المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الثاني - العدد السادس عشر
تأريخ الإصدار: فبراير 2021 م

استراتيجيات الوقاية القانونية والأمنية من مهددات الأمن الرقمي

د/ زهدور إنجي هند نجوى ريم سندس
أستاذة محاضرة قسم أ- كلية الحقوق والعلوم السياسية- جامعة محمد بن أحمد –وهران – الجزائر
ihzahdour@yahoo.fr

د/ درار نسيمة
أستاذة محاضرة قسم أ- كلية الحقوق والعلوم السياسية- جامعة محمد بن أحمد –وهران – الجزائر
derrar-nassima@outlook.fr

الملخص

ازدحم العالم بشبكات اتصالية دقيقة ومتطورة، تنقل وتشغل المعلومات والبيانات من مناطق متباعدة باستخدام تقنيات لا تكفل لها أمنا كاملا، ويتاح في ظلها التلاعب عبر الحدود بتلك المعطيات المنقولة أو المخزنة، مما قد يسبب لبعض الدول أو الأفراد أو الشركات أضرارا فادحة، يغدو عندها التعاون الدولي واسع المدى في مكافحة الجرائم المعلوماتية ومن بينها جرائم الإنترنت أمرا محتوما.

بنظرة متأنية للأنظمة القانونية القائمة في الكثير من الدول لمواجهة الجرائم المعلوماتية ومنها الجرائم المتعلقة بشبكة الإنترنت، يتضح عدم وجود اتفاق عام مشترك بين الدول حول نماذج إساءة استخدام نظم المعلومات وشبكة الإنترنت الواجب تجريمها، فما يكون مباحا في أحد الأنظمة قد يكون مجرّما وغير مباح في نظام آخر. ويمكن إرجاع ذلك إلى عدة أسباب وعوامل كاختلاف البيئات والعادات والتقاليد والديانات والثقافات من مجتمع لآخر، وبالتالي اختلاف السياسة التشريعية المنتهجة.

يطرح انتشار الإنترنت خارج حدود الدولة تحديات قانونية تتعلّق بسيادة الدول وصلاحية محاكمها التي تمتد فقط على مساحتها الجغرافية. ولكن بما أن جرائم الإنترنت ظاهرة عالمية جديدة تمتدّ خارج نطاق الحدود الوطنية فإن ذلك يستلزم لنجاح مكافحة تلك الجرائم تنسيقًا كبيرًا بين القوانين الداخلية والمعاهدات الدولية والتعاون بين مختلف البلدان. وعليه يبقى التساؤل مطروحا إذا كانت التدابير والإجراءات المتاحة لمراقبة الأنظمة الالكترونية وضمان حماية المستخدمين كفيلة بمواجهة خطر الجرائم السيبرانية؟

الكلمات المفتاحية: التكنولوجيا، الأمن، المعلومات، الجرائم المعلوماتية، مراقبة الأنظمة.

IJRSP
المجلة الدولية لنشر البحوث والدراسات
International Journal of Research and Studies Publishing
ISSN: 2709-7064
المجلد الثاني - العدد السادس عشر
تأريخ الإصدار: فبراير 2021 م

Legal and Security Prevention Strategies against Digital Insecurity Threats

Abstract:

The world is crowded with accurate and developed communication networks that transfer and make function information and data from distant regions using technologies that do not guarantee full , and through which these transferred or stored data can be manipulated, which may cause serious damages to countries, individuals and companies .Therefore, a broad-based international cooperation in combating information crime, including cybercrime, is seen as being imperative.

A careful look at the legal systems placed in many countries to confront information crimes, including crimes related to the Internet shows the absence of a common agreement among countries on the models for the misuse of information systems and internet that should be criminalized, for instance what is permissible in one system may be criminalized and impermissible in another system.

This can be attributed to several reasons and factors such as different environments, customs, traditions, religion and cultures from one society to another, and thus to the different legislative policy adopted.

The spread of the Internet outside the borders of the country poses legal challenges related to the sovereignty of states and the jurisdiction of their courts, which extends only to their geographical areas.

But, since cybercrime is a new global phenomenon that extends beyond national borders, combating it successfully requires a great coordination between domestic laws, international treaties, as well as cooperation between different countries.

Therefore, the question remains whether the measures and procedures available to control electronic systems and ensure the protection of users are sufficient to face the threat of cybercrimes.

Keywords: technology, security, data, cybercrime, measures control.

مقدمة:

كان الإنسان في حقبة زمنية معينة يعمل جاهدا على حماية حدود بلده من تدخل أي عدوّ قد يمس بسيادة دولته أو شعبها، فيحدّ من حريته ويغتصب ممتلكاته. لكن مفهوم العدو والحماية منه اتخذ منحى آخر ومفهوما أكثر تعقيدا لم يعد معتمدا على وضع جيش على طول الحدود أو القصف بالطائرات أو حتى رمي القنابل، لأن التهديد الذي نحن بصدد البحث فيه هو ما يمس المعلومات المخزنة إلكترونيا وتطور القدرة على العبث بها والاطلاع عليها وتخزينها وهو ما يختصر في مصطلح "الأمن الرقمي" الذي يهدف أساسا إلى حماية حسابات الشبكة العنكبوتية المخزنة في الحاسوب وحماية الملفات السرية من خطر التسلل إليها والتطفل عليها من قبل مستخدمين خارجيين.

أمام هذا الوضع وجد العالم نفسه مضطرا إلى مجابهة تحديات الأمن الرقمي لأنه لا قواعد تحكم الحروب السيبرانية أمام الهجمات الرقمية حول العالم والواضح أن معظم الدول -النامية منها خاصة-لا تعتمد على خطة واستراتيجيات مدروسة لحماية معلوماتها وتعاملاتها الإلكترونية التي غالبا ما تكون عرضة لتطفل بعض المقتحمين الذين يخترقون أو يسرقون المواقع من أجل الوصل إلى معلومات مهمة وسرية تجعل صاحبها عرضة للإبتزاز والتهديد المادي والمعنوي.

المبحث الأول: التكنولوجيا الرقمية الآمنة ضد المد الإجرامي الإلكتروني

المطلب الأول: التشفير السبراني والتواقيع الرقمية

المطلب الثاني: آلية المصادقة الإلكترونية المستحدثة

المبحث الثاني: المواجهة الدولية والجزائرية لتعزيز الأمن الرقمي

المطلب الأول: الأساليب التقنية لحماية المعطيات والمواقع الإلكتروني.

المطلب الثاني: التصعيد التشريعي الموضوعي والإجرائي الجزائري للوقاية من المد الإجرامي الرقمي

المبحث الأول: التكنولوجيا الرقمية الآمنة ضد المبدأ الإجرامي الإلكتروني

عُرف عن الجريمة بمفهومها التقليدي أنها سلوكيات أو أفعال خارجة عن القانون ولا تقوم الجريمة إلا على مفاهيم ومعايير اجتهد واختلف الفقه الجنائي في تحديدها، فمنهم من أسس الجريمة على معيار وسيلة ارتكاب الجريمة وهناك من عرف الجريمة قياما على محلها وفريق آخر حدد ماهيتها من خلال شخص مرتكبها وقصده الجنائي فيها، أما البعض الآخر فرأى ضرورة الجمع بين المعايير كلها من أجل ضبط مفهوم واسع لمصطلح الجريمة.

إلاّ أنّ قرننا الراهن فرض مفهوما مختلفا عن ذاك المفهوم التقليدي ويرجع تأصيل ذلك إلى استحداث نظام المعلوماتية التي تتربع عليه شبكة عنكبوتية وضعت بصمة عميقة غيرت ووسعت من مفهوم استعمال المعلومة وكيفية حفظها مما انعكس إيجابا على تطور الأنشطة اليومية سواء من حيث مضمونها أو شكلها أو زمن انعقادها أو مسافتها.

أمام هذه القفزة المعلوماتية غير المسبوقة أصبحت الجريمة ذات وصف إلكتروني وافتراضي (Cyber Crimes) تخطت حدود الدول الجغرافية حيث يستخدم هذا المصطلح لوصف فكرة استغلال جزء من الحاسوب أو عنصر من المعلومات لارتكاب الجريمة بفضل التدفق السريع للمعلومة.

فالجريمة الإلكترونية إذا هي المخالفات التي ترتكب ضد الأفراد أو المجموعات من الأفراد بدافع الجريمة وبقصد إيذاء سمعة الضحية أو تحقيق أذى مادي أو عقلي للضحية سواء كان الأذى مباشرا أو غير مباشر، لكن أداة الجريمة فهي الاستخدام الذكي لشبكات الاتصالات[1].

أما التعريف القانوني الذي وضعه المشرع الجزائري للجريمة الإلكترونية فقد جاء في نص المادة 02 من القانون 09-04 والذي عرفها أنها جرائم المساس بأنظمة المعالجة الآلية للمعلومات المحددة في قانون العقوبات أو أية جريمة ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكترونية[2].

أساس هذه المادة أن المشرع الجزائري حدد نطاق الجريمة الإلكترونية وأقرّ أن الجريمة الإلكترونية ترتكب في نظام معلوماتي أو يسهل ارتكابها فيه وهو ما يوسع نطاق مجال الجرائم الإلكترونية في القانون الجزائري [3].

ومن الواضح أنّ المجرم – وهذه صفة تقليدية أصبح اليوم يسمى المخترق أو Hacker كما قد يتخذ عدة أوصاف تبعا للغرض المرجو من جريمته إن كانت بدافع التجسس فقط أو بدافع تحقيق أرباح مالية أو إلحاق خسائر بالمجني عليه دون الحصول على أرباح- أنّ له قصدا وتعمّدا قائمين إذ يظهر ذلك من خلال اختراقه النظام المعلوماتي واختلاس البيانات واستغلالها في أعمال غير مشروعة، هذا المخترق الذي غالبا ما يتميز بالذكاء وسرعة البديهة وحسن استعمال الأنظمة الحاسوبية ولا يميل إلى إدخال العنف كعنصر في جرائمه خلافا لنسخته التقليدية.

---

[1]- ذياب موسى البداينة، "الجرائم الإلكترونية: المفهوم والأسباب"، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 2-2014/09/4، عمان، الأردن، ص 3.

[2]- المادة 02 من القانون رقم 09-04 المؤرخ في 2009/08/05 المتعلق بالقواعد للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 المؤرخة في 2009/08/06.

[3]- نمديلي رحيمة، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، طرابلس، ليبيا، 24-25 مارس 2017، ص 6.

وعليه فإن موضوع "أمن المعلومات" يكتسي أهمية بالغة ويمسّ أمن كل شخص يتعامل مع الوسائط الإلكترونية بشكل مباشر وأمام هذه الأهمية، فإن البحث في مجال تطوير أمن المعلومات أضحى ينمو بشكل سريع ورهيب.

فكلما ذُكر مصطلح "أمن المعلومات وجرائم الحاسوب" فإن ذلك يبعث على التفكير مباشرة أن هناك كشف لمعلومات من المفروض أن تبقى سرية، حيث يرى أصحاب هذا التخصص أن أمن المعلومات لا بد أن يرتكز على أسس ثلاث: سرية المعلومات (Data confidentiality) معنى ذلك اتخاذ التدابير اللازمة لمنع الغير من الاطلاع على المعلومات السرية والشخصية، سلامة المعلومات (Data integrity) والمقصود بها اتخاذ التدابير اللازمة لحماية المعلومات من الjزغيير.

وأخيرا ضمان الوصل إلى المعلومات والموارد الحاسوبية (availability) حيث أنه إضافة إلأى الحفاظ على سرية المعلومات وسلامتها والذي هو أمر أوّلي، لكن تصبح هذه المعلومات دون قيمة إذا لم يتمكن صاحبها من حق الاطلاع عليها والوصول إليها[4].

ويعتبر الأمن السبراني مجالا جديدا للحروب المستحدثة بعد حروب البر والبحر والجو والفضاء الحقيقي وهو يمثل جميع شيكات الحاسب الآلي المنتشرة عبر العالم كما يشمل الأجهزة الإلكترونية التي تربطها شبكة الألياف البصرية اللاسلكية.

معنى ذلك أن الأمن المعلوماتي هو مجموع العمليات والآليات التي يتم من خلالها حماية معدات الحاسوب الآلي من أي تدخل غير مقصود أو غير مصرح به أو تغيير أو إتلاف قد يحدث. حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع هذا الاستخدام غير المصرح به ومنع سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها[5].

وبالتالي فإن أمن المعلومات هو حماية للأنظمة الحاسوبية من أي وصول غير شرعي لها ومنع العبث بالمعلومات أثناء التخزين أو المعالجة. كما يهدف هذا الإجراء إلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين وهو يعنى بالوسائل الضرورية لاكتشاف وتوثيق وصدّ أي نوع من التهديدات مما يجعله يهتم بمجالات التشفير والتخزين والمعايير الأمنية.

وفي إطار تعزيز ورفع مستوى الأمن الرقمي في مجال الاتصال من أجل خلق الائتمان في التعامل والاستقرار فيه وتوطيد ثقة المستخدمين لهذه الآلات، عمل المتخصصون في هذا المجال على تعريف وتقريب وتمكين الأفراد من سبل حماية خصوصية المعلومة والأجهزة أثناء الاستخدام وذلك من خلال وضع برامج وميكانيزمات تعمل في هذا الشأن.

[4]– خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية للنشر، الطبعة الأولى، 2009، ص22.

[5]– صالح بن علي بن عبد الرحمان الربيعة، الأمن الرقمي وحماية المستخدم من مخاطر الانترنت، هيئة الاتصالات وتقنية المعلومات، ص 6.

المطلب الأول: التوقيع الرقمي والتشفير السبراني

أصبح النشاط الرقمي الإلكتروني يحتك بخصوصية وأمان الحريات والحق خاصة بعد التطور المذهل للتقنيات الرقمية وارتفاع نسبة الاستعمال النشط للأنترنت ومواقع التواصل الاجتماعي. هذه الأيقونات الرقمية أصبحت هاجسا عند البعض حيث أصبح استعمالها يخرج عن الإطار المشروع وتعدى حدود الشخصية والخصوصية فأصبح الاطلاع والعبث بمعلومات الغير وإلحاق الأذى أمرا هينا ويسيرا على المخترقين غير المصرح لهم بذلك، الأمر الذي وسع فضاء التجسس وارتكاب الجرائم التي تعدت حدود الدول.

أمام هذه الحرب الافتراضية عمد المتخصصون في هذا المجال إلى ضرورة النظر في تقنيات تضمن الحدّ الأدنى من الأمان على أوتار هذه الشبكة حيث اعتبر التوقيع الرقمي والتشفير السبراني كوسيلتين مبدئيتين لضمان أصالة الوثائق الإلكترونية عن طريق ترميزها (التشفير) بشكل يمكن فقط لحاسوب آخر فك تشفيره.

الفرع الأول: التوقيع الإلكتروني

شهد موضوع التوقيع بوجه عام عدة محطات عرف من خلالها عدة أنواع من التواقيع حيث تؤكد الأصول التاريخية أن التوقيع كان في بدايته يتم عن طريق وضع ختم، ثم تطور ليصبح توقيعا بخط اليد عن طريق الإمضاء وانتقل إلى وضع بصمة الأصبع التي أثبت العلم قدرتها على تحديد هوية الموقع وعدم تشابهها مع أي بصمة أخرى حتى في الإنسان نفسه.

وفي ظل عجلة التطور التي فاقت سرعة الضوء والتقدم الذي أصبح يمس الشبكة المعلوماتية وانفتاحها للجميع، اتجه الواقع العملي إلى البحث عن فكرة بديلة للتوقيع التقليدي تضاهي هذا التوقيع في حجيته وقدرته على الإثبات.

فالتوقيع الرقمي هو آلية يتم استخدامها في الأنظمة الإلكترونية لتحديد هوية المستخدم والتأكد منها وهو آلية لضمان عنصر الأمان والسرية ويساعد على منع وحظر القيام بأية تعديلات في الوثائق بعد وضع التوقيع وهو يعتبر من بين التوقيعات الأكثر أمانا.

وتنبع أهمية التوقيع الإلكتروني في تصديق أن الرسالة لم يتم تغييرها وهو يوفر ضمان عدم حصول أي تغيير على الرسالة لأنه من الصعب تزوير التوقيع والعبث به. بمعنى أوسع فإنه يمنع أي مستخدم غير شرعي من تعديل أي إجراء على البيانات (الخصوصية) ويتم بموجبه التحقق من هوية المرسل ومصدر البيانات عن طريق شهادات التصديق الإلكتروني المرخص بها دوليا (التحقق) كما يضمن خاصية البيانات عن طريق تقنية التشفير (وحدة البيانات) ويحقق خاصية عدم الإنكار.

ورد موضوع التوقيع الإلكتروني في القانون الجزائري في المادة 2/327 من القانون رقم 05-10 المؤرخ في 2005/06/20 المتضمن القانون المدني.

وأكد على أن الإثبات بالكتابة في الشكل الإلكتروني يعتبر في نفس مرتبة الإثبات بالكتابة على الورق، بشرط أمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها[6].

أما المشرع الفرنسي، فقد سبق الجزائري في هذا الشأن وأقر بالتوقيع الإلكتروني ابتداء من 13مارس 2000 من خلال القانون رقم 230 لسنة 2000 الذي صدر في صورة تعديل للنصوص المنظمة للإثبات في القانون المدني الفرنسي حيث توافق هذا القانون مع كثرة استخدام المحررات الإلكترونية وأدرج هذا التعديل في المادة 1316 من نفس القانون في ست فقرات أضفى من خلالها الحجية المطلقة للكتابة الإلكترونية في الإثبات وساوى بينها وبين الحجية التي تتمتع بها الكتابة الخطية.

يعتمد معيار التوقيع الرقمي Digital Signature Standard (DSS) على أسلوب من أساليب التشفير الذي يستخدم خوارزمية التوقيع الرقمي Digital Signature Algorithm (DSA) وهي صيغة من التواقيع الرقمية التي صادقت عليها الولايات المتحدة.

الفرع الثاني: التشفير من تقنيات الأمن المعلوماتي

يرتبط التوقيع الإلكتروني ارتباطا عضويا بالتشفير (Encryption) وهو عملية تغيير في البيانات حيث لا يتمكن من قراءتها سوى الشخص المستقبل وحده باستخدام مفتاح فك التسفير.

والطريقة الشائعة للتشفير تتمثل في وجود مفتاحين، المفتاح العام(Public key) وهو معروف للكافة ومفتاح خاص (Private key)الذي لا يكون إلا بحوزة الشخص الذي أنشأه.

فيمكن للشخص الذي يملك المفتاح العام أن يرسل الرسائل المشفرة، لكن لا يستطيع أن يفك شيفرة الرسالة إلا صاحب المفتاح الخاص. بمعنى أدقّ، فإن لكل حاسوب مفتاح سري (رمز) يمكن أن يستخدم لتشفير حزمة من المعلمات قبل إرسالها عبر الشبكة إلى حاسوب آخر.

يتطلب المفتاح الخاص معرفة مجموع الحواسيب التي تتصل مع بعضها ويقوم بتثبيت المفتاح على كل منها.

أما لتشفير المفتاح العام، فيستخدم مزيجا من المفتاح الخاص والعام حيث يكون المفتاح الخاص معروفا من قبل الحاسوب الشخصي للفرد فقط بينما المفتاح العام يعطى من قبل الحاسوب الخاص إلى أي حاسوب يريد أن يتصل معه بشكل آمن.

ولفك ترميز رسالة مشفرة يجب على الحاسوب أن يستخدم المفتاح العام الذي زوده به الحاسوب المرسل للرسالة مع المفتاح الخاص به[7].

---

[6]– درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني– دراسة مقارنة–، رسالة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، 2015–2016، ص203.

فالعلاقة القائمة بين التوقيع الرقمي والتشفير، أن التوقيع الرقمي هو ختم رقمي مشفر وإذا تطابق المفتاح الذي يملكه صاحب الختم مع التوقيع الرقمي على الرسالة الإلكترونية معنى ذلك أن مرسل الرسالة هو من أرسلها وليس شخصا آخر، الأمر الذي يضمن عدم تعرض الرسالة لأي تعديل أو تغيير[8].

هناك عدة جوانب في الحديث عن التشفير الأول تقني أو فني والآخر قانوني لذلك سنفصل الكلام فيهما تباعا وكما يلي:

أولا: الجانب الفني للتشفير

إن الطريقة الشائعة للتشفير تتمثل بوجود مفتاحان [9]، المفتاح العام public-key وهو معروف للكافة، ومفتاح خاص private-key، يتوفر فقط لدى الشخص الذي أنشأه، ويمكن بهذه الطريقة لأي شخص يملك المفتاح العام، أن يرسل الرسائل المشفرة، ولكن لا يستطيع أن يفك شيفرة الرسالة. إلا الشخص الذي لديه المفتاح الخاص .[10] (سبق التطرق إلى هذا المفهوم)

لذلك يعتبر التشفير إجراء تقني يسمح بزيادة الأمان والثقة في التجارة الإلكترونية ويضمن السرية الكاملة في ذلك والحيلولة دون تعديلها أو اختراقها.

وقد اكتشف التشفير سنة 1980 من قبل ثلاثة علماء، وعرفوا علم التشفير بأنه العلم الذي يعتمد على وسائل وطرق تجعل من المعلومة غير مفهومة وغير مقروءة إلا لأطرافها، حيث يتأكد كل من المرسل والمرسل إليه عدم تسليم الرسالة لطرف ثالث غيرهما، يتم الإطلاع على البيانات الكترونية في المعاملات التجارية والإدارية باستخدام مفتاحين الأول عام معروف لعامة الناس أما الثاني فهو مفتاح خاص لا يعلمه سوى صاحبه، استعمال المفتاحين دلالة قاطعة على التأكد من هوية الأطراف اللذين قد يثبت من ذلك الإجراء رغبتيهما في التعاقد[11].

وتتخلص أغراض التشفير في الآتي:

أ- توثيق الموقع: في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معين ومحدد فإن التشفير ينسب ويعزو الرسالة إلى الموقع.

---

[7]– ما هو التوقيع الإلكتروني؟، ناسا بالعربي، www.nasainarabic.net، ص 2.

[8] –Arab British Academy For Heigher Education, التوقيع الرقمي وتشفير البيانات المرسلة.

[9]– المادة 2 الفقرتين 8 – مفتاح التشفير الخاص : هو عبارة عن سلسلة من الأعداد يحوزها حصريا ا لموقّع فقط وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا ا لمفتاح بمفتاح تشفير عمومي.

مفتاح التشفير العمومي: هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني قانون رقم 15 - 04 مؤرخ أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[10] – لمزيد من التفصيل راجع بحث للأستاذ عبد المجيد ميلاد، تشفير البيانات والتوقيع الالكتروني على الموقع الاتي :
http://www.arabcin.net/modules.php?name=News&file=article&sid=948

[11] – .لمزيد من التفصيل راجع موضوع التحديات القانونية للتجارة الالكترونية على الموقع الالكتروني الاتي :
http://www.opendirectorsite.info/e-commerce/04.htm

ولا يمكن تزوير التوقيع الالكتروني ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه أو يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية.

ب-توثيق الرسالة: كذلك فإن التشفير يعمل على تحديد هوية الرسالة الموقعة بثقة ودقة ويقين أكثر من التوقيعات على الورق. إن عملية التثبت من الصحة تكشف أي تلاعب حيث أن أي مقارنة بين الواحدة يتم إعدادها عند التوقيع والأخرى عند التثبت من الصحة تبين ما إذا كانت الرسالة هو نفسها عندما تم توقيعها.

ج-الفعالية: إن عمليات إنشاء التوقيع الالكتروني والتثبت من صحته بالتشفير تتطلب مستوى عال من الضمان بأن التوقيع الالكتروني هو للموقع بدون تكلف أو رياء. مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة وتستغرق الكثير من الجهد بحيث أنه نادرا ما يتم استخدامها بالواقع – فإن التوقيعات الالكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيرا على الموارد المطلوبة للمعالجة[12].

ثانيا-الجانب القانوني للتشفير

إن كلمة تشفير يونانية الأصل وتعني باللغة الانكليزية (متخفي أو سري)[13] ويعرف التشفير اصطلاحا بأنه عملية تمويه الرسائل أو المعلومات أو البيانات بشكل لا تقرا من احد سوى من الموجهة إليه.وعرفه محمد حسين منصور بأنه (استبدال شكل البيانات من خلال تحويلها إلى رموز أو إشارات لمنع الغير من معرفتها أو تعديلها أو تغييرها ،فالتشفير وسيلة فنية لحماية البيانات من الآخرين [14].في حين عرفه ثالث بأنه (عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير لهم بذلك لا يستطيعون فهم أي شيء لان ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة)[15].

وقد تطرقت القوانين العربية المنظمة للتوقيع الالكتروني إلى تعريف التشفير وتبيان مدلوله فالقانون التونسي مثلا عرفه في الفصل الأول بالاتي (التشفير: إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو

[12]– بيل جيتس، المعلوماتية بعد الانترنت، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت: 1998 ص 47

[13] – باسل يوسف، الاعتراف القانوني بالسندات والتواقيع الالكترونية في التشريعات المقارنة، مجلة دراسات قانونية صادرة عن بيت الحكمة، بغداد: العدد الثاني، 2001 ص 23.

[14] – محمد حسين منصور، المسؤولية الالكترونية، الإسكندرية، دار الجامعة للنشر والتوزيع، ص 180

[15] – هدى قشقوش، الحماية الجنائية للتجارة الالكترونية، القاهرة: دار النهضة العربية، ص 60.

إشارات لا يمكن الوصول إلى المعلومة بدونها)[16]. كما انه قد استحدثت برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي[17].

المطلب الثاني: آلية المصادقة الإلكترونية المستحدثة ومدى نجاعتها

أصبحت المعاملات الإلكترونية تقوم أساسا على مبدأي الثقة والأمان لضمان وبعث الإئتمان في المتعاملين عبر هذه الشبكة. وكان هذا المنطلق دافعا لبعض التشريعات إلى ضرورة خلق طرف محايد يعمل على بث وترسيخ هذه الثقة من أجل حماية المعلومات وتأكيد مصداقيتها.

لذلك عمدت الهيئات المختصة على إسناد مهمة حماية البيانات الإلكترونية إلى جهات معتمدة تعمل على تصديق وتوقيع المعاملات الإلكترونية من أجل ضمان بيئة إلكترونية آمنة.

تنحصر مهمة هذه الجهات في وظيفة التصديق وتأكيد المعاملات بين أطراف العلاقة ويكون ذلك بموجب إصدار شهادة التصديق الإلكتروني التي تضم مجموعة من البيانات وتؤكد صحة ومصداقية التوقيع وانتسابه إلى موقّعه وأن البيانات الواردة في المعاملة لم يتم تغييرها أو تعديلها استنادا إلى وسائل تقنية تعمل على التحقيق في منظومة التوقيع الإلكتروني ورسالة البيانات المودعة.

وأمام هذه المهمة التقنية المعقدة، فإن النصوص التشريعية والتنظيمية الواردة في هذا الشأن لم تبخل في تحديد مسؤولية جهات التوقيع الإلكتروني والقائمين عليها وخصتها بنصوص ردعية خاصة وذلك لتدارك النقص والفراغ الذي يكتنف القواعد العامة التي تنظم مسؤولية القائمين على هذه الجات.

الفرع الأول: التأصيل الفقهي والقانوني لآلية التصديق الإلكتروني

لم يتفق مجموع الفقهاء "الإلكترونيين" على وضع تعريف كامل وشامل وموحد للتوثيق أو التصديق الإلكتروني وجهاته، بل اتخذ هذين الأخيرين تسميات مختلفة عبر التشريعات الدولية والوطنية.

حيث نجد له تعريفا على أساس أنه وسيلة فنية أمنة للتحقق من صحة التوقيع الإلكتروني أو المحرر، حيث يتمّ نسبته إلى شخص أو كيان معين، عبر جهة موثوق بها أو طرف محايد يطلق عليه "مقدّم خدمات التصديق الإلكتروني" [18].

---

[16]– إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة والقانون – مؤتمر القانون والكمبيوتر والإنترنت – المجلد الثالث – ص 976.و انظر كذلك، وليد العاكوم، مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والإنترنت، المجلد الأول، ص 968

[17]– لمنع ومكافحة الجريمة أيضا وقامت إحدى الشركات المعلوماتية بتصميم برامج هدفه الحيلولة دون الدخول الأطفال إلى المواقع الغير المناسبة لهم لاسيما وأن الجناة يقابلون الأطفال من خلال غرف الدردشة، ويوجد كذلك في أسواق الكمبيوتر في الوقت الحال برامج تمكن الآباء من التحكم في استخدام أطفالهم للانترنت. انظر، عبد الفتاح بيومي مجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، 2002،ص 295و ما بعدها.

كما قد عرف أنه الإسناد المؤكد للهويات الإلكترونية، حيث يسمح التصديق بمطابقة بين الهوية الإلكترونية والهوية الحقيقية عن طريق المزاوجة بين المفتاح وهوية المالك والشكل التقني لهذا الإجراء يسمى " شهادة التصديق الإلكنروني"[19].

أمّا من حيث المقصود بجهة التصديق الإلكتروني فهي تماما كمصطلح التصديق لم يتم اتفاق على وضع تسمية موحدة لهذه الجهات عبر كافة التشريعات.

حيث عرفت المادة 2 من قانون الأونسترال النموذجي للأمم المتحدة 2001 بشأن التوقيعات الإلكترونية أن القائم على خدمات التصديق هو شخص يصدر الشهادات ويجوز أن يقدم خدمات أخرى ذات صلة بالتوقيعات الإلكترونية. وبالتالي نجد هذا التعريف قد ألزم جهة التوثيق بضرورة توفير خدمة التصديق الإلكتروني كحد أدنى مع إمكانية تقديم خدمات أخرى لها صلة بالتوقيع الإلكتروني وبالتالي فإن نشاط مقدم الخدمة (Provider certification service)الإلكترونية قد يمتد إلى أنشطة أخرى ذات صلة.

أمّا قانون التوجيه الأوربي رقم 1999/93 المتعلق بالتوقيعات الإلكترونية، فإنه في تعريفه لمقدم خدمات التصديق عرفه بأنه كل كيان أو شخص طبيعي أو معنوي يقدم شهادات توثيق إلكترونية أو يقدم خدمات متصلة بالتوقيع الإلكتروني[20]. والمقصود بهذه الأخيرة التقنيات التي تسمح بإصدار توقيع نموذجي أو خدمة النشر والاطلاع والخدمات المعلوماتية الأخرى كالحفظ في الأرشيف[21].

ثمّ عرف المشرع المصري جهات التصديق الإلكتروني بأنها الجهات المرخص لها بإصدار شهادة التصديق الإلكتروني وتقديم خدمات تتعلق بالتوقيع الإلكتروني[22].

أمّا مشرع إمارة دبي فقد سمى جهة التصديق بمزود خدمات التصديق وعرفها في قانون المعاملات والتجارة الإلكترونية بأنها " أي شخص أو جهة معتمدة أو معترف بها تقوم بإصدار شهادات تصديق إلكترونية أو أية خدمات أو مهمات متعلقة بالتواقيع الإلكترونية المنظمة بموجب الفصل الخامس من هذا القانون"[23]

---

[18]– منصور محمد حسنين، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006، ص 286.

[19]– حسين الماجي، نظرات في قانون التجارة الإلكترونية، www.arablaw.info.com، 2016/03/30.

[20]– صدر عن البرلمان الأوربي في 1999/12/13 المنشور بالجريدة الرسمية للجماعات الأوربية (OJEC)، www.ojec.com، 2016/09/11.

[21]– عبد الحميد ثروت، التوقيع الإلكتروني (ماهيته، مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات)، دار الجامعة الجديدة، مصر، 2007، ص 163.

[22]– المادة 6/1 من اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، وزارة الاتصالات وتكنولوجيا المعلومات، قرار رقم 109 لسنة 2005، بتاريخ 2005/05/15.

[23]– المادة 2 من قانون المعاملات والتجارة الإلكترونية لإمارة دبي، قانون رقم 2 لسنة 2002. أنظر: زيد حمزة مقدم،" النظام القانوني للتوثيق الإلكتروني (دراسة مقارنة)"، مجلة الشريعة والقانون والدراسات الإسلامية، العدد 24، أوت 2014، ص 08.

حصرا لما سبق تقديمه من تعريف لجهات التصديق فإننا نلمس أن جل التشريعات أسست تعريفها لهذه الجهات على المهمة والوظيفة الأساسية التي تكتنف وجود هذه الجهات والمتعلقة بإصدار شهادات التوثيق الإلكتروني وربطتها بمهام أخرى ذات صلة بالتوقيع الإلكتروني.

أمّا المشرع الجزائري في المادة 11/2 و12 من القانون رقم 15-04 [24]، خلافا للتشريعات السابقة فقد ميز بين نوعين من الجهات المكلفة بالتصديق الإلكتروني حيث سمى الجهة الأولى "الطرف الثالث الموثوق" والجهة الثانية سماها " مؤدي خدمات التصديق الإلكتروني".

مفهوم الطرف الثالث قصد به الشخص المعنوي الذي يقوم بمنح شهادات تصديق إلكتروني موصوفة إضافة إلى الخدمات الأخرى المتعلقة بالتصديق لفائدة المتدخلين في الفرع الحكومي فقط، مثل الإدارات والوزارات. وهو يخضع لرقابة السلطة الحكومية للتصديق. هذه السلطة هي سلطة تنشأ لدى الوزير المكلف بالبريد وتكنولوجيات الإعلام والاتصال، تتمتع بالاستقلال المالي والشخصية المعنوية، تكلف بمتابعة ومراقبة نشاط التصديق الإلكتروني وكذا توفير خدمات التصديق الإلكتروني لفائدة المتدخلين في الفرع الحكومي[25].

أما المقصود بمؤدي خدمات التصديق فهو الشخص الطبيعي أو المعنوي الذي يقوم بمنح شهادات تصديق إلكتروني موصوفة إضافة إلى خدمات أخرى في مجال التصديق لفائدة الجمهور وهو يخضع لرقابة السلطة الاقتصادية للتصديق الإلكتروني. هذه السلطة الاقتصادية هي السلطة المكلفة بضبط البريد والمواصلات السلكية واللاسلكية، تكلف بمتابعة ومراقبة مؤدي خدمات التصديق الإلكتروني الذين يقدمون خدمات التوقيع والتصديق الإلكترونيين لصالح الجمهور[26].

الفرع الثاني: مسؤولية سلطات التصديق الإلكتروني

تفرض العلاقة الثلاثية لجهات التصديق والموقّع والمرسل إليه ضرورة نشوء بعض الالتزامات التي تقع على عاتق كل طرف، وأهم التزام هو ما يقع على جهات التصديق لأن أهميتها تعمل على دعم الثقة لدى المتعاملين وهذه الثقة تتجسد في صحة ومصداقية شهادة التصديق الإلكتروني.

تعمل جهات التصديق من أجل تحقيق ذلك على استخدام أنظمة إلكترونية وموارد بشرية تبذل كل العناية اللازمة لضمان صحة المعلومات الواردة في الشهادات التي يصدرها مؤدو خدمة التصديق. وبالتالي إذا ثبت اتخاذ الاحتياطات الكافية والإجراءات اللازمة قانونا وعملا،

[24]– القانون رقم 15-04 المؤرخ في 2015/02/01 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية عدد 06، المؤرخة في 2015/02/10.

[25]– المادة 26 و28 من القانون رقم 15-04.

[26]– المادة 29 و30 من القانون رقم 15-04.

فإن جهات التصديق تنفي عن نفسها المسؤولية التي تلحق الأضرار بالغير والثابتة في الشهادة حتى لو أثبت الغير أنها مزورة وغير صحيحة بسبب لا يكون لجهة التصديق يد فيه.

لقد فرضت القواعد العامة أن المسؤولية هي نتيجة مخالفة التزام قانوني أو التزام عقدي، معنى ذلك، في حالة ارتكاب الخطأ إما أن تترتب مسؤولية مدنية سواء عقدية إذا كان الخطأ عقديا أو تقصيرية إذا كان الخطأ مخالفا لالتزام قانوني حيث تترتب المسؤولية التقصيرية (المادة 124 من القانون المدني).

أو أن تترتب مسؤولية جزائية حيث يكيف الفعل غير المشروع الذي ارتكبه مؤدي خدمة التصديق سواء بصفته شخصا معنويا أو طبيعيا فعلا مجرما يعاقب عليه وفق الأحكام العامة المنصوص عليها في قانون العقوبات.

لذلك فقد أصبحت هذه المبادئ تدخل ضمن المفاهيم المكتسبة التقليدية وبالتالي لا داعي للتطرق إلى تفصيلها.

غير أن النصوص العامة لم تتمكن من تغطية الأخطاء المرتكبة من طرف جهات التصديق الإلكتروني وأمام عدم الكفاية تلك، فقد أولت العديد من التشريعات اهتماما واسعا لتنظيم أحكام مسؤولية جهات التصديق الإلكتروني ووضع قواعد قانونية خاصة تحدد مسؤولية جهات التصديق. ولن يسع المجال للتطرق إلى كل التشريعات بل سيتم الاكتفاء بالبعض منها فقط.

لقد أقر المشرع الأوربي على وجه العموم أن التوقيع الإلكتروني يتمتع بذات الحجية التي يتمتع بها التوقيع التقليدي غير أنه ميز بين نوعين من التوقيعات، التوقيع الإلكتروني المتقدم والتوقيع الإلكتروني غير المتقدم[27]. ولكي يكون التوقيع الإلكتروني متقدما فإنه يجب أن يكون ناشئا تحت رقابة منظومة آمنة لإنشاء التوقيع وأن يكون هذا الإنشاء بموجب شهادة معتمدة.

أمام ذلك نظّم التوجيه الأوربي مسؤولية الجهات المختصة بإصدار شهادات التوثيق بنصوص خاصة حيث جسد قيام هذه المسؤولية على قاعدتين، أولها المسؤولية المفترضة لجهات التصديق الإلكتروني وثانيها قاعدة جواز تحديد نطاق صلاحية شهادة التوثيق الإلكترونية.

تؤكد الفقرة الأولى من المادة السادسة من قانون التوجيه الأوربي أن المكلف بخدمة التوثيق الإلكتروني الذي يصدر شهادة معتمدة يكون مسؤولا عن الضرر الذي يتعرض له الشخص الطبيعي أو المعنوي الذي اعتمد هذه الشهادة.

[27]- المادة 02 من قانون التوجيه الأوربي المتعلق بالتوقيعات الإلكترونية: "يكون التوقيع الإلكتروني متقدما إذا استوفى الشروط التالية: 1- أن يرتبط وبشكل منفرد بصاحب التوقيع، 2- أن يتيح كشف هوية صاحب التوقيع، 3- أن يتم إنشاؤه من خلال وسائل موضوعة تحت رقابة صاحب التوقيع، 4- أن يرتبط بالبيانات التي وضع عليها التوقيع إلى درجة أن أي تعديل لاحق على البيانات يمكن كشفه"

غير أن هذه القرينة تبقى بسيطة يمكن إثبات عكسها حيث تتمكن جهة التصديق أن تنفي عن نفسها المسؤولية بإثبات أنها لم ترتكب أي إهمال أو تقصير فيقتصر أثر القرينة على مجرد نقل عبء الإثبات أو بإثبات السبب الأجنبي[28].

أما الفقرة الثالثة والرابعة من المادة السادسة من هذا القانون فإنها تبين أنه يجوز لجهات التصديق أن تحدد نطاق صلاحية شهادة التوثيق الإلكترونية في حالتين هما: تحديد نوع المعاملات التي تستخدم بشأنها شهادة التوثيق، وتحديد القيمة المالية للصفقات التجارية التي يتم بشأنها استخدام الشهادة.

فإذا ما حددت جهة التصديق نطاق صلاحية الشهادة على النحو السابق وكان التحديد قابلا للتمييز من قبل الغير وحدث تجاوز من قبل هذا الأخير للحدود المعينة من جهة التصديق الإلكتروني بأن تمّ استخدام الشهادة بصورة تعسفية فإن جهة التصديق لا تكون مسؤولة عن الضرر الناتج عن هذا الاستخدام المتجاوز.

أما عن مسؤولية جهات التصديق وفقا للقانون الجزائري، فإن هذا الأخير يفتقد إلى نصوص تساعد على توضيح وفهم طبيعة مسؤولية مؤدي خدمات التصديق. يتبين من النصوص الواردة في القانون رقم 15-04 أنه يتطلب لقيام مسؤولية مقدمي خدمات المصادقة صدور خطأ أو إهمال من قبل مزود الخدمة، ويتضح ذلك من مضمون العناية التي يجب أن يمارسها مزود الخدمة تجاه البيانات التي يوردها في الشهادة، والتي حددتها الفقرات من المادة53 بالعناية المعقولة، والعناية المعقولة هي العناية المعتادة التي يمارسها مزودو خدمات التصديق في مجال توثيق الشهادات الإلكترونية والتوقيع الإلكتروني.

وقد أعفت المادة 54 مزودي خدمات المصادقة الإلكترونية من المسؤولية إذا أثبت أنه لم يرتكب أي خطأ أو إهمال.وإعمالا للقواعد العامة في المسؤولية المدنية، فالخطأ وحده غير كاف لقيام مسؤولية مزود الخدمة، وإنما يجب أن يترتب على ذلك ضرر يلحق بالغير الذي عول بحسن نية على الشهادة الإلكترونية مع توافر علاقة السببية بين الخطأ والضرر.

ويتبين أيضًا من المادة 53 أنه يشترط لقيام مسؤولية مزود الخدمة من الأضرار التي تصيب الغير، أن يكون هذا الغير قد اعتمد بصورة معقولة على الشهادة التي تصدر عن مزود الخدمة، كما للشخص أن يعتمد على التوقيع الالكتروني أو الشهادة الالكترونية إلى المدى الذي يكون فيه مثل ذلك الاعتماد معقولا[29].

كما ذكر بهذا الشأن العقوبات الجزائية والغرامات المالية في حالة ثبوت مسؤولية جهة التصديق وهذه العقوبات قد تكون مالية يتراوح قدرها حسب تصنيف الأخطاء المنصوص عليها في دفتر الأعباء أو سياسة التصديق ومصادق عليها من طرف السلطة الاقتصادية. أو قد تكون هذه العقوبات سالبة للحرية[30].

---

[28]– عيسى غسان الربطي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 159.

[29] -لقد عبر المشرع التونسي عن الاعتماد المعقول بالاعتماد الذي يتم بحسن نية، وذلك في الفصل 22 من القانون رقم 83 لسنة 2000 المتعلق بالمبادلات والتجارة الالكترونية، حيث جاء فيه" يكون مزود خدمة المصادقة الالكترونية مسؤولا عن كل ضرر حصل لكل شخص وثق عن حسن نية في الضمانات المنصوص عليها بالفصل 18 من هذا القانون."

[30]– المادة 67 من القانون رقم 15-04.

كما تؤكد أحكام القانون رقم 15-04 أن هناك حالات يعفى فيها مؤدي خدمات التصديق من المسؤولية عن الأضرار في حالة تجاوز استعمال شهادة التصديق عن الحدود المفروضة لاستعمالها إذ يمكن لمؤدي خدمات التصديق أن يشير إلى الحدّ الأقصى أين تعفى جهات التصديق عند عدم احترام صاحب شهادة التصديق الموصوفة بشروط استعمال بيانات التوقيع الإلكتروني.

المبحث الثاني: المواجهة الدولية والجزائرية لتعزيز الأمن الرقمي

سنتطرق في هذا الشق إلى الأساليب التقنية لحماية المعطيات والمواقع الإلكتروني (المطلب الأول). التصعيد التشريعي الموضوعي والإجرائي الجزائري للوقاية من المد الإجرامي الرقمي (المطلب الثاني) على التوالي

المطلب الأول: الأساليب التقنية لحماية المعطيات والمواقع الإلكتروني[31]

إن أهّم الأساليب المنتشرة في الوقت الحالي لحماية ممتلكات مواقع المنشآت الإلكترونية هي كما يلي:

الفرع الأول: التشفير الإلكتروني[32] (cryptographie) [33]

تحظي تقنيات وسياسات التشفير في الوقت الحاضر باهتمام استثنائي في ميدان امن المعلومات، ومرد ذلك إن حماية التشفير يمثل الوسيلة الأكثر أهمية لتحقيق وظائف الأمن الثلاثة، السرية والتكاملية وتوفير المعلومات، فالتشفير تقنيات تدخل في مختلف وسائل التقنية المنصبة على تحقيق حماية هذه العناصر، فضمان سرية المعلومات أصبح يعتمد من بين ما يعتمد على تشفير وترميز الملفات والمعطيات بل تشفير وسائل التثبت وكلمات السر، كما أن وسيلة حماية سلامة المحتوى تقوم على تشفير البيانات المتبادلة والتثبيت لدى فك التشفير أن الرسالة الالكترونية لم تتعرض لأي نوع من التعديل أو التغيير.[34]

---

[31]– مصطفى محمد، أساليب إجرامية بالتقنية الرقمية، ماهيتها ومكافحتها، دار الكتب القانونية، المحلة الكبرى، 2005، ص 26 وما بعدها.

[32]– تشفير البيانات هي عملية ترميز البيانات قبل تحويلها أو إرسالها واستخدامها في إجراءات التبادل ومن ثم فك الترميز بعد الإرسال واهم ما في التشفير هي مفاتيح الرموز والأشخاص المخولين بمعرفتها ولها طريقتين أساسيتين تعرف ب Data Encryption Standard (DES) و (PKE) Public Key Encryption .

[33] – www.crybtographie.com

[34] Le décryptement est l'action consistant à retrouver le texte en clair sans connaître la clef de déchiffrement .Confidentialité est historiquement le premier problème posé à la cryptographie. Il se résout par la notion de chiffrement, mentionnée plus haut. Il existe deux grandes familles d'algorithmes cryptographiques à base de clefs : les algorithmes à clef .secrète ou algorithmes symétriques , et les algorithmes à clef publique ou algorithmes asymétriques. Ghislaine. Labouret. Introduction à la cryptographie. P 11.Hervé Schauer Consultants (HSC). 1999-2001 Hervé Schauer Consultants www.hsc.fr. Voir aussi Emmanuel.Bresson .CRYPTOGRAPHIE. Laboratoire de cryptographie - SGDN/DCSSI- Emmanuel.Bresson@sgdn.gouv.fr. Renaud Dumont. Cryptographie et Sécurité informatique .Université de Liège. Faculté des Sciences Appliquées.. 2010.p91.

ويعد التشفير بوجه عام وتطبيقاته العديدة وفي مقدمتها التواقيع الالكترونية، الوسيلة الوحيدة تقريبا لضمان عدم إنكار التصرفات عبر الشبكات الالكترونية، وبذلك فان التشفير يمثل الإستراتيجية الشمولية لتحقيق الأهداف الأمن من جهة، وهو مكون رئيس لتقنيات ووسائل الأمن الأخرى، خاصة في بيئة الأعمال الالكترونية والتجارة الإلكترونية والرسائل الالكترونية وعموما البيانات المتبادلة بالوسائط الالكترونية.

ومن حيث مفهومه، فان التشفير يمر بمرحلتين رئيسيتين، الأولى تشفير النص على نحو يحوله إلى رموز غير مفهومة أو مقروءة بلغة مفهومة، والثانية، فك الترميز بإعادة النص المشفر إلى وضعه السابق كنص مفهوم ومقروء، وهذه المسالة تقوم بها برمجيات التشفير التي تختلف أنواعها ووظائفها.

أما من حيث طرق التشفير، فثمة التشفير الترميزي، والتشفير المعتمد على مفاتيح التشفير، التي قد تكون مفاتيح عامة أو خاصة او مزيجا منها.

– هناك عدة جوانب في الحديث عن التشفير الأول تقني أو فني والآخر قانوني لذلك سنفصل الكلام فيهما تباعا وكما يلي:

أولا: الجانب الفني للتشفير

ان الطريقة الشائعة للتشفير تتمثل بوجود مفتاحان [35]، المفتاح العام public-key وهو معروف للكافة، ومفتاح خاص private-key، يتوفر فقط لدى الشخص الذي أنشأه، ويمكن بهذه الطريقة لاي شخص يملك المفتاح العام، ان يرسل الرسائل المشفرة، ولكن لا يستطيع ان يفك شيفرة الرسالة. الا الشخص الذي لديه المفتاح الخاص .[36]

1. انشاء التوقيع الالكتروني يستخدم نتيجة هاش يتم اشتقاقها من وتكون مقتصرة على كل من الرسالة الموقعة ومفتاح خاص معين. بغرض أن تكون نتيجة ال هاش آمنة ومحكمة يجب ألا يكون هناك إمكانية أو احتمال ضئيل فقط بأن نفس التوقيع الالكتروني يمكن إنشائه من خلال تركيبة أي رسالة أخرى أو مفتاح خاص آخر.

2. التثبت من صحة التوقيع الالكتروني: وهي عملية التأكد من التوقيع الالكتروني من خلال الرجوع إلى الرسالة الأصلية وإلى مفتاح عام معين وبهذا يتم تحديد ما إذا كان التوقيع الالكتروني قد تم إنشائه لتلك الرسالة باستخدام المفتاح الخاص المقابل للمفتاح العام المشار إليه.

---

[35]– المادة 2 الفقرتين 8 –مفتاح التشفير الخاص: هو عبارة عن سلسلة من الأعداد يحوزها حصريا ا لموقّع فقط وتستخدم لإنشاء التوقيع الإلكتروني ويرتبط هذا ا لمفتاح بمفتاح تشفير عمومي.

9 - مفتاح التشفير العمومي : هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكينهم من التحقق من الإمضاء الإلكتروني وتدرج في شهادة التصديق الإلكتروني قانون رقم 15 - 04 مؤرخ أوّل فبراير سنة 2015 يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين.

[36] – لمزيد من التفصيل راجع بحث للأستاذ عبد المجيد ميلاد، تشفير البيانات والتوقيع الالكتروني على الموقع الاتي:
http://www.arabcin.net/modules.php?name=News&file=article&sid=948

مما تقدم تظهر العلاقة بين التوقيع الكتروني والتشفير، فالتوقيع الالكتروني هو ختم رقمي مشفر، يملك مفتاحه صاحب الختم. ويعني تطابق المفتاح مع التوقيع الرقمي على الرسالة الالكترونية على ان مرسل الرسالة هو من ارسلها فعلا، وليست مرسلة من قبل شخص آخر. ويضمن التوقيع الرقمي عدم تعرض الرسالة لأي نوع من أنواع التعديل، بأي طريقة. لذلك يعتبر التشفير إجراء تقني يسمح بزيادة الأمان والثقة في التجارة الإلكترونية ويضمن السرية الكاملة في ذلك والحيلولة دون تعديلها أو اختراقها.

وقد اكتشف التشفير سنة 1980 من قبل ثلاثة علماء، وعرفوا علم التشفير بأنه العلم الذي يعتمد على وسائل وطرق تجعل من المعلومة غير مفهومة وغير مقروءة إلا لأطرافها، حيث يتأكد كل من المرسل والمرسل إليه عدم تسليم الرسالة لطرف ثالث غيرهما،

يتم الإطلاع على البيانات الكترونية في المعاملات التجارية والإدارية باستخدام مفتاحين الأول عام معروف لعامة الناس أما الثاني فهو مفتاح خاص لا يعلمه سوى صاحبه، استعمال المفتاحين دلالة قاطعة على التأكد من هوية الأطراف اللذين قد يثبت من ذلك الإجراء رغبتيهما في التعاقد[37].

وتتخلص أغراض التشفير في الآتي:

أ-توثيق الموقع: في حال كان هناك زوج من المفاتيح واحد عام والآخر خاص وكانا مرتبطين بموقع معين ومحدد فإن التشفير ينسب ويعزو الرسالة إلى الموقع. ولا يمكن تزوير التوقيع الالكتروني ما لم يفقد الموقع السيطرة على المفتاح الخاص (تعرض المفتاح الخاص للخطر) كأن يقوم بإفشائه او يفقد الوسط أو الوسيلة المحتفظ به فيها مثل البطاقة الذكية.

ب-توثيق الرسالة: كذلك فإن التشفير يعمل على تحديد هوية الرسالة الموقعة بثقة ودقة ويقين أكثر من التوقيعات على الورق. إن عملية التثبت من الصحة تكشف أي تلاعب حيث أن أي مقارنة بين الواحدة يتم إعدادها عند التوقيع والأخرى عند التثبت من الصحة تبين ما إذا كانت الرسالة هو نفسها عندما تم توقيعها.

ج-الفعالية: إن عمليات إنشاء التوقيع الالكتروني والتثبت من صحته بالتشفير تتطلب مستوى عال من الضمان بأن التوقيع الالكتروني هو للموقع بدون تكلف أو رياء. مقارنة مع الأساليب الورقية مثل بطاقات نموذج اعتماد التوقيع والتي هي أساليب مملة وتستغرق الكثير من الجهد بحيث أنه نادرا ما يتم استخدامها بالواقع – فإن التوقيعات الالكترونية تعطي وتولد درجة ضمان أعلى بدون أن تضيف كثيرا على الموارد المطلوبة للمعالجة[38].

---

[37] – .لمزيد من التفصيل راجع موضوع التحديات القانونية للتجارة الالكترونية على الموقع الالكتروني الاتي :
http://www.opendirectorysite.info/e-commerce/04.htm

[38]– بيل جيتس، المعلوماتية بعد الانترنت، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت: 1998 ص 47

ثانيا- الجانب القانوني للتشفير

إن كلمة تشفير يونانية الأصل وتعني باللغة الانكليزية (متخفي أو سري)[39] ويعرف التشفير اصطلاحا بأنه عملية تمويه الرسائل أو المعلومات أو البيانات بشكل لا تقرا من احد سوى من الموجهة إليه.وعرفه محمد حسين منصور بأنه (استبدال شكل البيانات من خلال تحويلها إلى رموز أو إشارات لمنع الغير من معرفتها أو تعديلها أو تغييرها ،فالتشفير وسيلة فنية لحماية البيانات من الآخرين [40].في حين عرفه ثالث بأنه (عملية الحفاظ على سرية المعلومات الثابت منها والمتحرك باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير لهم بذلك لا يستطيعون فهم أي شيء لان ما يظهر لهم هو خليط من الرموز والأرقام والحروف غير المفهومة)[41].

وقد تطرقت القوانين العربية المنظمة للتوقيع الالكتروني إلى تعريف التشفير وتبيان مدلوله فالقانون التونسي مثلا عرفه في الفصل الأول بالاتي (التشفير: إما استعمال رموز أو إشارات غير متداولة تصبح بمقتضاها المعلومات المرغوب تمريرها أو إرسالها غير قابلة للفهم من قبل الغير أو استعمال رموز أو إشارات لا يمكن الوصول إلى المعلومة بدونها)[42].

- كما انه قد استحدثت برامج تشفير متقدمة لحماية البيانات المخزنة على شبكات الحاسب الآلي[43].

الفرع الثاني: الشهادات الرقمية

الشهادة الرقمية هي بطاقة هوية رقمية لكيان (شخص اعتباري أو طبيعي) أو مورد معلوماتي يكون هو موضوع الشهادة. وهي تشمل، إلى جانب أشياء أخرى، هوية صاحب الشأن (حامل الشهادة)، والمفتاح العمومي المخصص لصاحب الشأن وهوية الجهة المُصدِرَة[44].

---

39 – باسل يوسف، الاعتراف القانوني بالسندات والتواقيع الالكترونية في التشريعات المقارنة، مجلة دراسات قانونية صادرة عن بيت الحكمة، بغداد: العدد الثاني، 2001 ص 23.

40 – محمد حسين منصور، المسؤولية الالكترونية، الإسكندرية: دار الجامعة للنشر والتوزيع، ص 180

41 – هدى قشقوش، الحماية الجنائية للتجارة الالكترونية، القاهرة: دار النهضة العربية، ص 60.

42– إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة والقانون – مؤتمر القانون والكمبيوتر والإنترنت – المجلد الثالث – ص 976.و انظر كذلك، وليد العاكوم، مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والإنترنت، المجلد الأول، ص 968

43– لمنع ومكافحة الجريمة أيضا وقامت إحدى الشركات المعلوماتية بتصميم برامج هدفه الحيلولة دون الدخول الأطفال إلى المواقع الغير المناسبة لهم لاسيما وأن الجناة يقابلون الأطفال من خلال غرف الدردشة، ويوجد كذلك في أسواق الكمبيوتر في الوقت الحال برامج تمكن الآباء من التحكم في استخدام أطفالهم للأنترنت. انظر، عبد الفتاح بيومي مجازي، الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، 2002،ص 295و ما بعدها.

44– حمدون إ. تورية، سامي البشير المرشد، دليل الأمن السبراني للبلدان النامية، الاتحاد الدولي للاتصالات، طبعة 2007، ص 63.

فالشهادات الرقمية هي ملفات تستخدم لأغراض الأمن الالكتروني تتضمن أسم وعنوان صاحب الشهادة وتاريخ التصريح ومفتاح التشفير المستخدم في الوثيقة والذي من خلاله يتم التعرف على التوقيع الالكتروني [45]والتأكد من صلاحيته .بالإضافة إلى اسم الشركة التجارية ويستخدم في العادة في نظام (SSL)[46]

طبقة المقابس الآمنة SSL وبروتوكولات نقل النص الفوقي HTTP (S-HTTP)، و**بروتوكول طبقة المقابس الآمنة SSL Secure Sockets Laye هو** بروتوكول تشفير يعمل على توفير بيئة آمنة، خلال نقل البيانات المشفرة بين المتصفح وجهاز الخادم في الموقع، وما يحدث باختصار هو أنّ المتصفح يقوم بإرسال رسالة من خلال بروتوكول SSL إلى جهاز الخادم فيستجيب ويرسل شهادة (SSL Certificate) تتضمن في محتواها المفتاح العام للموقع(Public Key) ، **ومن ثم يقوم المتصفح بالتحقق من هذه الشهادة من خلال ثلاثة ركائز أساسية:**

1. أن تكون الشهادة آتية من طرف موثوق به .
2. التحقق من سريان مفعولها في الوقت الحالي وذلك من خلال إلقاء نظرة على تاريخ إصدار الشهادة وتاريخ انتهائها
3. المقارنة بين اسم الموقع في الشهادة واسم الموقع في الخادم للتأكد من أن الشهادة مرتبطة بالموقع وقادمة منه.

وبعد التحقق من الشهادة يعمل على إنشاء مفتاح عشوائي للتشفير (Symmetric Key Encryption)يقوم بدوره على تشفير البيانات التي تنتقل من المتصفح إلى جهاز الخادم باستخدام بروتوكول التحكم بالإرسال وبروتوكول الإنترنت (TCP/IP)مما يضمن عدم التعرّض لهذه البيانات من قبل أي جهة أخرى فلا يمكن لأحد قراءتها سوى المرسل والمستقبل، وفي نهاية المطاف يقوم الموقع بفك شيفرة الرسالة الواردة إليه من المتصفح وذلك باستخدام مفتاح خاص بالموقع ذاته(Private Key) ، ثم يستخدم المفتاح العشوائي لبقية الاتصال.

---

[45] -Fritze Grupe – Stephen G. Kerr – William Kuechler and Nilesh Patel, "Understanding Digital Signatures", The CPA Journal, June 2003.

[46] SSL (Secure Sockets Layer)
SSL est un protocole de sécurité permettant l'encryptage de messages, l'authentification d'un serveur, le maintient de l'intégrité d'un message, et optionnellement, l'authentification d'un client dans une connexion tcp/ip.
TLS (Transport Layer Security) est le successeur de SSL basé sur ce dernier.
SSL est intégré dans Netscape, Internet Explorer, et la plupart des applications serveur web. Développé initialement par Netscape, SSL a tout de même bénéficié du support de Microsoft et d'autres éditeurs de logiciels Internet Clients/Serveur ; ainsi, il est devenu un standard, jusqu'à l'apparition de TLS. Le mot « Socket » fait référence à la transmission de données par cette méthode entre un client et un serveur sur un réseau, ou aussi entre 2 couches sur un même terminal. SSL utilise le système d'encryptage de clés public/privé de l'algorithme de cryptage RSA qui inclut aussi l'utilisation d'un certificat.

الجدير بالذكر أن استخدام هذه التقنية يعمل على إحداث تغيير طفيف في عنوان الموقع الإلكتروني كالبنك مثلاً وهذه دلالة واضحة على وجود أمن معلوماتي في الشركة أو الإدارة [47].

وعند التطرق إلى مثال البنك فإننا نلحظ عند الدخول إلى موقع البنك بأن عنوانه يبدأ ب"http" ولكن بمجرد الضغط على صفحة تسجيل الدخول إلى الحساب فإن العنوان يتغير من"http" إلى" https"، بالإضافة إلى أيقونة الأمان والتي تظهر في أسفل صفحة الموقع.

الفرع الثالث: برمجيات الجدران النارية والشبكات الافتراضية الخاصة: [48]

جدار النار: هو عبارة عن مجموعة من البرمجيات والأجهزة التي يتم إعدادها لتحتل الحدود الفاصلة بين شبكتنا والشبكة التي نريد ان نحمي او نقي حواسيب شبكتنا منها، وهي غالبا ما تكون شبكة الانترنت.

---

[47]– مهران زهير المصري، السياسات الأمنية للمواقع الإلكترونية، مجلة الباحثون العدد 40، 2010، متوفر على الموقع التالي:
http://kenanaonline.com/users/ahmedkordy/posts/330241

[48]– آلية عمل الجدران النارية، هناك ثلاثة طرق تستند إليها الجدران النارية في آلية عملها:

تصفية الحزم(Packet Filtering) :تنتقل المعلومات على هيئة حِزم تمّر خلال الجدار النّاري الذي يقوم بدوره بفحصها والتحقق من موافقتها للشروط.

وكيل الخدمة(Proxy Service) : يعيّن الجدار النّاري نفسه وكيلاً عن الشبكة الداخلية فيكون بذلك قد حجب عناوين الشبكة الداخلية وبالتالي يتّم إرسال البيانات إلى عنوان الجدار الناري الذي يقوم بدوره بتوجيهها إلى وجهتها الأصلية.

مراقبة السياق(Stateful Inspection)) :إن الجدار الناري هنا يقوم بفحص حقول معيّنة في الحزم فلا يفحص مكونات الحزم كلها بل يعمل على مقارنتها بالحقول المناظرة لها بنفس السياق (مجموعة الحزم الإلكترونية المتبادلة عبر شبكة الإنترنت)، وعندما يكتشف أن حزم معينة لم تلتزم بقواعد السياق فإن ذلك دليل قاطع على وجود اختراق يهدّد أمن الموقع.

وهناك عدة معايير يمكن استخدامها لمعرفة ما إذا كانت الحزم صحيحة وهي كالآتي :

أ– العنوان الرقمي :(IP Address) هو رقم لكل مشترك على الشبكة العنكبوتية يوفّر للجدار الناري المقدرة على التحكم بالسماح أو المنع لمرور الحزم القادمة.

ب– اسم النطاق (Domain Name) : يتيح للجدار الناري منع مرور الحزم القادمة من نطاق معيّن

ت– بروتوكول التخاطب(Protocol) : وهي طريقة للتخاطب وتبادل المعلومات بين العميل والمنشأة، أمّا بالنسبة للعميل فقد يكون شخصاً أو برنامجاً كالمتصفح .(Browser)

تتعدّد هذه البروتوكولات وأبرزها ما يلي :

بروتوكول :HTTP يستعمل لتبادل المعلومات بين المتصفح وجهاز الخادم .

بروتوكول : FTPيستخدم لنقل الملفات عوضاً عن إرسالها. كمرفقات (Attachment)في البريد الإلكتروني.

بروتوكول :SMTP يستعمل لنقل البريد الإلكتروني .

بروتوكول :SNMP يستعمل لإدارة الشبكات وجمع المعلومات .

بروتوكول :Telnet يستعمل للتحكم بالجهاز عن بعد .

وأخيراً فإن هناك خانة في الحزم تدل على نوع البروتوكول، يقوم الجدار الناري بالتحقق منها، وبناءً على ذلك فإذا كان البروتوكول مسموحاً به يقوم بتمريره وإلا فيمنعه من المرور.

Information Security Fundamentals (2nd Edition).How Encryption Works 2008 –
http://kenanaonline.com/users/ahmedkordy/posts/330241

الهدف من جدار النار: هو التغلب على أكبر قدر ممكن من الثغرات الأمنية من خلال بناء قناة اتصال توجه إليها المرسلات والمعلومات المتبادلة مع شبكة الانترنت لمراقبتها والسيطرة على خروجها أو دخولها من وإلى شبكتنا، فقد يمنع الجدار كل (أو جزء) حركة المرور من شبكتنا باتجاه خدمات الانترنت باستثناء البريد الالكتروني، أو يستخدم جدار النار لمنع الوصول على المواقع المشبوهة.

و بشكل عام يمكن القول: إن جدران النار هي عبارة عن برامج تقوم بصد محاولات الاختراق او الهجوم الوافد من شبكة الانترنت لتهديد الشبكة الداخلية أو النظام المعلوماتي، وتشبه برامج جدران النار حرس الحدود على الساحل، حيث تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيارة الشبكة المحمية دخولا أو خروجا دون أن يكون مصرحا له بذلك[49] .

أما برمجيات الجدران النارية الحديثة، ورغم أنها لا تزال تقوم باستخدام اسلون فلترة وتصفية البيانات الواردة، فإنها تقوم بعمل ما هو أكثر بكثير من إنشاء الشبكات الافتراضية الخاصة، رقابة محتوى البيانات الوقاية من الفيروسات، وحتى إدارة نوعية الخدمة، وهذه الخدمات جميعها تعتمد على ميزة أساسية وهي أن الجدران النارية تقع على طرف الشبكة، ومن خلال العقد الماضي، كانت الجدران النارية ببساطة، مجرد أدوات بسيطة تعمل كمنفذ للأنترنت – أو بكلمات أخرى كحراس على طرف الشبكة – تقوم بتنظيم حركة البيانات وحفاظ على امن الشبكة [50]

المطلب الثاني: التصعيد التشريعي الموضوعي والإجرائي الجزائري للوقاية من المد الإجرامي الرقمي

إن الخطوة الأولى للحكومة الجزائرية لمواجهة ما يعرف بالجريمة الالكترونية[51]، صدر سنة 2009 القانون رقم 09-04 المؤرخ في 05 غشت 2009[52]، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، إلا أن تجسيد بنوده على أرض الواقع ضعيف إلى حد الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالي. ويتضمن القانون 19 مادة موزعة على 6 فصول، أعده نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاما خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية،

---

[49]– جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية، ط1، 2010، ص 246

[50]– عبد الفتاح مراد، المرجع السابق، ص 420

[51] – الجريمة الالكترونية: معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني

http://www.aps.dz/ar/sante-science-technologie/63173-1100-2018

[52] – القانون رقم 09-04 المؤرخ في 05-اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر.47

بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الالكترونية، ونص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها،

ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الالكترونية وتحديد مكان تواجدهم، كما أن هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل.

الفرع الأول: قانون العقوبات رقم 04 -05 المؤرخ في 10 نوفمبر 2004 قانون الإجراءات الجزائية الجزائري.

أولا: قانون العقوبات رقم 04 -05 المؤرخ في 10 نوفمبر 2004

أحدث المشرع الجزائري القسم السابع مكرر من الفصل الثالث الخاص بجرائم الجنايات والجنح ضد الاموال تحت عنوان المساس بأنظمة المعالجة الألية للمعطيات (القانون رقم 04-05 المؤرخ في 10 نوفمبر 2004(المادة 394 مكرر " يعاقب بالحبس من ثلاثة اشهر الى سنة وبغرامة من خمسين ألف الى مائة ألف دينار كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من المنظومة للمعالجة الالية للمعطيات أو يحاول ذلك. تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظمة. وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام أشغال المنظومة تكون العقوبة الحبس من 06 أشهر الى سنتين وغرامة من خمسين ألف الى مائة وخمسون ألف دينار" المادة 394 مكرر 1 " يعاقب بالحبس من 06 اسهر الى 03 سنوات وبغرامة من 500.000 دج الى 2000.000 كل من ادخل بطريقة الغش معطيات في نظام أو أزال او عدل بطريقة الغش المعطيات التي يتضمنها" ...[53]

[53] – المادة394 مكرر2 " يعاقب بالحبس من شهرين الى03 سنوات وبغرامة من1000.000 دج الى5000.000 دج كل من يقوم عمدا وعن طريق الغش بما يلي -01 : تصميم أو بحث او تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن ترتكب بها الجرائم المنصوص عليها في هذا القسم. -02حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحل عليها من إحدى الجرائم المنصوص عليها في هذا القسم. المادة394 مكرر3 " تضاعف العقوبة المنصوص عليها في هذا القسم اذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات الخاضعة للقانون العام دون الاخلال بتطبيق عقوبات اشد". المادة394 مكرر4 " يعاقب الشخص المعنوي الذي يرتكب احدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى المقرر للشخص الطبيعي" المادة394 مكرر5 " كل من شارك في مجموعة أو في اتفاق تألف بغرض الاعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسد أو عدة أفعال مادية يعاقب بالعقوبات المقررة للجريمة ذاتها". المادة394 مكرر6 " مع الاحتفاظ بحقوق الغير حسن النية يحكم بمصادرة الأجهزة والبرامج والوسائل المستخدمة مع اغلاق المواقع التي تكون محلا لجريمة من الجرائم المعاقب عليها وفقا لهذا القسم على اغلاق المحل أو مكان استغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها". المادة394 مكرر7" يعاقب على الشروع في ارتكاب الجنحة المنصوص عليها في هذا القسم بالعقوبات المقررة على الجنحة ذاتها

ثانيا: قانون الإجراءات الجزائية الجزائري

بالنسبة لمتابعة الجريمة الالكترونية تتم بنفس الإجراءات التي تتبع بها الجريمة التقليدية، كالتفتيش والمعاينة واستجواب المتهم والضبط والتسرب والشهادة والخبرة.

غير أن المشرع الجزائري نص على تمديد الاختصاص المحلي لوكيل الجمهورية في الجرائم الإلكترونية في المادة 37 من قانون الإجراءات الجزائية[54]

كما نص على التفتيش في المادة 45 الفقرة 7من نفس القانون المعدلة [55] حيث أعتبر إن التفتيش المنصب على المنظومة المعلوماتية يختلف عن التفتيش المتعارف عليه، في القواعد الإجرائية العامة من حيث الشروط الشكلية والموضوعية، فالتفتيش وإن كان إجراء من الإجراءات التحقيق قد أحاطته المشرع بقواعد صارمة، وبالتالي لا تطبق الأحكام الواردة في المادة 44 من قانون الإجراءات الجزائية إذا تعلق الأمر بالجرائم ٱلكترونية. ونص على توقيف النظر في جريمة المساس بأنظمة المعالجة في المادة 51 الفقرة6 [56]وكذا على "اعتراض المراسلات وتسجيل الأصوات والتقاط الصور من المادة 65 مكرر 5/ 10.

كما أن قانون الإجراءات الجنائية نص على ألا يجوز ضبطها إلا في إطار تحقيق بأمر من السلطة القضائية أو قاضي التحقيق أو النيابة. غير أنه طبقا لقانون الإجراءات المعدل والمتمم في الفصل الرابع تحت عنوان "في إعتراض المراسلات وتسجيل الأصوات وإلتقاط الصور". نصت المادة (65 مكرر5/3)على أنه في حالة ضرورة التحري أو التحقيق في مجموعة من الجرائم من ضمنها الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات يجوز لوكيل الجمهورية المختص أن يأذن بالإعتراض ووضع ترتيبات تقنية دون موافقة المعنيين من أجل إلتقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية في أماكن خاصة أو عامة[57] .

- أما بالنسبة لنصوص إجراءات التحقيق والمحاكمة تطبق عليها نفس إجراءات الجريمة التقليدية.

---

[54]– المادة 37 من قانون الإجراءات الجنائية المعدل والمتمم بأمر رقم 02-15مؤرخ في 23 يوليو سنة 2015 ،يعدل ويتمم الأمر رقم 66-155 المؤرخ في 8 يونيو سنة 1966 والمتضمن قانون الإجراءات الجزائية،الجريدة الرسمية عدد 40.

[55]– المادة 45 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 .ص 6.

[56]– المادة **تمم الباب الثاني من الكتاب الأول بقانون رقم** قم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84 ص8 ،بفصل رابع51 من قانون الإجراءات الجنائية المعدل والمتمم بقانون رقم 06-22 المؤرخ في 20 ديسمبر2006،الجريدة الرسمية عدد84،ص7

[57]– القانون رقم 06 – 22 مؤرخ في 29 ذي القعدة عام 1427 الموافق 20 ديسمبر سنة 2006 يعدل ويتمم الأمر رقم 66-155المؤرخ في 18 صفر عام 1386 الموافق 8 يونيو سنة 1966. والمتضمن قانون الإجراءات الجنائية الجزائري. المادة 65 مكرر 3/5 "إذا أقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الإبتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات أو جرائم تبييض الأموال أوالإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهور ية المختص بأن يأذن بما يأتي : – وضع الترتيبات التقنية، دون موافقة المعنيين من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سرية من طرف شخص أو عدة أشخاص في أماكن خاصة أو عمومية **...".**

ثالثا: قانون البريد والاتصالات السلكية واللاسلكية

باستقراء القانون الذي يحدد القواعد العامة المتعلقة بالبريد والاتصالات بحيث لاحظنا أنه تسارع مواكبة التطور الذي شهدته التشريعات العالمية مسايرة التطور التكنولوجي لذلك بات من السهولة بمكان اجراء التحويلات المالية عن الطريق الالكتروني ذلك ما نصت عليه المادة 87 منه [58]، كما نصت المادة2/ 84 منه على استعمال حوالات دفع عادية أو الكترونية أو برقية[59]" ،كما نص في المادة 105 منه على إحترام المراسلات [60].

بينما أتت المادة 127 منه بجزاء لكل من تسول له نفسه وبحكم مهنته أن يفتح أو يحول أو يخرب البريد أو ينتهكه يعاقب الجاني بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات[61].

رابعا: قانون التأمينات

قد تطرق هذا القانون كذلك إلى تنظيم الجريمة الإلكترونية من خلال هيئات الضمان الاجتماعي' في نصوص قانونية عديدة تخص البطاقة الالكترونية التي تسلم للمؤمن له اجتماعيا مجانا بسبب العلاج وهي صالحة في كل التراب الوطني، وكذا للجزاءات المقررة في حالة الاستعمال غير المشروع او من يقوم عن طريق الغش بتعديل أو نسخ أو حذف كلي أو جزئي للمعطيات التقنية أو الإدارية المدرجة في البطاقة الالكترونية للمؤمن له اجتماعيا أو في المفتاح الالكتروني لهيكل العلاج أو في المفتاح الالكتروني لمهن الصحة للبطاقة الالكترونية حسب المادة 93مكرر2.

خامسا: القانون الخاص بالوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها

بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها إجراءات مراقبة الاتصالات الإلكترونية، وتفتيش وحجز المنظومة المعلوماتية،

---

[58]– المادة87 من قانون البريد والإتصالات السلكية واللاسلكية رقم 03- 2000 المؤرخ في2000/08/05. على أنه " يمكن أن ترسل الأموال ضمن النظام الداخلي بواسطة الحوالات الصادرة عن المتعامل والمحولة بالبريد أو البرق أو عن الطريق الإلكتروني"

[59]– المادة 2/84 من نفس القانون،" تطبق أحكام المادة 89 من هذا القانون عن استعمال حوالات دفع عادية أو الكترونية أو برقية'

[60]– المادة 105من نفس القانون"لايمكن في أي حال من الأحوال ابتهاك حرمة المراسلات"

[61]– لمادة127 من نفس القانون،" كل موظف أو عون من أعوان الدولة أو مستخدم أو مندوب عن مصلحة البريد يقوم اختلاس أو إتلاف رسائل مسلمة إلى البريد أو يسهل فضها أو اختلاسها أو إتلافها يعاقب بالحبس من ثلاثة أشهر إلى خمس سنوات وبغرامة من 30.000 دج إلى 500.000 دج ويعاقب بالعقوبة نفسها كل مستخدم أو مندوب في مصلحة البرق أو يختلس أو يتلف برقية أو يذيع محتواها .ويعاقب الجاني فضلا عن ذلك بالحرمان من كافة الوظائف أو الخدمات العمومية من خمس إلى عشر سنوات"

وعليه سنوجزها كالتالي:

1. مراقبة الاتصالات الإلكترونية وتجميعها

القاعدة أنه أضفى المشرع الجزائري الحماية القانونية للبيانات ذات الطابع الشخصي من خلال أسمى نص في النظام القانوني الجزائري، ألا وهو الدستور، وهذا في إطار القواعد العامة التي ت عنى بالحماية القانونية للحياة الخاصة للأفراد، وهو ما ينطوي عليه بالضرورة حماية بياناتهم الشخصية من المعالجة الآلية، بحيث اعترف المشرع الدستوري الجزائري بها في المادة 77 التي تنص على أنه: "يمارس كل واحد جميع حرياته، في إطار احترام الحقوق المعترف بها للغير في الدستور، لاسيما احترام الحق في الشرف، وستر الحياة الخاصة."...

كما أيدت ذلك المادة 46 من دستور سنة 1996 التي نصت على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة"، إلا أنه في تعديل الدستوري لسنة 2016، حاول المشرع مواكبة التطور الذي يشهده العالم في مجال حماية البيانات الشخصية، من خلال إضافة فقرتين للمادة أعلاه تنصان على أنه:" لا يجوز بأي شكل المساس بهذه الحقوق دون أمر معلل من السلطة القضائية، ويعاقب القانون انتهاك هذا الحكم[62]

إن أضافت الفقرتين الثالثة والرابعة في التعديل الأخير، إنما ينم عن اقتناع المشرع الجزائري بضرورة المبادرة إلى وضع الآليات القانونية الكفيلة بحماية البيانات الخاصة بالأشخاص الطبيعيين خلال عملية المعالجة الآلية لها، كما يدل الإقرار الدستوري على أن القانون الخاص بالحماية البيانات هو مسألة وقت فقط، خاصة في ظل النشاط التشريعي الذي الجزائر في العشرية الأخيرة، وأن وزارة البريد وتكنولوجيات الإعلام والاتصال تدرس ابتداء من نوفمبر 2014 مشروع قانون حول حماية البيانات الشخصية على الأنترنيت والذي يفترض أن يصدر قريبا.

علما أن الجزائري هو الوحيد بين الدساتير العربية الذي تطرق لحرمة البيانات الخاصة من المعالجة الإلكترونية، بحيث تكتفي جلها بتكريس الحماية الدستورية للمراسلات بكل أشكالها فقط[63]

وبهذا يكون المشرع الجزائري رغم ضمانه لسرية المراسلات والاتصالات بكل أشكالها، قد خول استثناء السلطة القضائية وفي إطار قرار معلل بأن تتبع إجراءات تمس البيانات الشخصية، بالنظر لخطورة بعض الجرائم المعلوماتية المحددة حصرا: تسجيل الاتصالات الإلكترونية في حينها.

كما بين القانون 04/09 الخاص بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها في مادته الرابعة، الحالات التي تسمح بتطبيق الإجراء الجديد المتمثل في مراقبة الاتصالات الإلكترونية، وذلك على سبيل الحصر،

---

[62] – القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14، الصادرة في 07 مارس 2016.

[63]– لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي، بالملتقى الوطني الموسوم ب: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7و8 فبراير 2017، ص 6.

وهذه الحالات هي:

- للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة.
- في حالة توفر معلومات عن احتمال الاعتداء على منظومة معلوماتية على نحو يهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني.
- لمقتضيات التحريات والتحقيقات القضائية، عندما يكون من الصعب الوصول إلى نتيجة تهم الأبحاث الجارية دون اللجوء للمراقبة الإلكترونية.

يظهر من خلال استقراء نص هذه المادة، أن المشرع الجزائري يحاول الاستفادة بدوره من التطور التكنولوجي والمميزات التي يخولها، من خلال وضع المشتبهين فيهم تحت المراقبة الإلكترونية، وهي على عكس المراقبة الشخصية أقل تكلفة من حيث الوقت والمال والمخاطر الأمنية إضافة إلى فعاليتها، إلا أنه من جهة أخرى، فإن وضع الشخص تحت المراقبة الإلكترونية سواء ما تعلق باتصالاته الهاتفية أو نشاطاته عبر الأنترنيت، من شأنه انتهاك حرمة البيانات ذات الطابع الشخصي له، باعتبار أنه لدواعي فرز المعلومة للتأكد من قيمتها كدليل إثبات أو نفي، يستدعي سماعها أو قراءتها بكل تأني، وهذا ما من شأنه الوصول إما لأنها معلومة ضرورية لاستكمال التحقيقات، أو أنها معلومات شخصية لا دخل لها بالقضية، كما يمكن أن يصار إلى تبرئة الشخص تماما، لكن بعد ماذا؟.

بغرض تأطير هذه العملية الحساسة وتخفيف تأثيراتها السلبية على حماية الحياة الخاصة للأفراد وضع المشرع عدة ضمانات هي:

أ. حصر الحالات التي يمكن اللجوء فيها إلى المراقبة الإلكترونية

هي الحالات التي أوضحتها المادة الرابعة من القانون 04/09 على سبيل الحصر:

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

بإستقراء الحالات هذه، نجد أن المشرع قلص من الحالات التي يمكن فيها اللجوء إلى عملية المراقبة الإلكترونية وحصرها في الجرائم التي تمس الأمن الوطني، ذلك أنه عندما يتعلق الأمر مثلا بالجرائم الإرهابية والتي تطال المدنيين فإنه لا يمكن الحديث عن حقوق الإنسان، وكذا في حالات تنفيذ المساعدة القضائية، إلا أن إضافة الحالة "ج" والتي تعني إمكانية اللجوء في كل قضية مستعصية إلى المراقبة الإلكترونية صغيرة كانت أو كبيرة، يؤدي إلى تعميم استخدام الآلية دون حد.

ب. وضع آلية إقرار المراقبة الإلكترونية تحت سلطة القضاء

تضيف المادة 2/4 من القانون 04/09، بأنه: "لا يجوز إجراء عمليات المراقبة، إلا بإذن مكتوب من السلطات القضائية المختصة."

كما أنه عندما يتعلق الأمر بجرائم الإرهاب أو التخريب أو الجرائم الماسة بأمن الدولة، يختص النائب العام لدى مجلس قضاء الجزائر بمنح ضباط الشرطة القضائية، إذنا لمدة 6 أشهر قابلة للتجديد وذلك على أساس تقرير يبين طبيعة الترتيبات التقنية المستعملة والأغراض الموجهة لها[64].

كما تنص المادة 41 من المرسوم الرئاسي رقم 15/261المؤرخ في 08 أكتوبر2015، الذي يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، على أن الهيئة تمارس اختصاصاتها الحصرية في مجال مراقبة الاتصالات الإلكترونية تحت مراقبة قاض مختص.

كما يخضع الموظفون الذين يدعون إلى الاطلاع على معلومات سرية إلى أداء اليمين أمام المجلس القضائي قبل تنصيبهم، وهم يلزمون بذلك بالسر المهني) المادتين 27و28 المرسوم الرئاسي (15/261

يعتبر وضع هكذا آلية تمس بالحريات الفردية والحياة الخاصة للأفراد تحت يد القضاء المستقل، ضمانة حقيقية باعتبار أن القاضي يهدف إلى الموازنة بين ضرورات التحقيق وإلزامية حماية الأفراد المشتبه فيهم، فمجرد الاشتباه لا يجعل من الفرد مجرما، وهذا ما يسمى ضمانات المحاكمة العادلة.

ج. تحديد تقنيات الرقابة الإلكترونية وحدود استعمال المعطيات المتحصل عليها

تكون الترتيبات التقنية الموضوعة للأغراض المراقبة الإلكترونية موجهة حصريا لتجميع وتسجيل معطيات ذات صلة بالحالات الواردة على سبيل الحصر أعلاه على غرار الأفعال الإرهابية أي الجرائم الأكثر خطورة.

أما عن التقنيات التكنولوجية التي يمكن أن تستعمل في إطار المراقبة الإلكترونية فهي تتمثل في: اعتراض المراسلات الإلكترونية[65]،

تسجيل الأصوات، التقاط الصور[66]تفتيش المنظومات المعلوماتية وحجزها) المادة 5 و7 من القانون 04/09، إلا أن السؤال الأهم هو ما مصير المعلومات المتحصل عليها؟

---

[64]- نصت المادة 65 مكرر 7 من قانون الإجراءات الجزائية، على أنه: " يتضمن الإذن كل العناصر التي تسمح على التعرف على الاتصالات ويسلم مكتوبا ويكون صالحا لمدة أربعة أشهر قابلة للتجديد بنفس الشروط الشكلية والزمنية، يسلم الإذن لوضع الترتيبات بغير رضا أو علم الأشخاص الذين لهم حق على تلك الأماكن."

[65]- تعرف المادة 2 /والاتصالات الإلكترونية على أنها": أي تراسل أو إرسال أو استقبال علامات أو إشارات أو كتابات أو صور أو أصوات أو معلومات مختلفة بواسطة أي وسيلة إلكترونية."

[66]- المادة 65 مكرر 5 من القانون رقم 15 – 19 المؤرخ في 30 ديسمبر 2015يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71، الصادرة في 30 ديسمبر

أجابت المادة 09 من القانون 04/09 المتعلقة بحدود استعمال المعطيات المتحصل عليها عن طريق الحجز بأنه لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية، ما تشير إليه هذه المادة هو أن الاستعمال المشروع للبيانات الشخصية المتحصل عليها من المراقبة الإلكترونية يتحدد بحدود ضرورات التحقيقات، وهو ما يستدعي تجريم كل استعمال لها خارج هذا الإطار.

د. سن عقوبات لجريمة إفشاء معلومات ذات طابع شخصي ناتجة عن المراقبة الإلكترونية

يكون الموظفين القائمين على عمليات المراقبة الإلكترونية قادرين على الاطلاع على معلومات ذات طابع مجرم وأخرى ذات طابع شخصي، وفي كلتا الحالتين يكون هؤلاء مطالبين باحترام السر المهني.

لهذا جرم المشرع كل محاولة من قبل هؤلاء الموظفين نحو استغلال عمليات المراقبة لأغراض شخصية، أو كل تجاوز لحدود المراقبة الإلكترونية نحو انتهاك حرمة الحياة الشخصية للأفراد أيا كان السبب، أو إفشاء مستندات ناتجة عن التفتيش أو إطلاع عليها شخص لا صفة له قانونا في الاطلاع عليه، وذلك بغير إذن مكتوب من المتهم أو من ذوي حقوقه أو من الموقع على هذا المستند أو من المرسل إليه ما لم تدع ضرورات التحقيق إلى غير ذلك[67].

2. إجراءات تفتيش المنظومة المعلوماتية

قررت المادة 5 من القانون رقم 04/09، أنه يجوز للسلطات القضائية المختصة، وكذا ضباط الشرطة القضائية في إطار قانون الإجراءات الجزائية، وفي الحالات المنصوص عليها في المادة 4 أعلاه الدخول بغرض التفتيش ولو عن بعد إلى:

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

في الحالة المنصوص عليها في الفقرة- أ -من هذه المادة، إذا كانت هناك أسباب تدعو للاعتقاد بأن المعطيات المبحوث عنها مخزنة في منظومة معلوماتية أخرى،

وأن هذه المعطيات يمكن الدخول إليها انطلاقا من المنظومة الأولى، يجوز تمديد التفتيش بسرعة إلى هذه المنظومة أو جزء منها بعد إعلام السلطة القضائية المختصة مسبقا بذلك.

وإذا تبين مسبقا بأن المعطيات المبحوث عنها، والتي يمكن الدخول إليها انطلاقا من المنظومة الأولى، مخزنة في منظومة معلوماتية تقع خارج الإقليم الوطني، فإن الحصول عليها يكون بمساعدة السلطات الأجنبية المختصة طبقا للاتفاقيات الدولية ذات الصلة ووفقا لمبدأ المعاملة بالمثل.

---

[67]- (المادة 46 من الأمر رقم 15 – 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40، الصادرة في 23 جويلية 2015.

وكمثال على المساعدة القضائية الدولية كإجراء جديد لتتبع مجرمي المعلوماتية، قضية توقيف مصالح الأمن الجزائرية لشاب جزائري ببلدية بومرداس بعد تقديم المكتب الفدرالي الأمريكي للتحقيقات شكوى ضده مفادها أن هذا الشاب قد بعث برسالة إلكترونية لهذا المكتب مهددا فيها بوضع قنبلة في أحد أحياء مدينة جوانسبورغ بجنوب إفريقيا تستهدف المناصرين الأمريكيين قبل انطلاق المباراة الكروية بين المنتخب الجزائري والأمريكي في بطولة كأس العالم.

والمشرع الجزائري في المادة الخامسة من القانون رقم 04/09 نص على التفتيش المنصوص عليه في قانون الإجراءات الجزائية، وحتى وأن اختلف مضمونه عن التفتيش العادي بحيث يجب توفر شروط التفتيش المنصوص عليها في المادة 45 من قانون الإجراءات الجزائية مع مراعاة أحكام الفقرة الأخيرة منها لأننا بصدد جرائم معلوماتية.

غير أن القانون رقم 09/ 04 أجاز إجراء التفتيش على المنظومة المعلوماتية عن بعد، وهذا إجراء جديد بحيث يمكن الدخول إليها دون إذن صاحبها بالدخول في الكيان المنطقي للحاسوب، للتفتيش عن أدلة في المعلومات التي يحتوي عليها هذا الأخير، وهي شيء معنوي غير محسوس، كما أجاز إفراغ هذه المعلومات على دعامة مادية أو نسخها للبحث عن الدليل فيها[68].

ويمكن للسلطات المكلفة بالتفتيش تسخير كل شخص له دراية بعمل المنظومة المعلوماتية محل البحث أو بالتدابير المتخذة لحماية المعطيات المعلوماتية التي تتضمنها، قصد مساعدتها وتزويدها بكل المعلومات الضرورية لانجاز مهمتها.

كما نص المشرع الجزائري، ودائما في نفس القانون 04/09 على إجراء آخر يسهل عملية التفتيش في الفقرة الأخيرة من المادة 5، وهذا الإجراء يتمثل في اللجوء إلى الأشخاص المؤهلين كالخبراء والتقنيين المختصين في الإعلام الآلي وفن الحاسوبات لإجراء عمليات التفتيش على المنظومة المعلوماتية، وجمع المعطيات المتحصل عليها والحفاظ عليها وتزويد السلطات المكلفة بالتفتيش بهذه المعلومات.

3. حجز المعطيات المعلوماتية

أكدت المادة 6 من القانون رقم 04/09، أنه عندما تكتشف السلطة التي تباشر التفتيش في منظومة معلوماتية معطيات مخزنة تكون مفيدة في الكشف عن الجرائم أو مرتكبيها وأنه ليس من الضروري حجز كل المنظومة، يتم نسخ المعطيات محل البحث وكذا المعطيات اللازمة لفهمها على دعامة تخزين الكترونية تكون قابلة للحجز والوضع في أحراز وفقا للقواعد المقررة في قانون الإجراءات الجزائية.

يجب في كل الأحوال على السلطة التي تقوم بالتفتيش والحجز السهر على سلامة المعطيات في المنظومة المعلوماتية التي تجري بها العملية،

[68]– طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2011-2012، ص 131-132.

غير أنه يجوز لها استعمال الوسائل التقنية الضرورية لتشكيل أو إعادة تشكيل هذه المعطيات، قصد جعلها قابلة للاستغلال لأغراض التحقيق شرط ألا يؤدي ذلك إلى المساس بمحتوى المعطيات، وإذا استحال إجراء الحجز وفقا لما هو منصوص عليه في أحكام المادة 06 أعلاه لأسباب تقنية، يتعين على السلطة التي تقوم بالتفتيش استعمال التقنيات المناسبة لمنع الوصول إلى المعطيات التي تحتويها المنظومة المعلوماتية والى نسخها، الموضوعة تحت تصرف الأشخاص المرخص لهم باستعمال هذه المنظومة.

ويمكن للسلطة التي تباشر التفتيش أن تأمر باتخاذ الإجراءات اللازمة لمنع الاطلاع على المعطيات التي يشكل محتواها جريمة، لاسيما عن طريق تكليف أي شخص مؤهل باستعمال الوسائل التقنية المناسبة لذلك.

وتحت طائلة العقوبات المنصوص عليها في التشريع المعمول به، لا يجوز استعمال المعلومات المتحصل عليها عن طريق عمليات المراقبة المنصوص عليها في هذا القانون، إلا في الحدود الضرورية للتحريات أو التحقيقات القضائية.[69]

وفي إطار تطبيق أحكام هذا القانون يتعين على مقدمي الخدمات تقديم المساعدة للسلطات المكلفة بالتحريات القضائية لجمع وتسجيل المعطيات المتعلقة بمحتوى الاتصالات في حينها وبوضع المعطيات التي يتعين عليهم حفظها وفقا للمادة 11 من القانون رقم 04/09 تحت تصرف السلطات المذكورة، وذلك لتمكين سلطات التحقيق من التعرف على مستعملي الخدمة.

ويتعين على مقدمي الخدمات كتمان سرية العمليات التي ينجزونها بطلب من المحققين وكذا المعلومات المتصلة بها وذلك تحت طائلة العقوبات المقررة لإفشاء أسرار التحري والتحقيق.

وقد حدد هذا القانون المدة اللازمة لحفظ المعطيات بسنة واحدة من تاريخ التسجيل كما أوجب من خلال المادة 12 من القانون رقم 04/09، على مقدمي الخدمات التزامات خاصة، هي:

- واجب التدخل الفوري لسحب المعطيات المخالفة للقانون وتخزينها أو منع الدخول إليها باستعمال وسائل فنية وتقنية.
- وضع الترتيبات التقنية لحصر إمكانيات الدخول إلى الموزعات التي تحتوي معلومات مخالفة للنظام العام وأن يخبروا المشتركين لديهم بوجود.

الفرع الثاني: الهياكل الخاصة للتصدي للجرائم الإلكترونية

أولا: الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال[70]

---

[69]- المادة 09 من القانون رقم 04/09 المؤرخ في 5 أوت 2009.

[70]- إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته التي سبق ونص عليها القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومرسوم رئاسي رقم 15-261 المؤرخ في 24من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وقع رئيس الجمهورية السيد عبد العزيز بوتفليقة على مرسوم رئاسي مرسوم رئاسي رقم 261/15 المؤرخ في 24 من ذي الحجة عام 1436 ه/ الموافق ل 8أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، والتي تعد سلطة إدارية مستقلة لدى وزير العدل ستعمل تحت إشراف ومراقبة لجنة مديرة يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين اثنين من المحكمة العليا يعينهما المجلس الأعلى للقضاء.

وكلفت الهيئة بتنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

وتتشكل هذه الهيئة من لجنة مديرة يرأسها الوزير المكلف بالعدل وثلاثة مديريات ومركز للعمليات التقنية وملحقات جهوية، كما يتمثل أعضاؤها في الوزير المكلف بالداخلية، الوزير المكلف بالبريد وتكنولوجيا

الإتصال، قائد الدرك الوطني، المدير العام للأمن الوطني، ممثل عن رئاسة الجمهورية، ممثل عن وزارة الدفاع الوطني، قاضيان من المحكمة العليا [71]

وبهذا ضمت الهيئة قضاة وضباط وأعوان من الشرطة القضائية تابعين لمصالح الاستعلام العسكرية والدرك الوطني والأمن الوطني وفقا لأحكام قانون الإجراءات الجزائية.

ويتمثل دور هذه الهيئة في تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام كالاتصالات ومكافحتها، وهي تلك التي تمس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للإتصالات الإلكتَّرونية.

كما تعنى بمساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم ذات الصلة بتكنولوجيات الإعلام والاتصال وضمان مراقبة الاتصالات الالكترونية للوقاية من الأفعال الموصوفة بجرائم الإرهاب أو التخريب أو الجرائم التي تمس بأمن الدولة، وذلك تحت سلطة القاضي المختص، وباستثناء أي هيئة وطنية أخرى.

أما فيما بخص مجال تطبيق الوقاية من هذه الجرائم ومع مراعاة الأحكام القانونية التي تضمن سرية المراسلات كالإتصالات، يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وضع ترتيبات تقنية لمراقبة الاتصالات الالكترونية وتجميع وتسجيل محتواها في حينها واقيان بإجراءات التفتيش والحجز داخل المنظومة المعلوماتية.[72]

---

[71]– المادة 6 و7 من المرسوم الرئاسي رقم 261-15 المؤرخ في 24 من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[72]– براهيم يمينة، "تطبيقات الأمن المعلوماتي"، بالملتقى الوطني الموسوم ب :الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان، يومي 7 و8 فبراير 2017، ص 9.

وإنشاء هذه الهيئة مكن بالفعل من تزويد العدالة بالمزيد من الموارد البشرية المؤهلة ومراجعة الترسانة التشريعية بما في ذلك في المجال الجزائي من أجل تحسين حماية حقوق وحريات المواطنين وتشديد العقوبات على أي تقصير في هذا المجال[73] .

ثانيا: الهيئات القضائية الجزائية المتخصصة

أنشئت بموجب القانون 14/04المؤرخ في 10/11/2004المعدل والمتمم لقانون الإجراءات الجزائية تختص بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات طبقا للمواد329،37،و40 من ق.إ.ج.ج تتمتع اختصاص إقليمي موسع طبقا للمرسوم التنفيذي رقم 348/06 المؤرخ في .05/01/2006بحيث تنظر في القضايا المتصلة بتكنولوجيا الإعلام والاتصال المرتكبة في الخارج حتى ولو كان مرتكبها أجنبيا إذا كانت تستهدف مؤسسات الدولة أو الدفاع الوطني المادة 15 من القانون رقم 09/04

ثالثا: المعهد الوطني للأدلة الجنائية وعلم الجرائم

يتكون من احدى عشرة دائرة متخصصة في مجالات مختلفة، جميعها تضمن إنجاز الخبرة، التكوين والتعليم وتقديم المساعدات التقنية، و دائرة الإعلام الآلي والالكتروني مكلفة بمعالجة وتحليل وتقديم كل دليل رقمي يساعد للعدالة، كما تقدم مساعدة تقنية للمحققين في المعاينات [74].

رابعا: المديرية العامة للأمن الوطني

تتصدى هده المديرية[75] للجريمة الإلكترونية من عدة جوانب وأمنها الجانب التوعوي بحيث لم تغفل المديرية العامة للأمن الوطني عن الوقاية التوعية وهذا من خلال برمجتها لتنظيم دروس توعوية في مختلف الأطوار الدراسية وكذا المشاركة في الملتقيات والندوات الوطنية وجميع التظاهرات التي من شأنها توعية المواطن حول خطورة الجرائم الالكترونية.

ودائما في إطار مكافحة الجريمة الالكترونية ونظرا للبعد الدولي الذي عادة ما يتخذه هذا النوع من الجرائم،

---

[73]– إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحته التي سبق ونص عليها القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.أنظر: مرسوم رئاسي رقم 261- 15 المؤرخ في 24من ذي الحجة عام 1436هـ/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

[74]– هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية ،المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة كلية الحقوق،2016،ص3.

فأكدت عضويتها الفعالة في المنظمة الدولية للشرطة الجنائيةINTERPOL هاته الأخيرة تتيح مجالات للتبادل المعلوماتي الدولي وتسهل الإجراءات القضائية المتعلقة بتسليم المجرمين، وكذا مباشرة الانابات القضائية الدولية ونشر أوامر القبض للمبحوث عنهم دوليا[76].

الخاتمة

أصبحت اليوم الهجمات الإلكترونية شبحا يهدد العالم بأسره، وهاجسا أمنيا يتحدى الأشخاص المعنوية وكذا الطبيعية كالحكومة الإلكترونية بجميع شراييها مما يستدعي تأمين البيانات والمعلومات والمعاملات التي تعتبر القوام للبيئة الرقمية المفتوحة، ولمجابهة هذا المد الاجرامي لابد من تحبيك استراتيجية دولية لمواجهته، وكذا إحلال السلام الرقمي.

صفوة القول وخلاصته أن غرس و تطوير الثقافة الحاسوبية وسط رجال القانون والشرطة ، وربطها بالثقافة القانونية والشرطية التقليدية يكفل للأجهزة الأمنية ولسلطات التحقيق النجاح الباهر في مواجهة الجرائم المعلوماتية ، ليس هذا فحسب بل لا بد وأن تسعى الأجهزة الأمنية المعنية بالتحقيق إلى استقطاب المتخصصين والكفاءات في المجال المعلوماتي وضمهم إليها ليكونوا ضمن كوادرها والاستفادة منهم ، ومن أجل ذلك ينبغي على كليات الشرطة من جهة أن تعمل جاهدة لقبول دفعات من الجامعين من خريجي كليات الحاسبات الآلية لتخرجهم ضباطاً مؤهلين قانونيا وتقنيا ،

كذلك يتعين على الكليات المعينة بتدريس القانون أن تسعى جاهدة إلى تدريس الحاسبات الآلية وكل ما يتعلق به إلى الطلبة، وأن تكون مادة الحاسب الآلي وتقنية المعلومات إحدى المواد الأساسية، لأن من شأن ذلك أن تتكون لدي خريجي هذه الكليات ثقافة قانونية وثقافة حاسوبية.بسبب تنوع واختلاف النظم القانونية الإجرائية، نجد أن طرق التحري والتحقيق والمحاكمة التي تثبت فائدتها وفاعليتها في دولة ما قد تكون عديمة الفائدة في دولة أخرى أو قد لا يسمح بإجرائها. كما هو الحال بالنسبة للمراقبة الإلكترونية، والتسليم المراقب، والعمليات المستترة، وغيرها من الإجراءات الشبيهه.

- كما تحتاج الدول العربية للمزيد من الاستثمار في مجال الأمن السيبراني وينقسم الاستثمار لجانبين، الأول توطين التكنولوجيا والبني التحتية السيبرانية، الثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة على بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.
- كما ينبغي الإشارة إلى ضرورة الاهتمام بالجانب التوعوي ونشر الثقافة الرقمية للتعريف بالجريمة الالكترونية وسبل الحماية منها ومكافحتها عن طريق مؤسسات المجتمع المدني وأجهزة الدولة المعنية وتبني استراتيجيات توعوية على المستوى المحلى والاقليمي تهدف الى حماية المجتمع من

[76] – علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، دار الجامعية للطباعة والنشر، بيروت، د ط،1999،ص120.

مخاطر هذا النوع من الجرائم لاسيما فئة الشباب مع دعم وتشجيع منظمات العمل المدني للمساهمة الفاعلة في هذا المجال.

- الأمر الذي يولد فجوة قانونية مستمرة في مجال مكافحة الجريمة الالكترونية لازالت قائمة وتعتبر من التحديات القانونية في العصر الحديث ويترتب عليها افلات الجاني في كثير من الحالات.

المقترحات والتوصيات

- إن التهديدات الإلكترونية يمكن أن تأتي من أي مكان في العالم، أومن عدة أماكن معا، يجب أن تكون بروتوكولات الاستجابة للأزمات واضحة فيما بين المناطق وعلى مستوى العالم، لهذا فالدول تحتاج الى حراك عالمي لمواجهة هكذا هجمات اوتهديدات لهذا يوصى ب:

1- تصنيع منظومات حماية أمنية وطنية ترتبط بمنظومات الحماية الأمنية، القائمة مع البِنَى المعلوماتية الوطنية.

2- المباشرة بإنشاء صرح صناعة برمجية وطنية لنظم حاسوب تطبيقية، تضمن سلامة البنى المعلوماتية من عائلة القرصنة المعلوماتية

3- ينبغي أن تضطلع وزارة التعليم العالي والبحث العلمي، بكلياتها المُتخصصة في هندسة الحاسوب وعُلُومه، وهندسة البَرمجيات والنظم، والمعاهد الفنية، ومراكز البُحُوث المتخصصة، والمراكز الاستشارية بإرساء جملة من الأمور الأساسية التي ترتبط بما يلي:

4- تهيئة القاعدة النظرية المتينة في ميدان علوم وتقنيات الأمن المعلوماتي، من خلال:

أ -إدخال مادة علوم التشفير Cryptography ضمن المواد الأساسيَّة في أقسام علوم الحاسبات، وهندسة الحاسبات.

ب -تشجيع الدراسات والبحوث في ميدان تشفير المعلومات لكل من طلبة الدراسات العليا والكادر التدريسي ؛لتعميق الفهم الوطني بهذا المضمار الحيوي، والارتقاء بالمعرفة العلمية في هذا الميدان إلى مُستويات متقدمة.

ج -إرسال البعثات العلميَّة خارج الجزائر للتَّخصص بالاختصاصات الدَّقيقة في شتَّى فروع المعرفة العلميَّة المرتبطة بالأمن المعلوماتي.

د -إعداد المؤتمرات العلميَّة واللقاءات بين شتَّى قطاعات الدولة؛ لتعميق أنشطة البحوث والدراسات في ميدان الأمن المعلوماتي وتقنياته.

ذ – استحداث مادة الحروب المعلوماتيَّة في جميع أقسام التعليم العالي.

هذا والدول مهما كانت مستويات التقدم التي تملكها الا ولا بد من:

1- تعميق الفهم للمخاطر، من حيث مصدر التهديدات وطبيعتها وكيفية تأثيرها المحتمل على الاستقرار المالي .ونحتاج إلى مزيد من البيانات عن هذه التهديدات وعن تأثير الهجمات الناجحة حتى نفهم المخاطر بصورة أفضل.

2- نحتاج إلى تحسين التعاون بشأن المعلومات الاستخباراتية عن التهديدات الإلكترونية، وإعداد التقارير عما يقع من حوادث إلكترونية، والممارسات الفُضلى في الصمود والاستجابة . وينبغي تحسين تبادل المعلومات بين القطاعين العام والخاص – وذلك، على سبيل المثال، بتخفيض الحواجز أمام قيام البنوك بإبلاغ الأجهزة الرقابية وسلطات إنفاذ القانون عن أي قضايا ذات صلة.

3- وينبغي للهيئات العامة المختلفة داخل كل بلد أن تتواصل في هذا الخصوص بسلاسة تامة . والتحدي الأكبر هو ضرورة تحسين تبادل المعلومات بين البلدان.

4- وهو أمر مرتبط أيضا، ينبغي تحقيق اتساق أكبر بين المناهج التنظيمية .فالبلدان تستخدم حاليا معايير وتنظيمات ومصطلحات مختلفة .وسيؤدي الحد من عدم الاتساق في هذه الجوانب إلى تيسير المزيد من التواصل بخصوص التهديدات الإلكترونية.

5- ضمان مصادقة آمنة للتطبيقات التي يتم الوصول إليها من خارج الشبكة

- يعد تأمين عمليات تسجيل الدخول للتطبيقات التي يتم الوصول إليها من خارج الشبكة باستخدام أساليب مصادقة قوية، الخطوة الأولى في طريق تحقيق الحماية المطلوبة ضد هجمات طلب الفدية .وهنا يُنصح باستخدام أسلوب مصادقة يتكون من عدة عوامل، ويجب على أقل تقدير التعامل مع قضايا اختراق كلمات المرور الافتراضية وبيانات الاعتماد المعروفة المسربة بشكل فوري.

6- تدريب الموظفين

- يجب رفع مستوى وعي الموظفين حول تقنيات التصيّد الاحتيالي المستخدمة .حيث يجب عليهم دوماً التشكيك وبشكل طبيعي في الملفات والروابط المرفقة . وفقاً لتقرير شركة إف 5نتوركس الخاص بعمليات التصيّد والاحتيال لعام2019 ، فإنما يصل إلى 71% من مواقع التصيّد الاحتيالي التي تم تحليلها قامت باستخدام بروتوكول HTTPS لتظهر أكثر شرعية .وخلُص التقرير أيضاً إلى أن الخدمات والعلامات التجارية الأكثر انتحالاً كانت فيسبوك وآبل ومايكروسوفت أوفيس إكستشينج.

7- فحص وتصفية حركة مرور البيانات على الإنترنت

- يجب توظيف قدرات مراقبة عالية والتعرف على سياق حركة بيانات الويب المشفرة بحيث يمكن القيام بحظر المواقع والمرفقات الضارة وحركة البيانات التي تعطي أوامر

التحكم بشكل تلقائي قبل حدوث عمليات تسلل إلى الشبكة .تتم استضافة غالبية البرمجيات الضارة على مواقع معروفة، لذلك منا لضروري القيام بفك تشفير المحتوى الذي يمر من خلال بروتوكولات SSL و TLS لضمان قيام أجهزة الحماية بفحصه.

8- ضمان وجود نسخة احتياطية للملفات الهامة

- يجب الاحتفاظ بنسخ احتياطية لجميع الأنظمة والبيانات الشخصية الهامة.

9- عزل الشبكات

- يجب تجنُب الاعتماد على تصميم الشبكات المسطحة، وهو ما يعني أن أي نظام مصاب يجب أن يمر على أدوات تصفية وعناصر تحكم إضافية في الوصول قبل خروجه من مجموعة الموارد المحلية.

قائمة المراجع:

الكتب:

1. ذياب موسى البداينة، "الجرائم الإلكترونية: المفهوم والأسباب"، الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، 2-2014/09/4، عمان، الأردن.
2. خالد بن سليمان الغثبر، محمد بن عبد الله القحطاني، أمن المعلومات بلغة ميسرة، مكتبة الملك فهد الوطنية للنشر، الطبعة الأولى، 2009.
3. بيل جيتس، المعلوماتية بعد الانترنت، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت: 1998 .
4. محمد حسين منصور، المسؤولية الالكترونية، الإسكندرية، دار الجامعة للنشر والتوزيع.
5. هدى قشقوش، الحماية الجنائية للتجارة الالكترونية، القاهرة: دار النهضة العربية.
6. منصور محمد حسنين، الإثبات التقليدي والإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.
7. عبد الحميد ثروت، التوقيع الإلكتروني (ماهيته، مخاطره وكيفية مواجهتها، مدى حجيته في الإثبات)، دار الجامعة الجديدة، مصر، 2007.
8. مصطفى محمد، أساليب إجرامية بالتقنية الرقمية، ماهيتها ومكافحتها، دار الكتب القانونية، المحلة الكبرى، 2005 .
9. بيل جيتس، المعلوماتية بعد الانترنت، سلسلة عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت: 1998 .
10. محمد حسين منصور، المسؤولية الالكترونية، الإسكندرية: دار الجامعة للنشر والتوزيع.
11. هدى قشقوش، الحماية الجنائية للتجارة الالكترونية، القاهرة: دار النهضة العربية.
12. عبد الفتاح بيومي مجازي، الأحداث والإنترنت، دار الفكر الجامعي،الإسكندرية.

13. جعفر حسن جاسم الطائي، جرائم تكنولوجيا المعلومات، رؤية جديدة للجريمة الحديثة، دار البداية، ط1، 2010.
14. علي عبد القادر القهوجي، الحماية الجنائية لبرامج الحاسب الالي، دار الجامعية للطباعة والنشر، بيروت، د ط،1999.
15. زيد حمزة مقدم،" النظام القانوني للتوثيق الإلكتروني (دراسة مقارنة)"، مجلة الشريعة والقانون والدراسات الإسلامية، العدد 24، أوت 2014.
16. عيسى غسان الربطي، القواعد الخاصة بالتوقيع الإلكتروني، دار الثقافة للنشر والتوزيع، عمان، 2009.

المقالات المنشورة والمداخلات العلمية:

1. وليد العاكوم، مفهوم ظاهرة الإجرام المعلوماتي، مؤتمر القانون والكمبيوتر والإنترنت، المجلد الأول.
2. باسل يوسف، الاعتراف القانوني بالسندات والتواقيع الالكترونية في التشريعات المقارنة، مجلة دراسات قانونية صادرة عن بيت الحكمة، بغداد: العدد الثاني، 2001.
3. إسماعيل عبد النبي شاهين، امن المعلومات في الانترنت بين الشريعة والقانون – مؤتمر القانون والكمبيوتر والإنترنت – المجلد الثالث،
4. باسل يوسف، الاعتراف القانوني بالسندات والتواقيع الالكترونية في التشريعات المقارنة، مجلة دراسات قانونية صادرة عن بيت الحكمة، بغداد: العدد الثاني، 2001 ص 23.
5. نمديلي رحيمة، "خصوصية الجريمة الإلكترونية في القانون الجزائري والقوانين المقارنة"، المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية، طرابلس، ليبيا، 24-25 مارس 2017.
6. Fritze Grupe – Stephen G. Kerr – William Kuechler and Nilesh Patel, "Understanding Digital Signatures", The CPA Journal, June 2003.
7. لوكال مريم، الحماية القانونية للبيانات ذات الطابع الشخصي في العالم الرقمي، بالملتقى الوطني الموسوم ب: الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان يومي 7و8 فبراير 2017، ص 6.
8. برابح يمينة، "تطبيقات الأمن المعلوماتي"، بالملتقى الوطني الموسوم ب :الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري، المنعقد بالمركز الجامعي غليزان، يومي 7 و8 فبراير 2017.
9. هواري عياش، مداخلة حول مسار التحقيقات الجنائية في مجال الجريمة المعلوماتية، المعهد الوطني للأدلة الجنائية وعلم الإجرام، جامعة بسكرة كلية الحقوق،2016.

الأطروحات والرسائل العلمية:

1. درار نسيمة، الأمن المعلوماتي وسبل مواجهة مخاطره في التعامل الإلكتروني-دراسة مقارنة-، رسالة دكتوراه، جامعة أبو بكر بلقايد، تلمسان، 2015-2016.
2. طرشي نورة، مكافحة الجريمة المعلوماتية، مذكرة الماجستير في القانون الجنائي، كلية الحقوق جامعة الجزائر 1، 2011-2012.

القوانين:

1. القانون رقم 09-04 المؤرخ في 2009/08/05 المتعلق بالقواعد للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، جريدة رسمية عدد 47 المؤرخة في 2009/08/06.
2. القانون رقم 15-04 المؤرخ في 2015/02/01 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، جريدة رسمية عدد 06، المؤرخة في 2015/02/10
3. القانون رقم 09-04 المؤرخ في 05-اوت 2009 يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، ج.ر.47
4. القانون رقم 16 – 01 المؤرخ في 6 مارس 2016 المتضمن التعديل الدستوري، الجريدة الرسمية العدد 14، الصادرة في 07 مارس 2016.
5. المادة 65 مكرر 5 من القانون رقم 15 – 19 المؤرخ في 30 ديسمبر 2015يعدل ويتمم الأمر رقم 66 – 156 المؤرخ في 8 جوان 1966، المتضمن قانون العقوبات، الجريدة الرسمية العدد 71، الصادرة في 30 ديسمبر
6. المادة 46 من الأمر رقم 15 – 02 المؤرخ في 23 جوان 2015 يعدل ويتمم الأمر رقم 66 – 155 المؤرخ في 8 جويلية 1966 المتضمن قانون الإجراءات الجزائية، الجريدة الرسمية عدد 40، الصادرة في 23 جويلية 2015.
7. المرسوم الرئاسي رقم 15-261 المؤرخ في 24 من ذي الحجة عام 1436ه/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
8. القانون رقم 04/09 المؤرخ في 5 أغسطس 2009 والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. ومرسوم رئاسي رقم 15-261 المؤرخ في 24 من ذي الحجة عام 1436ه/الموافق ل 8 أكتوبر 2015 يحدد تشكيلة وتنظيم وكيفيات سير الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.
9. قانون المعاملات والتجارة الإلكترونية لإمارة دبي، قانون رقم 2 لسنة 2002.

10. اللائحة التنفيذية لقانون التوقيع الإلكتروني المصري، وزارة الاتصالات وتكنولوجيا المعلومات، قرار رقم 109 لسنة 2005، بتاريخ 2005/05/15

المواقع الإلكترونية

1. حسين الماجي، نظرات في قانون التجارة الإلكترونية، www.arablaw.info.com، 2016/03/30.
2. لمزيد من التفصيل راجع بحث للأستاذ عبد المجيد ميلاد، تشفير البيانات والتوقيع الالكتروني على الموقع الاتي :
http://www.arabcin.net/modules.php?name=News&file=article&sid=948
3. .لمزيد من التفصيل راجع موضوع التحديات القانونية للتجارة الالكترونية على الموقع الالكتروني الاتي :
http://www.opendirectorysite.info/e-commerce/04.htm
4. مهران زهير المصري، السياسات الأمنية للمواقع الإلكترونية ،مجلة الباحثون العدد 40، 2010، متوفر على الموقع التالي:
http://kenanaonline.com/users/ahmedkordy/posts/330241
5. الجريمة الالكترونية: معالجة أزيد من 1100 قضية خلال 2018 على المستوى الوطني:
http://www.aps.dz/ar/sante-science-technologie/63173-1100-2018
6. ما هو التوقيع الإلكتروني؟، ناسا بالعربي، www.nasainarabic.net.
7. لمزيد من التفصيل راجع بحث للأستاذ عبد المجيد ميلاد، تشفير البيانات والتوقيع الالكتروني على الموقع الاتي :
http://www.arabcin.net/modules.php?name=News&file=article&sid=948
8. .لمزيد من التفصيل راجع موضوع التحديات القانونية للتجارة الالكترونية على الموقع الالكتروني الاتي :
http://www.opendirectorsite.info/e-commerce/04.htm