

الحماية القانونية للمستهلكين عبر الإنترنت



الثقة والأمان في التجارة الإلكترونية:

عندما يدخل مستخدم ما على موقع يباشر أنشطة التجارة الإلكترونية على الخط، يبدأ بطلب السلعة أو المنتج أو الخدمة، وبالنسبة للقائم على موقع التجارة الإلكترونية - فإنّ المهم لديه التوثق من صحة الطلب، ويتطلب ذلك الوثوق من أنّ مَن يخاطبه هو فعلاً من دون اسمه أو عنوان بريده الإلكتروني، أو غير ذلك من معلومات تطلبها مواقع التجارة الإلكترونية، فكيف يمكنه ذلك، خاصة في ظل تنامي إجراءات الاختراق وإساءة استخدام أسماء الغير في أنشطة إجرامية على الويب؟ ومن جانب آخر هناك إشكالية يعاني منها المستخدم، ما الذي يضمن للمستخدم أنّ ما وصله من معلومات جاءت من هذا الموقع؟ وما الذي يضمن له أيضاً أنّ هذا الموقع حقيقي وموجود على الشبكة؟ إنّ حل هذه المعضلة استتبع إيجاد حلول تقنية؛ كوسائل التعريف الشخصية عبر كلمات السر والأرقام السرية، أو وسيلة التشفير عبر ما عرف بوسيلة المفتاح العام والمفتاح الخاص، ووسائل التعريف البيولوجية للمستخدم؛ كبصمات الأصابع المنقولة رقمياً أو تناظرياً، وسمات الصوت أو حدقة العين أو غيرها، وهي وسائل الهدف منها ضمان تأكيد الاتصال وإثبات صحة صدور المعلومة عن النظام التقني الصادرة عنه. لكن لكلّ منها ثغراته الأمنية، وتعد بالعموم غير كافية، وهذا ما استتبع اللجوء لفكرة الشخص الوسيط في العلاقة، وهو جهة تؤكد صحة التعامل على الخط، وهي شركات ناشطة في ميدان خدمات التقنية تقدم شهادات تتضمن تأكيداً أنّ الطلب أو الجواب قد صدر عن الموقع المعني، وتحدد تاريخ ووقت صدور الطلب أو الجواب، وحتى تضمن شخصية المخاطب توفرت تقنيات التعرف على الشخص؛ بدءاً بكلمة السر وانتهاءً بالبصمة الصوتية، أضف إلى ذلك تقنيات التشفير التي يزداد الجدول حول مشروعيتها؛ لاسيّما في ظل أثرها المانع والمقيد لحرية تدفق البيانات وانسيابها ومساسها في كثير من الحالات بالخصوصية، لاسيّما عند إجراء عملية التوثيق، وتفتيش النظم التي تتطلب الاطلاع على معلومات مخزنة في النظام، خارجة عن العلاقة العقدية المعنية.

وقد أثير في ميدان العلاقات القانونية للتجارة الإلكترونية مسألة مسؤولية الشخص الثالث، وتحديدًا مزودي خدمات الإنترنت، وجهات استضافة المواقع أو الجهات المناط بها تسجيل الموقع، هل تسأل عن أنشطة المواقع التي تحتال عبر الإيهام بوجود نشاط تجاري إلكتروني، سواء أكان غير قائم أو غير محقق لما يعلن عنه؟ وتتجه التشريعات نحو إبراء الشخص الثالث من هذه المسؤوليات؛ لكونه غريباً عن العلاقة العقدية، ولتوفر وسائل الأمن التقنية، والشركات الموثوق بها المشار إليها التي تعطي أطراف العلاقة قدرة على ضمان حقوقهم بعيداً عن الشركات المزودة للخدمات التقنية، لكن ذلك استدعى نصوصاً قانونية صريحة؛ نظراً لما تطاله القواعد العامة أحياناً في ميدان المسؤولية التقصيرية،

التي تمتد إلى المتسبب في الخطأ لا إلى المباشر فقط.

أما عن مسؤولية الشركات المتعاقد معها لضمان إثبات شخصية الطرف الآخر وصحة الاتصال - فإنّ الاتجاه الغالب يذهب إلى مسؤوليتها عند إيرادها معلومات خاطئة أو غير دقيقة؛ باعتبار أنّ التعاقد انبنى على هذه المعلومات، وسنداً لوجود التزام قانوني عليها، في الغالب يكون لقاء ما يدفعه الزبون لها؛ لضمان صحة تعاملاته التجارية على الخط.

وسائل الأمن الإلكتروني:

استطاعت الشركات التقنية أن توفر وسائل ومعايير فاعلة في حقل أمن الشبكة، إلا أنّها ليست آمنة بالقدر الكافي. وليس معنى هذا أنّ هذا الرأي ضمن حقل واتجاهات إقامة العائق أمام استخدامها، أو عدم التشجيع على ذلك، ولكنّه رأي يستند إلى ما يظهر في الواقع العملي من أنشطة اختراق لا تلاقي حلاً قانونية رادعة، وإذا كان العالم قد اتّجه منذ منتصف الثمانينيات إلى إقرار قواعد لتجريم أنشطة إساءة استخدام الكمبيوتر والشبكات - فإنّ الحركة التشريعية في هذا الميدان لا تزال ضيقة ومتعثرة، وقد دفعت التجارة الإلكترونية وأهميتها المتزايدة إلى وجوب الوقوف أمام أهمية التدابير التشريعية لحماية نظم المعلومات، ومن هنا لم يكن كافياً اعتماد الحماية التقنية فقط؛ فحماية أنشطة التجارة الإلكترونية، وتحديدًا أنشطة الوفاء بالثمن والدفع عبر الخط ونقل المال والمعلومات المالية وسائر أنشطة البنوك الإلكترونية - تستلزم حلول أمن تقنية مميزة ومتجددة وشاملة، وفي الحقيقة أنّ مجرمي التقنية والشبكات يسبقون حمايتها بخطوة دائماً، الأمر الذي يستلزم حماية قانونية وتدخلًا تشريعيًا؛ لتجريم كافة صور جرائم الكمبيوتر وتحديدًا اختراق النظم دون تصريح، والتقاط المعلومات وإعادة استخدامها للحصول على منفعة، كما في إعادة بناء البطاقات المالية وأنشطة الغش المعلوماتي أو احتيال الكمبيوتر وأنشطة التزوير في عالم التقنية.

وهناك مطالب قانونية وأخلاقية تفرض وجوب احترام سرية البيانات الخاصة بالعملاء بوصفهم مستهلكين واحترام حقهم في الخصوصية، وذلك يستلزم عدم نشر أو بث أي بيانات خاصة بشخصية المستهلكين، أو كشف الغطاء عن حياتهم الشخصية أو بياناتهم المالية والمصرفية، كما أنّه لا يجوز الاحتفاظ بهذه البيانات إلا لفترة محدودة تتعلق بالنشاط التجاري أو العملية التجارية التي يقوم بها العميل، من ناحية أخرى فإنّه لا يجوز لأية جهة التعامل في هذه المعطيات إلا بعد الحصول على موافقة كتابية من صاحب الشأن.

إنّ حماية البيانات المتصلة بالحياة الشخصية داخل في معرض حماية قواعد المعلومات، لكنه عاد ليحتل مكاناً بارزاً لدى بحث أسرار العلاقات التجارية وخطورة تفتيش النظم وملاحقة المعلومات على حقّ الخصوصية؛ إذ تشيع وسائل تقنية استلزمها التجارة الإلكترونية، تتيح تعقب الاتصالات ومعرفة معلومات تفصيلية عن مستخدم الشبكة، وإذا كان التناقض قائماً بين موجبات الحماية الأمنية وبين موجبات حماية الخصوصية - فإنّ التوفيق بينها جاء عبر القواعد التشريعية التي وضعت المعايير، وأجازت أنشطة لا تخرق الخصوصية، وفي الوقت ذاته تحمي نشاط التجارة الإلكترونية. وتتنوع صور الحماية الجنائية للمستهلك الإلكتروني كما يلي:

أوّلًا: الحماية الجنائية ضد الغش التجاري والصناعي:

الغش التجاري أو الصناعي يعرف بأنّه: (كلّ فعل من شأنه أن يغيّر من طبيعة أو خواص المواد أو فائدتها التي دخل عليها عمل الفاعل، ولا تهم الوسيلة التي لجأ إليها الفاعل في سبيل تحقيق غايته، فقد يتم الغش بإحلال مواد أقل قيمة مكان أخرى أعلى منها، يراد إدخال الغش عليها، أو بإنقاص بعض المواد أو إضافة مواد أخرى عليها تزيد من كميتها وتقلل من مفعولها، وغير هذا من الصور التي لا تدخل تحت حصر، ويتفنن الغشاشون في استنباطها؛ بغرض الحصول على أرباح طائلة وغير مشروعة.

وقد يقع الغش بفعل الإنسان - كما في حالة الإضافة أو الخلط - وقد يكون الغش لأسباب خارجة عن إرادة الإنسان، كما هو الشأن في حال فساد السلعة نتيجة لطبيعتها، أو جعلها غير صالحة للاستخدام كاللحوم والبيض، وعلى ذلك فجرime الغش لها ركنان؛ أحدهما مادي والآخر معنوي. ويتحقق الركن المادي

بأي فعل من الأفعال الآتية:

- 1- الغش أو الشروع فيه، وكذلك بالفساد الذي يطرأ على المادة.
- 2- عرض أو طرح المواد المغشوشة أو الفاسدة للبيع.
- 3- الطرح للبيع أو العرض لذات الغرض، أو بيع المواد المغشوشة أو الفاسدة.
- 4- التحريض على استعمال هذه المواد في الغش.

وهذا الركن المادي يتوافر حتى في حالة البيع الإلكتروني عن طريق العرض أو الطرح للبيع من خلال شبكة الإنترنت، بالنسبة للسلع الفاسدة أو المغشوشة التي تصل إلى المستهلك لاحقاً، كما يتحقق الركن المعنوي في هذه الجريمة بتوافر نية الغش؛ أي: انصراف إرادة الفاعل إلى تحقيق الغش مع العلم بتوافر أركانه في الواقع. ويتعين توافر نية الغش وقت وقوع الفعل؛ لأن جريمة الغش من الجرائم العمدية الوقتية، أما فيما يتعلق بالطرح أو العرض للبيع فيعد الفاعل مرتكباً للجريمة من وقت العلم بالغش والفساد، لكننا لا نتفق مع ذلك فالمستقر فقهاً وقضاً أن البائع المحترف - لاسيما في عقد البيع الإلكتروني - من الصعب جهله بحقيقة العيوب في بضاعته أو المنتج الخاص به.

ثانياً: جريمة الاحتيال في عقود التجارة الإلكترونية:

قد يلجأ المنتج أو الموزع عامداً؛ ولأجل الترويج لمنتجاته إلى الدعاية المضللة التي قد تنطوي في بعض الأحيان على مغالطات علمية؛ بهدف تحقيق أقصى قدر ممكن من الربح على حساب المستهلك الذي تخدعه هذه الدعاية.

وتنتشر في هذه الوقائع وغيرها، جرائم الاحتيال أو النصب وإمكانية وقوعها بطريق الإنترنت، حيث تتمثل الطرق الاحتيالية فيها في صورة الدعاية المضللة لمزايا السلعة والفوائد المرجوة من ورائها؛ للاستيلاء على نقود المستهلك.

ولهذا نجد أن قانون الاستهلاك الفرنسي الصادر عام 1993 تضمن نصوصاً تحارب الغش والمخادعة؛ وذلك لحماية المستهلك، وتضم النصوص طائفتين من الأفعال؛ الأولى: تنظمها المواد 1-121 وما بعدها، وهي تعاقب كل من يقوم بالدعاية الكاذبة أو تلك التي من شأنها الإيقاع في الغلط، وأما الطائفة الثانية: فهي منظمة بالمواد 1-213 وما بعدها، وهي تعاقب على الغش والتدليس. وفي كلا الطائفتين فإن المخادع أو مرتكب الغش أو المدلس - يعاقب بالحبس والغرامة أو إحدى هاتين العقوبتين، ويمكن أن يضاف إليهما عقوبات تكميلية أخرى.

ثالثاً: الصور الأخرى للحماية الجنائية للمستهلك في عقود التجارة الإلكترونية:

حسب القواعد العامة في قانون عقوبات وتشريعات التجارة الإلكترونية، يمكن القول إن هذه النصوص تحقق - قدر الإمكان - حماية متكاملة في عقود البيع من خلال الإنترنت للمستهلك، وبصفة خاصة في الأحوال الآتية:

- 1- تجريم الدخول غير المشروع إلى مواقع التجارة الإلكترونية، والحصول على بيانات المستهلك.
- 2- حظر التعامل في البيانات الشخصية أو الاسمية للمستهلك دون إذنه.

- 3- الحماية الجنائية للمستهلك في مواجهة مقدمي خدمة الإنترنت في عقد البيع الإلكتروني.
- 4- حماية وسائل الدفع الإلكترونية من التعدي عليها في مجال التجارة الإلكترونية.
- 5- معاقبة الجاني عند إتلاف بيانات المستهلك بتلك العقوبة المقررة للإتلاف العمدي للمنقولات، بعد التسليم للبيانات والمعلومات بأزّها منقولة وأزّها من الأموال:
- 1- انتهاك سرية وخصوصية بيانات المستهلك.
- 2- جريمة التصريح - عمداً - ببيانات خاطئة للمستهلك توقعه في غلط في عقد التجارة الإلكترونية.
- 3- جرائم التعدي على التواقيع الإلكترونية أو البيانات المشفرة للمستهلك.
- 4- التعدي على بيانات البطاقة الائتمانية التي تخص المستهلك.
- 5- تزوير المحررات الإلكترونية التي يكون المستهلك طرفاً فيها.

الإنترنت والقواعد القانونية:

الإنترنت عالم بلا حدود، يستطيع فيه المستخدم الدخول إلى الشبكة من أي مكان في العالم، كما أن بنيته التحتية المتمثلة بأنظمة الكمبيوتر الخادمة (Servers) والاتصالات - قد تمتد إلى العديد من الدول، كما أن مكان ممارسة العمل الفعلي للشخص قد لا يكون هو المكان الذي تقدم من خلاله خدمة إطلاق الموقع على الشبكة.

ويتزايد الاعتماد على الإنترنت ظهر العديد من التحديات التنظيمية والقانونية، مصدرها عدم وجود جهة تحكم الإنترنت؛ ذلك أن الإنترنت مملوك لكل الأفراد والمؤسسات، وفي الوقت ذاته ليس مملوكاً لأحد، ويجمع الباحثون أن تحديد الموقف من مسائل القانون المتصلة بالإنترنت يجب أن ينطلق ابتداءً من فهم الطبيعة التقنية لهذه الوسيلة المعقدة من وسائط تكنولوجيا المعلومات، وبدون إدراك هذه الطبيعة يتخلف الشرط الموضوعي لتقييم مدى ملائمة القواعد القانونية القائمة ومدى الحاجة إلى إيجاد قوانين خاصة تنظم مسائل عصر المعلومات بما فيه الإنترنت، ولأنّ المقام لا يتسع للوقوف على مدى تأثير التقنية والإنترنت على القواعد القانونية وما أنشأته من فروع متخصصة كما في حقل جرائم الكمبيوتر والإنترنت أو حقل الخصوصية أو البنوك الإلكترونية أو المواصفات القياسية والتنظيم الإداري للخدمات التقنية. ▶

المصدر: كتاب التسويق الإلكتروني في العالم العربي