

مبررات الحماية القانونية للخصوصية الرقمية للمستهلك في عقد التجارة الإلكترونية

Legal justifications for consumer digital privacy

contracts protection in e-commerce

عباس ريمة¹، شداني نسيمة²،

¹ جامعة أكلي محند أولحاج البويرة، الجزائر

البريد الإلكتروني: abbasrima15@gmail.com

² جامعة أكلي محند أولحاج البويرة، الجزائر

البريد الإلكتروني: cheddarinassima@gmail.com

تاريخ النشر: 2025/06/30

تاريخ القبول: 2025/06/30

تاريخ الاستلام: 2025/05/10

ملخص:

تعد الأخطار الرقمية بمثابة مبررات دفعت بالتشريعات الدولية والوطنية إلى سن أحكام وضمانات قانونية لحماية الخصوصية الرقمية للمستهلك في عقد التجارة الإلكترونية؛ وتنقسم هذه المبررات إلى قسمين: مبررات عامة؛ كونها مبررات دافعة للحماية تتعلق بأخطار البيئة الرقمية بصفة عامة، أي بكل ما تشمله هذه الأخيرة من سرعة وتقنيات تكنولوجية وبرامج إلكترونية، أما القسم الثاني فيتعلق بالمبررات الخاصة للحماية، وتشتمل على مخاطر التوقيع الإلكتروني؛ وذلك لأن هذا الأخير له صورته الخاصة التي تطرح أخطارا تختلف من صورة لأخرى.

الكلمات المفتاحية:

أخطار رقمية؛ حماية قانونية؛ مبررات عامة؛ مبررات خاصة

Abstract:

Digital risks are justifications that have prompted international and national legislation to enact legal provisions and guarantees to protect consumers' digital privacy in e-commerce contracts. These justifications are divided into two categories: General justifications: These are justifications for protection related to the dangers of the digital environment in general, that is, everything the latter includes in terms of speed, technological techniques, and electronic programs.

*المؤلف المرسل

The second section relates to specific justifications for protection, and includes the dangers of electronic signatures, because the latter has its own forms that pose dangers that differ from one form to another.

Keywords:

Digital risks; legal protection; general justifications; specific justifications

مقدمة:

أمام التطورات التكنولوجية الحديثة أصبح من السهل جمع المعلومات والبيانات المتعلقة بالمستهلكين، ولم يصبح من السهل كذلك ضمان حفظ تلك البيانات من الخطر الرقمي؛ فالبيئة الرقمية تجعل من البيانات والمعلومات محل التبادل عرضة لعدة مخاطر رقمية. هذه الأخيرة أهم ما يميزها أنها تجعل من الصعب بل من المستحيل أحيانا إرجاع الحال إلى ما كان عليه قبل وقوع ذلك الخطر، فلا يمكن استعادة المعلومات التي تم الاستيلاء عليها واستغلالها، كما لا يمكن تصحيح ما لحقها من تشويه⁽¹⁾.

ومن هنا تطرح الإشكالية: ماهي أخطار البيئة الرقمية والتي استوجبت ضرورة سن حماية قانونية للخصوصية الرقمية للمستهلك الإلكتروني؟.

تعد هذه الأخطار بمثابة مبررات دفعت بالتشريعات الدولية والوطنية إلى سن أحكام وضمانات قانونية لحماية الخصوصية الرقمية للمستهلك الإلكتروني؛ لذا قسمنا هذه المبررات إلى قسمين: مبررات عامة؛ كونها مبررات دافعة للحماية تتعلق بأخطار البيئة الرقمية بصفة عامة، أي بكل ما تشمله هذه الأخيرة من سرعة وتقنيات تكنولوجية وبرامج إلكترونية... (المبحث الأول)، أما القسم الثاني فيتعلق بالمبررات الخاصة للحماية، وتشتمل على مخاطر التوقيع الإلكتروني؛ وذلك لأن هذا الأخير له صوره الخاصة التي تطرح أخطارا تختلف من صورة لأخرى (المبحث الثاني).

(1) - منى الأشقر جبور، محمد حيدر، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، لبنان، ط1، 2018، ص29.

المبحث الأول

المبررات العامة لحماية الخصوصية الرقمية للمستهلك الإلكتروني

يعتبر نظام تبادل المعلومات⁽²⁾ نظماً حديثاً ومعمولاً به في العديد من العمليات، سواء إبرام العقود أو غيرها من استعلامات ومعطيات أو بيانات الإنتاج... الخ. ومن أهم ميزات هذا النظام التقليل من مصاريف النقل، وسهولة الوصول إلى المعلومة، وقلة الخطأ واللبس في المعاملات التجارية⁽³⁾.

غير أنه يؤخذ على هذا النظام تعرض المعلومات والبيانات محل التبادل لمخاطر عدة ناتجة عن البيئة الرقمية التي يتم التبادل من خلالها (المطلب الأول)، وهو الأمر الذي دفع بالتشريعات إلى المسارعة لسن القوانين الحامية لهذه المعلومات، وجعلها ضمانات قانونية تهدف إلى تدعيم عنصر الثقة في التجارة الإلكترونية (المطلب الثاني).

المطلب الأول: مخاطر البيئة الرقمية

تمتاز البيئة الرقمية بالإمكانيات التقنية الكبيرة، التي لا يمكن تحديد مداها أو قدرتها، وإن كانت هذه ميزة إيجابية إلا أنها تشكل خطراً على البيانات الشخصية للمستهلك الإلكتروني؛ ذلك أن هذا الأخير وبإدلائه بهذه البيانات في العقد الإلكتروني فإنه يكون قد أدخلها إلى البيئة الرقمية وجعل منها معطيات رقمية، معرضة لمخاطر هذه البيئة⁽⁴⁾.

ويمكن تصنيف المخاطر التي تشكلها البيئة الرقمية على المعطيات الشخصية للمستهلك الإلكتروني إلى صنفين: أخطار متعلقة بالبرامج المتاحة على شبكة

(2) - عرف قانون اليونسترال النموذجي للتجارة الإلكترونية لعام 1996 في المادة 02 منه في فقرتها الثانية تبادل المعطيات الشخصية أنه: "نقل المعلومات إلكترونياً من حاسوب إلى آخر باستخدام معيار متفق عليه لتكوين المعلومات".

(3) - عبد الرحمان خلفي، حماية المستهلك الإلكتروني في القانون الجزائري: دراسة مقارنة، مجلة جامعة النجاح للأبحاث، فلسطين، المجلد 27، عدد 1، 2013، ص21.

(4) - Henri Isaac, Pierre Volle, E-Commerce de la stratégie à la mise en œuvre opérationnel, Person éducation, Paris, France, 2008, p16.

الأنترنت (الفرع الأول)، وأخطار متعلقة بالميزات التكنولوجية لهذه الشبكة (الفرع الثاني) الفرع الأول: الأخطار المتعلقة ببرامج شبكة الأنترنت

تحتوي شبكة الأنترنت على برامج من شأنها الاطلاع على خصوصية مستخدمي هذه الشبكة، وهي متوفرة لدى مزودي خدمة الأنترنت، ونذكر من هذه البرامج:

أولاً- برامج الرقابة:

تقوم برامج الرقابة بتسجيل ما يقوم به المستخدم عبر الأنترنت والمواضيع التي تهتمه والمواقع التي يتصل بها⁽⁵⁾؛ حيث تستطيع هذه البرامج الوصول إلى رغبات هذا المستخدم وعاداته في التسوق، وذلك بتحليل بياناته الشخصية، وهذه البيانات من شأنها عند تجميعها عبر وسائل تقنية مختلفة تخضع للتحاليل عبر برمجيات ذكية، أن تكشف عن مسائل كثيرة قد لا يرغب الشخص بكشفها، ويمكن أن تصل هذه البيانات للمتاجرة بها عن طريق بيعها بهدف تحقيق الربح، حيث ارتكبت العديد من جهات الرقابة أنشطة إساءة استخدام البيانات الشخصية حتى في أكبر الدول المتقدمة، وكان الهدف من وراء هذه الاعتداءات في الغالب سياسياً أو اقتصادياً⁽⁶⁾.

ثانياً- محركات البحث:

عرفت محركات البحث من وجهات نظر مختلفة، إذ لا يوجد تعريف جامع مانع لها؛ حيث عرف محرك البحث أنه برنامج يمكن المستخدمين من عمليات البحث عن كلمات أو صور محددة، وذلك ضمن مصادر الأنترنت المختلفة، في موقع واحد أو مجموعة كبيرة من

(5) - يتم تسجيل عناوين المواقع التي يزورها المستخدم مثل دخول مواقع منتديات الحوار أو قاعات الدردشة. وتسجل جميع البيانات الخاصة بالوقت الذي تم قضاؤه في الدردشة في كل صفحة، والبيانات التي تم تبادلها، ويتم تسجيل هذه البيانات والاحتفاظ بها لمدة طويلة من قبل مزودي خدمات الأنترنت في ملفات تعرف بـ Fichier log.. طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الأنترنت- دراسة مقارنة-، مذكرة ماجستير، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2006-2007، ص. ص 86-87.

(6) - ربيع نصيرة، ربيع نصيرة، الحماية القانونية للمعالجة الآلية للمعطيات الشخصية - دراسة مقارنة-، مجلة المحلل القانوني، جامعة البويرة، المجلد 3، عدد 2، ديسمبر 2021، ص 04.

المواقع⁽⁷⁾. ويعرف أيضا بأنه برنامج حاسوبي صمم للعمل على استرجاع المعلومات والمساعدة على البحث عن المعلومات والمستندات المخزنة في الشبكة العنكبوتية العالمية باستعمال كلمة أو عبارة ما، حيث تظهر نتائج البحث عادة على شكل قوائم منظمة وفق أماكن تواجدها وطبقا لمعايير معينة⁽⁸⁾، ومن أمثلة ذلك محركات البحث: Archie و Google و Yahoo و Bing و Baidu و duckduckgo.

تعد محركات البحث أدوات بحث فعالة في الحصول على المعلومة في وقت قياسي لا يتعدى الثانية الواحدة، غير أنها يمكن أن تهدد خصوصية المستهلك باعتبار محركاتها تساعد على معرفة الاتجاهات الخصوصية للزائر (المستهلك)، كما أن أغلبية هذه المواقع لا تطلع مستخدميها بأنهم تحت الرقابة، وهو ما يعد في حد ذاته انتهاكا لخصوصيتهم؛ لذلك نجد قانون التجارة الإلكترونية الجزائري ينص على وجوب إعلام المستخدم بذلك، ويبقى له الخيار بالقبول أو الرفض، فقد أوجبت المادة 26 منه على للمورد الإلكتروني الذي يقوم بعملية جمع المعطيات ذات الطابع الشخصي وتشكيل ملفات الزبائن والزبائن المحتملين: أن يقوم بجمع البيانات اللازمة لإبرام المعاملة التجارية فقط دون أن يتعدى إلى المعلومات الأخرى التي لا علاقة لها بذلك، كما يجب عليه الحصول على موافقة المستهلك الإلكتروني قبل جمع البيانات.

الفرع الثاني: الأخطار المتعلقة بالميزات التكنولوجية لشبكة الأنترنت

تشكى السرعة والانفتاح على العالم أبرز مزايا شبكة الأنترنت، غير أن هاتين الميزتين انعكستا سلبا على خصوصية المستهلك المستعمل لهذه الشبكة؛ وذلك من خلال سهولة تحديد هوية المستخدم (أولا)، وكذا عجز الأنترنت عن ضمان سرية ما ينقل عبرها من

(7) - صادق عباس مصطفى، الأنترنت والبحث العلمي. ذكره: عبده محمد المخلافي، طرائق وأدوات البحث عن المعلومات في الأنترنت وواقع استخدامها عند هيئات التدريس ومعاونهم بكلية الآداب- جامعة صنعاء دراسة استكشافية-، المجلة العراقية لتكنولوجيا المعلومات، المجلد 7، عدد 2، 2016، ص 39.

(8) - فاطمة الزهراء محمد عبده، محركات البحث على شبكة الأنترنت، مجلة Journal cybrairians. ذكرته: نبيلة رزاق، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي- دراسة مقارنة-، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 7، عدد 1، جوان 2021، ص 1995.

معلومات (ثانيا).

أولا- سهولة تحديد هوية المستخدم:

يعتبر أي دخول للفرد لشبكة الأنترنت تنزلا منه عن حقه في خصوصية بياناته، سواء كان ذلك بالتسجيل في مقهى الأنترنت أو الاشتراك في الشبكة اللاسلكية أو من خلال شراء هاتف نقال أو غيرها⁽⁹⁾. فالحواسيب الرقمية وتكنولوجيا المعلومات الاجتماعية وضعت الحياة الشخصية للفرد بجميع جوانبها الاجتماعية والثقافية والسياسية وميولاته ورغباته في عالم افتراضي، وهو الأمر الذي أدى إلى كشف العديد من الجوانب الشخصية في حياة المستهلك وتعرضه لأخطار الأنترنت⁽¹⁰⁾؛ لذا نجد القوانين والتشريعات تضع ضمانات معينة لحماية هذه الخصوصية عن طريق اتباع المستهلك إجراءات وخطوات معينة قبل الدخول لهذه الشبكات ، غير أن ذلك يبقى سلوكا شخصيا قد يقوم به صاحب الدراية بخبايا الأنترنت ويغفل عنه المستخدم العادي⁽¹¹⁾.

ثانيا- عجز الأنترنت عن ضمان سرية ما ينقل عبرها من بيانات

أدت وسائل تبادل المعلومات التي تتيحها الأنترنت وبرمجيات التصفح والتبادل والنقل إلى سهولة تنقل البيانات الشخصية من بين الدول والمنظمات والمؤسسات وحتى الأفراد، وهو ما يجعل هذه المعلومات عرضة للقرصنة والاعتداء، ويهدد سريتها⁽¹²⁾.

ورغم الجهود الكبيرة المبذولة في المجال التشريعي والتقني والمعلوماتي للحد من

(9) - انظر: مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية المقارنة، جامعة دمشق، المجلد 29، عدد 3، 2013، ص.ص 228-330.

في اعتقادي أن التنازل هذا لا يتعدى المعلومات البسيطة عن الشخص التي أوردتها عند تصفحه للأنترنت، مثل: الاسم واللقب، وتاريخ الميلاد، والجنس، والبلد. أما التدخل في البيانات التفصيلية للشخص فلا يمكن قبول التنازل بشأنها بمجرد الدخول العادي. فضلا عن ذلك، يعد أي استعمال لتلك البيانات لغرض شخصي بحث من طرف مزودي خدمة الأنترنت يعد انتهاكا للخصوصية حتى ولو تعلق بالبيانات البسيطة.

(10) - ربيع نصيرة، مرجع سابق، ص 10.

(11) - نبيلة رزاق، مرجع سابق، ص 1995.

(12) - طارق عثمان، مرجع سابق، ص 87.

الاعتداء على حياة الأفراد وأسرارهم، إلا أنه لاتزال المعطيات الشخصية معرضة للاعتداء. ولتوفير الحماية اللازمة لا بد أن يضاف إلى هذه الجهود تنسيق دولي فيما يخص انتقال المعلومات الشخصية عبر الفضاء الافتراضي⁽¹³⁾.

المطلب الثاني: دعم عنصر الثقة في التجارة الإلكترونية

تقوم المعاملات التجارية بصفة عامة سواء التقليدية أو الإلكترونية على أساس الثقة، ويعتبر التعدي على المعطيات الشخصية للمستهلك، سواء من طرف المورد أو الغير، زعزعة ومساسا بتلك الثقة، هذه الأخيرة التي تعد من أهم الضمانات القانونية لاستمرار المعاملة التجارية في البيئة الرقمية⁽¹⁴⁾.

وأمام التطورات التكنولوجية الحديثة، لم يعد صعبا جمع المعلومات والبيانات المتعلقة بالمستهلكين، ولم يعد سهلا كذلك ضمان حفظ تلك البيانات من الخطر الرقمي.

كل هذه المسائل جعلت من الزبون المستهلك يركز على خصوصيته، ويتابع كيفية استخدام معطياته ومدى ضمان سريتها⁽¹⁵⁾، ويعطي هذا الأمر أهمية كبيرة؛ حيث إن الكثير من مستخدمي شبكة الأنترنت يعزفون عن التعاقد إلكترونيا إذا طلب منهم تقديم معلومات شخصية، أو يقدمون معلومات خاطئة وغير صحيحة لحماية خصوصيتهم.

وتعزيزا لعنصر الثقة في التجارة الإلكترونية وتجنبنا للإحجام عن دخول عالم التجارة الإلكترونية؛ نجد التشريعات الداخلية والدولية تسهر دائما على ضرورة تدعيم منظوماتها القانونية بنصوص خاصة تضمن حماية ملفات الزبائن التي تحتوي على كافة المعطيات الخاصة بهم.

(13) - ربيع نصيرة، مرجع سابق، ص 10.

(14) - فاطمة الزهراء محمد عبده، محركات البحث على شبكة الأنترنت. ذكرته نبيلة رزاق، مرجع السابق، ص 1995.

Cynthia Chassigneux, l'encadrement juridique du traitement des données personnelles sur le site de commerce en ligne, thèse de doctorant, université de Montréal, 2003, p68.

(15) - سهام قارون، التزام المورد الإلكتروني بحماية المعطيات الشخصية للمستهلك في القانون 05-18 المتعلق بالتجارة الإلكترونية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، المجلد 7، عدد 2، 2020، ص 1017.

إن تبني سياسة خصوصية فعالة واحترامها هي من الواجبات التي تقع حتى على المورد الإلكتروني؛ لأن ذلك من شأنه بناء الثقة مع المستهلك الإلكتروني الذي يتعامل معه، وحماية للمعاملة الإلكترونية ككل، فأخطار البيئة الرقمية قد تمتد حتى للملفات التي بحوزة المورد الإلكتروني، والتي تتضمن معطيات شخصية للمستهلك الذي يتعامل معه، حيث تكون هذه الملفات عرضة للضياع في حالة هجوم فيروسات أو أي خطر تقني آخر، وهو ما قد يؤدي إلى فقدان الدليل الإلكتروني الذي يحتاج به الأطراف.

المبحث الثاني:

مبررات الحماية المرتبطة بالتوقيع الإلكتروني

نشوء التوقيع الإلكتروني كان كبديل للتوقيع التقليدي، وجاء مواكبة لظهور المعاملة التجارية الإلكترونية، ويلعب التوقيع الإلكتروني دورا كبيرا في تأمين خصوصية المتعاملين الإلكترونيين، فالتوقيع الإلكتروني قادر على تحديد هوية الشخص الموقع بدقة، وكذا التعبير عن قبوله الالتزام بمضمون السند الذي وقع عليه، وهما وظيفتان أساسيتان للتوقيع الإلكتروني، وعلى درجة كبيرة من الأهمية؛ لذا كانتا من المبررات التي دفعت لفرض حماية قانونية للتوقيع الإلكتروني (المطلب الأول)، يضاف إلى ذلك المخاطر الرقمية التي ينشأ في ظلها التوقيع الإلكتروني (المطلب الثاني).

المطلب الأول: أهمية وظائف التوقيع الإلكتروني

نصت على وظائف التوقيع الإلكتروني المادة 06 من القانون رقم 15-04 المتعلق بالتوقيع والتصديق الإلكتروني، حيث جاء فيها: «يستعمل التوقيع الإلكتروني لتوثيق هوية الموقع وإثبات قبوله مضمون الكتابة في الشكل الإلكتروني».

حسب نص هذه المادة فإن وظائف التوقيع الإلكتروني تنحصر في وظيفتين أساسيتين: الأولى تتمثل في تحديد هوية الموقع (الفرع الأول)، أما الثانية فهي التعبير عند

التزامه بما وقع عليه (الفرع الثاني)⁽¹⁶⁾.

الفرع الأول: تحديد هوية الموقع

التوقيع علامة شخصية؛ لذلك كان الشخص هو الذي يقوم بنفسه بعملية وضع التوقيع. فحتى وإن وقع شخص آخر باسم الموقع فإن هذا التوقيع لا يعد صحيحا ولو تم ذلك بموافقة صاحب التوقيع، فالتوقيع شكل مميز لصاحبه. والعبرة أن يكون صادرا ممن يحتج به.

ويترتب على اعتبار التوقيع علامة شخصية أنه لا يمكن أن تتوافر مجموعة نسخ لتوقيع واحد، فالتوقيع يعمل على تحديد شخص الموقع والبيانات الشخصية عنه، وبذلك يتميز الموقع عن غيره وتتحدد هويته⁽¹⁷⁾.

في التوقيع التقليدي يسهل للتوقيع أن يؤدي وظيفة تحديد هوية شخص الموقع، وذلك أن الأطراف حاضرة ماديا، وبالإمكان التأكد من هويتهم عن طريق تقديم وثائق إثبات الهوية، أما في التوقيع الإلكتروني الذي يتم في عالم افتراضي، فإنه يصعب معه تحديد هوية الشخص الموقع⁽¹⁸⁾.

وبالرجوع إلى التشريعات الدولية والوطنية، نجدها تشترط في التوقيع بشكل عام - دون تمييز إن كان تقليديا أو إلكترونيا- حتى يعتد به؛ يجب أن يكون محددا لهوية صاحبه ويميزه عن غيره، بغض النظر عن شكل ووسيلة هذا التوقيع، أو اتصاله المادي بصاحبه من عدمه، حيث نصت المادة 07 من قانون اليونسترال النموذجي بشأن التجارة الإلكترونية لعام 1996 على أنه يعتبر المحرر موقعا قانونا من قبل شخص متى استوفت رسالة البيانات شرطين أساسيين وهما: استخدام طريقة لتحديد هوية الشخص، والتدليل على

(16) - وهي نفس الوظائف التي يرى الفقه أن التوقيع التقليدي يؤديها. توفيق حسن فرج، قواعد الإثبات في المواد المدنية والتجارية، دار الثقافة الجامعية، الإسكندرية، 1981، ص 10.

(17) - عيبر ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني، دار وائل للنشر، عمان، الطبعة الأولى، 2010، ص 56.

(18) - يترجم المشرع الجزائري الموقع الإلكتروني في نص المادة 2 فقرة 2 من القانون رقم 04-15 بأنه: «شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثلته».

أنه قد وافق على المعلومات الواردة في رسالة البيانات، وأن تكون هذه الطريقة جديرة بالتعويل عليها بالقدر المناسب للغرض الذي نُشئت أو بلغت من أجله رسالة البيانات، وذلك في ضوء كل الظروف.

وهو الأمر الذي نص عليه المشرع الفرنسي في المادة 1367 من الأمر 2016-131 المتعلق بإصلاح العقود وإثبات الالتزامات؛ حيث نصت هذه المادة على أن التوقيع اللازم للاعتداد بالتصرفات القانونية يحدد هوية مصدره، ويعبر عن قبول الأطراف بالالتزامات المترتبة عن هذا التصرف. كما نصت المادة نفسها على أنه عندما يكون التوقيع إلكترونيًا، فإنه يتم استخدام وسيلة موثوق بها لتحديد الشخص، تضمن صلته بالتصرف الذي وقع عليه.

فالمهم - حسب المشرع الفرنسي- في وسيلة التوقيع أن تحدد هوية الموقع وتضمن صلته بالتصرف الذي وقع عليه، فإن توافر هذان الشرطان في وسيلة التوقيع الإلكتروني، كان التوقيع معتدا به ومؤديا لوظيفة تحديد هوية الموقع.

بنفس المعنى جاءت المادة 327 من القانون المدني الجزائري، التي تنص: «...ويعتد بالتوقيع الإلكتروني وفقا للشروط المذكورة في المادة 323 مكرر 1 أعلاه». وبالرجوع إلى نص المادة 323 مكرر 1 نجدها تحدد شروط الكتابة الإلكترونية، التي من بينها تحديد هوية الشخص الذي أصدرها. كما نصت المادة 2 فقرة 2 من القانون رقم 04-15 بأن الموقع هو: «شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله».

التوقيع الإلكتروني ووفقا لصوره المذكورة سابقا، بإمكانه تحديد هوية الشخص الموقع بصورة قد تفوق قدرة التوقيع التقليدي، فالتوقيع الرقمي مثلا، القائم كما رأينا سابقا على مفتاح عام ومفتاح خاص، يمكن الأطراف من تحديد هوية بعضهم؛ ولذلك يستخدم في شبكات مفتوحة مثل الأنترنت⁽¹⁹⁾. والتوقيع بالقلم الإلكتروني، الذي من خلاله لا يعتد بالتوقيع إلا إذا طابق التوقيع المخزن في ذاكرة الكمبيوتر، وكلما كان

(19) - زكرياء مسعودي، جعفر الزهرة، التوقيع الإلكتروني وحمايته للدفع الإلكتروني، المجلة الدولية للبحوث القانونية والسياسية، جامعة الوادي، المجلد 1، عدد 03، ديسمبر 2017، ص 162

الحاسوب المزود بوحدة القلم الإلكتروني مؤمنا من الاختراق كلما تمكن هذا التوقيع من تحديد هوية الموقع، إذ لا بد أن تكون هذه التقنية ذات درجة عالية من الأمان⁽²⁰⁾.

أما التوقيع البيومتري القائم على الخواص الذاتية للشخص، فإنه يؤدي إلى التحديد الدقيق لهوية الشخص⁽²¹⁾ والرقم السري؛ وذلك من خلال استخدام البطاقة الممغنطة الخاصة بالصراف الآلي. فالبطاقة الممغنطة بطاقة شخصية لا يتم استخدامها إلا من قبل صاحبها، وبالتالي لا يستجاب لطلب السحب إلا بعد التأكد من هوية الشخص عن طريق الرقم السري، الذي لا يمكن معرفته من قبل الغير ولا يتشابه مع الأرقام الأخرى⁽²²⁾، فهذا النوع من التوقيعات لا يمكن التلاعب فيه إلا بالحصول على البطاقة ومعرفة الرقم السري أيضا.

الفرع الثاني: التعبير عن إرادة الموقع في الالتزام بمضمون السند الموقع عليه

هناك علاقة وثيقة بين الوظيفة الأولى للتوقيع المتمثلة في تحديد هوية الشخص الموقع، والوظيفة الثانية المتمثلة في التعبير عن إرادة الموقع بالالتزام بمضمون السند الموقع عليه⁽²³⁾، فكلما تمكنت صورة التوقيع الإلكتروني من تحديد هوية الموقع كلما استطاعت التعبير عن إرادته، والعكس صحيح. وكل ذلك مرتبط بنوع التقنية المستعملة في التوقيع وقدرتها على توفير الأمان والسرية؛ فكلما كانت تقنية التوقيع قادرة على توثيق العلاقة بين التوقيع والمحرم كلما كانت تمكنت من التعبير عن إرادة الموقع فيها بالالتزام عند التوقيع عليه.

(20) - علاء حسين مطلق التميمي، الدليل الإلكتروني في الإثبات المدني، دراسة مقارنة، دار النهضة العربية، مصر، الطبعة الأولى، 2010، ص 202.

(21) - نزياء مسعودي، جعفر الزهرة، مرجع سابق، ص 163.

(22) - باهة فاطمة، آثار قواعد الإثبات القانوني على المراكز القانونية للخصوص: دراسة مقارنة، أطروحة دكتوراه في العلوم، تخصص قانون إجرائي، كلية الحقوق والعلوم السياسية، جامعة الجيلالي الياقوب، سيدي بلعباس، 2017-2018، ص 166.

(23) - عبد الرحمان عبد الله الخميس، المخاطرة في العمليات المالية المعاصرة، دار كنوز إشبيليا للنشر والتوزيع، الرياض، الطبعة الأولى، 2013، ص 506-507.

المطلب الثاني: المخاطر الرقمية على التوقيع الإلكتروني

يلعب التوقيع الإلكتروني دوراً مهماً في المعاملات التجارية الإلكترونية؛ نظراً للوظائف المهمة التي يؤديها، غير أن هناك جملة من المخاطر تحفه قد تؤدي إلى عدم الثقة في قدرته على أداء هذه الوظائف. هذه المخاطر قد تكون راجعة لصاحب التوقيع (الفرع الأول)، أو للبيئة الرقمية التي يتم من خلالها العمل بالتوقيع الإلكتروني (الفرع الثاني)، أو للوسيلة التقنية المستعملة في التوقيع الإلكتروني (الفرع الثالث).

الفرع الأول: المخاطر المرتبطة بصاحب التوقيع الإلكتروني

قد يرتكب صاحب التوقيع الإلكتروني أخطاء تجعل هذا التوقيع - بعدما كان حكراً على صاحبه - في يد شخص آخر؛ مما يترتب عنه مخاطر في مجال التجارة الإلكترونية، ومن هذه الأخطاء: نسيان صاحب التوقيع لرقمه السري، أو إعطاء هذا الرقم لشخص آخر أو إهماله مما يؤدي إلى وقوعه بيد أشخاص آخرين فيسيئون استعماله⁽²⁴⁾.

الفرع الثاني: مخاطر البيئة الرقمية

يقصد بمخاطر البيئة الرقمية، مخاطر الفضاء الإلكتروني الذي يتم فيه التوقيع الإلكتروني، وهي مخاطر لا يتعرض لها التوقيع التقليدي. فبرامج الحاسب التي يتم عن طريقها التوقيع الإلكتروني، قد تحتوي ثغرات أو أخطاء لا تكتشف إلا أثناء عمل هذا البرنامج، مما قد يترتب عنه فقد الثقة في هذا التوقيع⁽²⁵⁾.

وقد يحدث أن يتعرض التوقيع الإلكتروني للقرصنة؛ حيث يتم السيطرة على النظام المعلوماتي الخاص بالموقع، فتستغل الأرقام السرية في أغراض شخصية، بل قد يتم الاستيلاء على النظام المعلوماتي للطرف الثالث وإصدار شهادات التوثيق باسمه⁽²⁶⁾.

(24) - عبد الرحمن عبد الله الخميس، مرجع سابق، ص 506.

(25) - محمد حسين بدوي، التعاقد عبر الأنترنت: دراسة فقهية مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، 2015، ص 61.

(26) - سامح التهامي، التعاقد عبر الأنترنت - دراسة مقارنة -، دار الكتب القانونية، مصر، 2008، ص 541.

الفرع الثالث: المخاطر المتعلقة بالتقنية المستعملة في التوقيع الإلكتروني

إن المخاطر المتعلقة بالتقنية المستعملة في التوقيع الإلكتروني تختلف من تقنية لأخرى، وعلى حسب ودرجة السرية والأمان التي تقدمها كل تقنية؛ فالبطاقة الممغنطة قد تتعرض للسرقة، وتستخدم لأغراض شخصية من قبل أي شخص يحصل على رقمها السري⁽²⁷⁾. كما يمكن لقرصنة الأنترنت الحصول على المفتاح الخاص للتوقيع الرقمي واستعماله في عمليات لصالحهم الخاص⁽²⁸⁾.

التوقيع البيومتري هو الآخر معرض لخطر التغيير في الخصائص البشرية التي تتأثر بفعل الظروف، كتآكل البصمات بمرور الزمن، أو تأثر نبذة الصوت بالتوتر، أو تطابق التوائم⁽²⁹⁾، كما لا يسلم هذا التوقيع من خطر القرصنة، وذلك عن طريق تقليد البصمات الذي يتم بالبصمات البلاستيكية المقلدة أو العدسات اللاصقة⁽³⁰⁾.

خاتمة:

إن قيام التعاقد في التجارة الإلكترونية على الوسائل التقنية والتكنولوجية، بقدر ما يوفر فعالية ودقة كبيرة، بقدر ما تحيط به مخاطر كبيرة تهدد فيه أهم عنصر في التعامل وهو عنصر الثقة.

فالبيانات الشخصية التي ترسل عبر الفضاء الافتراضي، أهم ميزاتها أنها بيانات شخصية تتعلق بالحياة الخاصة للمستهلك، مما يجعل خصوصيته مهددة نظرا لإمكانية أي شخص الدخول لهذا الفضاء واستغلال والتلاعب بما يتداول فيه، من هنا كانت الحماية القانونية ضرورية للمستهلك في هذا المجال، وهو الأمر الذي سعت من أجله مختلف التشريعات الوطنية والدولية بوضع مبادئ وقواعد من شأنها حماية

(27)- خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2011، ص 253.

(28)- محمود عبد الرحيم الشريفات، التراضي في تكوين العقد عبر الأنترنت: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2009، ص 196.

(29)- محمود عبد الرحمان شريفات، مرجع سابق، ص 196.

(30)- طارق عثمان، مرجع سابق، ص. ص 86-87.

الخصوصية الرقمية لهذا المستهلك؛ وإيجاد توازن بين حاجة المجتمع لمعالجة المعطيات الشخصية للأشخاص، ووجوب ضمان حماية هذه البيانات من أخطار الاستخدام غير المشروع لتقنيات معالجتها. خاصة أن التعامل في هذه البيئة وفي ظل ما تحتويه من أخطار، يجعل من عملية الإصلاح أمراً عسيراً جداً، إذ لا يمكن استعادة المعلومات التي تم الاستيلاء عليها، وقد لا يمكن تصحيح ما لحقها من تشويه.

قائمة المصادر والمراجع:

أولاً: باللغة العربية

أ- الكتب

- (1) توفيق حسن فرج، قواعد الإثبات في المواد المدنية والتجارية، دار الثقافة الجامعية، الإسكندرية، 1981.
- (2) سامح التهامي، التعاقد عبر الأنترنت - دراسة مقارنة-، دار الكتب القانونية، مصر، 2008، ص 541.
- (3) محمد حسين بدوي، التعاقد عبر الأنترنت: دراسة فقهية مقارنة، دار الجامعة الجديدة، الإسكندرية، مصر، .
- (4) خالد ممدوح إبراهيم، إبرام العقد الإلكتروني، دار الفكر الجامعي، الإسكندرية، مصر، 2011.
- (5) عبير ميخائيل الصفدي الطوال، النظام القانوني لجهات توثيق التوقيع الإلكتروني، داروائل للنشر، عمان، الطبعة الأولى، 2010.
- (6) علاء حسين مطلق التميمي، الدليل الإلكتروني في الإثبات المدني، دراسة مقارنة، دار النهضة العربية، مصر، الطبعة الأولى، 2010.
- (7) محمود عبد الرحيم الشريفات، التراضي في تكوين العقد عبر الأنترنت: دراسة مقارنة، دار الثقافة للنشر والتوزيع، عمان، 2009.
- (8) عبد الرحمان عبد الله الخميس، المخاطرة في العمليات المالية المعاصرة، دار كنوز إشبيليا للنشر والتوزيع، الرياض، الطبعة الأولى، 2013.

- (9) منى الأشقر جبور، محمد حيدر، البيانات الشخصية والقوانين العربية، الهم الأمني وحقوق الأفراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، لبنان، ط1، 2018.

ب- الأطاريح والرسائل الجامعية

• أطاريح الدكتوراه

- (1) باهة فاطمة، آثار قواعد الإثبات القانوني على المراكز القانونية للخصوصية: دراسة مقارنة، أطروحة دكتوراه في العلوم، تخصص قانون إجرائي، كلية الحقوق والعلوم السياسية، جامعة الجيلالي اليااس، سيدي بلعباس، 2017-2018.

• رسائل ومذكرات الماجستير:

- (1) طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الأنترنت- دراسة مقارنة، مذكرة ماجستير، تخصص قانون جنائي، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر، بسكرة، 2006-2007.

ج- المقالات العلمية:

- (1) نبيلة رزاق، الحماية الجنائية للخصوصية الرقمية للمعطيات ذات الطابع الشخصي- دراسة مقارنة، مجلة الدراسات القانونية المقارنة، جامعة الشلف، المجلد 7، عدد 1، جوان 2021.
- (2) زكرياء مسعودي، جقريف الزهرة، التوقيع الإلكتروني وحمايته للدفع الإلكتروني، المجلة الدولية للبحوث القانونية والسياسية، جامعة الوادي، المجلد 1، عدد 03، ديسمبر 2017.
- (3) سهام قارون، التزام المورد الإلكتروني بحماية المعطيات الشخصية للمستهلك في القانون 05-18 المتعلق بالتجارة الإلكترونية، مجلة الباحث للدراسات الأكاديمية، جامعة باتنة 1، المجلد 7، عدد 2، 2020.

- (4) عبد الرحمان خلفي، حماية المستهلك الإلكتروني في القانون الجزائري: دراسة مقارنة، مجلة جامعة النجاح للأبحاث، فلسطين، المجلد 27، عدد 1، 2013.
- (5) عبده محمد المخلافي، طرائق وأدوات البحث عن المعلومات في الأنترنت وواقع استخدامها عند هيئات التدريس ومعاونهم بكلية الآداب- جامعة صنعاء دراسة استكشافية-، المجلة العراقية لتكنولوجيا المعلومات، المجلد 7، عدد 2، 2016.
- (6) مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الأنترنت، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية المقارنة، جامعة دمشق، المجلد 29، عدد 3، 2013.

د- النصوص القانونية

- قانون رقم 04-15، مؤرخ في 01 فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الإلكترونيين، ج.ر، عدد 06، صادر بتاريخ 10 فبراير 2015.

ثانيا: باللغة الأجنبية

- 1) Cynthia Chassigneux, l'encadrement juridique du traitement des données personnelles sur le site de commerce en ligne, thèse de doctorant, université de Montréal, 2003.
- 2) Henri Isaac, Pierre Volle, E-Commerce de la stratégie à la mise en œuvre opérationnel, Person éducation, Paris, France, 2008.