للأعمال، قسم الحقوق، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو، 2012.

ج-المقالات العلمية:

- جدو بن علي، تحديات الأمن السيبراني في مواجهة الجريمة السيبرانية، المجلة الجزائرية للأمن الإنساني، جامعة الحاج لخضر، باتنة، المجلد 07، العدد 02، جويلية 2022.
- سراح حليتم، خصوصية التوقيع الرقمي، مجلة الباحث للدراسات الأكاديمية، العدد الثالث عشر، باتنة، جويلية، 2018.
- محمد عقوني، الآليات التقنية والقانونية لحماية التوقيع الإلكتروني، مجلة المفكر، كلية الحقوق والعلوم السياسية جامعة محمد خيضر، بسكرة الجزائر، عدد 18، فيفري 2018.
- مصطفى محمد الحسبان، النظام القانوني لتقنية البلوك تشين في ظل تشريعات التجارة الإلكترونية، مجلة الحقوق والعلوم الإنسانية، المجلد الثاني عشر، العدد 03، نوفمبر 2019.
- عبيدات يوسف محمد، داركة لافي محمد، وسائل حماية التوقيع الرقمي التي جعلته عنصرا مهما في زيادة العمل عبر الانترنت "داسة تحليلية في قانون المعاملات الالكترونية الأردني، مؤتمر للبحوث والدارسات "سلسلة العلوم الإنسانية"، جامعة مؤتة، الأردن، مجلد 24، العدد 01، 2009.
- إسماعيل عبد النبي شاهين، أمن المعلومات في الأنترنت بين الشريعة والقانون، بحث مقدم إلى مؤتمر القانون الكمبيوتر والأنترنت، كلية الشريعة والقانون، جامعة الإمارات، مجلد 02، الجزء الثالث، 2000.
- نور الهدى قادري، الحماية المعلوماتية والجنائية لبيانات المحكمة الإلكترونية ودورها في مكافحة ظاهرة الفساد داخل مرفق القضاء، بحث منشور في كتاب جماعي حول المحكمة الإلكترونية كوسيلة لتقريب مرفق القضاء من المواطن، المركز المغربي - شرق أدني للدراسات الإستراتيجية - المملكة المتحدة - بريطانيا - سبتمبر 2022.

4-المواقع الإلكترونية:

-علي محمد دهب، التشفير وأمن المعلومات، كلية الدراسات والحاسوب الإحصاء، جامعة كردفان، السودان، المنشور
على الموقع:

<https://www.noor-book.com>; le 20/03/2024. H 20: 30