

المصلحة المحمية جزائيا في قانون التجارة الالكترونية الجزائري . The penally protected interest in Algeria's E-commerce law

موسى لسود

المركز الجامعي مرسلبي عبد الله -تيبازة- Lassoued.moussa@univ-tipaza.dz

سالم إنصاف

جامعلة علي لونيبي البليدة 02

Edi.salem@univ-blida.dz

ملخص:

ترفق الجريمة في نطاق التجارة الالكترونية تضر بأطراف عديدة وتصيب مصلحة كل منهم سواء أكان البائع أم المشتري وكذلك المنتج والمستهلك، وهو الأمر الذي حاولت كل التشريعات القانونية ذات الصلة بالتجارة الالكترونية بما فيها القانون النموذجي للأمم المتحدة التنبه إليه، وهو أن المساس بالمصلحة في نطاق التجارة الالكترونية يتحقق من خلال الاعتداء على كل ما يتعلق بالأنشطة التجارية، وبصدور القانون 05/18 المتعلق بالتجارة الالكترونية في الجزائر، والذي خصص حماية جزائية فعالة للمصالح الواجب حمايتها في التعاملات التجارية الالكترونية من حماية التوقيع الالكتروني و بيانات المستهلك الالكتروني إلى حماية الموقع التجاري الالكتروني والمورد الالكتروني

الكلمات مفتاحية: تجارة الكترونية ؛ توقيع الكتروني ؛ مورد الكتروني ؛ مستهلك الكتروني ؛ بيانات شخصية.

Abstract:

Crime in the scope of E-commerce harms many parties and harms the interests of each of them, whether the seller or the buyer, as well as the producer and consumer, which all legal legislation related to electronic commerce, including the United Nations Model Law, has tried to be aware of, namely, that the interest in the scope of e-commerce is compromised by attacking all matters relating to commercial activities, and by the issuance of law 18/05 on electronic commerce in Algeria, which has allocated a penalty for effective protection of interests to be protected in commercial transactions.

Keywords: E-commerce؛ Electronic signature؛ Personal data؛ Electronic consumer.

* لسود موسى

1. مقدمة:

الحياة في المجتمع التجاري الالكتروني تفرض بين أفرادها وجود مجموعة متعددة من العلاقات في شتى المجالات، كون الثقة عنصر أساسي في الاقتصاد والمال، وانعدام هذه الثقة أمر تستحيل معه التجارة الالكترونية بصفة عامة ويكون بداية لنزاعات وخصومات مدنية وجزائية، وتكاد تجمع التشريعات الجنائية على الاعتراف بأهمية الثقة العامة كمصلحة اجتماعية جديرة بالحماية الجزائية، فالمصالح المحمية في التجارة الالكترونية على هذا النحو تعد دستور النظام التجاري الالكتروني الذي يعمل المجتمع على حمايته من خلال تجريم الاعتداء على التجارة الالكترونية، ومن بين المصالح القانونية في التجارة الالكترونية التي حماها المشرع بل أن جوهر هذه المصالح هي الثقة العامة، فحماية الثقة العامة في التجارة الالكترونية بما لها من مكانة كبيرة في الاقتصاد والاستثمار العالمي فإنها لا تؤدي هذا الدور إلا إذا كانت محل ثقة بين المتعاملين بها، وهو ما كان جليا في المصلحة المحمية بالعقاب على الجرائم الواقعة عليها بصفة عامة، ومع ذلك لا تزال الثقة تمثل فجوة كبيرة في منظور معاملات التجارة الالكترونية، هذا النقص الكبير في الثقة، هي حتى الآن أكبر عقبة أمام تطوير التجارة الالكترونية مع الأفراد.

والمصالح المحمية جزائيا هي التي يكون تهديدها أو المساس بها دافعا إلى تدخل القانون بما يحويه من نصوص رادعة ردعا عاما وخصوصا، فالغاية من تجريم الاعتداء على المصلحة المعنية في التجارة الالكترونية هي التوصل إلى فرض حماية جنائية فعالة في مواجهة خطر أو ضرر يحيط بمصلحة أو مجموعة مصالح قائمة ومشروعة، وفي ذلك يكون اتجاه ومسعى المشرع الجنائي الجزائري في بنائه لقانون العقوبات والتشريع الجنائي في عمومته والمتعلق بالتصدي لجرائم التجارة الالكترونية.

والمصالح المحمية في التجارة الالكترونية متعددة وان كانت تصب في حماية حرية ممارسة تداول السلع والخدمات بالشكل الالكتروني عن طريق شبكة الانترنت، فمنها شرعية تداول البيانات، وسرية البيانات وخصوصيتها، حماية التوقيع الالكتروني، حماية المستهلك من الغش الالكتروني، حماية أسماء الدومين والعلامة التجارية وغيرها.

وقبل أن يثور التساؤل في مدى نجاعة النصوص الجنائية في حماية المعاملات التجارية الالكترونية، وجب معرفة فيما تتمثل المصلحة المحمية جزائيا التي وضعها المشرع الجزائري من أجل مكافحة الجرائم المتعلقة بالتجارة الالكترونية في ظل القانون 05/18 وتعزيز الثقة في الاقتصاد الرقمي؟

وللإجابة عن إشكالية الدراسة وكون كل دراسة تستوجب مناهج علمية من اجل البحث والتوغل فيها، كونها تشكل الطريق الذي يرسمه الباحث للوصول إلى نتائج علمية بطريقة علمية صحيحة، ولهذا اعتمد الباحث على المنهج الوصفي والتحليلي، وذلك من خلال دراسة وتحليل المواد القانونية المتعلقة بالتجارة الالكترونية، سواء في قانون التجارة الالكترونية الجزائري، أو في القوانين الأخرى المنظمة للمبادلات التجارية، وذلك لأن أسلوب الوصف والتحليل هو الأقرب والأنسب لتحديد معالم وأجديات موضوع دراستنا بدقة. كما اعتمد الباحث إلى المنهج المقارن من خلال النظر إلى موقف بعض التشريعات والاتفاقيات الدولية في مجال ضوابط التجارة الالكترونية والمقارنة بينهما من حيث نتائج تطبيقها على التشريع الجزائري.

ومن خلال الإشكالات السالفة الذكر تبلورت إلى أذهاننا عدة تقسيمات للموضوع، إلا انه في الأخير اهتدينا إلى تقسيم الدراسة مبدئيا إلى التقسيم الذي نعتقد أنه الأقرب للإجابة على إشكالات الموضوع، وذلك من خلال أربعة محاور رئيسية تضمن كل محور مصلحة محمية جزائية في قانون التجارة الالكترونية في القانون 05/18 كالتالي:

2. الحماية الجزائية لمواقع التجارة الالكترونية:

أولت كافة القوانين وخاصة قوانين الولايات المتحدة الأمريكية وأوروبا أهمية بالغة لمسألة حماية مواقع شبكة الانترنت بصفة عامة ومواقع التجارة الالكترونية بصفة خاصة من خلال القوانين التي تجرم الاعتداء على الكمبيوتر بشكل عام، وهو ما سار عليه المشرع الجزائري في القانون 05/18 المتعلق بالتجارة الالكترونية، والقصد من ذلك هو أن يكون لمواقع التجارة الالكترونية حرمة ويمنع المساس بها أو الاعتداء عليها كون الموقع الالكتروني يعتبر حق خاص تقع عليه ملكية خاصة لا يجوز التعدي عليها (عجيلة، 2013، ص 177) وتمثل صور الاعتداء على مواقع التجارة الالكترونية بالدخول غير المشرع إلى نظم معالجة البيانات وكذلك تحريف أو إعاقة تشغيل نظم معالجة البيانات، وأيضا التلاعب في بيانات نظم معالجة البيانات، وغيرها مما يمس الحق في الخصوصية في بيانات ومعلومات مواقع التجارة الالكترونية وهي الجرائم المنصوص عليها في قانون العقوبات الجزائري تحت عنوان المعالجة الآلية للمعطيات، ويتم الدخول غير المصرح به إلى أنظمة المعلومات بإحدى طريقتين: طريقة مباشرة عن طريق الحاسب الآلي الذي يحتوي على المعلومات والنظام ويكون عادة من قبل أشخاص داخل المؤسسة الموجود بها النظام أو أشخاص كانوا لهم صلة بالنظام كعاملين سابقين بالمؤسسة التي بها النظام، وطريقة غير مباشرة: عن طريق الدخول إلى المعلومات الموجودة من خلال نظام آخر

يتصل به بواسطة شبكة الاتصالات، أي بطريق اعتراض لهذا النظام، على انه يلاحظ أن اعتراض اتصال هذا النظام من أجل نقل المعلومات الموجودة به يمكن أن يتم دون الحاجة إلى الدخول إلى شبكة محلية، كما في حالة التقاط الإشارات التي يحدثها جهاز إلكتروني دون الحاجة إلى الدخول مباشرة داخل الشبكة التي تحمل الرسالة (قوة، 2005، ص 343).

وتتمثل هذه المصلحة - حماية مواقع التجارة الالكترونية - في ضرورة عدم المساس بها وان يتم التعامل بالبيانات الخاصة بهذه المواقع بشكل مشروع، والنص على تجريم الاعتداء عليها بأي سلوك إجرامي (بن يونس، 2004، ص 186)، وهو ما جرمه المشرع الجزائري في قانون حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، حيث شعر المشرع الجزائري بخطورة هذه الجرائم الواقعة على المواقع الالكترونية، فسن التشريعات التي تنص على تجريمها، وهو ما فعله المشرع الجزائري حينما نص على ذلك من خلال المواد (394 مكرر حتى 394 مكرر 7) من قانون العقوبات الجزائري الذي ينص صراحة على تجريم الدخول غير المشروع أو البقاء في داخل نظام لمعالجة البيانات والمعلومات بما في ذلك أنظمة معالجة مواقع التجارة الالكترونية، حيث نص المشرع الجزائري في المادة 394 مكرر من قانون العقوبات على عقوبة كل من يدخل أو يبقى عن طريق الغش بكل أو بجزء من نظام معالجة البيانات آليا أو يحاول ذلك بالسجن من 03 أشهر إلى 01 سنة، وغرامة من 50000 إلى 200000 دج، بينما يعاقب بالسجن من 06 أشهر إلى 02 سنة وغرامة تقدر من 50000 إلى 300000 دج في حالة ما إذا احدث إلغاء أو تعديل في البيانات الموجودة في نظام معالجة البيانات، أما القانون 07/18 المتعلق بحماية المعطيات ذات الطابع الشخصي فقد نصت بعض موادها على تجريم العديد من صور الانتهاك على البيانات ذات الطابع الشخصي والتي يمكن إسقاطها على السلوكات المجرمة الواقعة على المواقع الالكترونية كالمعالجة الغير القانونية للمعطيات ذات الطابع الشخصي واستعمال الأساليب الغير المشروعة للجمع الآلي للمعطيات ذات الطابع الشخصي (قشقوش، دون سنة، ص 18). ومن المعلوم قانونا أن جريمة الدخول غير المصرح به إلى المواقع الالكترونية التي تقوم عليها التجارة الالكترونية بشكل خاص هي من قبيل الجرائم العمدية التي تتطلب لقيامها الركن المعنوي بالقصد العام من علم وإرادة، ومع ذلك هناك بعض التشريعات القانونية تطلب قصدا خاصا بجانب القصد العام لقيام جريمة الدخول غير المصرح به إلى نظام الحاسب الآلي وتشدد العقوبة بناء عليه، ومن هذه التشريعات التشريع الاسترالي والذي يشدد العقوبة متى ارتكب فعل الدخول غير المصرح به إلى نظام الحاسب الآلي بنية الأضرار بالغير، وفي الدنمارك تم تشديد العقوبة متى ارتكب فعل الدخول بنية الإحاطة بمعلومات تتعلق بالأسرار المتعلقة بعمل إحدى الشركات، وفي البرتغال تعاقب المادة 07 من القانون الصادر عام 1991 بشأن الجرائم المعلوماتية كل من يقوم على نحو

غير مصرح به بالدخول إلى أنظمة أو شبكات المعلومات بنية الحصول له أو للغير على ربح أو فائدة غير مشروعة، وتشدّد العقوبة متى كان هذا الربح أو هذه الفائدة مرتفعين بصورة كبيرة نسبياً (شمس الدين، 2006، ص 61). ومن الجرائم الواقعة على المواقع الإلكترونية الخاصة بالتجارة الإلكترونية أيضاً جريمة إتلاف وتدمير المواقع الإلكترونية، وتعتبر هذه الجريمة من أخطر الجرائم الإلكترونية وأكثرها انتشاراً على شبكة الانترنت، ويقصد بهذه الجريمة محو المعلومات أو البيانات أو البرامج كلية أو تدميرها الكترونياً أو تشويه المعلومات والبرامج على نحو فيه إتلاف مما يجعلها غير صالحة للاستعمال، وتقع جريمة الإتلاف المعلوماتي لنظم المعلوماتية عن طريق شبكة الانترنت وذلك بالاعتداء على الوظائف الطبيعية للحاسب الآلي أو عن طريق التعدي على البرامج والبيانات المخزنة والمتبادلة عن طريق شبكة الانترنت أو التلاعب بالبيانات وإتلاف المعلومات المخزنة بالحواسيب بمحوها أو تعديلها أو تغيير نتائجها أو بالتشويش على النظام المعلوماتي وإعاقة سير عمل النظام المعلوماتي، مما يجعلها غير صالحة للاستعمال (فشقوش، دون سنة، ص 571).

ويتخذ فعل الإتلاف المكون للركن المادي لجريمة الإتلاف العمدي لنظم المعلوماتية إحدى صورتين : صورة الإتلاف الكلي للبرامج والبيانات والمعلومات الخاصة بالنظم المعلوماتية ويتمثل في محوها كلياً أو تدميرها الكترونياً، وصورة الإتلاف الجزئي للبرامج والبيانات والمعلومات الخاصة بالنظم المعلوماتية ويتمثل في تشويهها على نحو فيه إتلاف بها يجعلها غير صالحة للاستعمال (رستم، 2009، ص 161). ويتحقق فعل الإتلاف للمواقع الإلكترونية بما فيها البيانات والمعلومات التي تقوم عليها التجارة الإلكترونية باستخدام الجاني إحدى وسائل ثلاث هي :

أ- الفيروسات: وهي عبارة عن برامج صغيرة يتم تسجيلها أو زراعتها على الأقراص أو الاسطوانات الخاصة بالحاسب وتظل خاملة لفترة محددة ثم تنشط فجأة في توقيت معين ليهدم البرامج أو المعلومات المخزنة أو يتلفها جزئياً وذلك بالحذف والتعديل، وتمتاز هذه الفيروسات بعدد من المميزات والخصائص منها القدرة على التخفي والاختراق والانتشار داخل أنظمة المعلومات وتدمير ما بها من برامج وبيانات ومعلومات (الشوا، 1992، ص 194).

ب- برامج الدودة : وهي عبارة عن برامج تستغل أي فجوات في نظم التشغيل لكي تنتقل من حاسب إلى آخر، أو من شبكة إلى أخرى عبر الوصلات التي تربط بينها، وتتكاثر أثناء عملها وأثناء انتقالها بإنتاج نسخ منها مثل البكتيريا، وتهدف هذه البرامج شغل أكبر حيز ممكن من سعة الشبكة ومن ثم العمل على تعطيل أو تخفيض كفاءتها، وأحياناً تتعدى هذا الهدف لتبدأ بعد بالتكاثر والانتشار في التخريب الفعلي للملفات والبرامج ونظم التشغيل (الملط، 2006، ص 518).

ت- القنابل المنطقية والزمنية : وهي عبارة عن برنامج أو جزء من برنامج يتخذ في لحظة محددة أو كل فترة زمنية منتظمة، ويتم وضعه في شبكة معلوماتية بهدف تحديد ظروف أو حالة فحوى النظام بغرض تسهيل تنفيذ عمل غير مشروع، وعلى ذلك يتضح أن القنابل المنطقية تظل ساكنة وبدون فاعلية وبالتالي غير مكتشفة لمدة قد تطول أو تقصر يحددها مؤشر موجود في برنامج القنبلة، والقنبلة الزمنية على نقيض القنبلة المنطقية في أنها تثير حدثا في لحظة زمنية محددة بالساعة واليوم والسنة ويتم إدخالها في برنامج وتنفذ في جزء من الثانية أو في بعض ثوان أو دقائق وفقا للتحديد اللازم (قشقوش، دون سنة، ص 588).

ومن الأمثلة الواقعة لوضع قنابل منطقية أو زمنية في الأنظمة المعلوماتية ما حدث في ولاية لوس انجلوس الأمريكية، حيث تمكن أحد العاملين بإدارة المياه والطاقة من وضع قنبلة منطقية في نظام الحاسب الآلي الخاص بها مما أدى إلى تخريب هذا النظام عدة مرات، وفي فرنسا قام محاسب " خبير في نظم المعلومات " وبدافع الانتقام على أثر فصله من المنشأة التي كان يعمل فيها، بوضع قنبلة زمنية في شبكة المعلومات الخاصة بالمنشأة وبحيث تنفجر بعد مضي 06 أشهر من رحيله عن المنشأة وترتب على ذلك إتلاف كافة البيانات المتعلقة بها (مطر، 2006، ص519).

3. حماية سرية وخصوصية تبادل البيانات الالكترونية :

حماية الخصوصية في مجال التجارة الالكترونية، يجب أن ترتبط بمنظومة متكاملة تحدد عناصر الحماية ونطاقها، ويمكن أن نتبين بوضوح الإطار القانوني الذي وضعه المشرع الجزائري، لتنظيم المعالجة الآلية، والغير آلية للمعطيات الشخصية بما يضمن حماية الحريات الأساسية للمواطن في إطار احترام الحياة الخاصة، بما أقره من مبادئ أساسية لحماية المعطيات، تتم وفق لأحكام القانون بما يضمن سرية وسلامة المعطيات، وهناك خمسة مبادئ أساسية تحكم ما يسمى بالممارسات العادلة والمقبولة والنزيهة في نطاق خصوصية المعلومات أو حماية البيانات الشخصية(رمضان، 2011، ص102) ، والتي نستشفها ضمنا من القانون 07/18 المتعلق بحماية المعطيات ذات الطابع الشخصي وهذه المبادئ هي :

- الإبلاغ أو الإخطار: ويراد بهذا المبدأ التزام مزود الخدمة أو القائم بالمعالجة الآلية للمعطيات ذات الطابع الشخصي بإخطار مستخدمي المواقع بما إذا كان مقتضيات الخدمة تنطوي على جمع بيانات شخصية وبيان إلى أي مدى يتم تجميع هذه البيانات وفيما تستخدم.

- الاختيار: ويوجب هذا المبدأ التزام الشركات صاحبة المواقع أو مزودي الخدمة بتوفير خيار للمستخدم بخصوص استخدام بياناته في غير الغرض المخصصة من اجله.

- الوصول للبيانات : ويوجب هذا المبدأ منح القدرة للمستخدمين للوصول إلى بياناتهم والتثبت من صحتها وتحديثها.

- الأمن والسرية : ويتعلق هذا المبدأ بالتزامات المواقع ومزودي الخدمة بمعايير الأمن المتعين تطبيقها لضمان سرية البيانات وسلامة الاستخدام وحظر الوصول غير المصرح به لهذه البيانات، وتتضمن أيضا كلمات السر والتشفير وغيرها من وسائل أمن المعلومات، وهو ما نص عليه القانون 05/18 المتعلق بالتجارة الالكترونية. وعرف المشرع الجزائري البيانات أو المعطيات ذات الطابع الشخصي في المادة 03 الفقرة 01 من القانون 07/18: " كل معلومة بغض النظر عن دعائها متعلقة بشخص معروف أو قابل للتعرف عليه والمشار إليه أدناه " الشخص المعني " بصفة مباشرة أو غير مباشرة، لاسيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"

والمهم في التجارة الالكترونية اعتمادها أساسا على تبادل البيانات الكترونيا على الشبكة المعلوماتية من خلال تجميع البيانات من عدة مواقع الكترونية لمعرفة طلبات الشراء وإرسال تلك البيانات على نطاق واسع وفتح أسواق لحركة التجارة، وقد تتعلق البيانات بالتعاقد أو شرط البيع أو الثمن، ومن هنا تأتي أهميتها في إتمام تعاملات التجارة الالكترونية (حجازي، 2007، ص281)، والسرية في البيانات الالكترونية هنا تعني حصر المعلومة المتعلقة بالتجارة الالكترونية وعدم حركتها إلا في نطاق عدد محدود من الأشخاص، بحيث أنه لا يمكن تصور جريمة انتهاك البيانات إذا انعدم هذا الحصر، ولهذا فان سرية البيانات في التجارة الالكترونية تتوقف على سهولة أو عدم سهولة اختراق نظامها للأمن والحماية، وكذلك حرية البيانات وإتاحتها وتداولها (قشقوش، دون سنة، ص21) ، وذلك كون معاملات التجارة الالكترونية تحوي بعض البيانات السرية الخاصة بالأفراد أو المؤسسات، فيستطيع بعض الأشخاص الدخول إلى أنظمة وأجهزة تخص أشخاصا آخرين والحصول على معلومات عن أسرار حياتهم الخاصة وأية معلومات أخرى تخصهم قد يرغب صاحبها في إضفاء طابع السرية عليها. كذلك المؤسسات والشركات التجارية، والتي غالبا ما تكون بياناتها ومعلوماتها التجارية والتنافسية تتسم بالسرية الكاملة، لذا هنا يتعاظم دور المصلحة المحمية في الاعتداء على التجارة الالكترونية باحترام الحق في الخصوصية في السرية في البيانات الالكترونية (كعبي، 2009، ص153).

4. حماية التوقيع الالكتروني:

أصبحت الحاجة ملحة لاستخدام التوقيع الالكتروني في عصر التكنولوجيا وتقنية المعلومات، فلم يعد التوقيع التقليدي كافيا في عالم تسوده المعاملات الالكترونية، التي حلت المستندات الالكترونية فيها محل المستندات الورقية التقليدية، فما أن بدأت تقنيات الاتصال تتطور يوما بعد يوم حتى أصبح من الضرورة العمل

على مواكبة هذا التطور من خلال تطوير الوسائل المستخدمة في المعاملات المختلفة، وقد جاء التوقيع الإلكتروني ليتناسب مع تقنيات الاتصال الحديثة، ليؤدي الدور الوظيفي نفسه الذي يقوم به التوقيع التقليدي مع اختلاف البيئة التي يتم فيها كل منهما، فالتوقيع الإلكتروني يتم بوسائل الكترونية في بيئة الكترونية تتم فيها المعاملات عن بعد بواسطة وسائل الاتصال الحديثة (الشوا، 1992، ص 192).

ونظرا لأهمية المعاملات الالكترونية في وقتنا المعاصر ولتنامي التجارة الالكترونية، وظهر مفاهيم جديدة مثل الحكومة الالكترونية، أجبرت الدول على غرار الجزائر لتبني تشريعات قانونية من أجل تنظيم التوقيع الإلكتروني، وهو ما جسده المشرع في قانون التجارة الالكترونية الجزائري 05/18، حيث أدرج التوقيع الإلكتروني في المعاملات التجارية الالكترونية بناء على القانون 04/15 المتعلق بالتوقيع والتصديق الإلكتروني، من خلال إضفاء حماية جنائية للتوقيع الإلكتروني، ولكن المشرع الجزائري لم يعرف التوقيع الإلكتروني، وإنما استعمل عبارة "يعتد بالتوقيع الإلكتروني" في الفقرة الثانية من المادة 327 المعدلة بموجب القانون 10/05 المؤرخ في 20 جوان 2005 المعدل والمتمم للقانون المدني، وربط شروط الاعتراف بالتوقيع الإلكتروني وفق الشروط الواردة في المادة 323 مكرر 1 من نفس القانون، وذلك متى تأكد من هوية الشخص الذي صدر منه، وأن يكون محفوظا وفق شروط الأمان والسلامة، ولم يحدد تلك الشروط، فيلاحظ على المشرع الجزائري أنه لم يخص التوقيع الإلكتروني بشروط منفردة واكتفى بربطها بالشروط المتعلقة بالكتابة الإلكترونية كأن التوقيع والكتابة لهما نفس الوظيفة (رمضان، 2011، ص 101).

وقبل صدور قانون التجارة الإلكترونية رقم 05/18، بالرجوع إلى أحكام القانون المدني بعد تعديله بموجب القانون رقم 10/05 الصادر بتاريخ 20 يونيو 2005 والذي تناول في باب الإثبات الحديث عن الكتابة الإلكترونية والتوقيع الإلكتروني، من خلال المواد من 323 مكرر إلى 327 منه.

غير أن المشرع الجزائري لم يواكب هذا التعديل، بقانون أو مرسوم يفسر كيفية العمل بهذه التقنية، وكيفية الحصول عليه، على خلاف معظم التشريعات العربية، ولعل أن هذا الفراغ القانوني تسبب في إضاعة الوقت للعمل بهذه التقنية، والمشرع بإدخاله للتعديلات الواردة في القانون المدني دون ضبط تقنيات العمل بها، أراد من ورائه التصدي إلى بعض الحالات التي عرضت على القضاء بشأن المعاملات الإلكترونية، فجاء القانون 04-15 المتعلق بالتوقيع والتوثيق الإلكترونيين، وقد اكتفى هذا القانون بالعقاب على المساس بأنظمة المعالجة الآلية للمعطيات، وبالتالي فالمصلحة التي يريد حمايتها المشرع من تجريمه للاعتداء على نظام المعالجة الآلية للمعطيات هي هذا النظام في حد ذاته، ويهدف التوقيع الإلكتروني إلى الحفاظ على مستويات الأمن والخصوصية للمتعاملين مع الشبكة من حيث الحفاظ على سرية المعلومات أو الرسائل المرسله وعدم قدرة أي شخص آخر على الاطلاع أو تعديل أو تحريف الرسالة الموقعة الكترونيا، كما انه يحدد هوية المرسل والمستقبل (قشقوش، دون سنة،

ص18)، ومن أشهر صور الاعتداءات التي تقع على التوقيع الإلكتروني والتي يجب حمايته جنائياً منها هي إتلاف التوقيع الإلكتروني والتزوير أو التقليد والدخول غير المشروع إلى أنظمة المعلوماتية أو قواعد البيانات الخاصة بالتوقيع الإلكتروني وسوف نوضح ذلك بشيء من التفصيل على النحو التالي :

4.1 حماية التوقيع الإلكتروني من جريمة الإتلاف :

عرف بعض الفقهاء الإتلاف بأنه: "التأثير في مادة الشيء على نحو يذهب أو يقلل من قيمته الاقتصادية عن طريق الإنقاص من كفاءته للاستعمال المعد له"، والركن المادي لجريمة إتلاف التوقيع الإلكتروني قد يتخذ صورة إجراء تعديلات غير مشروعة لبيانات أو معلومات التوقيع الإلكتروني أو تدميرها ، أو الإدخال غير المشروع للمعلومات داخل أنظمة الحاسبات الآلية (رمضان، 2011، ص102).

فالتعديل غير المشروع لمعلومات التوقيع الإلكتروني هو كل تغيير غير مشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الكمبيوتر، أما تدمير المعلومات المدرجة بالتوقيع الإلكتروني فقد أوصى التقرير الصادر عن المجلس الأوروبي بخصوص جرائم المعلوماتية بتجريم الأفعال التي تؤدي إلى تدمير المعلومات بمحوها أو إخفائها دون محوها بحيث لا يمكن الوصول إليها (الصلاحى، 2016، 203)، ويشترط لقيام هذه الجرائم على التوقيع الإلكتروني توافر القصد الجنائي العام حيث يكفي ثبوت علم الجاني بان التوقيع الإلكتروني الذي يعتدى عليه بالإتلاف هو ملك الغير، وأن فعله من شأنه أن ي تلف الشيء أو يجعله غير صالح للاستعمال أو ينقص من قيمته، ويجب أيضاً أن تنجّه إرادة الجاني إلى إحداث الإتلاف أو التخريب أو التعطيل وينتج عن فعله تحقق الضرر المترتب على جرمته مع علمه أن فعله غير شرعي (قشقوش، دون سنة، ص19).

وغالبا ما يتم الاعتداء على التوقيع الإلكتروني بواسطة الفيروسات التي تصيب الجهاز الآلي وهي في الغالب متعددة ومتنوعة ويمكن أن نقسمها إلى الآتي:

أ- فيروس محدود الانتشار: وهو يصيب نوعا معينا من الأنظمة، ويتميز عن سابقه بالبطء في الانتشار وصعوبة اكتشافه.

ب- فيروس عام الانتشار: وهو يصيب أي برنامج أو ملف داخل الكمبيوتر.

ت- فيروس عام الهدف: يمتاز بسهولة إعداده واتساع مدى تدميره والغالبية العظمى من الفيروسات تندرج تحت هذا النوع .

ث- فيروس محدود الهدف: وهذا النوع من الفيروسات يقوم بتغيير الهدف من عمل البرنامج دوت تعطيله. وفي سبيل حماية التوقيع الإلكتروني من الفيروسات هناك برمجيات ضد الفيروسات يمكن تركيبها على جهاز الحاسب الآلي لتقوم بعمل نسخ للقرص الصلب وذلك في كل مرة يتم تشغيل الجهاز أو بطريقة منتظمة كل فترة زمنية محددة، ومن تلك البرمجيات أيضا الجدران النارية الحديثة، وهي تقوم باستخدام

أسلوب فلترة وتصفية البيانات الواردة وتعمل على إنشاء الشبكات الافتراضية الخاصة لرقابة محتوى البيانات والوقاية من الفيروسات (الصلاحى، 2016، ص205).

ومن ناحية أخرى فان هناك وسائل أخرى لإتلاف التوقيع الالكتروني بوسائل أخرى غير الفيروسات مثل محو البيانات عن طريق تعريض الاسطوانات أو الأقراص الممغنطة المسجلة عليها لقوى مغناطيسية أو قطع التيار أثناء معالجة البيانات أو وضع شريحة أو دائرة مطبوعة في غير مكانها الصحيح.

2.4. حماية التوقيع الالكتروني من جريمة التزوير :

ترجع الحكمة من تجريم التزوير على التوقيع الالكتروني إلى حماية الثقة التي تنبعث منه وما يؤديه هذا التوقيع من دور في المعاملات التجارية الالكترونية، وبالتالي فان وقوع التزوير على التوقيع الالكتروني يزعزع هذه الثقة ويؤدي إلى المساس بحقوق الأفراد، بحيث يعتبر التزوير في المستندات المعترف بها في نظام معلوماتي من أخطر صور الغش في نطاق المعلوماتية نظرا لخطورة الدور الذي يقوم به الحاسب في الوقت الحاضر (الجنيبي، 2006، ص31).

وقد عرف التزوير المعلوماتي بأنه: "أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريقة الطابعة أو كانت مرسومة عن طريق الراسم ويستوي في المحرر المعلوماتي أن يكون مدونا باللغة العربية أو لغة أخرى لها دلالتها، كذلك يتم في مخرجات غير ورقية، شرط أن تكون محفوظة على دعامة وشرط أن يكون المحرر المعلوماتي ذا اثر في إثبات حق أو اثر قانوني معين. ويقصد بتغيير الحقيقة إظهار المستند في غير الحالة الحقيقية التي ينبغي أن يكون عليها، وينطبق ذلك على المستندات المعترف بها في نظام معلوماتي، ويقوم الركن المادي في جريمة تزوير التوقيع الالكتروني على تغيير الحقيقة على مستند معالج الكترونيا أو معترف بها في ظل نظام معلوماتي بإحدى طرق التزوير المبنية في القانون وتغيير الحقيقة في المستند هو جوهر التزوير وبدونه لا تقوم الجريمة، ولا بد أن يترتب على تغيير الحقيقة تحقق الأضرار بالغير حيث يعتبر الضرر عنصرا من عناصر الركن المادي في جريمة تزوير المستندات (قشقوش، دون سنة، ص21).

ولما كانت جرائم التزوير من الجرائم العمدية التي يتطلب الركن المعنوي فيها توافر القصد الجنائي العام بالإضافة إلى توافر القصد الجنائي الخاص، فهي من الجرائم العمدية التي لا تتوقف فيها العقوبة على تحقيق نتيجة معينة، لذلك لا بد أن يعلم الجاني أنه يغير الحقيقة في مستند الكتروني، ومن شأن فعله أن يترتب ضررا حالا أو محتملا، وكذلك يجب أن تتجه إرادة الجاني إلى ارتكاب فعل تغيير الحقيقة في المستند، وبالإضافة إلى ذلك لا بد أن تتجه نية الجاني إلى استعمال المستند المزور فيما زور من أجله لأن الجاني لا يرغب في التزوير في حد ذاته وإنما يستهدف من ذلك استعمال المستند المزور (قنديل، 2006، ص67)، ولا عبرة في الباعث على

ارتكاب الجريمة فيستوي أن يكون الباعث هو تحقيق مصلحة للغير أم دفع ضرر أو الإضرار بالغير أو الإثراء غير المشروع.

3.4. جريمة اختراق أنظمة التوقيع الالكتروني :

قد تتعرض كثير من الأنظمة المعلوماتية للتوقيع الالكتروني إلى الاختراق بواسطة أشخاص غير مصرح لهم بالدخول إليها، والاختراق هذا قد عرفته المادة 01 من القانون العربي النموذجي الموحد في شأن مكافحة جرائم إساءة استعمال أنظمة تقنية المعلومات بأنه : "الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات وذلك عن طريق انتهاك الإجراءات الأمنية " (الصلاحى، 2016، ص213).

والمقتضى المادة 394 مكرر من قانون العقوبات عاقب المشرع على الدخول والبقاء عن طريق الغش في كل جزء من منظومة المعالجة الآلية للمعطيات أو حاول ذلك، وذلك بالحبس من 3 أشهر إلى سنة وغرامة من 50.000 دج إلى 100.000 دج، وضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا تم تخريبها تكون العقوبة الحبس من 6 أشهر إلى سنتين وغرامة من 50.000 دج إلى 150.000 دج، أما المادة 394 مكرر 1 عاقبت على كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو زال أو عدل بطريق الغش المعطيات التي يتضمنها وقد عاقبت المادة 394 مكرر 2 على :

- أ- كل تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مرسله عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم.
- ب- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها في إحدى الجرائم المنصوص عليها في هذا القسم.

وأمام هذا القصور النسبي لنصوص القانون في مجال المعلوماتية، وجب على المشرع تحيين نصوص قانون العقوبات بما يتوافق مع القانون المدني، إذ أن نصوص الملكية الفكرية ونظام المعالجة الآلية لم يتحدث عن الانتهاكات التي يمكن أن تقع على التوقيع الالكتروني والمحركات الالكترونية كوسيلة للإثبات، وفي انتظار ذلك، نحاول من خلال بحثنا هذا المقارنة بين نصوص التزوير في المحركات التقليدية والتزوير في المحركات الالكترونية.

إن التشكيك في مصداقية المحركات في الإثبات لا تكون إلا بالطعن فيها بالتزوير، وإذا كان قانون العقوبات قد تحدث عن جرائم التزوير في المحركات التقليدية عرفية كانت أو رسمية، فما مدى اتساع هذه النصوص لتشمل الحديث عن الالكترونية منها، وقد انقسم الفقهاء في هذا الطرح؛ فذهب رأي إلى أنه من الشروط الأولية لقيام جريمة التزوير أن تتم على محرر مكتوب وهو ما لا ينطبق على معطيات النظام المعلوماتي قبل أن نأخذ شكل المحرر أو المستند الالكتروني والتي تمثل أحد مستخرجات

الحاسب الآلي (الشوابكة، 2004، ص233)، وبالتالي لا يمكن تصور التزوير إلا في المحررات الالكترونية المستخرجة من الحاسب الآلي، وعليه يكون مشمولاً بالنص الجنائي، أما الدعامات والأشرطة الممغنطة فتفتقر إلى صفة المحرر، وبالتالي فإن النصوص لا تشملها.

في حين يرى جانب آخر إلى إمكانية تصور اتساع نصوص التزويد في المحررات التقليدية لتشمل الالكترونية منها، مستندين في ذلك إلى عدة أدلة أهمها أن كثير من التشريعات عرفت التزوير أنه تغيير الحقيقة بأي وسيلة كانت سواء كان ذلك في محرر أو دعامة أو سند طالما أن هذه الدعامة ذات أثر في إنشاء حق أو لها شأن في إحداث نتائج معينة، وقد ذهب هذا الرأي إلى المساواة بين المستند الورقي والمستند الإلكتروني، وقرروا أن سجلات الحاسب الآلي ومخرجاته، وما يسجل في ذاكرته والأسطوانات والشرائط الممغنطة تعتبر من قبيل المستندات. وفي هذا الإطار نجد المشرع الفرنسي، ومنذ تعديله لقانون العقوبات سنة 1992 والذي دخل حيز التطبيق سنة 1994، نص على أن التزوير يكون بأي وسيلة مهما كانت في محرر أو أي سند للتعبير عن الرأي والذي يكون أو من الممكن أن يكون له أثر في إنشاء دليل على حق أو فعل تكون له نتائج قانونية، ولذا جاء النص الفرنسي مستوعباً للمحررات الالكترونية بالنص على لفظ أي سند أو دعامة أو بأي وسيلة مثل الشرائط الممغنطة والمسجلة (الشوابكة، 2004، ص233).

وإذا كانت النصوص الفرنسية تستوعب المحررات الالكترونية فإن النصوص الجزائرية في هذا الشأن ما تزال قاصرة وأن القانون رقم 04/15 بالتوقيع والتصديق الإلكترونيين يحتاج إلى تعديل خاص بمقتضى نصوص خاصة تشمل جميع حالات الاعتداء عليه والجزاء المقررة لذلك، مسايروا في ذلك التشريعات المقارنة.

5. حماية المستهلك الإلكتروني من الغش والخداع التجاري

حماية المستهلك الإلكتروني من الغش والتحايل مصلحة مهمة يحميها القانون، وهي حق للمستهلك الذي يستخدم التجارة الالكترونية في إتمام معاملاته التجارية والحياتية العادية، وتكمن أهمية توفير الحماية الجنائية للمستهلك الإلكتروني لأنه الطرف الضعيف في التعاقد، بينما المورد أو العون الاقتصادي في مركز القوة في العقد التجاري، وأيضاً لأنه في المعاملات الالكترونية يكون التعاقد عن بعد ولا يكون المنتج محل التعاقد بين يدي المستهلك.

فالمستهلك الإلكتروني هو ذلك الشخص الذي يبرم العقود الالكترونية المختلفة من شراء وإيجار وقرض وانتفاع وغيرها من أجل توفير كل ما يحتاجه من سلع وخدمات لإشباع حاجاته الشخصية أو العائلية دون أن يقصد من ذلك إعادة تسويقها ودون أن تتوافر له الخبرة الفنية لمعالجة هذه الأشياء وإصلاحها، وعرف المجلس الأوروبي المستهلك بأنه: "كل شخص طبيعي أو معنوي تباع له أشياء أو تؤدي له خدمات لاستخدامه الخاص".

فالمستهلك في نطاق تعاملات التجارة الالكترونية هو نفسه المستهلك في عملية التعاقد التقليدية ولكنه فقط يتعامل عبر وسيلة الكترونية، وهذا يعني أن للمستهلك هنا كافة حقوق المستهلك التقليدي مع إضافة خصوصية الوسيلة المستخدمة في التعامل ووضع قواعد خاصة بحماية المستهلك في العقود التي تبرم عبر الانترنت خاصة كون الخداع يعد من الآفات الاجتماعية المعاصرة التي تستفحل مختلف مجالات الحياة، ومن أجل التصدي لهذه الآفة الماسة بأمن وسلامة المستهلك فإن المشرع نظم هذه الجريمة تنظيمًا مزدوجًا وذلك من خلال المادة 68 من القانون رقم 03/09 المتعلق بحماية المستهلك وقمع الغش، وقبلها المادة 429 من قانون العقوبات، والواردة في الباب الرابع من الكتاب الثالث تحت عنوان "الغش في بيع السلع و التديليس في المواد الغذائية و الطبية " (كريم، 2012، ص12).

مع الإشارة أن المشرع الجزائري على غرار المشرع الفرنسي لم يعرف جريمة الخداع وإنما اكتفى بتبيان نطاقها و عقوبتها، وتدخل الفقه من خلال اجتهاداته لسد هذا الفراغ التشريعي وإعطاء مفهوم للخداع على أنه: "القيام بأعمال من شأنها إظهار الشيء على غير حقيقته أو إباسه مظهرًا يخالف ما هو عليه في الواقع" وبالتالي فالخداع هو كل تصرف من شأنه إيقاع المتعاقد في الغلط حول البضاعة أو الخدمة، وكقاعدة عامة اعتبر المشرع أن جنحة الخداع قائمة بغض النظر عن الوسائل المستعملة في الخداع إذ لم يشمل الوسائل بالتنظيم، وحسنا فعل المشرع باعتبار أن جرائم الإستهلاك من الجرائم المتطورة التي تكشف في كل يوم عن وجه جديد مختلف عن سابقه، غير أنه باستقراء المادتين 429 من قانون العقوبات و المادة 68 من قانون حماية المستهلك السابقتين، فإن المشرع من خلال نص المادة 429 استعمل عبارة "...يخدع أو يحاول أن يخدع المتعاقد..." في حين أنه في المادة 68 استعمل عبارة "... يخدع أو يحاول أن يخدع المستهلك بأية وسيلة أو طريقة كانت..."، وبالتالي فقد أضاف المشرع عبارة بأية وسيلة أو طريقة كانت، مما يفيد أن نص المادة 68 من قانون الحماية و القمع جاء أكثر واقعية وتوسعا ليدخل في نطاقه الواسع طرق الخداع التقليدية أو الالكترونية (بودالي، 2009، ص15).

6. الخاتمة:

إن الجريمة في نطاق التجارة الالكترونية تضر بأطراف عديدة وتصيب مصلحة كل منهم سواء أكان البائع أم المشتري وكذلك المنتج والمستهلك، وهو الأمر الذي حاولت كل التشريعات القانونية ذات الصلة بالتجارة الالكترونية بما فيها القانون النموذجي للأمم المتحدة التنبيه إليه وهو أن المساس بالمصلحة في نطاق التجارة الالكترونية يتحقق من خلال الاعتداء على كل ما يتعلق بالأنشطة التجارية، ولذلك قامت التشريعات الجنائية المختلفة بحماية المصالح الأساسية في التعاملات التجارية الالكترونية، وهو ما جاء به القانون 05/18 المتعلق بالتجارة الالكترونية الجزائرية، حيث وضع حماية جزائية للجرائم الواقعة على التجارة الالكترونية بصفة

عامة، وعلى المستهلك الإلكتروني بصفة خاصة، من خلال حماية بيانات المستهلك الإلكتروني، أو حمايته من الخداع والغش التجاريين، أو حماية الموقع التجاري الإلكتروني من خلال النصوص العقابية التي تجرم جميع أنواع السلوكات الماسة بهذه المواقع التجارية، وكذلك حماية العقد الإلكتروني الذي يتعرض للعديد من الصور الإجرامية كالتهريب والاستعمال الغير المشروع، ولهذا نقترح جملة من التوصيات أهمها:

- العمل على وضع اتفاقيات ثنائية ودولية من أجل مكافحة اجرام التجارة الالكترونية خاصة في مجال التعاون الدولي للحفاظ على المصالح المحمية جزائيا في التعاملات التجارية الالكترونية.
- ضرورة تعديل القانون 04/15 المتعلق بالتوقيع والتصديق الإلكترونيين خاصة في الجانب الجزائي وتجريم السلوكات الأخرى الماسة بالتوقيع الإلكتروني والتي نجدها في قانون العقوبات القانون 07/18 المتعلق بحماية المعطيات ذات الطابع الشخصي.
- ضرورة التأكيد في القوانين الخاصة على منح التوقيع الإلكتروني الحجية التي يتمتع بها التوقيع التقليدي.
- تعديل قانون التجارة الالكترونية 05/18 على اساس عادات واعراف التجارة الالكترونية الدولية.
- النص على عقوبة حجب المواقع الالكترونية بالنسبة للمورد الإلكتروني الاجنبي في حال ارتكابه لجرائم التجارة الالكترونية واعلامه في اجراءات الصلح أنه سيتعرض لحجب الموقع الإلكتروني في الاقليم الجزائري، كونه طريقة فعالة لمكافحة هذه الجرائم.

6. قائمة المراجع:

- أحمد خليفة الملط، الجرائم المعلوماتية، الطبعة 02، دار الفكر الجامعي، الإسكندرية، مصر، 2006.
- احمد عاصم احمد عجيلة، الحماية الجنائية للمحركات الالكترونية، رسالة دكتوراه في القانون، جامعة القاهرة، مصر، 2013 .
- أشرف توفيق شمس الدين، الحماية الجنائية للمستند الإلكتروني، دراسة مقارنة، ط1، دون دار نشر، 2006.
- أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني، دون طبعة، دار النهضة العربية، القاهرة، مصر، 2011،
- أيمن رمضان محمد أحمد، الحماية الجنائية للتوقيع الإلكتروني-دراسة مقارنة، دون طبعة، دار النهضة العربية، القاهرة، مصر، 2011.

- خالد ممدوح ابراهيم، الحماية الجنائية للتوقيع الالكتروني، مجلة الفكر الشرطي، المجلد 23، العدد 88، سنة 2014.
- سعيد السيد قنديل، التوقيع الالكتروني، الطبعة 01، دار الجامعة الجديدة، مصر، 2006.
- عبد الفتاح بيومي حجازي، التجارة الالكترونية وحمايتها القانونية، الكتاب الثاني، الطبعة 01، دار الكتب القانونية، مصر، 2007.
- عمر محمد أبو بكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، الأحكام الموضوعية والجوانب الإجرائية، دار النهضة العربية، القاهرة، مصر، 2004.
- كريم زينب، حماية المستهلك جنائيا من مخاطر الغش و التحايل التجاري الالكتروني، مداخلة في الملتقى الوطني الخامس حول أثر التحولات الاقتصادية على تعديل قانون حماية المستهلك، كلية الحقوق، جامعة حسيبة بن بوعللي، شلف، 6، 5 ديسمبر 2012.
- محمد أمين أحمد الشوابكة، جرائم الحاسوب والانترنت، الطبعة 01، دار الثقافة، الأردن، 2004.
- محمد بودالي، شرح جرائم الغش في بيع السلع و التدليس في المواد الغذائية و الطبية- دراسة مقارنة، ديوان المطبوعات الجامعية، الجزائر، 2006 .
- محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، الطبعة 01، دار النهضة العربية، القاهرة، 1992.
- محمد عبيد الكعبي، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2009.
- مفيد عبد الجليل الصلاحي، الحماية الجنائية للتجارة الالكترونية، الطبعة 01، دار النهضة العربية، القاهرة، مصر، 2016.
- منير محمد الجنبهي وممدوح محمد الجنبهي، تزوير التوقيع الإلكتروني، دار الفكر الجامعي، الإسكندرية، 2006.
- ناثلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصادية، الطبعة 01، منشورات الحلبي الحقوقية، بيروت، 2005 .
- هدى حامد قشقوش، الحماية الجنائية للتجارة الالكترونية عبر الانترنت، الطبعة 01، دار النهضة العربية، القاهرة، مصر، دون سنة.
- هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنيات المعلومات، الطبعة 01، مكتبة الآلات الحديثة، دون بلد، 2009.

الأمر 156/66، المؤرخ في 8 يونيو 1966، المتضمن قانون العقوبات الجزائري، المعدل والمتمم.
القانون رقم 03/09، المتعلق بحماية المستهلك و قمع الغش، الصادر بتاريخ 25 فبراير 2009 .
القانون 04/15، المؤرخ في 01 فبراير 2015، المتعلق بالتوقيع والتصديق الإلكترونيين.
القانون 07/18، المؤرخ في 10 يونيو 2018، المتضمن حماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي.