الحماية الجنائية للتوقيع الإلكتروني
وفق القانون الجزائري رقم 15_04

رحال بومدين: طالب دكتوراه
الدكتورة: سعداني نورة، أستاذة محاضرة قسم - أ-
قسم الحقوق، كلية الحقوق والعلوم السياسية،
جامعة طاهري محمد، بشار، الجزائر

الملخص

يعتبر التوقيع الإلكتروني أهم وسيلة مناسبة للمعاملات الإلكترونية والتجارة الإلكترونية خاصة، حيث يساهم في تثبيت المعاملات وخلق الثقة لدى الأطراف ويشجع على التعاقد إلكتروني مما يشجع في زيادة حجم تبادلات التجارة الإلكترونية.

ورغم الإيجابيات التي يقدمها التوقيع الالكتروني إلا أنه كان هدفا لعدة اعتداءات إضافة إلى الاعتداءات التي مست شهادة التصديق الإلكتروني المنشأ له، كما لم تسلم البيانات التي يتضمنها.

نستعرض في هذا المقال صور الاعتداءات التي تقع على التوقيع الإلكتروني وأيضا حماية البيانات الخاصة من هذه الاعتداءات.

الكلمات الدالة: الحماية الجنائية، التوقيع الإلكتروني، القانون رقم 15_04.

Résumé :

La signature électronique est considérée comme la plupart des moyens appropriés pour les transactions électroniques et e-commerce privé, ce qui contribue à l'installation des transactions et créer la

confiance celui qui a encouragé les parties à la lettre du contrat, ce qui encourage une augmentation du volume des échanges d'e-commerce

Malgré les avantages offerts par qui était la cible de plusieurs attaques touché signature électronique autonome et la certification électronique du certificat d'origine pour lui, n'a pas reconnu les données qu'il contient.

Dans cet article, nous passons en revue les photos des attaques qui se trouve sur la signature électronique et de protéger également les données privées de ces attaques.

Mots clés : protection pénale, la signature électronique, loi n ° 15_04.

مقدمة:

إن التطور الذي أحدثته تكنولوجيا المعلوماتية وإفرازاتها وتحول الأشخاص من التعاملات التقليدية إلى التعاملات الإلكترونية لما توفره من وقت وجهد ومال للمتعاملين بها، أدت إلى ظهور عقود لم تكن معروفة من قبل وهي العقود الإلكترونية كنتيجة محتومة للتعاملات الإلكترونية بصفة عامة، ومعاملات التجارة الإلكترونية بصفة خاصة، والتي أصبحت ميدانا للتفاوض وإبرام العقود وأحد إفرازات هذا التطور، فتنامت العلاقات والتبادلات بين مختلف الأشخاص عبر العالم وتشابكت وأضحت العقود الإلكترونية وسيلة لثبات هذه المعاملات، فتمحورت في شكل محررات إلكترونية تحمل التزامات وحقوق كل طرف، وكان لا بد من شيء يثبت هذه العلاقة ويؤكد انتماء محتواه إلى الأطراف التي صدرت منهم ويخلق ثقة بينهم، فكان التوقيع الإلكتروني الوسيلة التي تلائم هذا النوع من التعاملات ويحقق

حجية لهذه العقود، وبما أن هذا النوع من التوقيع عبارة عن معلومات إلكترونية تحدد البيانات الخاصة بهوية صاحبه من جهة، وأيضا وسيلة ضمان من التحريف في محتوى العقود الإلكترونية من جهة أخرى، ومن أجل هذا لم يسلم التوقيع الإلكتروني ولا البيانات المنشأة له من الاعتداءات فهو مثل البيانات والمعلومات الإلكترونية الأخرى.

وقد نص المشرع الجزائري على المحررات الالكترونية كوسيلة للإثبات بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها بمقتضى أحكام المادة 123 مكرر01 من القانون المدني [1] كما نص بعد ذلك على القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين من خلال القانون رقم 15-04،[2] غير أن التساؤل الذي يطرح يكمن في مدى استطاعة المشرع الجزائري أن يوفر الحماية القانونية للتوقيع الالكتروني سيما في الشق الجنائي؟

قصد الإجابة على هذا التساؤل سنتطرق إلى:

المطلب الأول: صور الاعتداءات على التوقيع الإلكتروني.

المطلب الثاني: حماية البيانات الخاصة.

المطلب الأول: صور الاعتداءات على التوقيع الإلكتروني

يعتبر التوقيع الالكتروني وسيلة لإثبات المعاملات الالكترونية حيث يحدد صاحبه وينسب إليه ما ورد في مضمون المحرر ويعطيها حجية في الإثبات ويحافظ على حقوق والتزامات أطراف معاملات التجارة الالكترونية، غير أنه ليس بمنأى عن الاعتداءات من عدة أطراف سواء من مانح هذا التوقيع أو من صاحبه أو الغير.

ولتحديد صور الاعتداء على التوقيع الالكتروني فإننا سوف نتعرض للتعريف بالتوقيع الإلكتروني (**الفرع الأول**)، ثم الجرائم اواقعة عليه (**الفرع الثاني**).

الفرع الأول: التعريف بالتوقيع الإلكتروني

قصد التعريف بالتوقيع الالكتروني ارتأينا التطرق لتعريفه أولا، فتحديد شروطه ثانيا.

أولا: تعريف التوقيع الالكتروني

عرفت المادة الثانية من قانون الأونسيترال النموذجي التوقيع الالكتروني بأنه: "يعني بيانات في شكل إلكتروني مدرجة في رسالة بيانات، أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات"[3].

وقد عرفته المادة الثانية من القانون رقم 15_04 على أنه: " بيانات في شكل إلكتروني[4]، مرفقة أو مرتبطة منطقيا ببيانات إلكترونية أخرى، تستعمل كوسيلة توثيق".

وقد عرفته المادة الأولى من القانون المصري رقم 115 لسنة 2004 المتعلق بتنظيم التوقيع الإلكتروني بأنه: " ما يضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، ويكون له طابع منفرد، يسمح بتحديد الشخص صاحب التوقيع، ويميزه عن غيره"[5].

ثانيا: الشروط الواجب توفرها في التوقيع الإلكتروني:

نصت المادة 2/327 من القانون المدني الجزائري على: "ويعتد بالتوقيع الإلكتروني وفق الشروط المذكورة في المادة 323 مكرر1".

وبالرجوع لنص المادة 323 مكرر1 من القانون المدني الجزائري نجدها تقضي بأنه: "يعتبر الإثبات بالكتابة في الشكل الإلكتروني كالإثبات بالكتابة على الورق، بشرط إمكانية التأكد من هوية الشخص الذي أصدرها وأن تكون معدة ومحفوظة في ظروف تضمن سلامتها".

ومن خلال هذين النصين يتضح أنه يجب توافر الشروط التالية في التوقيع الالكتروني:

i. **أن يحدد التوقيع الالكتروني هوية الشخص الموقع:** يعتبر التوقيع الإلكتروني علامة مميزة وخاصة بصاحبها، يعمل على التعريف عن هوية الموقع خصوصا في الشبكات المفتوحة بين الأشخاص الذين لا يعرف بعضهم البعض، عكس الشبكات المغلقة التي ينتسب إليها بطلب التسجيل وتدار وتراقب عادة من قبل هيئة تتحكم بها، حيث يتعارف مستخدمو الشبكة ويوقعون على اتفاقيات في إطار تنظيم علاقاتهم[6].

ولقد أصبح ارتباط هذا التوقيع بصاحبه معتمدا بالخصوص على التكنولوجيا اللازمة لتأمين المواقع، ومتابعة رقابية من جهات معتمدة لها القدرة على التوثق من شخصية أصحاب التوقيع[7] باستخدام مفاتيح شفرة يتم وضعها على المحررات الإلكترونية، ولذلك فإن نوع التكنولوجيا المستخدمة في إنشاء التوقيع الإلكتروني يؤثر على درجة الموثوقية التي يتمتع بها التوقيع الإلكتروني[8].

ويقصد به تعيين الشخص الذي ينسب إليه المحرر الإلكتروني، والذي يتحمل كل الإلتزامات الناشئة عنه، وتثبت له كل الحقوق التي يتضمنها المحرر[9].

ب- **أن يعبر التوقيع الالكتروني عن إرادة الموقع:** يجب أن يكون التوقع دالا على موافقة الموقع على ما يتضمنه المحرر الإلكتروني، واتجاه إرادته إلى الالتزام بمضمونه[10].

ج- **أن يكون التوقيع الالكتروني معد ومحفوظ في ظروف تضمن سلامته:** وقد نص المشرع الجزائري على عدة شروط لضمان سلامة التوقيع الإلكتروني من خلال المادة 11 من القانون رقم 15_04 التي تنص على أن: " الآلية المؤمنة لإنشاء التوقيع الإلكتروني هي آلية إنشاء توقيع إلكتروني تتوافر فيها المتطلبات الآتية:

1_ يجب أن تضمن بواسطة الوسائل التقنية والإجراءات المناسبة، على الأقل، ما يأتي:

أ- ألا يمكن عمليا مصادفة البيانات المستخدمة لإنشاء التوقيع الإلكتروني إلا مرة واحدة، وأن يتم ضمان سريتها بكل الوسائل التقنية المتوفرة وقت الاعتماد،

ب- ألا يمكن إيجاد البيانات المستعملة لإنشاء التوقيع الإلكتروني عن طريق الاستنساخ وأن يكون هذا التوقيع محميا من أي تزوير عن طريق الوسائل التقنية المتوفرة وقت الاعتماد،

ج- أن تكون البيانات المستعملة لإنشاء التوقيع الإلكتروني محمية بصفة موثوقة من طرف الموقع الشرعي من أي استعمال من قبل الآخرين.

2_ يجب أن لا تعدل البيانات محل التوقيع وأن لا تمنع أن تعرض هذه البيانات على الموقع قبل عملية التوقيع".

الفرع الثاني: الجرائم الواقعة على التوقيع الإلكتروني

لقد تعددت صور الاعتداءات على التوقيع الالكتروني وهي كالتالي:

أولا: جريمة تزوير وتقليد التوقيع الإلكتروني:

تنص المادة 1/214 من قانون العقوبات الجزائري على أنه: "يعاقب بالسجن المؤبد كل قاض أو موظف أو قائم بوظيفة عمومية ارتكب تزويرا في المحررات العمومية أو الرسمية أثناء تأدية وظيفته:

1) إما بوضع توقيعات مزورة ".

و نصت المادة 1/216 من نفس القانون على أنه: "يعاقب بالسجن المؤقت من عشر (10) سنوات إلى عشرين سنة وبغرامة من 1.000.000 دج إلى 2.000.000 دج، كل شخص، عدا من عينتهم المادة 215، ارتكب تزويرا في محررات رسمية أو عمومية.

1) إما بتقليد أو بتزييف الكتابة أو التوقيع".

ومن خلال نص المادتين يتضح أن **الركن المادي** لهذه الجريمة هو تقليد وتزوير التوقيع، بحيث يتخذ الجاني سلوك إيجابي وهو الاعتداء على التوقيع بتقليده وإيجاد صورة طبق الأصل له أو تزويره جزئيا أو كليا[11].

ويهدف المشرع من وراء المعاقبة على تزوير التوقيع أو المحرر الإلكتروني (شهادة التصديق)، حماية الثقة المفترضة في هذا التوقيع أو هذا المحرر من العدوان الواقع عليهما باعتبارهما وسيلتي إعلان عن الإرادة،[12].

جدير بالإشارة أن الشهادات المصادق عليها من مؤدي خدمات التصديق الإلكتروني تعتبر وسلية لاعتماد التوقيعات الإلكترونية، كما يترتب على الشهادات آثارا قانونية تتمثل في إنشاء الالتزامات وإثبات الحقوق بالنسبة لطرفي العقد في التجارة الإلكترونية في حالة اعتماد التوقيع الإلكتروني بينهما، ولذلك فإن تزوير أو تقليد شهادات التصديق على التوقيع الإلكتروني يعادل في خطورته تزوير أو تقليد التوقيع الإلكتروني ذاته[13].

أما الأستاذان "منير محمد الجنبهي" و"ممدوح محمد الجنبهي" ينفيان عملية تقليد التوقيع الإلكتروني، لأنه حسب رأيهما لا يمكن تقليده، ولكن يمكن استعماله دون علم ورضا صاحبه باعتباره يتم بواسطة منظومة الكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها، فيما يقران بإمكانية تزوير التوقيع التقليدي عن طريق التقليد، مما يعني أن التوقيع المقلد لا يمكن أن يكون بذات التوقيع الأصلي وبالتالي لا يمكن أن يكون متماثلا معه[14].

وتتم عملية تقليد أو تزوير التوقيع الإلكتروني، باستخدام برامج حاسوبية أو أنظمة معلوماتية مخصصة لذلك، على غرار البرامج والأنظمة المصممة لكسر الشفرة والوصول إلى الأرقام الخاصة بالتوقيع الإلكتروني، والقيام بنسخها، وإعادة نسخها بعد ذلك[15].

أما فيما يتعلق **بالركن المعنوي** فالأكيد أن هذه الجريمة تعتبر من الجرائم العمدية التي تستلزم توافر القصد الجنائي العام المتمثل في عنصريه العلم والإرادة، ويتحقق العلم بإدراك الجاني بفعل تغيير بيانات التوقيع الإلكتروني بذاته أو شهادات التصديق المنشأة له بالتقليد أوالتزوير، وهذا العلم مفترض فلا يدفع مسؤوليته عن ذلك بجهله، أضف إلى ذلك يجب أن تتجه إرادة الجاني للقيام بهذا الفعل المجرم قانونا، ولذلك فإن عدم علم الجاني أنه يغير الحقيقة في بيانات التوقيع الإلكتروني تجعله يتمتع بحماية قانونية لانتفاء القصد الجنائي لديه.

يضاف إلى القصد الجنائي العام القصد الجنائي الخاص حيث لا تقوم جريمة التزوير إلا بتوافر نية استعمال التوقيع المزور فيما زور من أجله[16].

مع التنويه أن استعمال التوقيع المزور يعتبر جريمة مستقلة عن جريمة التزوير، لأن جريمة التزوير تقوم وأن لم يستعمل الجاني هذا التوقيع المزور[17].

ثانيا: جريمة الإدلاء بقرارات كاذبة للحصول على شهادة تصديق إلكترونية موصوفة

تنص المادة 66 من قانون 15_04 على أنه: "يعاقب بالحبس من ثلاث (3) أشهر إلى ثلاث (3) سنوات وبغرامة من عشرين ألف دينار (20.000 دج)، إلى مائتي ألف دينار (200.000 دج) أو بإحدى هاتين العقوبتين فقط، كل من أدلى بإقرارات كاذبة للحصول على شهادة تصديق إلكترونية موصوفة"[18].

والمشرع عند نصه على هذه الجريمة، كان يهدف إلى إعطاء شهادة تصديق إلكترونية موصوفة، مصداقية عند طالبها، لأن مؤدي الخدمات لا يجمع إلا المعلومات الصحيحة والضرورية عنه، كما يهدف إلى خلق ثقة لدى الغير المتعامل مع صاحب هذه الشهادة مما يدفعه قدما إلى التعاقد معه خاصة في مجال التجارة الإلكترونية.

تقوم هذه الجريمة على على ركنيين هما:

أ. **الركن المادي:** يتحقق متى قام الجاني بالتصريح بمعطيات كاذبة، وهي البيانات الضرورية للحصول على شهادة تصديق إلكترونية موصوفة، إلى مؤدي خدمات التصديق الإلكتروني، وهو شخص الذي له ترخيص مزاولة هذه المهنة مثلما بينا سلفا.

ب. **الركن المعنوي:** إن فعل إعطاء إقرارات كاذبة للحصول على شهادة تصديق إلكترونية موصوفة يعتبر فعلا عمديا يتحدد من خلاله ماهية الركن المعنوي لهذه الجريمة، فلا يتصور إذن تحقق

الجريمة بصورة غير عمدية، فالإعطاء في حد ذاته يفيد معنى الإرادة والسعي والعلم معا[19].

والنص يعاقب على جريمة التصريح عمدا بمعطيات كاذبة، لأنه لا يعقل أن يحدث عن طريق الخطأ، وهذا وفق ما جاء في المادة بنصه على أنه " **كل من أدلى بإقرارات كاذبة** "، ولن يكون هناك خطأ في كذب بل يكون خطأ عند الإدلاء بمعطيات صحيحة وهذا ما بينته المادة 1/45 من هذا القانون[20].

وهذه الجريمة لا يشترط لقيامها قصد جنائي خاص أو نية خاصة يتعين توافرها لذى الجاني، ذلك أن مجرد قيامه بالإدلاء بمعطيات أو إقرارات كاذبة، تقوم الجريمة في حقه[21].

ثالثا: جريمة استخدام شهادة التصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها

تنص المادة 74 من قانون 15_04: " يعاقب بغرامة من ألفي دينار (2.000 دج)، إلى مائتي ألف دينار (200.000 دج) كل شخص يستعمل شهادته للتصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها".

ولقيام هذه الجريمة يجب توفر **الركن المادي** المتمثل في اتيان الجاني سلوك ايجابي، وهو استعمال شهادة التصديق الإلكتروني الموصوفة لغير الأغراض التى منحت من أجلها، ويقتضي هذا أن يكون الجاني طالب شهادة التصديق الإلكتروني أما شخص طبيعي أو معنوي[22].

ويستثنى مؤدي الخدمات من تحمل مسؤولية الضرر الناتج عن استخدام شهادة التصديق الإلكتروني الموصوفة لغير الأغراض التي منحت من أجلها وفق نص المادتين 56 و57 من قانون 15-04[23].

وتعتبر هذه الجريمة من الجرائم العمدية توجب توافر القصد الجنائي المتمثل في **الركن المعنوي**، حيث لا يقوم هذا الركن إلا بتوافر القصد الجنائي

العام في عنصريه العلم والإرادة، فيتحقق العلم عندما يعلم الجاني أنه يتجاوز الحدود المفروضة على استعمال شهادته أو الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل بها الشهادة[24] في غير الغرض الذي قدمت من أجله، وأيضا يكفي أن تتجه إرادته للقيام بهذا الفعل المكون للركن المادي لهذه الجريمة.

ولا يشترط توفر القصد الجنائي الخاص المتمثل في نية الإضرار بالغير لقيام هذه الجريمة لأنه بمجرد الانحراف في استعمال الشهادة لغير الغرض الذي منحت من أجله تقوم هذه الجريمة، وفي حالة حدوث ضرر للغير يتحمل المسؤولية صاحب الشهادة ويستثنى منها مؤدي خدمات التصديق الإلكتروني وفق المادتين 56 و57 من نفس قانون 15-04.

مع التنويه بأن العقوبة المفروضة على الشخص المعنوي تضاعف خمسة مرات عن الشخص الطبيعي[25]، كما أن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال[26].

المطلب الثاني: حماية البيانات الشخصية

تعتبر البيانات الشخصية قبل وبعد التطور التكنولوجي كتاب يدل على صاحبه ويستدل عن هويته، فلها قيمة عند صاحبه لا يرضى أن يتعامل بها أحد أو بتداوله دون رضاه، لكن بعد التطور أصبحت البيانات الشخصية تتدفق عبر شبكة المعلوماتية خارج حدود الدول بعد معالجتها إلكترونيا فزاد القلق حيال التهديدات التي تواجهها من الجمع وحالفظ والاستخدام غير المشروع لهذه البيانات الشخصية، مما استدعى تدخل التشريعات الدولية والوطنية بحماية هذه البيانات وتؤسس لها قواعد تحكمها وتنظيم الكيفية التي يتم بها جمع، وحفظ، ومعالجة البيانات الخاصة بالأشخاص.

ورغم هذا لم تسلم هذه البيانات من الاعتداءات الإجرامية عن طريق معالجتها بدون إذن أو الاعتداء على البيانات المعالجة بمختلف صور الاعتداء، وعلى هذا سنتطرق إلى مفهوم الخصوصية للبيانات المعلوماتية (الفرع أولا)، ثم إلى صور الاعتداءات على هذه البيانات (الفرع ثانيا).

الفرع الأول: تعريف الخصوصية المعلوماتية

هي تلك المعلومات التي تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الإسم والعنوان ورقم الهاتف وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلزم الالتصاق بكل شخص طبيعي معرف أو قابل للتعريف[27].

وقد عرف فويستن الخصوصية في المعلومات بأنها "حق الأفراد في تحديد متى وكيف وإلى أي مدى تصل المعلومات عنهم للآخرين"؛ كما عرفها ميلر بأنها:" قدرة الأفراد على التحكم بدورة المعلومات التي تتعلق بهم"[28].

الفرع الثاني: صور الاعتداءات على البيانات الشخصية

نتطرق من خلال هذا الفرع إلى جريمة افشاء سرية البيانات الإلكترونية أولا، و جريمة جمع البيانات الشخصية دون موافقه الصريحة من صاحبها ثانيا.

أولا: جريمة افشاء سرية البيانات الإلكترونية

إن علة تجريم إفشاء الإسرار يعود إلى أن المشرع أرد تأمين السير السليم للمهن والوظائف التي يمارسها الأمناء على الأسرار، حيث لا يستطيعون ممارسة مهنهم أو وظائفهم وتحقيق مصلحة عملية لعملهم أو مصلحة عامة إلا إذا عملوا بهذه الأسرار[29].

وقد نص المشرع في المادة 70 من القانون رقم 15_04 على أنه: " يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج)، أو بإحدى هاتين العقوبتين

فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 42 من هذا القانون".

ونص في المادة 42 من نفس القانون على أنه: " يجب على مؤدي خدمات التصديق الإلكتروني الحفاظ على سرية البيانات والمعلومات المتعلقة بشهادة التصديق الإلكتروني الممنوحة."

أما في المادة 73 من نفس القانون فقد نص على أنه: "يعاقب بالحبس من ثلاثة (3) أشهر إلى سنتين (2) وبغرامة من عشرين ألف دينار (20.000 دج) إلى مائتي ألف دينار (200.000 دج)، أو بإحدى هاتين العقوبتين فقط، كل شخص مكلف بالتدقيق يقوم بكشف معلومات سرية اطلع عليها أثناء قيامه بالتدقيق."[30].

ومن خلال نصوص المواد نستخلص **الركن المادي** لهذه الجريمة يتمثل في قيام مؤدي خدمات التصديق الإلكتروني، أو من له حق التدقيق في المعلومات حسب طبيعة عمله في إفشاء البيانات والمعلومات المتعلقة بشهادات التصديق الإلكتروني الممنوحة، والتي كان يجب عليه أن يحفظ سريتها وفق التزاماته التي على عاتقة حسب المادة 42 و المادة 73 المذكورتين أعلاه.

والإفشاء جوهره نقل المعلومات التي تعتبر نوع من السر الشخصي الذي لا يرغب صاحبه في إطلاع الغير عليه وإرادته في الاحتفاظ بهذا السر في حيز الكتمان[31].

وقد يقصد من فعل الإفشاء بيع هذه المعلومات، أو استعمالها في غرض غير مشروع كتهديد وابتزاز أصحابها أو الضغط عليهم للقيام بعمل أو الامتناع عن القيام به، وسواء صدر هذا الفعل ممن أفشى هذه المعلومات والبيانات أو

سلمت لشخص يهمه الأمر، بدافع الرشوة والحصول على المال حيث يستغلها هذا الأخير ضد صاحب الشأن[32].

ويستوى في فعل الإفشاء أن يكون شفاهة أو كتابة، فيكون شفاهة عن طريق التحدث، أما الكتابي فيتحقق بعدة صور منها تقديم معلومات على ورق أو على دعامة إلكترونية أو تمكين الغير من الإطلاع على المعلومات الظاهرة على شاشة الحاسب الآلي، ولا يشترط أن ينصب على المعلومات كافة بل قد يقتصر على البعض منها دون الآخر[33].

ويجب في هذه الجريمة توفر صفة خاصة في المتهم، حيث يتعين أن يرتكب هذه الجنحة من له رخصة إصدار شهادات التصديق الإلكتروني أو من له حق التدقيق الذي يعمل في الهيئة التي له حق تقديم الترخيص، ويترتب على ذلك أن الجريمة لا تقع ممن لا يعمل في الهيئة أو الجهة المرخص لها، لأن المتهم في هذه الجريمة قد أؤتمن على المعلومات أو البيانات بسبب وظيفته أو عمله[34].

أما بخصوص الركن المعنوي فجريمة إفشاء السر تعد جريمة عمدية تقتضي توافر القصد الجنائي العام المتمثل بعنصري العلم والإرادة، أي أن يكون الجاني عالما بأن المعلومات التي أفضى بها إلى الغير انتهاك لالتزاماته القانونية، وأن هذا الفعل يعاقب عليه القانون كما يعلم بأنه تعدي على حقوق صاحب المعلومات بإفشاء أسراره، كما يجب لهذه الجريمة أن تتجه إرادته إلى فعل الإفشاء ولا عبرة بالباعث الذي دفع الجاني إلى ارتكاب هذه الجريمة[35].

وفي ما يتعلق بالقصد الجنائي الخاص فنرى أن المشرع من خلال نص المادة 70 سالفة الذكر قد عاقب الجاني بمجرد مخالفته لنص المادة 42 أو المادة 73 من نفس القانون أي بمجرد إفشاء البيانات والمعلومات السرية،

دون أن يتطرق إلى النتيجة المرجوة من هذا الفعل، وبذلك تعتبر هذه الجريمة من الجرائم الشكلية، حيث تقوم بمجرد إتيان الفعل، سواء تحققت النتيجة أم لم تتحقق[36].

ثانيا: جريمة جمع البيانات الشخصية دون الموافقه الصريحة من صاحبها

نص المشرع الجزائري في المادة 71 من قانون رقم 15_04 على أنه: "يعاقب بالحبس من ستة (6) أشهر إلى ثلاث (3) سنوات، وبغرامة من مائتي ألف دينار (200.000 دج) إلى مليون دينار (1.000.000 دج) أو بإحدى هاتين العقوبتين فقط، كل مؤدي خدمات التصديق الإلكتروني أخل بأحكام المادة 43 من هذا القانون."

ونص في المادة 43 من قانون رقم 15_04 على أنه: "لا يمكن مؤدي خدمات التصديق الإلكتروني جمع البيانات الشخصية للمعني، إلا بعد الموافقة الصريحة.

ولا يمكن مؤدي خدمات التصديق الإلكتروني أن يجمع إلا البيانات الشخصية الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ولا يمكن استعمال هذه البيانات لأغراض أخرى"[37].

ومن خلال المادتين 43 و 71 من قانون العقوبات الجزائري، فإن **الركن المادي** لهذه الجريمة يتحقق بإتيان الجاني السلوك الإجرامي في الصورتين التاليتين:

- **الصورة الأولى:** جمع البيانات الشخصية للمعني دون موافقة صريحة من هذا الأخير، حيث يتمثل السلوك الإجرامي للجاني هنا بنشاط الإيجابي في جمع البيانات دون موافقة صاحب الشأن، وهنا يمكن أن يتصور في حالتين،

حالة قيام الجاني بفعل جمع البيانات دون علم صاحبها أو جمعها رغم رفض صاحب البيانات من جمعها وهذه الحالة أيضا تكون دون علم هذا الأخير.

والعلة في ضرورة الحصول على موافقة صاحب الشأن أن هذه البيانات وإن كانت ضرورية لإصدار شهادة التصديق الإلكتروني إلا أنها تمس خصوصية الشخص نفسه، وقد تمتد إلى حياته العائلية[38].

ولقد نص المشرع الفرنسي في المادة 226_18 من قانون العقوبات الفرنسي على حالة إجراء معالجة لمعلومات اسمية تتعلق بشخص طبيعي رغم معارضة هذا الشخص، متى كانت هذه المعارضة تقوم على أسباب مشروعة[39]؛ فنجد أن المشرع الفرنسي حصر فعل جمع البيانات الشخصية على الشخص الطبيعي فقط، أما بخصوص المشرع الجزائري وضع مصطلح " **شخص** " ويعني شخص طبيعي كما يعني شخص معنوي، وبذلك وسع في حماية كل بيانات الشخصية سواء كانت لشخص طبيعي أو معنوي، أما مصطلح "**دون موافقة صريحة**" تحتمل كلا الحالتين من جمع البيانات بدون علم صاحبها أو جمعها رغم رفض صاحب البيانات من جمعها.

كما استثنى المشرع جمع البيانات الضرورية لمنح وحفظ شهادة التصديق الإلكتروني، ونكون هنا أمام موافقة صاحب الشأن عندما يقدم طلب استصدار شهادة التصديق الإلكترونية وفق المادة 2/44 من قانون 15_04 سالفة الذكر.

- **الصورة الثانية:** استعمال البيانات الشخصية لأغراض أخرى، فيكون سلوك الجاني في هذه الصورة سلوكا ايجابيا، وهو استعمال البيانات الشخصية التي جمعها على أساس صفته كمقدم خدمات التصديق التي يتمتع بها في أغراض أخرى غير مسموح له بها، وهي جمعها لمنح وحفظ شهادة

التصديق الإلكتروني، وهذا الفعل قد يقع أيضا في حالة جمع البيانات دون موافقة صاحب الشأن مثل الصورة الأولى[40].

وتعتبر هذه الجريمة من الجرائم السلوكية التي لا تحتاج إلى تحقق نتيجة معينة فيكفي ارتكاب السلوك الإجرامي لقيام الركن المادي له[41].

وعلى ما سبق فلن نكون أمام جريمة تامة إلا بتوافر **الركن المعنوي**، وتعتبر هذا الجريمة من الجرائم العمدية حيث تتمثل في القصد الجنائي العام، فيتحقق القصد الجنائي العام بعلم الجاني بصفة البيانات الشخصية وأن يعلم أنه لا يمكن جمعها الى بموافقة صاحبها وهذا بطلب وفي حال كان الطلب يجمع فقط المعلومات الضرورية، وأيضا بأن فعله يخالف الواجباته كمقدم خدمات تصديق إلكتروني، كما تتجه إرادته في الصورة الأولى في جمع البيانات دون موافقة صاحبه، كذلك في الصورة الثانية إلى استعمال هذه البيانات في غرض غير التي منحة له، سواء كانت البيانات المجمعة عن طريق مشرع كالبيانات الضرورية لمنح شهادة التصديق الإلكتروني أو جمع بيانات عن طريق غير مشروع واستخدمها لغرض أخر.

أما القصد الجنائي الخاص متمثل في نية إضرار بصاحب البيانات فلا يشترط توافره لقيام هذه الجريمة لأنها كما بينا سلفا أنه من الجرائم السلوكية، أما الضرر سواء تحقق أو لم يتحقق لا ينفي متابعة الجاني على هذه الجريمة.

الخاتمة

نخلص في الأخير إلى أن تزايد التطور التكنولوجي واتساع التعامل في البيئة الإلكترونية زاد من حدة المخاطر التي قد تمس بالتوقيع الإلكتروني والبيانات الشخصية، لا سيما إذا استغلت لغايات وأغراض مختلفة، وقد تنبهت الدول المتقدمة مبكرا إلى هذه المخاطر وسجلت غياب النصوص التي

تجرم الأفعال الواقعة على التوقيع الإلكتروني والبيانات الشخصية، إلا أنها اختلفت في موضوع النص على حمايتها جنائيا فمنها من أصدر قانونا مستقلا عاقب بمقتضاه على هذه الجرائم، ومنهم من ذهب إلى إدخال تعديلات على النصوص التشريعية من بينها التشريع الفرنسي، أما المشرع الجزائري فقد خصص لها قانونا خاصا هو القانون رقم 15_04، ورغم الجهود التي يبذلها المشرع الجزائري لمواكبة هذا التطور ورصد له قوانين تنظمه وأخرى تعاقب على الأفعال المستحدثة، إلا أن هذه النصوص لا تكفي للحماية لوجود صور أخرى من الاعتداءات لم ينص عليها المشرع الجزائري، نذكر منها على سبيل المثال جريمة إعداد أو تصميم أو حيازة برنامج لإعداد توقيع إلكتروني، كذلك جريمة الدخول بسوء نية على قاعدة بيانات تتعلق بالتوقيع الإلكتروني، وأيضا في حماية البيانات الشخصية في حق العميل في الاعتراض على معالجة بياناته الشخصية، وعدم جواز معالجة البيانات متى ما سببت ضررا للأشخاص الذين جمعت عنهم البيانات أو تنال من حقوقهم أو من حرياتهم.

وعلى هذا يجب على التشريع الجزائري إعادة النظر في حماية التوقيع الالكتروني والبيانات الشخصية بتوسيع نطاقها من حيث تجريم الأفعال الأخرى التي تلحق بهما.

الهوامش

1- أضيفت المادة بموجب القانون رقم 05-10 المؤرخ في 20 يونيو 2005، يعدل ويتمم الأمر رقم 75- 58 المؤرخ في 26 سبتمبر 1975 والمتضمن القانون المدني، المعدل والمتمم، الجريدة الرسمية العدد رقم 44، الصادرة بتاريخ 26 يونيو 2005.

2- القانون 15-04 المؤرخ في الأول من فبراير 2015، يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، الجريدة الرسمية رقم العدد رقم 06، الصادرة بتاريخ 10 فبراير 2015.

3- المادة 2 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع 2001.

_ **تعني رسالة بيانات:** هي معلومات يتم إنشاؤها أو إرسالها أو استلامها أو تخزينها بوسائل إلكترونية أو ضوئية أو بوسائل مشابهة، بما في ذلك، على سبيل المثال لا الحصر، التبادل الإلكتروني للبيانات أو البريد الإلكتروني أو البرق أو التلكس أو النسخ البرقي.

_ **الموقع:** شخص طبيعي يحوز بيانات إنشاء التوقيع الإلكتروني ويتصرف لحسابه الخاص أو لحساب الشخص الطبيعي أو المعنوي الذي يمثله.

4- **بيانات الإلكترونية:** هي بيانات إنشاء التوقيع الإلكتروني، وتعني بيانات فريدة، مثل الرموز أو مفاتيح التشفير الخاصة، التي يستعملها الموقع لإنشاء التوقيع الإلكتروني.

_ **مفاتيح التشفير** نوعان، مفتاح التشفير الخاص، والمفتاح التشفير العمومي:

* **مفتاح التشفير الخاص:** هو عبارة عن سلسلة من الأعداد يحوزها حصريا الموقع فقط، وتستخدم لإنشاء التوقيع الإلكتروني، ويرتبط هذا المفتاح بمفتاح تشفير عمومي.

* **مفتاح التشفير العمومي:** هو عبارة عن سلسلة من الأعداد تكون موضوعة في متناول الجمهور بهدف تمكنهم من التحقق من الإمضاء الإلكتروني، وتدرج في شهادة التصديق الإلكتروني.

5- **ثروت عبد الحميد:** التوقيع الإلكتروني (ماهيته، مخاطره، وكيفية مواجهتها، مدى حجيته في الإثبات)، دار الجامعة الجديدة، الإسكندرية، 2007، ص47.

6- **أمين اعزان:** الحماية الجنائية للتجارة الإلكترونية، أطروحة لنيل درجة الدكتوراه، كلية الحقوق، جامعة عين شمس، بدون تاريخ، ص245.

7- المادة 12 من قانون رقم 15_04 بأنه: "يجب أن تكون آلية التحقيق من التوقيع الإلكتروني الموصوف موثوقة".

8- **براهمي حنان:** جريمة تزوير الوثيقة الرسمية الإدارية ذات الطبيعة المعلوماتية، أطروحة لنيل شهادة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر بسكرة، 2015/2014، ص155،154.

_ وقد نصت المادة 06 من قانون الأونسيترال النموذجي بشأن التوقيعات الإلكترونية مع دليل الاشتراع 2001 على:

1_ حيثما يشترط القانون وجود توقيع من شخص، يعد ذلك الاشتراط مستوفي بالنسبة إلى رسالة البيانات إذا استخدم توقيع إلكتروني يعول عليه بالقدر المناسب للغرض الذي أنشئت أو بلغت من أجله رسالة البيانات، في ضوء كل الظروف، بما في ذلك أي اتفاق ذي صلة.

2_ تطبيق الفقرة 1 سواء أكان الاشتراط المشار إليه فيها في شكل التزام أم كان القانون يكتفي بالنص على تبعات تترتب على عدم وجود توقيع.

3_ يعتبر التوقيع الإلكتروني قابلا للتعويل عليه لغرض الوفاء بالاشتراط المشار إليه في الفقرة 1 إذا:

(أ) كانت بيانات إنشاء التوقيع مرتبط، في السياق الذي تستخدم فيه، بالموقع دون أي شخص آخر،

(ب) كانت بيانات إنشاء التوقيع خاضعة، وقت التوقيع، لسيطرة الموقع دون أي شخص آخر،

(ج) كان أي تغيير في التوقيع الإلكتروني، يجرى بعد حدوث التوقيع، قابلا للاكتشاف،

(د) كان الغرض من اشتراط التوقيع قانونا هو تأكيد سلامة المعلومات التي يتعلق بها التوقيع وكان أي تغيير يجري في تلك المعلومات بعد وقت التوقيع قابلا للاكتشاف."

9- **ثروة عبد الحميد:** مرجع سابق، ص178.

10- **أمين اعزان:** مرجع سابق، ص252.

11- ويتم تزوير التوقيع الإلكتروني، بعدة صور نذكر منها:

_ **تزوير التوقيع البيومتري:** فإن تزويره يكون أسهل من غيره لضعف إجراءات الأمان فيه، لأنه يعتمد على الخواص والصفات الفيزيائية والطبيعية للإنسان، مثل بصمة العين، وبصمة الأصبع، أو بصمة معالم الوجه وغيرها، حيث يتم تخزين صورة دقيقة عن هذه الصفات أو الخواص في ذاكرة النظام في الكمبيوتر، وهذه الطريقة يسهل تزويرها بمهاجمة أو نسخها من قبل قراصنة الحاسب الآلي بعد فك تشفيرتها وستخدامها مرة آخرى.

_ التوقيع الذي يتم بالرقم السري: وأكثر تطبيقاتها بطاقات الصرف البنكي بأنواعه المختلفة، وتكون إما باستخدام بطاقات بنكية مزيفة جزئيا، أو مزيفة كليا، بطاقات مسروقة، أو بطاقات صحيحة صدرت بطريقة غير مشروعة.

_ **تزوير التوقيع الرقمي:** يتم بواسطة منظومة إلكترونية تتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها بحيث لا يمكن تقليدها وإنما يمكن استعمالها دون علم مالكها، ويكون هذا عندما يتم حصول الجاني على منظومة التوقيع الرقمي الخاصة بشخص آخر. **إبراهيم بن سطم بن خلف العنزي:** التوقيع الإلكتروني وحمايته الجنائية، رسالة لنيل درجة دكتوراه، جامعة نايف العربية للعلوم الأمنية، كلية الدراسات العليا، 2009، ص111،109.

12- **محمد الشهاوى:** شرح قانون التوقيع الإلكتروني رقم 15 لسنة 2004، الطبعة الأولى، دار النهضة العربية، القاهرة، 2010، ص194.

13- **حسين بن سعيد بن سيف الغافري:** الجرائم الواقعة على التجارة الإلكترونية، سلطنة عمان مسقط، 2006، ص18. www.minshawi.com

14- **براهمي حنان:** مرجع سابق، ص239.

15- **حسين بن سعيد بن سيف الغافري:** مرجع سابق، ص18. www.minshawi.com

_ ومن تطبيقات عملية تزوير التوقيع الإلكتروني ما حدث في الإمارات العربية المتحدة في 2006/10/22، وتتضمن وقائع الجريمة، أن المتهم (ب) عن طريق الصدفة علم أن زميله في سكن يحتفظ بالرقم السري الخاص ببطاقة السحب البنكي في هاتفه النقال، فقام

بالاحتيال عليه بطلب هاتفه الجوال بحجة رغبته بسماع بعض النغمات فدون الرقم السري دون علم زميله، ثم في ساعات متأخرة من الليل سرق محفظة نقود زميله وقام بأخذ بطاقة الصرف، واستخدمها في سحب مبلغ وقدره 1700 درهم ثم أعاد بطاقة إلى مكانها، ثم اكتشف المجني عليه (ر) حصول سرقة من رصيده فتقدم ببلاغ وبعد التحري وجه الجاني بما جاء في شريط التصوير الخاص بكاميرا الصراف البنكي والذي تضمن صورة المتهم وهو يقوم بسحب المال، وعلى هذا حكمت المحكمة الجنائية أول درجة في خورفكان بمعاقبة المتهم (ب) من الجنسية الآسيوية بالحبس لمدة ستة أشهر وإعادته إلى بلده، ثم عدل الحكم بثلاثة أشهر وإبعاد إلى بلده من محكمة الاستئناف، ومن الإتهامات التي أتهم بها، استعمال محرر المزور وهذا كان قبل صدور قانون الإتحادي رقم 2 لسنة 2006 الخاص بمكافحة جرائم تقنية المعلومات؛ **إبراهيم بن سطم بن خلف العنزي:** مرجع سابق، ص160_163.

16- **محمد الشهاوى:** مرجع سابق، ص215.

17- تنص المادة 217 من قانون العقوبات الجزائري على أنه: "في الحالات المشار إليها في هذا القسم يعاقب بالسجن من خمس إلى عشر سنوات كل من استعمل الورقة التي يعلم أنها مزورة".

18- ويقابل نص المادة 66 من قانون 15_04 النص المادة 45 من قانون التجارة التونسي على أن: "يعاقب كل من صرح عمدا بمعطيات خاطئة لمورد خدمات التوثيق الإلكتروني ولكافة الأطراف التي طلب منها أن تثق بإمضائه بالسجن لمدة تتراوح بين 6 أشهر وعامين وبغرامة تتراوح بين 1000، 10.000 دينار أو إحدى هاتين العقوبتين".

لكن لو قارنا بين المادتين نجد أن المشرع التونسي قد وسع في حماية، فعاقب كل من صرح عمدا بمعطيات لكافة الأطراف التي لها علاقة، لتشمل عملية التعاقد بين الأطراف أو إلى طرف ثالث كبنك أحد الأطراف، أما المشرع الجزائري ضيق على من أدلى فقط بمعطيات كاذبة على مؤدي خدمات التصديق الإلكتروني، مما يطرح تسأل في حالة إدلاء بمعطيات كاذبة على غير، نرى أن المشرع أكتف بالرجوع إلى القواعد العامة لنعاقب على هذا التصرف مثل جريمة النصب التي تقع بطرق احتيالية.

ويرى جانب من الفقه أن جريمة التصريح عمدا بمعطيات خاطئة تقوم في حق الجاني، متى أدلى بمعطيات خاطئة إلى مورد خدمات التوثيق الإلكتروني أو إلى أطراف عملية التعاقد خاصة فيما يتعلق بعملية التجارة الإلكترونية، أو إلى أي طرف آخر كبنك أحد الاطراف مثلا، **هدى حامد قشقوش:** الحماية الجنائية للتجارة الإلكترونية عبر الانترنت، دار النهضة العربية، 2000، ص45.

19- نفس المرجع.

20- تنص المادة 45 من القانون 15-04 على أنه: "يلغي مؤدي خدمات التصديق الإلكتروني شهادة التصدي الإلكترونية في الآجال المحددة في سياسة التصديق، بناء على طلب صاحب شهادة التصديق الإلكتروني الموصوفة الذي سبق تحديد هويته.

ويلغي مؤدي خدمات التصديق الإلكتروني أيضا شهادة التصديق الإلكتروني الموصوفة عندما يتبين:

1_ أنه قدم تم منحها بناء على معلومات خاطئة أو مزورة، أو إذا أصبحت المعلومات الواردة في شهادة التصديق الإلكترونية غير مطابقة، أو إذا تم انتهاك سرية بيانات إنشاء التوقيع".

21- **عبد الفتاح بيومي حجازي:** التجارة الإلكترونية في القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2006، ص70.

22- تنص المادة 2/44 من قانون 15_04 على أنه: "يجب على مؤدي خدمات التصديق الإلكتروني، قبل منح شهادة التصديق الإلكتروني، أن يتحقق من تكامل بيانات الإنشاء مع بيانات التحقق من التوقيع.

يمنح مؤدي خدمات التصديق الإلكتروني شهادة أو أكثر لكل شخص يقدم طلبا وذلك بعد التحقق من هويته، وعند الاقتضاء، التحقق من صفاته الخاصة.

وفيما يخص الأشخاص المعنوية، يحتفظ مؤدى الخدمات التصديق الإلكتروني بسجل يدون فيه هوية وصفة الممثل القانوني للشخص المعنوي المستعمل للتوقيع المتعلق

بشهادة التصديق الإلكتروني الموصوفة، بحيث يمكن تحديد هوية الشخص الطبيعي عند كل استعمال لهذا التوقيع الإلكتروني".

23- المادة 56 من قانون 15_04 على أنه: "يمكن مؤدي خدمات التصديق الإلكتروني أن يشير، في شهادة التصديق الإلكتروني الموصوفة، إلى الحد الأقصى لقيمة المعاملات التي يمكن أن تستعمل في حدودها هذه الشهادة، بشرط أن تكون هذه الإشارة واضحة ومفهومة من طرف الغير.

وفي هذه الحال لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن تجاوز ذلك الحد الأقصى".

_ المادة 57 من قانون 15_04 على أنه: "لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن عدم احترام صاحب شهادة التصديق الإلكتروني الموصوفة لشروط استعمال بيانات إنشاء التوقيع الإلكتروني".

24- المادة 55 من قانون 15_04 على أنه: "يمكن مؤدي خدمات التصديق الإلكتروني أن يشير، في شهادة التصديق الإلكتروني الموصوفة، إلى الحدود المفروضة على استعمالها، بشرط أن تكون هذه الإشارة واضحة ومفهومة من طرف الغير".

وفي هذه الحال لا يكون مؤدي خدمات التصديق الإلكتروني مسؤولا عن الضرر الناتج عن استعمال شهادة التصديق الإلكتروني الموصوفة، عند تجاوز الحدود المفروضة على استعمالها".

_ المادة 56 من قانون 15_04 سالفة الذكر.

25- المادة 75 من قانون 15_04 عاى أنه: "يعاقب الشخص المعنوي الذي ارتكب إحدى الجرائم المنصوص عليها في هذا الفصل بغرامة تعادل خمس (5) مرات الحد الأقصى للغرامة المنصوص عليها بالنسبة للشخص الطبيعي".

26- تنص المادة 51 مكرر من قانون العقوبات الجزائري على أنه: " باستثناء الدولة والجماعات المحلية والأشخاص المعنوية الخاضعة للقانون العام، يكون الشخص المعنوي مسؤولا جزائيا عن الجرائم التي ترتكب لحسابه من طرف أجهزته أو ممثليه الشرعيين عندما ينص القانون على ذلك.

إن المسؤولية الجزائية للشخص المعنوي لا تمنع مساءلة الشخص الطبيعي كفاعل أصلي أو كشريك في نفس الأفعال".

27- **راشد بن حمد البلوشي:** حماية البيانات الشخصية في قانون المعاملات الإلكترونية رقم 2008/69، مقدم إلى ندوة الجوانب القانونية للتعاملات الإلكترونية براعية هيئة تقنية المعلومات، سلطنة عمان، 2008، بدون رقم الصفحة.

28- **حسين بن سعيد الغافري:** الحماية القانونية للخصوصية المعلومات في ظل مشروع قانون المعاملات الإلكتروني العماني، مؤتمر أمن المعلومات والخصوصية في ظل قانون الانترنت من 2_4 يونيو 2008، القاهرة، 2008، بدون رقم الصفحة .

وفي 17 سبتمبر 1980 صدقت لجنة الوزراء التابعة لمجلس أوربا على اتفاقية خاصة بحماية الأشخاص في مواجهة مخاطر المعالجة الآلية للبيانات ذات الطبيعة الشخصية، وقد أصبحت سارية المفعول في أول أكتوبر 1985، وتضمنت عشرة مبادئ أساسية تدور حول كون البيانات صحيحة وكاملة ودقيقة ومستمدة بطرق مشروعة ومدة حفظها محددة زمنيا وعدم إفشائها أو استعمالها في غير الأغراض المخصصة لها وحق الشخص المعني في التعرف والإطلاع عليها وتصحيح البيانات ومحورها وإحاطة البيانات بسياج أمني وتحديد الأشخاص والجهات المرخص لها بالوصول والإطلاع على البيانات وإخضاعهم لقيد الالتزام بسر المهنة.

ثم نشرت مفوضية الجماعات الأوربية في يوليو 1990 مسودة "توجيه المجلس عن حماية الأفراد فيما يتعلق بمعالجة البيانات ذات الطبيعة الشخصية، وحرية انتقال كثل هذه البيانات" وسمية التوجيهة "المعالجة والتجهيز" وإضافة مبادئ أخرى منها أن المعلومات التي تتعلق بالشخص ليس فقط المعلومات النصية ولكن أيضا الصور الفوتوغرافية والصور المسموعة والمرئية والتسجيلات الصوتية لشخص معروف أو يمكن معرفته ولا يقتصر التوجيهة على الأحياء؛ **علاء عبد الباسط خلاف:** الحماية الجنائية للحاسب الإلكتروني والانترنت في ضوء (قانون العقوبات، قانون الإجراءات الجنائية، قانون حماية حقوق الملكية الفكرية، مع الإشارة لتصرفات النيابة وأحكام المحاكم الابتدائية ومحكمة

النقض)، الطبعة الثانية، معهد الكويت للدراسات القضائية والقانونية، الكويت، 2008_2009، ص125،124.

29- **مدحت محمد عبد العزيز إبراهيم:** الجرائم المعلوماتية الواقعة على النظام المعلوماتي (دراسة مقارنة)، الطبعة الأولى، دار النهضة العربية، القاهرة، 2015، ص131.

30- وتنص المادة 1/301 من قانون العقوبات الجزائري على أنه: " يعاقب بالحبس من شهر إلى ستة أشهر وبغرامة مالية من 500 إلى 5.000دج الأطباء والجراحين والصيادلة والقابلات وجميع الأشخاص المؤتمنين بحكم الواقع أو المهنة أو الوظيفة الدائمة أو المؤقتة على أسرار أدلى بها إليهم وأفشوها في غير الحالات التي يجب عليهم فيها القانون إفشاءها ويصرح لهم بذلك".

ويقابلها نص المادة 226_22 من قانون العقوبات الفرنسي التي تنص على أنه: " يعاقب بالحبس سنة وغرامة مائة ألف فرنك فرنسي كل شخص كان قد استقبل أو (تلقى) بمناسبة التسجيل أو التصنيف أو النقل أو أي إجراء آخر من إجراءات المعالجة الإلكترونية، بيانات اسمية من شأن إفشائها الإضرار باعتبار صاحب الشأن أو حرمة حياته الخاصة، وقام بنقلها إلى من لا حق له في العلم بها وإذا وقع هذا الإفشاء للبيانات الاسمية بطريق الإهمال تكون العقوبة هي الغرامة خمسين ألف فرنك فرنسي، ولا تسري الدعوى العمومية وفقا للفقرتين السابق الإشارة إليهما، إلا من خلال شكوى المجني عليه أو ممثله القانوني، أو من له صفة في ذلك".

_ التدقيق: هو التحقق من مدى المطابقة وفقا لمرجعية ما.

31- **عصام عبد الفتاح مطر:** التجارة الإلكترونية في التشريعات العربية والأجنبية، دار الجامعة الجديدة للنشر، الإسكندرية، 2009، ص333.

32- **عبد الفتاح بيومي حجازي:** مرجع سابق، ص140.

33- **دلخار صلاح بوتاني:** الحماية الجنائية الموضوعية للمعلوماتية (دراسة مقارنة)، الطبعة الأولى، دار الفكر الجامعي، الإسكندرية، 2016، ص286،287.

34- **محمد الشهاوى:** مرجع سابق، ص235.

_ ويشترط المشرع الفرنسي وفق نص المادة 226 _22 لقيام الركن المادي لجريمة الإفشاء توافر ثلاثة شروط:

1_ أن يكون من شأن فعل الإفشاء أن يضر بالمجني عليه، ولا يتوجب أن تكون مصادر هذه البيانات صحيحة لكي يتحقق الاعتداء فيستوي أن تكون صحيحة أو غير صحيحة في نظر القانون، ما دام أن إفشاء هذه البيانات يحقق هذا الاعتداء.

2_ أن يكون الإفشاء بدون رضاء المجني عليه صحاب العلاقة.

3_ أن يكون الإفشاء إلى شخص ليس له حق الاطلاع على هذه البيانات، **محمد أيمن الشوابكة:** جرائم الحاسوب والانترنت (الجريمة المعلوماتية)، الطبعة الأولى، دار الثقافة للنشر والتوزيع،عمان، 2007، ص102.

_ ولو قارنا بين المواد 42 و 70 و 73 من قانون 15_04 والمادة 226_ 22 من قانون العقوبات الفرنسي نجد أن المشرع الجزائري لم يشترط توافر الضرر لقيام هذه الجريمة، فمجرد قيام الجاني بفعل الإفشاء نكون أمام جريمة، عكس المشرع الفرنسي الذي اعتبر الضرر شرط لقيام الجريمة، أي متى انتفى الضرر رغم قيام الجاني بالإفشاء لا يتابع جنائيا.

35- ولقد جرم المشرع الفرنسي إفشاء البيانات سواء تم ذلك بقصد، أي مع توافر عنصري العلم والإرادة أم عن طريق الخطأ وذلك بالإهمال وقلة الاحتياط وفق المادة 43 من قانون العقوبات الفرنسي؛ **بن سعيد صبرينة:** حماية الحق في حرمة الحياة الخاصة في عهد التكنواوجيا "الإعلام والاتصال"، شهادة نيل درجة دكتوراه، كلية الحقوق والعلوم السياسية، جامعة الحاج لخضر، باتنة، 2014_2015، ص225.

36- يوجد استثناء على قاعدة عدم إفشاء السر المكون للجريمة بمجرد القيام بهذا الفعل، وهو ما جاء في المادة 10 من قانون 09_04 على أنه: "في 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 أدناه، تحت تصرف السلطات المذكورة.

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

37- ومن الحماية الدولية للبيانات الشخصية نجد أن دليل منظمة التعاون الاقتصادي والتنمية لسنة 1980 يعتبر مصدرا أساسيا للتشريعات الوطنية الداخلية، حيث يطبق على جميع البيانات المرتبطة بهوية الأفراد، وعلى كافة أنواع وسائل المعالجة الآلية للبيانات، ذلك أنه يتضمن المبادئ الأساسية التي أصبحت تعرف بمبادئ الخصوصية، وهي تمثل الحد الأدنى من المبادئ الواجب احترامها، وهي في الوقت نفسه تحكم عمليات المعالجة الآلية للبيانات الشخصية، ويمكن إجمال هذه المبادئ كالآتي:

أ_ تقييد كيفية جمع البيانات الاسمية مع فرض قيود على هذه العملية، بحيث يجب أن تحصل بطريقة قانونية وشرعية بعيدا عن الإكراه والخداع وبمعرفة الشخص المعني؛

ب_ تجميع البيانات الاسمية على أساس غرض محدد، ويجب أن يكون هذا الغرض ضروري مبني على أساس من الصحة والمشروعية؛

ج_ يجب تحديد المدة الزمنية لحفظ البيانات، حيث تمحى هذه البيانات بعد انتهاء هذه المدة؛

ت_ يجب أن لا يتم إفشاء البيانات الاسمية، ولا تكون متاحة لغير الأغراض المحددة للجمع والمعالجة، باستثناء الحالات التي يتوفر فيها رضاء صاحب البيانات أو الحالات التي يقرها القانون؛

د_ يجب اقتران الحماية القانونية للبيانات الاسمية بالحماية التقنية؛

هـ_ ضرورة وجود سياسة عامة تتمتع بالوضوح والانفتاح بشأن الاستعمالات المنصبة على البيانات الاسمية كالتعريف بجهات المعالجة وأماكن تواجدها؛

ي_ يجب أن يحظى الفرد بحق المعرفة فيما إذا كانت هناك بيانات شخصية تعود له لدى جهة المعالجة، وإعطاء الحق له في التوصل مع هذه الجهة إن وجدت بأسلوب ملائم وديمقراطي، وللفرد الحق كذلك في أن يتم إخطاره بسبب منع ممارسته لأي من الحقوق

المتقدمة مع حقه في رفض عدم قبول ممارسته لحقوقه المشار إليها وحقه في أن تشطب تلك البيانات إذا تبين صحة إنكاره،

_ تكون جهة المعالجة مسؤولة عن تطبيق هذه المبادئ المتقدمة وضمان تنفيذها". **بن سعيد صبرينة:** مرجع سابق، ص219،220.

38- **راشد بن حمد البلوشي:** مرجع سابق، بدون رقم الصفحة.

39- تنص المادة 226_18 قانون العقوبات الفرنسي على أنه: "الحبس خمس سنوات وغرامة مليوني فرنك فرنسي كعقوبة لجمع معلومات اسمية بطريقة التدليس أو الخديعة أو أي طريق غير مشروع، أو إجراء معالجة لمعلومات اسمية تتعلق بشخص طبيعي رغم معارضة هذا الشخص، متى كانت هذه المعارضة تقوم على أسباب مشروعة".

_ فقد أورد المشرع الفرنسي قيد من الناحية الشكلية على جمع وتسجيل البيانات الشخصية إلا بوجود موافقة الصاحب الشأن وفق نص المادتين 226_18 و226_19 ق ع ف ج، كما لم يقف عند هذا الحد ووسع في نطاق الحماية لتشمل الناحية الموضوعية، حيث يشمل التسجيل جمع البيانات التي تقتضي طبيعتها عدم جمعها، مثل البيانات الخاصة بالمعتقدات الدينية والاتجاهات السياسية أو الفلسفية أو الانتماءات النقابية أو الأخلاق الشخصية وذلك حماية لحرية الفكر والاعتقاد، باستثناء الجهات التي سمح لها بجمع هذه البيانات؛ **محمد أمين الشوبكة:** مرجع سابق، ص94.

40- ولقد أناط المشرع الفرنسي للجنة الوطنية للمعلومات والحريات وفق المادة 226_ 21 تحديد ما إذا كان فعل جاني يشكل انحرافا عن الغاية من فعل المعالجة، وهذا بالرجوع الى الطلب المقدم إليها مسبقا والذي يحدد الغاية من المعالجة الإلكترونية للبيانات، وذلك وفقا لنص المادة 20 من قانون 1987، بهدف فرض الرقابة من قبل اللجنة الوطنية لتجنب إساءة استخدام البيانات دون الحد من الإمكانيات المتاحة لاستغلال هذه البيانات، ويستوي أن يكون الشخص حائزا على هذه البيانات بغرض تصنيفها أو نقلها أو علاجها؛ **محمد أمين الشوبكة:** مرجع سابق، ص100.

41- **محمد الشهاوى:** مرجع سابق، ص237.