الحماية المدنية للمعلومات الشخصية
في مواجهة الثورة التكنولوجية لوسائل
الاتصال والتواصل

إعداد

د /محمد محمد القطب مسعد
مدرس القانون المدني
كلية الحقوق- جامعة المنصورة

المقدمة

أهمية البحث:

إذا كانت خصوصية الأفراد لها أهمية كبيرة جعلتها تحظي باهتمام الفقه والقضاء منذ قديم الأزل، فإن هذه الأهمية تزداد عندما يتعلق الأمر بالأضرار التي يسببها التطور الهائل في مجال الاتصالات والتواصل. هذا ويكتسب البحث في هذا المجال أهميته للأسباب التالية:

١- يعتبر الحق في الخصوصية وحماية البيانات الشخصية من أهم الحقوق الدستورية اللصيقة بالإنسان، بيد أن التقدم التكنولوجي في الاتصالات الالكترونية أضحى أهم الأسباب التي تمثل مساسا بهذا الحق.

٢- انغمس الأفراد وبشدة في استخدام التقنيات الحديثة بما تشمله من وسائل اتصال، وتكنولوجيا للمعلومات، فضلا عن بروز الدور الجديد لوسائل التواصل الاجتماعي بكافة أنواعها، حتى أصبحت جزءا مهما في حياتنا، اخترقت خصوصياتنا، وزاحمت علاقتنا الاجتماعية.

٣- تطورت خصوصية الإنسان عن المعنى التقليدي المألوف نتيجة التطور العلمي الهائل في مجال التكنولوجيا، فبظهور الحواسيب أصبحت هناك خصوصية بالبيانات المخزنة عليها، كما أضحت هناك خصوصية للبيانات الشخصية عبر شبكة الانترنت.

٤- من لوازم التعامل عبر التقنيات الحديثة للاتصال كالبريد الالكتروني وهواتف التجوال النقالة وشبكات التواصل الاجتماعي ضرورة قيام الأفراد صغار كانوا أم

كبارا بوضع معلوماتهم وبياناتهم الشخصية وصورهم، بل وبعض مقاطع الفيديو الخاصة بهم وأسرهم، مما يمثل خطرا لا يستهان به علي حرمة الحياة الخاصة للأفراد، ويُعرض معلوماتهم وبياناتهم الشخصية لخطر الانتهاك والاعتداء من قبل الغير.

٥- خلفت ثورة المعلومات والاتصالات أثرا عميقا في مختلف المجالات، ولم تعد وسائل الحماية التقليدية صالحة لمواجهة التعدي على حقوق ملكية البيانات والمعلومات ، لاسيما مع التزايد المستمر لآليات الحصول على المعلومة عبر شبكة الإنترنت، وسهولة الحصول عليها عبر مواقع التواصل، والمدونات والمنتديات والمواقع الإلكترونية الحكومية وغير الحكومية، المفتوحة وذات الاشتراك [١].

مشكلة البحث:

إذا كانت تكنولوجيا الإعلام والتقنيات الحديثة للاتصال أضحت من لوازم الحياة الضرورية في عصر التكنولوجيا والأقمار الصناعية لما توفره من مميزات للمستخدمين جعلت من العالم بمثابة القرية الكونية الصغيرة التي تلاشت حدودها وتقاربت شعوبها [٢]. بيد أنها تعد في المقابل مسرحا خصبا لجرائم انتهاك الخصوصية

(١) د. عبد الحميد نجاشي ، حدود التزام المشترك بحقوق الملكية الفكرية لمؤلف قاعدة البيانات على شبكة الانترنت، ص ٢٦٦. بحث منشور بمجلة الفكر القانوني والاقتصادي ـ كلية الحقوق – جامعة بنها، لأعمال مؤتمر " الجوانب القانونية والاقتصادية للانفتاح المعلوماتي- ثورة المعلومات المنعقد في ٣١ مايو ٢٠١١.

(٢) راجع في ذلك د. مدحت محمد محمود، مفهوم وأهداف وخصائص شبكات التواصل الاجتماعي، بحث مقدم لمؤتمر ضوابط استخدام شبكات التواصل الاجتماعي في الإسلام، الجامعة الإسلامية، الرياض،٢٠١٦، ص ٣٢٠.

والاعتداء علي البيانات الشخصية، وتنبع مشكلة البحث من الإجابة علي بعض التساؤلات: هل غيرت تكنولوجيا الإعلام والاتصال الحديثة من المفهوم التقليدي لحرمة الحياة الخاصة للأفراد؟ وما هي أهم التهديدات التي أفرزتها تلك الوسائل على البيانات الشخصية الخاصة للأفراد؟ وهل نجحت القوانين في ملاحقة وتيرة التطور التكنولوجي في مجال الاتصال والتواصل أم مازلت تحاول الزحف نحو فهم الفجوة التي أحدثتها تلك الوسائل؟ هل الحماية التي توفرها القوانين لحماية حرمة الحياة الخاصة كفيلة لصد الهجوم الغاشم لتلك الوسائل على بياناتنا الشخصية؟

وأيضا ما مدي مواءمة القواعد التقليدية لملاحقة التطورات الجارية في مجال التكنولوجيا ونقل المعلومات. حيث يُثار التساؤل حول مدي خصوصية الالتزامات المفروضة علي المنتجين والمبتكرون لتلك الوسائل وكذلك على من يتولي إداراتها؟ وهل الشروط التقليدية اللازمة لتحقق المسئولية المدنية مازالت تتلاءم والتطورات الحاصلة في ظل هذه التقنيات المعقدة، أم أن هناك حاجة ماسة لتخطي تلك الثلاثية التقليدية والبحث عن شروط جديدة تتناسب مع خصوصية الأضرار الناشئة في هذا المجال؟

كما يثور التساؤل حول تحديد المسئول الذي يمكن تحريك دعوى المسئولية المدنية ضده وملاحقته بالتعويض اللازم؟ حال الاعتداء علي بيانات الأفراد الشخصية وانتهاك خصوصياتهم؟ وما هو موقف القانون المقارن إزاء حماية البيانات الشخصية؟

نطاق البحث:

نحاول الوقوف على أجوبة التساؤلات السابقة من خلال بحثنا للحماية المدنية التي توفرها قواعد القانون المدني المصري للبيانات الشخصية ومقارنتها مع بعض التشريعات المقارنة، دون التعرض لمظاهر الحياة الخاصة الأخرى للأفراد.

منهج البحث:

تنحو الدراسة إلي إتباع منهج تحليلي تأصيلي مقارن: حيث نقوم بتحليل النصوص ومطابقتها، وهو منهج تأصيلي علي سند من القول بأن أي حديث عن الحماية المدنية لن يتم إلا من خلال الرجوع أولا إلى جذور القواعد التقليدية للمسئولية المدنية، حيث إنه من خلال هذا المنهج نستطيع رد الفروع إلى أصولها العامة الواردة في قواعد المسئولية المدنية، حتى يمكن التوصل إلي حكم ينظم تلك الفروع. وهو منهج مقارن، اعتبارًا، من فوائد الدراسة المقارنة لبعض التشريعات العربية والأوربية.

خطة البحث:

الفصل الأول: أثر تكنولوجيا الاتصال والإعلام على خصوصية المعلومات الشخصية

الفصل الثاني: حماية المعلومات الشخصية في عصر التقنيات الحديثة

الفصل الأول
أثر تكنولوجيا الاتصال والإعلام على خصوصية المعلومات الشخصية

ينقسم هذا الفصل إلى مبحثان، يعرض الأول منهما للمفهوم القانوني للمعلومات الشخصية في ظلال الثورة المعلوماتية، بينما يناقش المبحث الثاني مظاهر الاعتداء على المعلومات والبيانات الشخصية عبر الوسائل التكنولوجية في عصر الإعلام والاتصال.

المبحث الأول
المفهوم القانوني للمعلومات الشخصية في ظلال الثورة المعلوماتية

كان للثورة المعلوماتية التي اجتاحت وسائل الاتصال والتواصل أثرها البالغ في تنامي الوعي، واختلاف المفاهيم بشأن حرمة الحياة الخاصة، حيث ساعدت علي ظهور جوانب جديدة حيال فحوى ومضمون فكرة الحياة الخاصة للأفراد، جعلت من الأهمية بمكان ضرورة اضافة البيانات والمعلومات الشخصية لنطاق خصوصية الأفراد.

لذا كان لزاما قبل التعريف بالمعلومات والبيانات الشخصية أن نعرض لأهمية الثورة المعلوماتية، وما أفرزته تكنولوجيا الاتصال.

المطلب الأول

ماهية الثورة المعلوماتية

تعريف الثورة المعلوماتية:

يقصد بثورة المعلومات في معناها البسيط " تدفق كم هائل من المعلومات في شكل طوفان هادر أغرق العالم، وفي معناها الواسع: مجموعة المتغيرات التي أحدثتها تقنية المعلومات، والتي يأتي علي رأسها تقنيات الاتصال الحديثة لبث المعلومات، وأنظمة المعالجة الالكترونية للبيانات والمعلومات الشخصية" [(١)].

ويرى البعض[(٢)] أن مفهوم تكنولوجيا المعلومات يتكون من شقين:

الشق الأول: التكنولوجيا : **ويقصد بها** :التطبيق العملي للاكتشافات العلمية المختلفة التي يتم التوصل إليها من خلال البحث العلمي. والتي تشكل في الوقت ذاته مجموعة المعارف والخبرات المتراكمة، والأدوات والوسائل المادية والإدارية، التي يستخدمها الإنسان في أداء عمل وظيفة معينة، في مجال حياته اليومية؛ لإشباع حاجته المادية.

(١) د. فيصل على خالد فرحان المخلافى، المؤسسات الإعلامية في عصر تكنولوجيا المعلومات، دراسة لواقع المؤسسات الصحفية اليمنية، المكتب الجامعي الحديث، ٢٠٠٥، ص ٥٣.

(٢) د. السيد حمد مرجان، ثورة المعلومات والحق في بناء مجتمع معرفي بين سياسات السلطة وأخلاقيات المهنة، ص٢٥١. بحث منشور بمجلة الفكر القانوني والاقتصادي - كلية الحقوق – جامعة بنها، لأعمال مؤتمر " الجوانب القانونية والاقتصادية للانفتاح المعلوماتي- ثورة المعلومات المنعقد في ٣١ مايو ٢٠١١.

الشق الثاني: **المعلومات**: ويقصد بها المعطيات الناتجة عن معالجة البيانات يدويا أو بواسطة الحاسبات الالكترونية

أهمية الثورة المعلوماتية:

أتاحت الثورة التكنولوجية الهائلة التي شهدتها وسائل الاتصال إمكانية تبادل البيانات والمعلومات عبر شبكة الانترنت وتقديم العديد من الخدمات عبر الحكومة الالكترونية.

من خلال ذلك أصبحت تكنولوجيا المعلومات والاتصالات بما تشمله من حواسيب شخصية وتليفونات محمولة وأجهزة كمبيوتر محمولة يدوية، وما شابها من وسائل الاتصالات الحديثة، السلكية واللاسلكية من ضرورات الحياة الحديثة العامة والخاصة على السواء وغدت تتغلل فيها لتدير عالمنا اليوم في شتى المجالات، هذا بالإضافة إلى الأقمار الصناعية وما تشتمل عليه من قنوات فضائية وأيضا القنوات الأرضية وعددا من أجهزة البث الإذاعي المتنوعة بالإضافة إلى الصحف والمجلات وغيرها من وسائل معلوماتية.

ولم يعد هناك مجال لإنكار أثر هذه المعلوماتية في حياة الإنسان حيث صارت تغزو كل قطاعات ومجالات وأنشطة الإنسان كالأنشطة العلمية والطبية، والتجارة الإلكترونية، وتعلم اللغات المختلفة، حتى مجال الدعوة الإسلامية، ومجال الفن والسياحة والتسوق والمجال القانوني والقضائي، الأمر الذي لم يعد يثار الجدل بشأنه على المستوى العام أو الشخصي[١].

(١) د. السيد احمد محمد مرجان، مقتضيات حماية النظام العام في مجال الاتصالات الإلكترونية الحديثة والهواتف المحمولة في ضوء نظرية الضبط الإداري، دراسة مقارنة، ص٧٧. بحث منشور في مجلة الفكر القانوني والإقتصادي -كلية الحقوق – جامعة بنها، سنة ٢٠١٠.

كما تطور الاتصال الهاتفي ليواكب عصر المعلومات وظهرت خدمات الهواتف المحمولة التي تتيح الاتصال الفوري بأي إنسان أو جهة أيا كان مكان تواجده[١]، فضلا عن ذلك فقد تم استخدام الكمبيوتر في مجال المراقبة الإلكترونية كوسيلة للحفاظ على الأمن داخل وخارج المنازل.

وبذلك غيرت تكنولوجيا المعلومات كل شيء في حياة الدول والمنظمات والأفراد والشعوب، حتى أصبح من غير الممكن تصور وجود أي نشاط إنساني، أو أي عمل جماعي منظم، دون توافر العلم والمعرفة والقدرة على استيعاب تكنولوجيا المعلومات [٢].

المطلب الثاني

ماهية المعلومات والبيانات الشخصية

أولا: مفهوم المعلومات والبيانات الشخصية:

تعرف المعلومة عامة بأنها" كل رسالة أو مضمون في مسألة أو تخصص ما يتم نقله أو تداوله بأي طريقة لشخص آخر، أو هي حالة خاصة بمادة من شأنها الإخبار أو الإعلام بأمر معين"[٣].

(١) د. عبد المنعم أحمد سلطان، التقنيات المعلوماتية وأثرها على حماية الحياة الخاصة بين الفقه الإسلامي والقانون الوضعي، ص ٢٤١. بحث منشور بمجلة الفكر القانوني والاقتصادي ـ كلية الحقوق – جامعة بنها، لأعمال مؤتمر " الجوانب القانونية والاقتصادية للانفتاح المعلوماتي- ثورة المعلومات المنعقد في ٣١ مايو ٢٠١١.

(٢) د. ليلي حسام الدين أحمد،:أثر التقدم في تكنولوجيا المعلومات على الخصائص النوعية والكمية للموارد البشرية، مؤلف من إصدارات المنظمة العربية للتنمية الإدارية، القاهرة، ٢٠١١، ص ٨.

(٣) د. عبد الحميد نجاشي ، حدود التزام المشترك بحقوق الملكية الفكرية لمؤلف قاعدة البيانات على شبكة الانترنت، المرجع السابق، ص ٢٧٠.

كما تعرف المعلومات بأنها" مجموعة من الرموز والحقائق أو المفاهيم أو التعليمات التي تصلح لأن تكون محلا للتبادل والاتصال أو التفسير أو التأويل أو المعالجة بواسطة الأفراد أو الأنظمة الالكترونية، وهي تتميز بالمرونة بحيث يمكن تغييرها وتجزئتها وجمعها أو نقلها بوسائل متعددة.

وكثيرا ما تستخدم البيانات كمرادف للمعلومات رغم الاختلاف بينهما في المعنى والمفهوم والدلالة، حسب ما جرى به العرف. أما البيانات فتعني تحليل وتفسير المعلومة، وذلك بمعالجتها الكترونيا بغرض تمكين ذوي الشأن من الحكم على الظواهر والمشاهدات(١). وقد ارتبط مفهوم حماية البيانات الشخصية بتقنية المعلومات ومدى تأثيرها على النظام القانوني وضرورة حماية الأفراد من مخاطرها التي تهدد حياتهم الخاصة وتمس خصوصياتهم وأسرارهم وذلك منذ ستينات القرن الماضي.

وقد أثير مفهوم خصوصية البيانات الشخصية في الفقه لأول مرة كمفهوم مستقل وذلك في أواخر ستينات وأوائل سبعينات القرن الماضي على يد المؤلفين الأميركيين: ألان ويستون (Alain Westin) في مؤلفة الخصوصية والحرية Privacy and Freedom ١٩٦٧، وألان ميلير (Alain Miller) في مؤلفه الاعتداء على الخصوصية (The Assaulton Privacy)، حيث رأى الأول أن المقصود بخصوصية المعلومات "حق الأشخاص في تحديد متى وكيف تصل المعلومات الخاصة عنهم للآخرين"، كما رأى الثاني أن خصوصية المعلومات تعني "قدرة الأشخاص على التحكم بدورة المعلومات المتعلقة بهم" واعتبر أن الشخص يكون متمتعاً بالخصوصية في حالة "العزلة والألفة، والتستر" (٢).

(١) د. نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان ٢٠٠٨، ص١٠١.

(٢) د. فريد جبور، حماية البيانات الشخصية، مقال منشور على الموقع الإلكتروني التالي:
https://lita-lb.org/archive/56-questions-answers-html.

ويعتبر بيانا شخصيا أي معلومة تتعلق بشخص طبيعي محددة هويته أو من الممكن تحديد هويته بطريقة مباشرة أو غير مباشرة ، سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه أو يميزه" [١]. ووفقا لذلك، فإن أي معلومة تتعلق بشخص طبيعي تعتبر بيانا شخصيا، مادام هذا الشخص الطبيعي محددة هويته، أو من الممكن تحديد هويته بأي طريقة مباشرة أو غير مباشرة.

وبناء على ذلك فإن الحماية القانونية تقتصر على البيانات الشخصية للأشخاص الطبيعيين فقط دون الأشخاص الاعتبارية[٢]. كما يخرج من نطاق الحماية البيانات الشخصية الخاصة بالحسابات غير محددة هوية أصحابها، كما إذا كان صاحب الحساب يستخدم اسم لا يحدد هويته، أو لا يمكن بطريقه ولو غير مباشرة تحديد هويته.

ووفقا لنص المادة الرابعة من قانون ٦ يناير لسنة ١٩٧٨ في فرنسا قبل تعديله، يعد بيانا شخصيا" كل البيانات، أيا كان شكلها، التي تسمح بطريق مباشر أو غير مباشر بالتعرف على الأشخاص الطبيعية التي تسرى عليهم، سواء تمت المعالجة من قبل شخص طبيعي أو معنوي".

ومن ثم، فإن البيانات التي تتعلق بالشخص الطبيعي، والتي لا تسمح بالتعرف عليه تكون خارج نطاق البيانات الشخصية محل الحماية وفقا لهذا القانون.

كما أن المادة الثانية من الاتفاقية الأوربية بشأن حماية الأشخاص من المعالجات الآلية للبيانات ذات الطبيعة الشخصية الموقعة في ٢٨ يناير ١٩٨١ تعرف البيانات الشخصية بأنها " كل معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد".

---

(١) مادة (٢) من القانون الفرنسي رقم ٧ لسنة ١٩٧٨ المعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤.

(2) Sophie LOUVEAUX, électronique et la protection de la vie privée, Art disponible sur, http://www.crid.be/pdf/crid/4710.pdf la data de mise en ligne est:17/1/2017.

ومن ثم تنصب خصوصية البيانات الشخصية على حق الأفراد أن يحددوا متى وكيف وإلى أي مدى يمكن للمعلومات الخاصة أن تصل للآخرين، كما تعني حق الفرد في أن يضبط عملية جمع بياناته الشخصية وعملية معاملتها آليا وطريقة حفظها وتوزيعها[١].

ويعد الشخص المعني بالبيانات ذات الطبيعة الشخصية محل المعالجة هو وحده الذي تتعلق به تلك البيانات[٢].

ثانيا: صور البيانات الشخصية للأفراد:

يدخل ضمن صور البيانات الشخصية للأفراد على سبيل المثال لا الحصر المعلومات الآتية:

١- الاسم واللقب: سواء في ذلك الاسم الأصلي أو اسم الشهرة أو الاسم المستعار طالما يمكن من خلاله التعرف على هوية صاحبه، فضلا عن اللقب الذي يميز الأسرة التي ينتمي إليها الشخص.

٢- الصوت والصورة : حيث تعد صورة الشخص الطبيعي سواء كانت صورة ثابتة أم متحركة بيان شخصي يخضع للحماية القانونية، فضلا عن صوت الإنسان حيث اعتبرتهما اللجنة القومية للحريات في فرنسا من قبيل البيانات الشخصية، استنادا إلى أن التكنولوجيا الرقمية الحديثة قد سمحت بمعالجة الصوت والصورة

---

(١) د. محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، الكويت، بدون ناشر، ١٩٩٢، ص٤٥.

(2) »La personne concernée par un traitement de données à caractère personnel est celle à laquelle se rapportent les données qui font l'objet du traitement». Article 2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux liberté (Modifié par Loi n°2004-801 du 6 août 2004).

ووضعهم على دعامة واحدة بجانب النص[١].

٣- الأرقام الشخصية: مثل رقم تحقيق الشخصية أو الرقم الشخصي الذي يميز كل شخص على مستوى الدولة التي يقيم فيها، فضلا عن الرقم التأميني أو رقم التأمن الصحي، شريطة ألا تكون أرقاما مكررة [٢].

٤- العنوان: حيث يعتبر عنوان الشخص بيانا شخصيا سواء كان عنوان منزله أو عنوان عمله أو عنوان مخصص لقضاء عطلاته.

٥- بيانات الحالة الاجتماعية.

٦- خصائص الحالة الجسمانية والصحية والنفسية.

٧- الأصول العرقية والجنسية.

٨- الآراء السياسية والمعتقدات الدينية

٩- البصمة: حيث تعتبر اللجنة القومية للحريات بصمة الإنسان من ضمن البيانات الشخصية أيا كانت صورة هذه البصمة، وسواء كانت بصمات إصبع أو بصمات محيط اليد.

١٠- أرقام الهواتف

١١- أرقام السيارات

---

(١) هذا ويعد اعتبار صوت الإنسان وصورته من ضمن البيانات الشخصية أمرا مستجدا، حيث كانت البيانات الشخصية قاصرة وحتى وقت قريب جدا علي الاسم واللقب والسن والوظيفة. فصوت الإنسان وصورته أصبحت من أهم مظاهر حق الإنسان في الخصوصية. راجع في ذلك : د. حسام الدين الأهواني، الحق في احترام الحياة الخاصة، المرجع السابق، ص٧٦ وما بعدها.

(٢) د. سامح عبد الواحد، الحماية القانونية للبيانات الشخصية، مجلة الحقوق الكويتية، العدد الرابع ٢٠١١، ص٣٩٢.

١٢- أرقام الحسابات البنكية

١٣- عناوين البريد الالكتروني

١٤- ملفات البيانات ذات الطبيعة الشخصية، وتشمل كل مجموعة من البيانات المنظمة والمستقرة للمعلومات ذات الطبيعة الشخصية، والتي يمكن الوصول إليها وفقا لمعايير محددة(١).

ثالثا: الطبيعة القانونية للبيانات والمعلومات الشخصية:

اختلف موقف الفقه بشأن الطبيعة القانونية للبيانات الشخصية، ما بين اتجاه تقليدي يرى أن البيانات الشخصية أصبح لها طبيعة من نوع خاص، تخرجها عن نطاق القيم المادية، لتدخلها في نطاق الحقوق المعنوية ذات القيمة المالية القابلة للتملك، باعتبار أن البيانات أصبحت لها قيمة اقتصادية لا يمكن إنكارها ارتقت بها لمصاف المنافع والخدمات(٢). ورأى البعض ضرورة إسباغ الحماية المدنية لتلك البيانات إذا ما جرى الاستيلاء عليها أو استخدامها استخداما غير مشروع، وفقا لقواعد المسئولية المدنية من خلال نص المادة ١٣٨٢ من القانون المدني الفرنسي، حيث يمثل اعتراف القضاء بالخطأ في مجال البيانات الشخصية اعترافا بوجود الحق في المعلومات

(1) »Constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés ». Article 2 de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux liberté (Modifié par Loi n°2004-801 du 6 août 2004).

(٢) د. أحمد محمود مصطفى، جرائم الحاسب الآلية في التشريع المصري، دراسة مقارنة، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، ص١٢-١٣.

والبيانات الشخصية، الأمر الذي يضفي على المعلومة الشخصية الطبيعة الخاصة التي تسمح بأن يكون الحق الوارد عليها من نوع الملكية العلمية ذات القيمة المالية[١].

بينما يرى اتجاها أخر أن المعلومات والبيانات الشخصية لها قيمة مالية أشبه بالسلعة، غير أنه يشترط لكي تكون صالحة للتملك، أن يكون صاحبها قد حازها بطريقة مشروعة، وأن تكون موضوعة بشكل يسمح بالاطلاع عليها، وتبليغها بشكل مفهوم، بغض النظر عن الوسيط المادي الذي يمكن أن يتضمنها[٢].

ومن جانبنا نتفق مع هذا الاتجاه الأخير لقوة الحجج التي استند أنصاره إليها، فمن ناحية لم يعد هناك مجالا للشك حول القيمة الاقتصادية للمعلومات والبيانات الشخصية، وإمكان تقويمها بسعر السوق، الأمر الذي يعكسه انتشار شركات تجميع البيانات والمعلومات الشخصية والتعامل بها، وتزايد السبق نحو الحصول على بيانات الأفراد ومعلوماتهم الشخصية بطرق الكترونية مستحدثة ومتعددة كما سيأتي بيانه لاحقاً، ومن ناحية أخرى علاقة التبعية التي تربط المعلومة الشخصية بصاحبها، هي نفسها العلاقة التي تربط المالك بالشيء المملوك، الأمر الذي يعطي لصاحب المعلومات والبيانات الشخصية الحق في ضمان سرية معلوماته وبياناته، فضلا عن حقه في الحصول على التعويض عن أي اعتداء غير مشروع يلحق بها.

وبذلك يمكن القول بأن المعلومات والبيانات الشخصية باتت تندرج ضمن نطاق القيم المعلوماتية، غير المستحدثة، وأن لها قيمة معنوية مالية مثل حق الملكية التي تعد محلا له. وتلك القيمة الاقتصادية من شأنها أن تغير من النظرة التقليدية للأشياء،

(١) د. خالد ممدوح إبراهيم، الجريمة الإلكترونية، الدار الجامعية، ٢٠٠٨، ص٣٥.
(٢) د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، ٢٠٠٦، ص١٠٧.

وتتطلب توفير حماية قانونية فعالة من شأنها أن تساير التطور التكنولوجي بما يستتبعه من أخطار واعتداءات على هذه البيانات الشخصية.

بيد أنه إذا رجحنا اعتبار البيانات والمعلومات الشخصية من قبيل القيم المعلوماتية ذات القيمة المالية التي تعطي لصاحبها حق معنوي مالي أشبه بحق الملكية؛ فإننا نتساءل من ناحية أخرى عن المالك الحقيقي للبيانات الشخصية وفقا للطبيعة القانونية المستقر عليها، والذي يملك وحده حق استغلالها أو استثمارها؟؟

اختلف الفقه في ذلك؛ حيث يذهب البعض إلى أن البيانات الشخصية للمستخدمين على وسائل التواصل والاتصال بكافة صورها وتطبيقاتها ليست مملوكة لهؤلاء المستخدمين، بل إن قيمتها التجارية أو الاقتصادية تكون لمن جمعها وعالجها وحللها، بإعتبار أن مواقع الاتصال والتواصل تعرض خدمات مجانية بالعموم، لكنها غالبا ما تتاح مقابل الاستخدام التجاري للبيانات الشخصية للمستخدمين(1)، الأمر الذي يعني عدم تملك المستخدمين للبيانات العائدة لهم، ومن ثم لا يحق لهم المطالبة بأي حماية، باعتبار أن حقائق المعلومات تكون مستبعدة من نطاق الحماية بموجب قوانين الملكية الفكرية التي تحمي فقط الابتكار، كما تستبعد أيضا من الحماية وفقا للقوانين المتعلقة بأسرار التجارة التي تقتصر حمايتها على المعلومات التي تبقيها الشركات سرية إذا كانت لها قيمة اقتصادية، ولا تكون البيانات الشخصية عبر مواقع الاتصال والتواصل من قبيل تلك المعلومات. وبالتالي عندما تجمع مواقع الاتصال والتواصل بيانات حول ميول واهتمامات المستخدمين بالخدمات، يكون لها وحدها حق المطالبة بملكية تلك البيانات.

(1) Céline CASTETS-RENARD, Droit de l'Internet: Droit français et européen, 2ème edition, Montchrestien, L'extenso éditions, 2012, p .78.

ومن ثم عند المطالبة بحماية قواعد البيانات بما تحتويه من بيانات شخصية، فيمكن توفيرها من خلال القوانين الأوربية المتعلقة بقواعد البيانات باعتبارها ملكا لشركات الاتصال والتواصل وليست ملكا للمستخدمين[١] . وتحرص الغالبية العظمى من مواقع التواصل الاجتماعي على النص ضمن الشروط العامة للاستخدام على أحقيتها في استخدام البيانات الشخصية للمستخدمين، فمن ضمن الشروط التي يدرجها موقع فيسبوك، أن التسجيل على الموقع من قبل المستخدمين هو بمثابة ترخيص باستخدام البيانات الشخصية مع المحتوى التجاري، حيث يتم استخدام تلك البيانات ونشرها دون علم المستخدمين، فضلا عن أحقية احتفاظ الموقع بتلك البيانات وحق استخدامها ولو انسحب المستخدم من الموقع[٢] . كما أن موقع توتير قد نص ضمن شروط استخدامه على أنه في حالة دمجه أو بيع أصوله أو الاستحواذ عليه أو إعادة تنظيمه؛ فإنه يمكن بيع المعلومات المجمعة أو نقلها في إطار العملية المنفذة.

وبذلك يرى أنصار هذا الاتجاه ملكية مواقع الاتصال والتواصل للبيانات الشخصية لمستخدمي صفحاتها الإلكترونية.

غير أن جانبا أخر يرى أن ملكية البيانات الشخصية حق لصيق بشخصية أصحابها وبالتالي لا تعود الملكية للمواقع الإلكترونية، حيث يستند أنصار ذلك الاتجاه إلى النصوص القانونية التي حرصت على توفير الحماية لأصحاب البيانات الشخصية عند معالجة تلك البيانات من قبل جهات وهيئات مختصة، فالمادة ٢١ من النظام الأوروبي الجديد حول البيانات الشخصية لعام ٢٠١٦ تنص على أنه " يحق للشخص المعني بالبيانات أن يعترض على معالجة بياناته الشخصية لأهداف الترويج التجاري"،

(1) Lothar Determann, Social Media Privacy: A Dozen Myths and Facts, 2012 STANFORD TECHNOLOGY LAW REVIEW. 7, p3. http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf

(2) Céline Castets -Renard, op cit, p .79.

ومن ثم قد يؤدي الاعتراض لوقف المعالجة. كما أن المادة الرابعة حظرت إنشاء سيرة حول الشخص وحول ميوله وحاجاته دون إذن منه، ويمتد الحظر ليشمل أي شكل من المعالجة الآلية للبيانات التي تتضمن استعمال البيانات الشخصية لتقييم بعض مظاهر الشخصية أو جوانب الشخصية المتعلقة بشخص طبيعي، خاصة أي تحليل أو تنبؤ لجوانب متعلقة بأداء الشخص في العمل أو وضعه المالي والصحي أو مفضلاته وموقعه وتنقلاته[١].

كما تعطي المادة ٢٢ من النظام الأوروبي لسنة ٢٠١٦ لصاحب البيانات الحق في ألا يكون موضوع قرار يستند فقط لمعالجة آلية، موضوعها إنشاء سيرة ذاتية حوله، ما لم يكن ذلك بإنشاء أو تنفيذ عقد بين الشخص وبين المسئول عن المعالجة، أو أجاز ذلك القانون، أو استند إلى الموافقة الصريحة لصاحب البيانات.

ويتضح من ذلك أن البيانات الشخصية بما أصبحت تمثله من قيم معنوية لها قيمة مادية واقتصادية تعد ملكا لمن تمثله فلا يجوز أن يتم تعميم تصنيفها لفعل معين ضمن فئة معينة أو لوقت معين لأخذ قرارات تعتمد على هذا التصنيف دون موافقة مالكها، فالتعميم وترتيب القرارات الهامة على أساسه قد يؤدي لمزيد من الإشكالات بالنظر لكون هذا التصنيف لا يعكس إلا جانبا من شخصية الفرد، وقد تشوبه الأخطاء وعدم الدقة حول حقيقة ما يحتويه من بيانات، الأمر الذي يمثل انتهاكا للحياة الخاصة للأفراد[٢].

---

(١) د.وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت –لبنان، ٢٠١٧، ص٧٩.

(2) Guillaume Florimond, Droit et Internet, De la logique internationaliste à la logique réaliste, Bibliothèque des thèses, Editions Mare & martin, 2016, p 340, 341.

وبدورنا نؤيد الرأي الثاني، حيث أن تضمن مواقع الاتصال والتواصل لشروط تحفظ لها حق استخدام أو استغلال البيانات الشخصية للمستخدمين يعني وبمفهوم المخالفة أن تلك البيانات ملكا خاصا لمن تمثله لا يجوز للشركات أو المواقع الإلكترونية استغلاله أو التعامل فيه إلا من خلال إذن صاحبها، كما أنه على فرض موافقة المستخدم للموقع باستغلال البيانات، أو حتى اعتبار مجرد اشتراكه بحساب على الموقع الإلكتروني بمثابة ترخيص عام للحق في استغلال تلك البيانات، ليس من شأنه أن ينقل ملكية البيانات للموقع أو أن يسلب من تمثله تلك البيانات حق ملكيتها، فثمة فارق كبير بين حق الملكية، وحق الاستغلال باعتباره أحد عناصر الملكية، والذي يمكن أن يباشره المالك بشخصه أو يعطي لغيره حق استغلاله واستعماله دون أن يسلبه الترخيص بالاستعمال أو الاستغلال ملكية الرقبة المتمثلة في ملكية تلك البيانات.

المبحث الثاني

مظاهر الاعتداء على المعلومات والبيانات الشخصية

عبر تكنولوجيا الإعلام والاتصال

نتيجة للاستخدامات المذهلة للآلات والأجهزة الإلكترونية، فقد تحول الإنسان إلى مجموعة من البيانات التي تشغل حيزا محدودا، يسهل إمكانية وضعها بأي مكان، مما لم يعد يحتاج الفرد معه لمزيد من الخبرات للوصول إلى أسرار وبيانات الأخريين.

ذلك أن الاعتداء الالكتروني يكون على ما هو مخزن داخل نظم الآلات أو الأجهزة، أو على أحد وسائط التخزين الصلبة التي تكون في طور النقل أو التبادل ضمن وسائل الاتصال المحوسبة.

وقد يكون الاعتداء على مضمون البيانات والمعلومات الشخصية ذاتها، أو على ما تمثله من قيمة معرفية، ويساعد على سهولة الاعتداء عليها ما تتميز به الأجهزة والوسائل التكنولوجية الحديثة للاتصال والتواصل من إمكانات وتطبيقات، كما تتعدد وتختلف طرق الاعتداء على هذه البيانات.

لذا يقسم هذا المبحث إلى مطلبين يعرض الأول منهما لعوامل الاعتداء الالكتروني على البيانات والمعلومات الشخصية، بينما يتناول المطلب الثاني لطرق وصور الاعتداء على البيانات والمعلومات الشخصية.

المطلب الأول

عوامل الاعتداء الالكتروني على البيانات والمعلومات الشخصية

أضحت تكنولوجيا الاتصال بمثابة الشبكة العنكبوتية التي تربط الكل بالكل بطرق متناسقة عبر خيوط متينة، تتواجد بكل مكان ويتواصل بها الأفراد من كل اتجاه.

بيد أن التكنولوجيا المعلوماتية لا تعمل من تلقاء ذاتها بل تفعل عبر نظام يطلق عليه التغذية، وتوصف هذه التغذية بالضارة خاصة في هذا العصر الحديث، خاصة وأن جميع وسائل التتبع والترقب بما تحويه من صور وبيانات عن نتائج الفحوصات الطبية، والتحاليل الوراثية، والأرقام الشخصية مآلها الجهاز الالكتروني، الذي لم يعد وسيلة أمان كافية، حيث تحوطه المخاطر من كل صوب واتجاه، فما هي أبرز العوامل التي جعلت هذه التكنولوجيا بهذه الخطورة؟

١- السعة غير المحدودة لذاكرة الأجهزة والحواسيب الالكترونية:

فعلى الرغم من تضاؤل حجم الوسائط وأوعية البيانات، كالبيانات الممغنطة والأقراص الصلبة، إلا أن قرص ضوئي واحد منها قد يحتوي على ما قد يكون كافيا لأن يملأ عشرين ورقة من البيانات، وبالتالي يمكن عن طريق إنشاء بنوك أو مراكز للمعلومات أن تقوم الدولة بجمع ما تريد جمعه من معلومات خاصة عن الأفراد، تتضمن كل كبيرة و صغيرة عنهم في قرص ضوئي واحد[١].

(١) د. عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي، بيروت، ٢٠٠٣، ص٦٢٩.

فيذكر أن حكومة الولايات المتحدة الأمريكية تحفظ بالحاسبات ما يقرب من ثلاثة بليون ملف تحتوي على معلومات شخصية، حيث يكون نصيب كل مواطن أمريكي في المتوسط ما يقارب من مائة ملف؛ كما يشاع حاليا أن هناك أنظمة كومبيوتر في بلجيكا حيث المقر العام لحلف الأطلسي، تختزن فيها المعلومات عن جميع الأشخاص على ظهر الكرة الأرضية(١).

لعل ذلك ما يفسر لنا سهولة الاطلاع على قدر لا يستهان به من المعلومات و البيانات الشخصية شديدة الخصوصية للأفراد، بمجرد القيام بجولة قصيرة في أنظمة الكمبيوتر، الأمر الذي يعني أننا أصبحنا في عالم شفاف صارت فيه كل معاملتنا المالية والاجتماعية، وما يخص كل تفاصيل حياتنا عرضة لأي مشاهد عابر.

٢- البيانات العديدة التي تجمعها المؤسسات الخاصة والحكومية:

طغى على الساحة حديثا اهتمام الشركات التجارية والمؤسسات الخاصة أو الحكومية بتجميع بيانات عديدة ومفصلة تتعلق بالوضع المادي والصحي والتعليمي والعائلي والاجتماعي والوظيفي للأفراد، فضلا عن استخدامها للحاسبات وشبكات الاتصال في تخزين تلك المعلومات وتحليلها والربط بينها واسترجاعها ومقارنتها ونقلها، الأمر الذي سهل كثيرا من فرص الوصول لتلك البيانات على نحو غير مأذون به وإمكانية إساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا، بغية مراقبة الأفراد وتعرية خصوصياتهم(٢). يزيد على هذه التهديدات ما تتميز به بنوك المعلومات من خاصية عدم النسيان وعدم التقادم، ومن ثم يصعب التوقع مستقبلا لأوجه استخدام

(١) د. عفيفي كامل عفيفي، المرجع السابق، ص٦٢٩.

(٢) يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، المرجع السابق.

تلك البيانات والمعلومات المخزنة عليها، وهو ما يمثل أحد الأخطار التي تهدد الحياة الخاصة للأفراد[١].

٣- شيوع النقل الرقمي للبيانات :

أدى شيوع النقل الرقمي للبيانات إلى خلق مشاكل أمنية وطنية كبيرة، حيث سهل عملية استراق السمع، والتجسس الإلكتروني، بسبب عدم قدرة شبكات الاتصال على توفير الأمان المطلق أو الكامل لسرية ما ينقل عبرها من بيانات ومعلومات، وإمكانية استعمال تلك البيانات بصورة غير مشروعة، وإمكانية اختراق ذاكرة الحواسيب عن بعد، ولا يقتصر هذا الاختراق على مجرد الاطلاع على حاوية الذاكرة من بيانات أو معلومات، بل يتعدى الأمر ليصل إلى الاستنساخ أو الإتلاف وإساءة الاستخدام.

فعلى عكس الطرق التقليدية أصبح بإمكان أي شخص يملك قدرا ضئيلا من المعرفة التقنية أن يصل لهذه البيانات والمعلومات، بما يمثله ذلك من انتهاك لخصوصية الأفراد؛ حيث أنه ومع تزايد مظاهر الاعتداء ظهرت مشكلة أخرى تتمثل في عجز وسائل الأمان التقنية عن توفير الحماية في مواجهة سيل التعديات على بياناتنا الشخصية، وبالرغم من التقدم الكبير في مجال التكنولوجيا والاتصال إلا أن احدث

(١) قد يحدث أن تسيء أحد المؤسسات أو الشركات استخدام هذه البيانات بعدما تنتهي حاجاتها إليها، وهو ماحدث بالفعل؛ حيث استطاع أحد كبار موظفي أحد البنوك السويسرية من مساعدة سلطات الضرائب الفرنسية بشريطا يحتوي على أرصدة عدد من الزبائن، فضلا عن ظهور العديد من حالات الابتزاز لأصحاب البيانات الشخصية لزبائن البنوك، خاصة المتهربين من الالتزامات الضريبية. راجع د. نعيم مغبغب، مخاطر المعلوماتية والانترنت منشورات الحلبي القانونية، بيروت، الطبعة الثانية، ٢٠٠٨، ص١٦٣.

تقارير الخصوصية تشير إلى أنه لا تزال حياة الأفراد وأسرارهم في بيئة النقل الرقمي معرضة للانتهاك في ظل عدم تكامل حلقات الحماية [١].

٤- انتشار بنوك ومراكز المعلومات الشخصية المنشئة من قبل الدول:

تقوم الدول بإنشاء بنوك أو مراكز للمعلومات تجمع فيها قدرا هائلا من البيانات والمعلومات الشخصية عن الأفراد وتقوم بتحليلها والربط بينها ومن ثم تخزينها في النظام المعلوماتي مما يتيح للدول فرض رقابة على مواطنيها ومعرفة أدق تفاصيل حياتهم بمجرد استخدام الرقم القومي مما يهدد خصوصياتهم[٢].

٥- انتشار وسائل التواصل الاجتماعي :

حيث بدأت شبكات التواصل الاجتماعي في الظهور في بداية تسعينات القرن العشرين، ففي عام ١٩٩٥ صمم راندي كونرادز Conradz randy موقع Classmates.com الذي كان يهدف من خلاله التواصل مع زملاء الدراسة الذين كانت بينه وبينهم روابط قوية أيام الدراسة بعد أن فرقت بينهم الأيام، لإعادة التواصل بينهم عبر الوسائل الالكترونية[٣].

---

(١) يونس عرب، المخاطر التي تتهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، المرجع السابق.

(٢) يطلق على ذلك " النظام الموحد للمعلومات" الذي يهدف لجمع كل ما يتعلق بالفرد من معلومات في جهاز حاسوب مركزي واحد يشمل البيانات الضريبية والاجتماعية والسياسية والصحية والمالية والحياتية للفرد. راجع د. نعيم مغبغب، مخاطر المعلوماتية والانترنت، المرجع السابق، ص١٦٦.

(٣) د. مدحت محمد محمود، مفهوم وأهداف وخصائص شبكات التواصل الاجتماعي، بحث منشور بمؤتمر ضوابط استخدام شبكات التواصل الاجتماعي في الإسلام، الجامعة الإسلامية، الرياض، ٢٠١٦،ص٢٥ وما بعدها.

وفي عام ١٩٩٧ ظهرت شبكات أخري للتواصل الاجتماعي تحت اسم ٦ درجات Six-Degrees والتي أتاحت الفرصة لوضع ملفات شخصية للمستخدمين علي الموقع، وإمكانية التعليق علي الأخبار وتبادل الرسائل مع باقي المشتركين. تبع ذلك أن قام جون بارجر John Barger أيضًا بعمل مدونات تتمثل في مواقع شخصية يقوم الفرد بإنشائها للتعبير عن آرائه، وتكون هذه الآراء مدونة بشكل تسلسلي، ومؤرخة بشكل تصاعدي، وزاع انتشارها في عام ١٩٩٩، ثم أعقب ذلك ظهور موقع ماي سباس الذي فتح آفاقًا واسعة لشبكات التواصل الاجتماعي، وحقق نجاحا هائلا منذ نشأته في عام ٢٠٠٣ [(١)].

كما يعد مارك زوكربيرج Mark ZUCKERBERG الذي كان طالبا في جامعة هارفارد من أبرز مؤسسي هذه المواقع، فقد كان له دور بارز في تسهيل تبادل المعلومات بين الطلاب في الجامعة عبر شبكة للتواصل الاجتماعي تحولت لاحقا للموقع الذي بات أشهر موقع للتواصل الاجتماعي "فيسبوك – وقد أحدثت مواقع التواصل الاجتماعي ثورة رقمية نتيجة استخدامها في نشر المعلومات، فالمستخدم يمكن له نشر برامج، أو مؤلفات على صفحات الويب، وإبرام صفقات تجارية، والتواصل مع أقرانائه، والتنقل بين أرجاء العالم، الأمر الذي جعل هذه الشبكات ذات طبيعة عالمية.

ثم ظهر لاحقًا موقع توتير Twitter بالإضافة إلي عدد من شبكات التواصل الاجتماعي الأخرى، وكذا موقع الإنستجرام Instagram ، وهو تطبيق لتبادل الصور وشبكة اجتماعية أيضا، يتيح للمستخدمين التقاط صور، ومن ثم مشاركتها في مجموعة متنوعة من خدمات الشبكات الاجتماعية، وشبكات إنستجرام نفسها.

(١) د. عباس مصطفي صادق، الصحافة والكمبيوتر، الدار العربية للعلوم، بيروت، ٢٠٠٥، ص٥١.

أعقب ذلك ظهور تطبيقات الهاتف المحمول أو الجوال أو المتحرك ، والتي يأتي أكثرها انتشارًا، الواتس آب، والفايبر، والتانجو، والسكايب، ولينكد إن .....، حيث سهلت هذه التطبيقات عملية التواصل الاجتماعي بين الأفراد بصورة كبيرة لكونها متاحة على الهاتف المحمول بشكل مجاني(١).

ومن ثم يطلق مصطلح شبكات التواصل، على مجموعة من المواقع على شبكة الانترنت، والتي ظهرت مع ظهور الجيل الثاني للويب، وتتيح التواصل بين مستخدميها في بيئة مجتمع افتراضي يجمعهم وفقا لاهتماماتهم أو انتماءاتهم الدينية أو الفكرية أو الاجتماعية أو الاقتصادية، بحيث يتم ذلك عن طريق خدمات التواصل المباشر، كإرسال الرسائل أو وسائل العرض المرئية أو المسموعة أو الصور، والاطلاع على الملفات الشخصية للأخريين ومعرفة الأخبار والمعلومات المتاحة للعرض(٢).

وتعددت تعريفات الفقه بشأن مواقع التواصل الاجتماعي، حيث عرفها البعض باعتبارها مواقع إلكترونية تتيح للأفراد إنشاء صفحة خاصة بهم، يقدمون من خلالها لمحة عن شخصيتهم أمام الجمهور، وتبادل المعلومات، أي إنها مجموعة المواقع التي تتيح للأفراد التواصل في مجتمع افتراضي، يعرفون فيه بأنفسهم ويتبادلون الاهتمام، ويقومون من خلاله بنشر عدد من الموضوعات والصور الشخصية (٣).

---

(١) د. مدحت محمد محمود، المرجع السابق، ص٢٦.

(2) David Beer: Social network (ing) sites…revisiting the story so far : A response to danah body & Nicole Ellison, Journal of computer – Mediated Communication, V.13 (2),P516-529. Janury 2008.

(٣) أ. مريم نريمان نومار، استخدام مواقع الشبكات الاجتماعية وتأثيره في العلاقات الاجتماعية- دراسة عينة من مستخدمي الفيسبوك بالجزائر، رسالة ماجستير، جامعة الحاج لخضير- باتنة، ٢٠١١،ص ٤٦.

وتتيح شبكات التواصل الاجتماعي ومواقعه للمستخدم إيجاد شخصية افتراضية تسمى (الملف الشخصي) تضم قائمة من المستخدمين، ويتم من خلالها تبادل المعلومات، والصداقات، والاتصال عبر شبكة الإنترنت بمختلف أشكاله.

ويقتضي التواصل الاجتماعي عبر هذه الشبكات وجود أجهزة مترابطة تستخدم لتدفق المعلومات، وعليه فالإنترنت هي السبب الرئيسي في ظهور مواقع التواصل الاجتماعي وتحويل المستخدم السلبي إلى مستخدم نشط، وقادر على إنشاء معلومات ومحتوى، والتفاعل مع الآخرين.

وقد عرف المشرع الفرنسي التواصل الاجتماعي عبر شبكة الإنترنت في المادة "٤" من القانون٥٧٥ لسنة ٢٠٠٤ بأنه برتوكول اتصال مفتوح، أو ربط بيانات وتبادلها بأي شكل يصل للجمهور من دون قيد علي أي محتوي تبادلي من قبل مقدمي الخدمات التقنية(١).

هذا وتُمكن تقنية تجميع المعلومات الجديدة لوسائل التواصل الاجتماعي من تجميع وتخزين واسترجاع وتحليل كميات هائلة من البيانات الشخصية التي يتم تجميعها من قبل المؤسسات والدوائر والوكالات الحكومية ومن قبل الشركات الخاصة، ويعود الفضل لهذا إلى مقدرة الحوسبة الرخيصة، وأكثر من هذا فانه يمكن مقارنة المعلومات المخزونة في ملف مؤتمت بمعلومات في قاعدة بيانات أخرى، ويمكن نقلها عبر البلدان في ثوان وبتكاليف منخفضة نسبيا(٢).

---

(١) د.محمد بن عبد العزيز بن صالح، المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي الحديثة – دراسة تأصيلية تطبيقية- رسالة دكتوراه، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤، ص٢٨.

(٢) تتميز شبكات التواصل الاجتماعي بعدد من الخصائص التي أعلت من قدرها وجعلت منها مقصدا هاما لمتصفحي الإنترنت في جميع أنحاء العالم، وأهم هذه الخصائص: ١- سهولة الاستخدام: حيث تم تطوير شبكات التواصل الاجتماعي لتكون سهلة الاستخدام، فلا يحتاج ولوج باب هذه الشبكات سوي الإلمام بقدر يسير من المعرفة حول أسس التكنولوجيا، فضلا عن مجانية امتلاك =

وتتمثل آلية تجميع بيانات المستخدمين عبر مواقع التوصل في متابعة الصفحات التي يزورها المستخدمين باستمرار عبر الإنترنت، وكذلك السلع التي يشترونها عادة، ومن ثم صنع سيرة ذاتية قريبة من الحقيقة عنهم، يتم استخدامها في اقتراح عروض أقرب إلى حاجاتهم الفعلية، وكذلك القيام بإجراء تحاليل تنبؤية تستبق نوع السلع والخدمات التي تتلاءم مع طلباتهم. كما تتمكن مواقع التواصل من خلال معرفتها الوثيقة بمستخدمين معينين من خلال البيانات والمعلومات التي وفروها عن أنفسهم خلال فترة مهمة من الزمن أو من خلال ربطهم بحسابات مصرفية أو خطوط هاتفية بتقديم حصيلتها من تلك البيانات لمواقع إلكترونية أخرى تمارس نشاطا تجاريا إلكترونيا في مقابل ربح مادي[١].

المطلب الثاني

صور الاعتداء على البيانات والمعلومات الشخصية

نتيجة لكل العوامل السابقة، فقد أصبحت بنوك المعلومات، وشبكة الانترنت ساحة للاعتداء على البيانات والمعلومات الشخصية للأفراد، وليس هذا فحسب بل

=

هذه المواقع.٢- التفاعل: حيث ساعدت التقنيات الحديثة لمواقع التواصل الاجتماعي في تسهيل عملية التواصل والتفاعل بين المشتركين عبر صفحاتها.٣- الحرية المطلقة من القيود: حيث تخلو بيئة التواصل من القيود، ويمكن لمستخدمها عرض أي معلومات ومناقشة أي موضوعات بدون قيود ودون حدود. ٤- تساعد علي إعادة تشكيل المجتمع: حيث تسمح بإقامة صداقات جديدة من أشخاص جدد من كل مكان، مما يساهم بشكل فعال في تجسيد مفهوم المجتمع الافتراضي. لمزيد من التفصيلات، راجع د.محمد بن عبد العزيز بن صالح، المرجع السابق، ص٢٨.

(١) د.وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت –لبنان، ٢٠١٧، ص٦٧.

ساعدت على إمكانية التلاعب بهذه البيانات عن طريق محوها أو تغييرها، مما أصبح معه حق الخصوصية للأفراد محل شك من حيث تواجده.

ونعرض فيما يلي لمظاهر الاعتداء علي البيانات والمعلومات الشخصية للأفراد من خلال بنوك المعلومات في فرع أول، نتبعه بمظاهر الاعتداء على البيانات الشخصية للأفراد عبر شبكة المعلومات الدولية (الانترنت) في الفرع الثاني.

الفرع الأول

مظاهر الاعتداء على البيانات والمعلومات الشخصية من خلال بنوك المعلومات

يعتبر الاعتداء على البيانات الشخصية للأفراد أحد أهم انتهاكات وسائل التقنية في العصر الحديث، ويرجع تاريخ ظهور وقائع تلك الاعتداءات إلى ستينيات القرن الماضي، حيث تم آنذاك نشر أول المقالات حول قضايا جرائم الحاسوب في الصحف العامة، خاصة جرائم التلاعب ببيانات الحاسوب وتخريب الحاسوب والجاسوسية الحاسوبية والاستخدام غير المنظم لنظم الحاسوب وكلها جرائم تتعلق ببنوك المعلومات.

ويمكن حصر الانتهاكات التي طالت البيانات الشخصية للأفراد من خلال بنوك المعلومات فيما يلي:

أولا: - **جمع البيانات الشخصية وتخزينها على نحو غير مشروع**:

يقصد بالجمع أو التخزين غير المشروع، جميع الأفعال التي تتم في نطاق الأنشطة المعروفة بالمعالجة الآلية للبيانات الشخصية في نظم المعلومات أو الكمبيوتر، والتي تتمثل في :

١- **الأساليب غير المشروعة المستخدمة للحصول على البيانات والمعلومات**:

فقد يتم الحصول على المعلومة عبر ولوج طرق غير مشروعة مثل التقاط الارتجاجات التي تحدثها الأصوات في الجدران الأسمنتية للحجرات وترجمتها إلى عبارات وكلمات بواسطة حاسوب مزود ببرنامج خاص، وقد يتم التعدي عبر اعتراض الرسائل المتبادلة أو التقاطها عن طريق توصيل أسلاك بطريقة خفية إلى الحاسوب الذي يختزن بداخله البيانات والمعلومات، أو الوصول بأي وسيلة أخرى غير مشروعة كالتدليس والاحتيال أو التصنت أو التسجيل خلسة(١).

٢- **الوصول للبيانات المحظور جمعها قانونا**:

وهي تلك التي يضع لها المشرع ضوابط قانونية أم فنية لضبط عملية الجمع والتخزين. ويتمثل الحد الأدنى من هذه البيانات في تلك المتعلقة بالفحوصات الجينية والبيانات الخاصة بالمعتقدات الدينية أو الاتجاهات السياسية ، أو الأصول العرقية أو الفلسفية ، أو الانتماء النقابي ، والبيانات الصحية أو القضائية(٢).

(١) د. نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان ٢٠٠٨، ص١٧٥.

(٢) د. نهلا عبد القادر المومني ، الجرائم المعلوماتية، المرجع السابق، ص١٧٦. ومن أبرز صور ذلك " تخزين شركة S K F الفرنسية في أجهزتها معلومات تتعلق بالاتجاهات السياسية وعضوية الاتحادات والنقابات العمالية لموظفيها، والتي استمدتها من طلبات التوظيف التي قدمت لها دون موافقة مسبقة من لجنة المعلوماتية والحريات، الأمر الذي يدخل في نطاق نص المادة ٤٢ من قانون الاتصالات الفرنسي المتعلقة بجريمة التسجيل والحفظ غير المشروع. أنظر د. صلاح محمد دياب، الحماية القانونية للحياة الخاصة للعامل وضمانتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب القانونية، الإسكندرية، ٢٠١٠، ص ٩٢.

ثانيا: إساءة استعمال البيانات المخزنة:

إن السماح بتجميع وتخزين البيانات الاسمية أو الشخصية للأفراد، ومن ثم معالجتها في جهاز الحاسوب ، يجب أن يتقيد بالهدف المحدد سلفا للقيام بذلك، حيث يعتبر الغرض المتوخى من معالجة البيانات الشخصية هو المبرر الوحيد للسماح بعملية المعالجة، حيث يتعين مراعاة الضوابط والشروط التي حددتها نص المادة السادسة من البيان الصادرة بالقانون الصادر في ٦ يناير ١٩٧٨ المعدل بمقتضى قانون ٦ أغسطس ٢٠٠٤، والتي تتماثل مع الشروط التي نصت عليها المادة الخامسة من الاتفاقية الأوربية الموقعة في ٢٨ يناير ١٩٨١ بشأن حماية الأشخاص في مواجهة المعالجة الإلكترونية للبيانات الشخصية، والتي تتضمن طبقا للقانون الفرنسي الداخلي:

١- ضرورة أن يتم تجميع البيانات ومعالجتها بصورة عادلة وقانونية.

٢- أن يتم جمعها لأغراض محددة وصريحة ومشروعة، ولا يتم معالجتها بطريقة لا تتفق مع تلك الأغراض.

٣- أن تكون كافية وذات صلة وغير مفرطة فيما يتعلق بالأغراض التي تم جمعها والمعالجات اللاحقة.

٤- أن تكون دقيقة وكاملة، وإذا لزم الأمر، تحديثها، يجب اتخاذ الإجراءات المناسبة لضمان أن المعلومات غير دقيقة أو غير كاملة الأغراض التي من أجلها تم جمعها أو معالجتها أن يتم مسح البيانات أو تصحيحها.

٥- أن يتم الاحتفاظ بها في الشكل الذي يسمح بتحديد الأشخاص المتعلقة بالبيانات الشخصية لمدة لا تتجاوز المدة اللازمة للأغراض التي يتم جمعها ومعالجتها

من أجلها [١]. ذلك ما طبقته المحكمة الدستورية لألمانيا الاتحادية " إذ لا حرية رأي أو حرية اجتماع ولا حرية مؤسسات يمكن أن تمارس كاملة ما دام أن الفرد غير متيقن في ظل أي ظروف ولأجل أي غرض جمعت تلك المعلومات الشخصية عنه ولأي هدف عولجت آليا في الحاسوب[٢].

ولعل من أهم المجالات التي برزت فيها مخاطر سوء استخدام البيانات المخزنة هو المجال الطبي، إذ يجب أن يكون لجمع وتخزين ومعالجة وتعديل ونشر وتبادل كشف المعلومات الطبية الشخصية وإلغاؤها أو استثمارها في وثائق بنوك المعلومات ضمانات تكفل احترام قواعد القانون، وأهمها السرية المهنية.

فللمريض الحق في سرية المعلومات المتعلقة به، ولا يمكن كشفها للأخريين إلا بطلب أو إذن منه، كما لا يمكن جمع أو كشف معلومات تتصل بالتعريف بهويته الشخصية أو بحياته الخاصة أو العائلية أو تتعلق بأصوله العرقية وآرائه السياسية أو الدينية أو حالته الصحية، عبر طرق احتيالية وغير شرعية رغما عن إرادته.

فقد درجت بعض المستشفيات الطبية أو العيادات الخاصة للأطباء على استخدام جهاز الكمبيوتر في إنشاء سجلات طبية الكترونية تعتمد على الكمبيوتر بكل إمكانياته المتطورة من جمع البيانات الطبية وتخزينها ومعالجتها وتزويد الأطباء والباحثين بما يحتاجونه منها في عملهم، بل الأكثر من ذلك فقد بدأ الأطباء استغلال تلك الإمكانات المتاحة، في عملية تبادل المعلومات بين الفريق الطبي المتعدد الاختصاصات، حيث بدأ الأطباء في التماس الحاجة المتزايدة إلى الخروج من عزلتهم ومحاولة الاتصال فيما

(1) Article ٦ de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux liberté (Modifié par Loi n°2004-801 du 6 août 2004).

(٢) د. نهلا عبد القادر المومني ، الجرائم المعلوماتية، المرجع السابق، ص١٧٦.

بينهم وتبادل المعلومات الموثقة بغية تأمين أفضل علاج لمرضاهم، غير أن تلك المعلومات المتبادلة غالبا ما تكون اسمية أو على الأقل تمكن من كشف هوية المريض بشكل مباشر أو غير مباشر، الأمر الذي يمثل مساسا بخصوصية المريض في معلومات وبيانات قد توصف بالحساسة[١]. فضلا عن إمكانية تعرضها للعبث أو السرقة عبر الدخول غير المأمون أو حال سرقة الملفات أو الأجهزة، الأمر الذي يترتب عليه إساءة استخدامها[٢].

وتزداد الخطورة أكثر عندما نعلم أن بنوك المعلومات لا تحوي هذه البيانات فقط وإنما أصبح التعامل يكمن في تبادل البيانات الجينية التي لا تندثر باعتبار أن الجين لا يمثل حامله فقط، بل يمثل تاريخ ومستقبل أسرة كاملة، حيث لم يعد الأمر قاصرا على الجانب الصحي فقط بل امتد إلى الجانب التجاري المادي، إذ أصبحت البيانات التي تحملها الجينات بفضل التكنولوجيا محلا للبيع والشراء في الأسواق[٣]، فأي حديث بعد ذلك عن السرية المهنية الملزمة للأطباء؟؟

ثالثا: الخطأ في البيانات والمعلومات الاسمية:

تتعدد المخاطر التي تسببها بعض الأخطاء في حفظ وتخزين المعلومات الاسمية، تلك الأخطاء قد تكون أخطاء تقنية أو فنية، كما يمكن أن تكون أخطاء بشرية.

---

(1) Cf. la Directive 95/46/ CE ; et la Loi française l'informatique et libertés.

(٢) حدثت عملية إساءة استخدام للبيانات الشخصية المدونة بالسجلات الطبية للسباق الألماني – مايكل شوماخر- حيث تعرضت بياناته للسرقة وتم عرضها للبيع. تقرير لقناة -CNN – الإخبارية ، أتلانتا ، الولايات المتحدة، حيزران ٢٠١٤.

(٣) د. نعيم مغبغب، مخاطر المعلوماتية والانترنت، المرجع السابق، ص١٣٨.

وتقع الأخطاء التقنية أو الفنية عند إجراء عملية التخزين والمعالجة الالكترونية، إما بسبب عيب فني لحق بالجهاز نفسه، أو حدثت نتيجة اختلال الضغط الكهربائي أو بسبب الفيروسات التي تؤدي لتحول البيانات الاسمية إلى بيانات مختلطة مبهمة، أو يترتب عليها وقوع اختلال في تصنيفها وتنظيمها، الأمر الذي ينتج عنه نسبة هذه البيانات لغير أصحابها مما يعطي صورة غير حقيقة عن الحالة الاجتماعية أو السياسية أو المهنية للأشخاص. أما الأخطاء البشرية فتكون من قبل الأطراف الذين يقومون بعملية الجمع والتخزين للبيانات الاسمية أو ترتيبها أو توزيعها، حيث يقع الخطأ في أي من هذه المراحل مما قد يسبب إضرار بسيرة الشخص صاحب البيانات المغلوطة.

رابعا: الإفشاء غير المشروع للبيانات والمعلومات الاسمية والشخصية:

يقصد بإفشاء البيانات نقلها من جانب المسيطر عليها أثناء قيامه بأي من عمليات المعالجة أو الحفظ إلى شخص أو أشخاص ليس لهم صفة مشروعة في تلقيها.

فتخزين البيانات أو معالجتها حتى وإن كان بموافقة ورضاء صاحبها لا يعني موافقته على السماح بتداولها أو خروجها من نطاق الخصوصية إلى دائرة الإعلام ولو للأشخاص العاملين بمجال المعلوماتية طالما انتفت صفتهم القانونية في العلم بها. ذلك الأمر قد يؤدي في كثير من الحالات إلى انتهاك خصوصية الأفراد[1]، فضلا عن إمكانية استغلال تلك البيانات في ابتزاز أصحابها.

(١) عرب يونس، الجزء الثاني، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة لمنتدى العمل الالكتروني، إتحاد المصارف العربية، عمان، ٢٠٠١، ص٥١٠.

ولعل مجال البنوك والمصارف من أكثر المجالات التي تبدو فيها مخاطر عمليات الإفشاء غير المشروع للبيانات الاسمية والشخصية للعملاء. إذا إنه وكنتيجة حتمية للتطور التكنولوجي، لم تعد البنوك والمصارف تستغني عن الكمبيوتر في تعاملاتها، مستخدمة في ذلك استمارة للزبائن مرتبطة ببعضها عن طريق العقل الالكتروني، تتضمن العديد من البيانات عن الزبائن مثل الاسم والوضع المدني، وتاريخ ومحل الإقامة، والمهنة ، ومكان العمل، وجميع المعلومات المرتبطة بعمليات تحويل الأموال والاعتماد، فضلا عن العديد من البيانات الشخصية الأخرى بالعميل، وبناء على تلك المعلومات يحمل الشخص شهادة من البنك بوضعه سواء أكان جيد أم شخص سيء، ولا تربط الشهادة العميل بالبنك فقط، بل أصبحت مرآة يرتبط بها مصير العميل في سائر معاملاته المالية(١).

لذا لنا أن نتخيل حجم المخاطر التي يتعرض لها العميل حال مخالفة أي من مسئولي البنك لالتزامه بالسرية المصرفية وإفشاؤه تلك المعلومات لأي شخص بصورة غير مشروعة.

خامسا: إتلاف ملفات البيانات الشخصية :

لا يقتصر نطاق الاعتداء على البيانات الشخصية على الكشف عنها أو استعمالها استعمالا غير مشروع، بل قد يكون الاعتداء في صورة محو أو إتلاف لتلك البيانات من خلال ولوج أغوار بنوك المعلومات، وتخريبها عبر عدد من البرامج أو الفيروسات التي لها قدرة فائقة على التخريب والإتلاف. ولا شك أن عملية الإتلاف يترتب عليها أن تضيع على المالك قيمة بياناته أو قيمة المعالجة الآلية لها(٢).

(١) د. عبد الفتاح بيومي حجازي، مكافحة جرائم المصارف الالكترونية، ورقة عمل ضمن ندوة المصارف الإلكترونية، الجمعية المصرية لقانون الإنترنت المنعقدة في ١٣ مايو ٢٠٠٧.

(٢) من الوقائع التي وردت في هذا الشأن، قيام أحد العاملين في شركة Fort Worth للتأمين على الحياة بولاية تكساس الأمريكية، باختراق النظام المعلوماتي للشركة، حيث تمكن من محو أكثر ١٦٨ ألفا من سجلات الشركة المتضمنة لبيانات العملاء بغرض الانتقام لفصله.

الفرع الثاني

مظاهر الاعتداء على البيانات والمعلومات الشخصية من خلال شبكة المعلومات الدولية

كان لتعاظم دور شبكة المعلومات الدولية (الإنترنت) أثره البالغ في تحقيق كثيرا من مظاهر الرفاهية لبني البشر، حيث اعتمد الفرد على تلك الشبكة في إدارة شئون حياته، فأصبح من الممكن أن يدير الفرد شركاته، ويوجه تعليماته، ويبرم كافة معاملاته وصفقاته، وهو لم يبرح سريره أو مقعده الخاص في بيته. بل كان لتكنولوجيا الاتصال الحديث عبر شبكات الانترنت والأقمار الصناعية دورها الهام أيضا في إحداث نوعا من التقارب والترابط بين الأفراد، مهما تباعدت أماكنهم واختلفت دولهم، بحيث يمكن لأسرة كاملة، يتواجد أفرادها بدول مختلفة تبعد كلا منها عن الأخرى جغرافيا ملايين الأميال، أن يلتقوا في نفس اللحظة بالصوت والصورة ، كأن أحدا منهم لم يبرح بيته. ولعل الفضل في ذلك يعود لبعض تقنيات الاتصال والتواصل الحديثة التي تعتمد اعتمادا كاملا على شبكة الانترنت وإشارات الأقمار الصناعية، والتي أصبح من أبرزها البريد الالكتروني، ومواقع التواصل الاجتماعي.

بيد أنه وبالرغم من الايجابيات التي تحققت بفضل تلك الوسائل الحديثة، فإنه لا يخفي علينا ما ارتبطت به تلك الوسائل من مخاطر وسلبيات، هددت الإنسان في خصوصياته، وسببت له العديد من الأضرار.

أولا: مظاهر الاعتداء على البيانات الشخصية عبر البريد الالكتروني:

بالرغم من عدم توافر نص قانوني صريح يعتبر البريد الالكتروني للفرد من المراسلات الخاصة، إلا أنه لم يعد هناك جدلا بين الفقه حول اعتباره من أهم صور المراسلات الخاصة[1].

(١) د.عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، القاهرة، بدون سنة نشر، ص١٠.

أكد القضاء الفرنسي على ذلك، عندما أدانت محكمة جنح باريس في حكمها الصادر في ٢ نوفمبر سنة ٢٠٠٠، مسئولين بإحدى المدارس العامة لقيامهم باعتراض ومراقبة رسائل البريد الالكتروني لأحد الطلاب، واعتبرتها من المراسلات الخاصة التي لا يجوز انتهاكها إلا بنص قانوني يبيح ذلك، حيث اعتبرت المحكمة أن إرسال رسالة الكترونية من شخص لأخر عبر البريد الالكتروني يشكل مراسلة خاصة تخضع لأحكام القانون رقم ٦٤٦ الصادر في ١٠ يوليو ١٩٩١ الخاص بحماية المراسلات التي تتم عن طريق وسائل الاتصال عن بعد(١).

كما اعتبرت محكمة استئناف باريس الرسائل الالكترونية الشخصية التي يرسلها العامل أو يستقبلها على الحاسوب الخاص برب العمل تدخل في نطاق الحياة الخاصة للعامل، ويحظر الاطلاع عليها أو المساس بسريتها(٢).

وتزايدت أهمية البريد الإلكتروني باعتباره أصبح الوسيلة المثلى في الاتصال لمميزاته الاقتصادية فضلا عن سرعته الزمنية في الإرسال والاستقبال، فلا يقيده مكان أو زمان، مما ساعد على اعتبار العالم كله بمثابة البيت الواحد الذي يجمع بين جدرانه كل أفراده(٣).

---

(1) L.Rapp, secret des correspondences et couriers électroniques , D.2000. n°.41, p.3 et s.

(2) Cour d' appel de paris, 17 Dec.2000. www.legalis.net

(٣) يتسم البريد الإلكتروني بالعديد من السمات التي تميزه عن غيره من الوسائل التقليدية وحتى الحديثة في التعامل الإلكتروني:

أ- سرعة التواصل :حيث يتسم بإرسال وتلقي الرسائل الالكترونية في وقت شبه متزامن وبسرعة فائقة مهما كان الفارق المكاني، ومهما كان حجم الرسالة ومحتواها الرقمي.

=

وتتمثل آلية عمل البريد الالكتروني، في إرسال رسالة البريد عبر الشبكة باستخدام الشخص لبريده الالكتروني، ليتلقاها مورد خدمات الاتصال المشترك معه، الذي يقوم بدوره بإعادة تمريرها في الشبكة بطريقة الترانزيت إلى ملقم البريد الالكتروني لدى مورد خدمات الاتصال مانح الاشتراك، منه إلى المرسل إليه صاحب العنوان الأخر الذي قصده المرسل. وفي كثير من الأحيان يكون البريد الالكتروني للفرد مرآة تعكس محل إقامته، وكذلك اسمه الحقيقي(١). الأمر الذي دفع ببعض التشريعات إلى النص علي استخدامه في مجال التبليغ القضائي، ذلك أن قوانين الإعلان والتبليغ القضائي بدأت تعتمد على إعلام المتخاصمين عن طريق البريد الالكتروني، وفي ذلك نصت المادة الثامنة من قانون الإجراءات المدنية والتجارية لدولة الإمارات العربية رقم ١٠ لسنة٢٠١٤ على أنه" :تسلم صورة الإعلان لشخص المعلن إليه أينما وجد أو في موطنه أو محل إقامته أو الموطن المختار أو محل عمله، فإذا تعذر إعلانه أو امتنع عن استلام الإعلان جاز لمكتب إدارة الدعوى إعلانه أو التصريح بإعلانه بالبريد المسجل بعلم الوصول أو بالفاكس أو بالبريد الإلكتروني، أو ما يقوم مقامها من وسائل التقنية

=

ب- نظام المرفقات :فبواسطة البريد الإلكتروني يمكن تضمين الرسالة عددا معتبرا من المرفقات الرسمية الممسوحة ضوئيا وبألوانها الأصلية، وهذا ما يميزه عن السبل الأخرى للتواصل كالفاكس والتلكس وبجودة فائقة بالإضافة إلى الصور والفيديوهات المختلفة.

ج- قلة التكلفة :حيث لا يكلف إرسال رسالة بكل مرفقاتها شيئا يذكر بخلاف ما تكلفه الطرود والمغلفات والرسائل التقليدية التي تتسم بالتكلفة والبطء، بالإضافة إلى إمكانية إرسال الرسالة إلى العديد من الأشخاص في الوقت ذاته، وفي حال الخطأ في عنوان المرسل إليه يتم تلقي رسالة فورية بوجود الخطأ. أنظر د. إبراهيم بن داود، د. أشرف شعت، الاطلاع على البريد الالكتروني بين متطلبات النظام العام والحق في سرية المراسلات، دفاتر السياسة والقانون، العدد ١٦، ٢٠١٧، ص ٢٧.

(١) د.يونس عرب، المرجع السابق.

الحديثة التي يصدر بتحديدها قرار من وزير العدل أو بأي وسيلة يتفق عليها الطرفان(١).

بيد إن الأهمية العملية للبريد الالكتروني في الاتصال والتواصل يقابلها العديد من المخاطر، حيث يؤدي سهولة وإمكانية اعتراضه إلى عدم الوثوق به، إذ يمكن اعتراض الرسائل التي يتم تحميلها حرفيا عبر الشبكة، وكشف مضمونها من خلال الموزع، وكذلك عبر برامج محددة تتمكن من قراءاتها وفهم محتواها أثناء عملية نقلها من المرسل للموزع ومنه إلى المرسل إليه.

ذلك الاعتداء قد يقع من جانب بعض الموظفين المختصين في هذا المجال بشكل تطفلي تعززه الرغبة في الاطلاع على خصوصيات الأخريين، وقد يكون بناءً على أوامر وتعليمات من الإدارة لدى الموزع، وقد تكون تعليمات أمنية بالتجسس لصالح السلطات المختصة بدعوى حماية الأمن والحفاظ على النظام العام.

تلك المخاطر حاول القانون الفرنسي الصادر في ١٠ يوليو ١٩٩١ الخاص بالاتصالات عن بعد مواجهتها من خلال نصه صراحة على أن سرية المراسلات التي تتم عن بعد يكفلها القانون، ولا يجوز المساس بسريتها إلا بواسطة السلطة العامة وفي حالات تقتضيها المصلحة العامة وفقا للشروط المنصوص عليها والمحددة قانونا(٢).

---

(١) المادة الثامنة من قانون الإجراءات المدنية والتجارية لدولة الإمارات العربية رقم ١٠ لسنة ٢٠١٤، المتمم والمعدل للقانون الاتحادي رقم ١١ لسنة ١٩٩٢ المتضمن قانون الإجراءات المدنية والتجارية.

(2) Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des communications électroniques. www.legifrance.gouv.fr

- الاختراق والتصنت على البريد الإلكتروني كأبرز مظاهر الاعتداء :

يعد الاختراق والتصنت أبرز مظاهر الاعتداء على البريد الإلكتروني وهذا ما تم تحريمه وتجريمه ضمن العديد من النصوص والتشريعات.

أ- اختراق البريد الإلكتروني :

يقصد بالاختراق " الدخول غير المصرح به أو غير المشروع لنظام المعالجة الآلية للبيانات، عن طريق انتهاك الإجراءات الأمنية"[١]. وغالبا ما يتم ذلك بمساعدة بعض البرامج المختصة، في سرقة وفك كلمات السر عن طريق المهارات والفنيات المكتسبة. الأمر الذي يحدث بالاعتماد على طريقين وهما:

- البرنامج المسيطر ويعرف بالعميل "Client".

- الخادم Server الذي يسهل عملية الاختراق.

ويتم اختراق البريد الإلكتروني من خلال بعض البرامج ووسائل متعددة من أبرزها:

- **أحصنة طروادة Trojan Horses ويكون مصدرها البريد الإلكتروني والمواقع المشبوهة التي يكمن ضررها في إمكان التجسس والتعرف على كلمات المرور.**
- **عن طريق IP Address ويتم الاختراق من خلال دخول شخص على حاسوب شخص آخر أو ربط جهازين مع بعض عن طريق المودم وباستخدام بروتوكول TCP/IP حيث يمكن بذلك السيطرة على الجهاز الآخر بطريقة أو أكثر إما بالتخفي أو بطرق ظاهرة ويمكن إرسال ملفات أو تحميل ملفات وإجراء محادثة أو كتابة أو مسح بيانات الطرف الآخر[٢].**

---

(١) د. إبراهيم بن داود، د. أشرف شعت، المرجع السابق، ص٢٨.

(٢) د. عبد الله بن ناصر بن أحمد العمري، رسالة ماجستير، كلية الدراسات العليا،جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٠،ص٦١.

ب- **التنصت على البريد الالكتروني** :

يعد التنصت على البريد الالكتروني للأفراد من أكثر صور الاعتداء شيوعا، حيث تبدو خطورة مثل هذا التعدي، أنه غالبا ما يقع من قبل السلطات الرسمية بدواعي التصدي لقضايا الأمن العام أو قضايا الإرهاب أو الحفاظ على النظام العام؛ وبذريعة ذلك صدر قانون التصنت الأمريكي الذي يسمح لوكالة الاستخبارات الأمريكية بمراقبة المكالمات الهاتفية والبريد الإلكتروني الخاص بالأجانب المقيمين في الولايات المتحدة الأمريكية دون إذن قضائي ويمنح السلطات الأمريكية حق التجسس على كل المكالمات والرسائل الإلكترونية.

ولا يقتصر فعل التنصت على الحكومات والجهات الرسمية، وإنما يشمل موردي الخدمة والقائمين على الانترنت، غير أن خطورة الاعتداء هنا تتمثل في وقوعه بموافقة صاحب البريد الذي يكون قد سمح مقدما عند إنشاؤه للحساب بمثل هذا الأمر دون علم أو دراية منه بخطورة تلك الموافقة المسبقة، التي تضفي على مثل هذا الاعتداء ستار المشروعية [١].

---

(١) ذلك أن المستخدم عند إنشاؤه لحساب البريد يكون ملزم بالمرور من خلال الموزع، الأمر الذي يعني ضرورة تقديم موافقة على طلب الاشتراك، في المقابل يكون طلب الاشتراك متضمنا للعديد من الشروط والبنود التي تعلن فيها شركات التوزيع عن عدم مسئوليتها عن مضمون الرسائل وعن ما يبث على الشبكة، كما تعلن عن سلطتها بمراقبة الخطوط والتنقل بين مواقع الشبكات، ونقل المعلومات إلى الشركات الإحصائية والإعلانية. ولا يكون أمام المستخدم سوى الرضوخ لقبول تلك الاشتراطات أملا في تملكه لحساب بريد الكتروني، دون أن يفكر جديا في خطورة تلك الموافقة المسبقة على خصوصيته.

ثانيا: مظاهر الاعتداء على البيانات الشخصية عبر وسائل التواصل الاجتماعي:

لا شك أن خصوصية المجتمع الافتراضي عبر وسائل التواصل الاجتماعي انعكست علي خصوصية الأفراد، وخصوصية بياناتهم الشخصية بالسلب، حيث ظهرت العديد من المخاطر التي لحقت بهما بسبب خلو هذا المجتمع الافتراضي من الرقابة ومن القيود. وتتزايد مخاطر التقنيات الحديثة لوسائل التواصل الاجتماعي، من خلال تقنيات رقابة (كاميرات) الفيديو، وبطاقات الهوية والتعريف الالكترونية، وقواعد البيانات الشخصية، ووسائل اعتراض ورقابة البريد والاتصالات، ورقابة بيئة العمل وغيرها.

إن حجم المعلومات المباشرة على الانترنت المتوفرة لموقع فيسبوك على سبيل المثال عن كل فرد مشترك يمكن استخدامها في أغراض تسويقية وأغراض أخرى غير مشروعة.

وتمر المخاطر التي تتعرض لها البيانات الشخصية بعدة مراحل، يأتي في مقدمتها مرحلة تجميع هذه البيانات الشخصية، تليها مرحلة تصنيفها لمحاولة عمل ملف كامل لكل شخص يحوي بياناته، ثم تأتي مرحلة التعامل في تلك البيانات.

ونعرض لتلك المخاطر بشيء من التفصيل من خلال ما يلي:

أ: مرحلة تجميع البيانات الشخصية:

لم تعد تمر لحظة إلا ويتعامل الإنسان مع العديد من المواقع الالكترونية الحديثة، ويتطلب الدخول أو التسجيل لهذه المواقع ضرورة الإدلاء ببعض البيانات الشخصية، بل إن بعض مواقع التواصل الاجتماعي أصبحت تطلب مما يسجل بياناته تقديم أدلة إثبات على صدق بياناته المقدمة كإرفاق صورة الرقم الشخصي أو بطاقة الرقم القومي

للشخص، أو تقديم نسخ من شهاداته العلمية.....، ومن ثم أصبحت الجهات الخاصة بتلك المواقع تجمع عن الشخص بيانات قد تفوق الحد المطلوب لتقديم الخدمة [١].

وقد ارتبط تجميع البيانات الشخصية للأفراد بظهور نظرية جديدة أطلق عليها نظرية التسويق المباشر، والتي من خلالها تحرص كل منشأة على التعامل مع كل فرد أو عميل على حدة وفقا لذوقه الخاص، من خلال تجميع أكبر عدد من البيانات الشخصية الممكنة عن هذا الفرد، سواء من حيث اسمه أو لقبه أو عنوانه أو رقم هاتفه، وعنوانه الالكتروني، وبعض جوانب الأنشطة والمهارات التي يفضلها، ومن ثم التعرف على ذوق العميل[٢]، حتى يتسنى الاقتراب من العملاء ومعرفة ميولهم، ومن ثم تقديم بعض العروض التجارية، أو عمل دعاية خاصة لكل عميل على حدة وفقا لبياناته والمعلومات المجمعة عنه.

ومن ثم أصبحت المعلومة بالنسبة للمشروعات تمثل أهمية تجارية، فبعد أن كانت المعلومة مجرد أداة فإنها أضحت منتجاً قائما بذاته تستثمر فيها الشركات أموالها، وعرف سوق المعلومات تنمية قوية متزايدة.

تلك النظرية شاعت في التطبيق مع زيادة عدد مستخدمي الشبكة العنكبوتية، حيث اتجهت معظم الشركات التجارية إلى إنشاء مواقع لها عبر شبكات التواصل

(1) Michael SAX, data collection and privacy protection: An international perspective,on line at, 6 august,1999,p5.

(2) sulliman OMARJEE, le data mining Aspect juridiques de l'intelligence artificielle au regard de la protection des données personnelles, memoire,faculté de droit, université Montpellier,2001/2002, p15. ets disponible sur: www.droit-ntic.com/pdf/Data_mining.pdf

الاجتماعي، وتحرص من خلال هذه المواقع علي تجميع أكبر قدر من البيانات الشخصية لمستخدمي تلك الوسائل(١).

ب: مرحلة تصنيف البيانات الشخصية:

بعد أن يتم تجميع البيانات الشخصية، تحدث عملية تصنيف وتقسيم لهذه البيانات، يتبعها إنشاء ملف لكل عميل يتضمن البيانات الخاصة به، حيث يمكن أيضا استخدام تلك البيانات المجمعة في عملية "التسويق المباشر" (٢).

كما أنه في كثير من الأحيان تعتمد المواقع علي تكملة بعض البيانات من خلال الاستعانة بالبيانات المجمعة عبر مواقع أخري، مما يؤدي إلى التعامل في البيانات

(١) يتم تجميع البيانات الشخصية عبر شبكة الانترنت عن طريق خاصية مستحدثة يطلق عليها (الكوكيز)، وتتمثل في ملف يقوم الموقع الخاص بالمنشأة التجارية بزرعه علي القرص الصلب للكمبيوتر الخاص بمستخدم الانترنت عند زيارته لهذا الموقع، هذا الملف يخزن فيه العديد من البيانات الشخصية لمستخدمي الانترنت. انظر يونس عرب، المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، ص٩. متاح عبر الرابط الالكتروني التالي: http://alyaseer.net/vb/showthread.php?t=19032

(٢) يعتمد تصنيف البيانات الشخصية علي تقنيات وبرامج كمبيوتر تسمح بتصنيف البيانات وفرزها والربط بينها أوتوماتيكيا دون حاجة لأي تدخل بشري. كما قد نشأت عدة شركات متخصصة وظيفتها القيام بتثمين وإعطاء القيمة للبيانات الشخصية، ولا تكون لهذه القيمة من معنى إلا عبر تداول البيانات وتفاعلها مع أنظمة أخرى خارجية أو داخلية، ومن ثم تكون البيانات الشخصية ذات قيمة إستراتيجية وسوقية بالنسبة لتلك الشركات تسمح بتطوير نماذج خدمة الزبائن، وتساعد في اختيار القرارات الملائمة، في الوقت الذي لا تعدو فيه تلك البيانات للمستخدم سوى مجرد تعبيرا عن حياته الخاصة. راجع في ذلك:

- Flora Fischer, CIGREF, Marie-Noelle Gibon, Jean-Luc Raffaelli, Christophe Boutonnet, Economie des données personnelles, Les enjeux d'un business éthique, octobre 2015, CIGREF, Réseau de grandes enterprises.

http://www.cigref.fr/wp/wp-content/uploads/2015/11/CIGREF-Economie-donnees-perso-Enjeux-business-ethique-2015. pdf, p 1, 3, 8.

والاتجار بها دون علم صاحبها. فقد أثبتت دراسة حول حسابات طلاب على موقع فيسبوك أن ٨٨,٨% يفشون كامل بياناتهم من تاريخ ميلاد، وجنسيتهم، وأرقام هواتفهم لوسيلة التواصل الاجتماعي، وأشارت إلى أن نسبة ٤٥,٨% منهم، ينشرون عناوين سكنهم، ولاشك أن تلك المعلومات تكون كافية لتحديد هوية الشخص وميوله، حتى وإن لم يذكر اسمه الحقيقي، وفضلا عن مساس ذلك بخصوصية المستخدمين، فإنه بالمقابل أيضا قد يؤثر على دور وسيلة التواصل كوسيط بين المستخدمين وبين الشركات(١).

ج: مرحلة التعامل في البيانات الشخصية والاتجار بها:

كما بينا فإنه وبطريقة ما تصبح البيانات التي يتم تسجيلها وتجميعها عبر كل موقع أو وسيلة تواصل محلا للتبادل مع غيرها من البيانات المسجلة بهدف الوصول لبيانات متكاملة عن كل فرد، مما يجعل تلك البيانات محلاً للاتجار المشروع وغير المشروع بها من قبل بعض الجهات التي تهدف إلى جمع الأموال.

فقد أثبتت دراسة أنه يوجد عدة طرق للوصول لبيانات مستخدمي شبكات التواصل وسيرهم الذاتية عبر اختراق قاعدة بيانات الموقع، وهو ما تمكن منه طلاب في جامعة إم أي تي (MIT)، حيث نجحوا في الحصول على ما يقرب من ٧٠ ألف سيرة ذاتية على موقع الفيسبوك من برنامج قاموا بابتكاره، الأمر الذي يعني أنه لم يعد من الصعب على الفنيين المحترفين تجاوز إعدادات الخصوصية لموقع الفيسبوك (٢).

---

(1) Adrienne Felt, David Evans, Privacy Protection for Social Networking APIs, University of Virginia Charlottesville, VA, http://www.cs.virginia.edu/~evans/pubs/proxy/privacybyproxy. pdf, p 1.

(2) Christopher F. Spinelli, Social Media: No 'Friend' of Personal Privacy, The Elon Journal of Undergraduate Research in Communications, Vol 1, No 2, Fall 2010, p 66.

وتتمثل المخاطر التي يمكن أن تلحق بهذه البيانات في الأتي:

١- **سرقة الهوية وعمليات الانتحال، والتشهير**:

يقصد بسرقة الهوية الحصول بوسائل احتيالية على معلومات من الإنترنت تخص شخصاً معينا مثل (الاسم وتاريخ الميلاد، والمهنة، والجنسية) دون علمه، ويقع ذلك في الأغلب الأعم بهدف ارتكاب جرائم احتيال إلكتروني، ومن ذلك أن ينتحل الجاني هوية شخص معين، ويحصل على قروض أو بطاقات ائتمان، أو يقوم بفتح حساب مصرفي.

ومن الوقائع التي مثلتها جرائم سرقة الهوية في الولايات المتحدة الأمريكية احتيال شخص على آخرين بادعائه أنه مالك لعقار بعد أن حصل على المعلومات الشخصية عن المالك الحقيقي من الإنترنت، واصطنع وثائق مزورة، وتمكن بذلك من بيع العقار لآخرين وحصل منهم علي مبلغ مالي كبير. وفي فرنسا قضي بتعويض امرأة عن الضرر الناجم لها بسبب قيام شخص بانتحال هويتها، وقام بوضع رقم هاتفها علي مواقع تواصل اجتماعية، مدعيا أنها تمارس الدعارة، وحصل علي أموال جراء ذلك.

كما تم اختراق شبكة سوني للألعاب الرقمية Sony PlayStation Network في عام ٢٠١١، وتم تسريب معلومات حول ٧٧ مليون زبون؛ تكبدت الشركة على إثره خسائر تقارب ١,٢٥ مليار دولار من خسارة الأعمال، وطلبات التعويضات[1].

(1) Nemone Franks, Social media and the law: A handbook for UK companies, January 2014, http://www.linklaters.com/pdfs/mkt/london/TMT-Social-Media-Report.pdf,p18.

وفي مصر أصدرت محكمة جنح مدينة نصر حكما قضائيا بالحبس ٣ سنوات مع الشغل وكفالة مقدارها ٥ ألاف جنيه مع إيقاف التنفيذ على شاب خريج لكلية التجارة، لاتهامه بإنشاء موقع مخل بالآداب على شبكة الانترنت ونسبه لابنة موظف كبير بإحدى الهيئات العامة، حيث ضمن الموقع جميع البيانات الشخصية عنها وصورها الخاصة وأرقام تليفونها، والتي استطاع الوصول إليها وسرقتها من خلال حسابها على موقع التواصل الاجتماعي – فيسبوك – وضمن الموقع بيانات تفيد رغبة الفتاة في إقامة علاقات جنسية مع الشباب، مقابل مبالغ مالية، الأمر الذي عرضها وأسرتها لمضايقات ومعاكسات، وألفاظ نابية من جانب زوار الموقع، مما أحال حياتها وأسرتها إلى نوع من الجحيم. اتضح من التحقيقات أن سبب ذلك يتمثل في رغبته في الانتقام من والد الفتاة الذي رفض خطبتها له. وكيفت المحكمة تلك الجريمة على أنها جريمة اعتداء على حرمة الحياة الخاصة للمجني عليها من خلال التعدي على البيانات الشخصية للفتاة وتسريبه لمحادثات جرت في مواقع خاصة على الانترنت إلى مواقع عامة، واعتدائه على حق الفتاة في الصور التي قام بنشرها عبر مواقع عامة على الانترنت(١).

٢- **الإعلانات الوهمية، والرسائل غير المرغوب فيها**:

تعد الإعلانات الوهمية سبب من أسباب ازدياد جرائم سرقة الهوية ثم استغلالها في ارتكاب جرائم احتيال، وتفيد التقارير بأن ما يقرب من٣,٥ مليون مستخدم تكبدوا خسائر تقدر بـ ٣,٢ مليون دولار بسبب هذه الإعلانات عبر البريد الالكتروني غير المرغوب فيه باستغلال بوابة البنوك . وهذه المعلومات يسيء

(١) د. شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٥، ص ٢٢٧-٢٢٨.

المحتالون على شبكة الإنترنت استخدامها من خلال سرقة بطاقات الائتمان وسحب أموال أصحابها من البنوك، أو اصطياد الضحايا عبر الإنترنت من خلال إجراء مزاد وهمي أو عرض تأشيرات وهمية مزورة [١].

٣- **استغلال العيوب التقنية**:

برغم التقدم التكنولوجي لتقنيات وسائل الاتصال الاجتماعي، إلا أن بعض مجرمي الانترنت يستطيعون استغلال الثغرات الموجودة في نظام معلوماتي معين لاختراق هذا النظام لسرقة البيانات الشخصية للمستخدمين، أو للإطلاع على المعلومات المتوافرة في النظام وتسجيلها واستغلالها.

ومن الوقائع التي رصدت في سرقة البيانات الشخصية: اعتراف دار النشر (lex-nexis) في عام ٢٠٠٥ بسرقة البيانات الشخصية لنحو ٣٢ ألف مشترك من قواعد البيانات التي تخصها. كما أعلنت احدي المؤسسات المالية الأمريكية عن عملية قرصنة لقواعد البيانات الخاصة بها إلى سرقة ما يقرب من ٤٠ مليون رقم كارت بنكي لعملائها.

وفي فرنسا فقدت احدي الشركات في عام ٢٠٠٦ اسطوانة عليها البيانات الشخصية لتسعة آلاف عامل، كما تشير بعض الإحصائيات إلى أنه في عام ٢٠٠٧ تم فقد نحو ١٦٢ مليون ملف يحوي بيانات شخصية للأفراد[٢] .

---

(١) د. خالد حامد مصطفي، المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل، مجلة رؤى إستراتيجية- مركز الإمارات العربية للدراسات والبحوث، المجلد الأول، العدد الثاني، مارس ٢٠١٣، ص١٢.

(٢) د. خالد حامد مصطفي، المرجع السابق، ص١٣.

وعليه يتضح تزايد المخاطر التي تتعرض لها البيانات الشخصية للأفراد عبر مواقع الشبكة العنكبوتية أو عبر مواقع التواصل الاجتماعي والتي قد تحدث بسبب سرقتها أو قرصنتها.

٤- **التجسس الإلكتروني علي البيانات الشخصية**:

حيث تقوم بعض الفيروسات بمعالجة المعلومات الاسمية لشخص معين للحصول علي معلوماته، بوسائل معينة مثل التقريب والمقابلة بين المعلومات المتاحة علي صفحات التواصل الاجتماعي، وإعداد الإحصائيات، وإدماج العناصر المختلفة، وربطها مع بعضها، ومن ثم، ترجمة حياة الفرد في ثوان معدودة، ثم استخدامها في أغراض غير مشروعة.

ثالثا: **مظاهر انتهاك الخصوصية في الإعلام الجديد**:

١- **التجسس على بيانات الهواتف النقالة**:

كشف باحث مختص في أمن تقنية المعلومات يدعى (تريفور) من خلال شريط فيديو عرضه في موقع اليوتيوب في مطلع العام ٢٠١١، أن جميع أجهزة الهاتف النقال من ماركات (الأبل – البلاك بيري –الإتش تي سي – الأيفون) تخضع لسيطرة كاملة من شركة استخبارات أمريكية. وعرض من خلال الفيديو وجود برنامج تثبته شركات صنع المحمول أشبه بفيروس خفي يعمل دون معرفة صاحب الجهاز على تسجيل موقع الهاتف وكل ما يقوم به صاحبه على شبكة الانترنت، ويعرض جميع اتصالاته ورسائله، ثم يقوم بإرسال جميع النصوص التي يتلقاها إلى شركة carrier1@ حتى بعد وضع الهاتف لحالته الأولية كما ورد من المصنع. وسارعت شركة (أبل) إلى الإعلان عن توقفها التام عن تضمين برامج التجسس التي تعمل على تسجيل جميع التحركات والنقرات، وظنت الشركة أنها نأت بنفسها عن مشاكل غير

محتملة مع مستخدمي هواتفها في البلاد الأجنبية لكنها لم تدرك أنها بذلك تدين الشركات الأخرى. وللتخفيف من كلمة (استخبارية) برر مختصون في شركة أبل إنها لا تعمل (أي الشركة) لصالح دول أو منظمات، وإنما ترسل المعلومات إلى شركات الاتصالات ومصنعي الهواتف الجوالة لاستخدامها في تحليل أساليب استخدام الجوال ومعرفة أي عيوب محتملة في الخدمات، وأضافت أن أي معلومات ترسل من خلال أجهزتها لشركة carrier1@ تستدعي إخبار المشترك بذلك وأنه يجري تمكين عمل برنامج التجسس لدى موافقة المستخدم على السماح بإرسال بيانات تشخيصية للصيانة Diagnostic Data لشركة (أبل) وهي خطوات تظهر عند تحديث نظام التشغيل أو بالاختيار اليدوي من إعدادات الهاتف. وما يزيد من قوة التخوف أن برنامج التجسس يواصل عمله في حال عدم وجود إشارة اتصال بشبكة الجوال، كما يمكنه التجسس لدى الاتصال بشبكات (واي فاي) ليرسل للشركة ما يسجله [1].

٢- **التجسس على أجهزة الحاسوب ومكوناتها**:

نجح مجموعة من الباحثين بجامعة كولومبيا في العام ٢٠١١، من التوصل إلى أنه يمكن استخدام الطابعات المتصلة بالانترنت لاختراق أجهزة الكمبيوتر. حيث قام الباحثون باختيار طابعات لشركة معروفة بعد أن قاموا بتوصيلها بشبكة الانترنت وتمكنوا بالفعل من خلال خاصية Firmware Update Remote التي تقوم بالتحقق من طرح أي تحديث للطابعة مع بداية أية مهمة طباعة - وكشفوا اختراق أجهزة الكمبيوتر المتصلة بالطابعات إذ يمكن للقراصنة الاحتيال على المستخدم لتثبيت

(١) د. جلال الدين الشيخ زيادة، العلاقة بين الإعلام التقليدي وشبكات التواصل الاجتماعي: الخصوصية والمهنية، دراسة مقارنة، ص٢٢. بحث منشور ضمن أعمال مؤتمر وسائل التواصل الاجتماعي- التطبيقات والإشكاليات المنهجية- التي نظمته كلية إدارة الأعمال – جامعة الأمام محمد بن سعود الإسلامية في الفترة من ١٠-١١ مارس ،٢٠١٥.

Firmware خبيث من تصميمهم مختص لهذا الغرض، وهو ما يضمن لهم التحكم التام في الطابعة. وعلى أثر ذلك تعرضت شركة سوني لأكبر اختراق خلال هذا العام، حيث استطاعت مجموعة من مخترقي الكمبيوتر (الهاكرز) الدخول إلى شبكة (بلاي ستيشن) وسرقة جميع المعلومات الشخصية المتعلقة بما يقارب ٧٧ مليون مستخدم بما في ذلك البريد الإلكتروني وكلمة السر، مما اضطر بالشركة إلي التوقف عن العمل لمدة ٢٣ يوم وعرضت كثيرا من التعويضات على المعتدى على بياناتهم[١].

(١) د. جلال الدين الشيخ زيادة، ، المرجع السابق، ص٢٣.

الفصل الثاني

حماية المعلومات الشخصية في عصر التقنيات الحديثة

بعد أن قمنا ببيان مظاهر الاعتداء التي تتعرض لها البيانات الشخصية للأفراد، كأحد أثار استخدام التكنولوجيا الحديثة للاتصال والتواصل، كان لابد أن نقف على مدى الحماية القانونية التي تكفلها القوانين الحديثة لمواجهة تلك الاعتداءات الغاشمة على أحد أهم جوانب الخصوصية للأفراد، ومدى ملاءمتها، لمواجهة شتى صور ومظاهر التعدي على البيانات الشخصية.

المبحث الأول

قواعد حماية الخصوصية المعلوماتية للبيانات الشخصية عبر وسائل الاتصال والتواصل الحديثة

بالنظر إلى قدسية الحق في الخصوصية، واعتباره من أسمى وأهم حقوق الإنسان، فقد حرصت التشريعات الدولية والوطنية على محاولة توفير الحماية القانونية للخصوصية المعلوماتية، غير أن الثورة التكنولوجية الهائلة في مجال الاتصال والتواصل قد أثارت التساؤلات حول جدوى القواعد المنصوص عليها دوليا ووطنيا لتوفير الحماية الفعلية للبيانات الشخصية للأفراد.

المطلب الأول

دور التشريعات الدولية والوطنية في حماية الخصوصية المعلوماتية

نظراً للتباين الملموس بين صور الاعتداء التقليدية على خصوصية الأفراد وبين صور الاعتداء المستحدثة لانتهاك الحق في الخصوصية من خلال التعرض للبيانات الشخصية للأفراد عبر وسائل التواصل الإلكترونية الحديثة بطرق غير مشروعة قد تصل إلى حد التغيير أو الاستغلال غير المشروع لها، وكذلك التباين في الوسيلة المستخدمة في الاعتداء التقليدي التي تعتمد غالبا على الحركة والقوة، وبين وسيلة الاعتداء على البيانات التي تعتمد على تقنيات إلكترونية بحته؛ فقد استوعبت التشريعات تلك الأبعاد الجديدة لتلك الجرائم المستحدثة، وأدركت بعدها عن النصوص التقليدية. لذا حاولت هذه التشريعات العمل على تحقيق الانسجام التشريعي من خلال إقرار قواعد مستحدثة ومستقلة تستوعب تلك المستجدات في مجال جرائم الخصوصية.

ونعرض في فرع أول لدور التشريعات الدولية في توفير الحماية للخصوصية المعلوماتية، ثم نعرض لدور التشريعات الوطنية حيال ذلك في الفرع الثاني.

الفرع الأول

دور التشريعات الدولية

بدأ الحديث عن مفهوم الحق في الخصوصية كأحد الحقوق الدستورية الهامة للإنسان منذ مطلع القرن العشرين، حيث كان الإعلان العالمي لحقوق الإنسان الصادر في عام ١٩٤٨ بمثابة نقطة البدء لكفالة الحماية القانونية لخصوصية الأماكن والاتصالات. فقد نصت المادة ١٢ من الإعلان العالمي على أنه " لا يعرض أحد لتدخل

تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات". أعقب ذلك اعتراف العهد الدولي للحقوق المدنية والسياسية بالحق في الخصوصية، إذ نصت المادة ١٧ من العهد الدولي (ICCPR) على حق كل شخص في عدم التعرض بشكل تعسفي، أو غير مشروع، للتدخل في خصوصياته أو شئون أسرته، أو بيته أو مراسلاته، ولا لأي حملات قانونية تمس بشرفه وسمعته. ونفس تلك الأحكام جاء النص عليها في اتفاقية الأمم المتحدة للعمال المهاجرين واتفاقية الأمم المتحدة لحماية الطفولة [١].

كما بدا الاهتمام بالحق في الخصوصية وقواعد حمايته على المستوى الإقليمي من خلال بعض الاتفاقيات، كما هو الحال في الاتفاقية الأوربية لحماية حقوق الإنسان والحريات الأساسية (روما لعام ١٩٥٠)، حيث قررت في المادة الثامنة منها حق كل إنسان في احترام حرمة حياته الخاصة، وحرمة منزله ومراسلاته، وحظرت تدخل السلطة العامة في ممارسة الإنسان لحقه في الخصوصية إلا في الأحوال التي يبينها القانون، وفي حالة حماية الأمن القومي للمجتمع الديمقراطي، أو لحماية سلامة الناس، أو للمصلحة الاقتصادية، أو لمنع حالات الفوضى أو ارتكاب الجرائم، أو لحفظ الصحة والأخلاق العامة، أو لحماية ورعاية حقوق وحريات الآخرين [٢].

---

(١) د. شريف خاطر، حماية الحق في الخصوصية المعلوماتية، مجلة كلية الحقوق - جامعة المنصورة للبحوث القانونية والاقتصادية، الجزء الثاني، العدد ٥٧، أبريل ٢٠١٥، ص١٤.

(٢) وطبقا لهذه الاتفاقية تم إنشاء المفوضية الأوربية لحقوق الإنسان، وأعقبها إنشاء المحكمة الأوربية لحقوق الإنسان لمراقبة تطبيق بنود تلك الاتفاقية، حيث تم العمل على محاولة التضييق من نطاق الاستثناءات على حكم المادة الثامنة وما تقرره من حماية للحق في الخصوصية. راجع د. شريف خاطر، المرجع السابق، ص١٥.

فضلا عن ذلك كان للاتفاقية الأمريكية لحقوق الإنسان دورا بارزا في حماية الحق في الخصوصية، من خلال نص المادة ١١ الذي جاء مطابقا للنص المقرر في الإعلان العالمي لحقوق الإنسان. وفي عام ١٩٦٥ تبنت الولايات المتحدة الأمريكية الإعلان الأمريكي للحقوق والواجبات الذي تضمن مجموعة من الحقوق، كان من بينها الحق في الخصوصية.

وكنتيجة لتطور مفهوم الحق في الخصوصية تحت تأثير ثورة تكنولوجيا المعلومات، انضمت البيانات الشخصية لمجال الحق في الخصوصية، الأمر الذي استوجب وضع قواعد معينة تحكم جمع ومعالجة البيانات الخاصة. وكانت اللبنة الأولى لمعالجة تشريعية في ميدان حماية البيانات، قد ظهرت في عام ١٩٧٠ في مدينة هيس بألمانيا، تبعها سن أول قانون وطني متكامل في السويد عام ١٩٧٣، ثم الولايات المتحدة عام ١٩٧٤. أعقب ذلك توالي الاهتمامات الدولية لحماية البيانات الشخصية، والتي نعرض لبعض منها فيما يلي:

١- دليل منظمة التعاون الاقتصادي والتنمية لعام ١٩٨٠.

ابتداء من عام ١٩٧٨ بدأت منظمة التعاون الاقتصادي والتنمية، وضع أدلة وقواعد إرشادية بشأن حماية الخصوصية ونقل البيانات. أعقب ذلك في عام ١٩٨٠، وضع دليل منظمة التعاون الاقتصادي والتنمية ، والذي يعد المصدر الأساسي للتشريعات الوطنية الداخلية، حيث تطبق قواعده على جميع البيانات المرتبطة بهوية الأشخاص، ولكافة أنواع ووسائل المعالجة الآلية للبيانات، ذلك أنه يتضمن المبادئ الأساسية التي أصبحت تعرف بمبادئ الخصوصية، وتتمثل في الأتي:

أ- فرض قيود على عملية تجميع البيانات الشخصية، بحيث يجب أن تتم بطريقة قانونية وشرعية بعيدا عن القيود والإكراه والخداع ، وبمعرفة الشخص المعني.

ب- يتم تجميع البيانات الشخصية على أساس غرض محدد، ويجب أن يكون الغرض ضروري، وقائم على أساس من الصحة والمشروعية.

ت- يجب تحديد المدة الزمنية لحفظ البيانات، بحيث تمحى هذه البيانات بعد انقضاءها.

ث- يجب عدم إفشاء البيانات الشخصية، وعدم إتاحتها إلا للأغراض المحددة للجمع والمعالجة، باستثناء الحالات التي يتوافر فيها رضا صاحبها، أو الحالات التي يقرها القانون.

ج- يجب اقتران الحماية القانونية للبيانات الشخصية بالحماية التقنية.

ح- ضرورة وجود سياسية عامة تتمتع بالوضوح والانفتاح بشأن الاستعمالات المنصبة على البيانات الشخصية، كالتعريف بجهات المعالجة، وأماكن تواجدها.

خ- يجب أن يحظي الفرد بحق المعرفة فيما إذا كانت هناك بيانات شخصية تعود له لدى جهة المعالجة، وإعطاءه الحق في التواصل مع هذه الجهة أن وجُدت بأسلوب ملائم وديمقراطي، مع إعطاء الفرد الحق في أن يعلم بسبب منع ممارسته لأي من الحقوق المتقدمة مع حقه في الاعتراض على عدم السماح له بممارسة حقوقه المشار إليها، وحقه في أن تشطب تلك البيانات إذا ثبتت صحة اعتراضه. وتكون جهات المعالجة مسئولة عن تطبيق تلك المبادئ وضمان تنفيذها.

٢- اتفاقية مجلس أوروبا ١٩٨١:

في عام ١٩٨١ وضع الاتحاد الأوربي اتفاقية حماية الأفراد من مخاطر المعالجة الآلية للبيانات الشخصية، حيث تبنت لجنة وزراء من مجلس أوروبا مناط بها معالجة موضوع الخصوصية اتفاقية حماية الأفراد في نطاق المعالجة الآلية للبيانات

الشخصية، حيث وقعت على هذه الاتفاقية ٣١ دولة، صادق منها ٢١ دولة، وبتاريخ ٢٥ يناير ٢٠١٢ صدقت باقي الدول الموقعة على هذه الاتفاقية، كما انضمت إليها ثمانية دولة أخرى، ليصبح عدد أعضاؤها ٣٩ دولة موقعة ومصدقة على الاتفاقية.

وعلى خلاف توصيات منظمة التعاون الاقتصادي والتنمية، فإن هذه الاتفاقية ملزمة للأعضاء الموقعين عليها، وينحصر نطاقها بالأشخاص الطبيعيين والملفات المعالجة آليا. وتقرر هذه الاتفاقية عشر مبادئ تمثل الحد الأدنى لمعايير حماية الخصوصية المتعين على الدول الأعضاء تضمينها في تشريعاتها وقوانينها الداخلية التي تضعها، وتقارب تلك المبادئ ذات مبادئ منظمة التعاون الاقتصادي والتنمية، مع إضافة بعض التفصيلات التي تتعلق بالمسائل التالية (تحقيق العدل الاجتماعي، قيود الجمع، الوقاية، العلنية، تأقيت الغرض وتحديد المدى، الدقة، مشاركة الأفراد)، واستنادا إلى هذه المبادئ الأساسية للحماية فإن قواعد الاتفاقية تغطي مسائل نقل وتبادل البيانات بين الدول المتعاقدة، وتمنع نقل أية بيانات خارج الحدود إلا للدولة التي تتوافر لها حماية موازية، كاستثناءات من هذه القاعدة.

وبالنظر إلى أهمية وكثافة تبادل البيانات بين الدول المختلفة، وبالتالي زيادة تدفق البيانات من دولة لأخرى، فكان من الضروري العمل على تقوية الحماية الفعالة للبيانات الشخصية، الأمر الذي استلزم تعديل تلك الاتفاقية، عن طريق توقيع بروتوكول إضافي بتاريخ ٢٠٠١/١١/٨، كان من أهم مميزاته، النص على إنشاء لجان متخصصة لمراقبة حسن تطبيق الاتفاقية الأصلية، وكذلك النص على إمكانية تدفق البيانات عبر الحدود الدولية، على أن يكون البلد المرسل إليه متمتعا بمستوى مماثل للحماية المقررة للبيانات الشخصية[1].

(١) اتفاقية مجلس أوروبا، متاح على الرابط التالي: http//conventions.coe

٣- الدليلين الإرشاديين للاتحاد الأوربي:

في عامي ١٩٩٥ ، ١٩٩٧ وضع الاتحاد الأوربي دليلين إرشاديين من أجل تحقيق الانسجام والتناسق بين قواعد حماية الخصوصية في دول الاتحاد الأوروبي، ولتوفير مستوى معين بالنسبة لحماية المواطنين الأوروبيين، والسماح بالتدفق الحر للبيانات الشخصية داخل نطاق الاتحاد الأوروبي.

وقد قرر هذان الدليلان مستوى معين لحماية الخصوصية لا يقف فقط عند حد البيانات وفق مفاهيم القوانين القائمة حاليا، ولكن يتجاوزه إلي تأسيس مزيد من الحقوق وتوسيع نطاق الحق ذاته[١]. ومن ثم فقد اهتم دليل حماية البيانات لعام ١٩٩٥ بمسألة توجيه القوانين الوطنية لتنظيم معالجة البيانات الشخصية بالشكليين الإلكتروني واليدوي، حيث عمل على توفير الحماية الفاعلة ضد استخدام البيانات الشخصية الحساسة، مثل البيانات المتعلقة بالصحة والأمور المالية للفرد، بينما اهتم دليل الاتصالات لعام ١٩٩٧ بتوفير حماية خاصة تغطي الهاتف والتليفون الرقمي وشبكات الهاتف الخلوية وغيرها من نظم الاتصالات، حيث يفرض التزامات واسعة على جهات خدمة الاتصالات وتزويدها لضمان خصوصية المستخدمين، بما في ذلك الأنشطة المتصلة بالإنترنت، ويتضمن قواعد تغطي العديد من المسائل التي لم يتم تغطيتها في قوانين حماية البيانات القائمة، ويتضمن القواعد التي تتعلق بتزويد الخدمات التقنية، ومسائل الاشتراكات، والتعرف على المشتركين، وغيرها من المسائل التي نشأت بسبب ثورة الاتصالات.

ومن أهم المبادئ التي قررها هذين الدليلين من أجل حماية البيانات، ما يلي:

- الحق في معرفة مكان معالجة البيانات.

---

(١) د. شريف خاطر، المرجع السابق، ص١٩.

- الحق في الوصول إلى هذه البيانات وتصحيحها.
- الحق في الدفاع والحماية من أنشطة المعالجة غير القانونية.
- الحق في الحصول على إذن لاستخدام البيانات في بعض الظروف والأغراض، ودون مقابل.

وفي عام ٢٠٠٠، أصدرت اللجنة الأوروبية نموذجا جديدا لدليل تشريعي لمعالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الالكترونية، ليحل محل دليل الاتصالات لسنة ١٩٩٧. حيث حرص الدليل الجديد على التوسع في نطاق الحماية المقررة للأفراد، وتضمن قواعد مستحدثة بشأن التقنيات الحديثة وأنواعها الجديدة، كما يتضمن تعريفات جديدة لخدمات الاتصال والشبكات، وكذلك يضيف تعريفات جديدة للمراسلات والبيانات المنقولة والمكالمات وموقع البيانات وغيرها، كل ذلك بهدف توسيع نطاق حماية الخصوصية والسيطرة على كافة أنواع البيانات المعالجة من خلال نصوص تؤكد على حماية البيانات المنقولة عبر شبكة المعلومات الدولية، وتمنع السلوكيات الاتصالية الضارة، كرسائل البريد الموجهة دون رغبة المتلقي وبأعداد كبيرة، وعلى نحو دوري أحيانا. كما تهدف لحماية مستخدمي الهواتف الخلوية من الرقابة والمتابعة المتصلة بالموقع.

٤- دليل حماية الحق في حرمة الحياة الخاصة ضمن إطار شبكة الاتصالات الدولية لعام ٢٠٠٢.

حيث تضمن الدليل بعض القواعد التي حاول من خلالها العمل على حماية خصوصية البريد الالكتروني الدعائي المكثف، وأكد على عدم جوازه إلا بموافقة الشخص المعني.

كما حرص على معالجة مشكلة برامج التنصت، حيث اعتبر هذه التقنيات تشكل خطرا جسيما على حرمة الحياة الخاصة لمستخدمي شبكة الاتصالات الالكترونية، بل شدد المسئولية الجنائية (في المواد من ١-٨) على كافة أشكال التعدي على البيانات الشخصية للأفراد واستخدامها في طرق غير شرعية خاصة إذا ما تم تجميعها دون الموافقة الصريحة من صاحبها. كما نص هذا الدليل في المادة الرابعة على بعض الالتزامات المفروضة على الدول الأعضاء أهمها موجب الأمن، حيث فرض هذا الدليل على عاتق مورد خدمة الاتصال اتخاذ كافة التدابير التقنية والتنظيمية واعتماد مستوى عالي من الأمن لمنع الوصول إلى المعلومات أو خرق شبكات الاتصال وإعلام المشتركين في حال وجود أي خطر في خرق أمن الشبكة وعجز مورد خدمة الاتصال عن تلافيه، واتخاذ وسائل الحماية الواجب اعتمادها.

كما نص كذلك على مبدأ سرية الاتصالات، بحيث يمتنع على أي شخص أن يقوم بتخزين أو تسجيل البيانات أو الاتصالات في معرض قيامه بموجب الرقابة إلا في حالة موافقة الشخص المعني. وأوجب على الدول الأعضاء اتخاذ كافة التدابير الجزائية لمعاقبة كل من يقدم على مخالفة أحكام القوانين الداخلية المتعلقة بهذا الموضوع [1].

الفرع الثاني

دور التشريعات الوطنية

أولا: التشريعات الغربية

آولت التشريعات الوطنية الغربية منذ قديم الأزل اهتماما ملحوظا بشأن حماية الحق في الخصوصية، حيث ترجع جذور ذلك الاهتمام إلى عام ١٣٦١ حيث تم سن

(١) القواعد التي قررها دليل حماية الحق في حرمة الحياة الخاصة، متاح عبر الموقع التالي: www.foruminternet.org

قانون في بريطانيا يمنع النظر واستراق السمع، ويجعل العقوبة على ذلك الحبس (The Justices of the Peace Act)، وفي عام ١٧٦٥ أصدر اللورد البريطاني Camden قراره بعدم جواز تفتيش منزل وضبط أوراق فيه، كما وضعت العديد من الدول الغربية حماية خاصة للحق في الخصوصية بعد هذا التاريخ، ففي عام ١٧٧٦ سن البرلمان السويدي قانون الوصول إلى السجلات العامة، والذي ألزم كافة الجهات الحكومية التي لديها معلومات أن تستخدمها لأهداف مشروعة، وفي عام ١٨٥٨ منعت فرنسا نشر الحقائق الخاصة، وفرضت عقابا على المخالفين، كما منع قانون العقوبات النرويجي لعام ١٨٨٩ نشر معلومات تتعلق بالشخصية والأوضاع الخاصة.

وظلت حماية الحق في الخصوصية محل متابعة واهتمام أيضا في التشريعات الحديثة، فكانت دولة السويد هي الأسبق على مستوى التشريعات الغربية في وضع تشريع لحماية المعطيات عام ١٩٧٣ والذي تم تعديله لاحقا، إلى أن حل محله قانون حماية البيانات الشخصية عام ١٩٩٨، حيث جاءت هذه المعالجة التشريعية نتيجة للتدخل الدستوري في الفقرة الثانية من المادة الثالثة من الفصل الثاني من الدستور السويدي لعام ١٩٩٨.

ثم تبعت دولة السويد في ذلك الولايات المتحدة الأمريكية عام ١٩٧٤، حيث أصدرت عدة تشريعات بشأن حماية الحق في الخصوصية: قانون الخصوصية لعام ١٩٧٤، قانون خصوصية الاتصالات الالكترونية لعام ١٩٨٦، قانون حماية خصوصية المستهلك لعام ١٩٩٧، قانون حماية خصوصية الضمان الاجتماعي لعام ١٩٩٧، قانون خصوصية المعطيات لعام ١٩٩٧.

واحتلت ألمانيا المرتبة الثالثة بعد السويد والولايات المتحدة الأمريكية بشأن تشريعات حماية البيانات الشخصية، حيث أصدرت في عام ١٩٧٧ قانونا بشأن

المعطيات وأجريت عليه تعديلات لاحقة، إلى أن صدر قانون حماية البيانات لعام ٢٠٠٠. وتبعتها بعد ذلك العديد من الدول الغربية مثل النمسا، والدنمرك، والنرويج، واستراليا، وبلجيكا، وكندا، وبريطانيا، والبرازيل، وهولندا، وغيرها من الدول التي اهتمت بحماية الحق في الخصوصية المعلوماتية.

- قانون حماية المعطيات الشخصية في فرنسا

لم تتأخر فرنسا أيضا عن الركب، حيث أصدرت قانون في ٦ يناير ١٩٧٨ بشأن حماية المعالجات الآلية للبيانات والحريات المعدل عدة مرات، ونعرض لقانون حماية المعطيات الشخصية بشيء من التفصيل من خلال ما يلي:

١- أثر تقنية المعلومات على الحق في الخصوصية المعلوماتية في فرنسا:

كغيرها من الدول؛ لم تكن فرنسا تسمح حتى السبعينات من القرن الماضي للمواطن الفرنسي بالحق في الاطلاع على البطاقات أو السجلات الإدارية الاسمية المتضمنة بيانات شخصية، لمعرفة حقيقة صحتها من عدمه، وبالتالي ليس له الحق في طلب تعديل بياناته حتى لو اتضح له ثبوت خطؤها.

غير أنه لما تعددت مظاهر المخاطر التي تتعرض لها الحياة الخاصة للمواطنين؛ كأثر يصاحب التوسع في استخدام الحاسبات الإلكترونية في شتى المجالات، وما تحتويه من إمكانية تخزين وتجميع المعلومات الخاصة بالأفراد المتعاملين مع الجهات الإدارية. مما قد ينتج عنه إساءة استخدام البيانات ذات الصلة بالحياة الخاصة للمواطن، أو احتمالية الخطأ في إدخال البيانات الشخصية، أو سهولة التعرض لها من قبل الغير.

وعلى أثر ذلك، قامت الحكومة الفرنسية بإصدار مرسوما في ٨ نوفمبر عام ١٩٧٤ يقضي بإنشاء لجنة أطلق عليها لجنة المعلوماتية والحريات تم إلحاقها بوزارة

العدل الفرنسية. تكون وظيفتها دراسة واقتراح الإجراءات التي يمكن من خلالها ضمان حماية الحياة الخاصة للمواطنين والحريات العامة من مخاطر التوسع في استخدام الأجهزة الإلكترونية في معالجة البيانات الشخصية للأفراد المدونة بالبطاقات الإدارية، حيث أعدت اللجنة تقريرا في ٢٥ يونيو ١٩٧٥ قدمته لرئيس الجمهورية عرف باسم "تقرير مسيو" المقرر للجنة والمستشار بمجلس الدولة، حيث وضح التقرير خطورة البطاقات والمعالجات الإلكترونية، وتهديدها لسرية المواطنين نتيجة إطلاع الإدارة على بياناتهم ومعلوماتهم الشخصية.

ونتيجة لذلك أصدرت الحكومة الفرنسية قانون ٦ يناير ١٩٧٨ بشأن المعالجة الإلكترونية للبيانات والمعلومات والبطاقات، وأدخلت عليه العديد من التعديلات كان آخرها تعديل عام ٢٠٠٤، حيث كان الهدف من هذا القانون متمثلا في جعل المعلوماتية في خدمة المواطن وليست سببا للإضرار بهويته البشرية، أو حرمة حياته الخاصة.

وقد ركز القانون المذكور على إضفاء الحماية القانونية لبنوك المعلومات والملفات التي تحتوي على بيانات ذات طابع شخصي، باعتبار أن الخطر الأكثر بروزا للمعلوماتية هو إنشاء بيانات اسمية في بنوك معلوماتية لا يعرف المعني أين هي بياناته، وهل هي بمنأى عن التطفل من عدمه. فضلا عن ذلك فقد هدف هذا القانون أيضا لإيجاد قدرا من الحماية للحياة الخاصة للأشخاص من خلال وضع العديد من الضمانات التي تمنع استغلال البيانات المدونة على البطاقات يدويا أو إلكترونيا من جانب موظفي الإدارة أو الغير.

وفي ذلك نصت المادة الأولى من قانون ٦ يناير ١٩٧٨ على أن المعلومات يجب أن تكون في خدمة كل مواطن. وتطورها وتنميتها يجب أن يأخذ في الاعتبار علاقة التعاون الدولي. هذه المعلومات أو البيانات لا يجب أن تتضمن اعتداء على الهوية

الإنسانية، ولا حقوق الإنسان، ولا الحياة الخاصة، ولا الحريات الفردية أو العامة. كما وضع المشرع من خلال هذا القانون عقوبات قاسية في حالة الاعتداء على حرمة الحياة الخاصة للأشخاص المودع بياناتهم إلكترونيا أو يدويا، أو حال الاطلاع عليها واستغلالها دون وجه حق[1].

٢- **شروط وضوابط معالجة البيانات الشخصية**:

اشترطت المادة ٦ من قانون ٦ يناير ١٩٧٨، المعدل في ٦ أغسطس ٢٠٠٤ بعض الضمانات من أجل حماية الأشخاص في مواجهة المعالجات الإلكترونية للبيانات الشخصية، والتي تتمثل فيما يلي:

- ضرورة أن يتم جمع البيانات ومعالجتها بصورة عادلة وقانونية.
- أن يتم جمعها لأغراض محددة وصريحة ومشروعة ولا يتم معالجتها بطريقة لا تتفق مع تلك الأغراض.
- أن تكون كافية وذات صلة وغير مفرطة فيما يتعلق بالأغراض التي تم جمعها والمعالجات اللاحقة.
- أن تكون دقيقة وكاملة، وإذا لزم الأمر، تحديثها، يجب اتخاذ الإجراءات المناسبة لضمان أن المعلومات غير دقيقة أو غير كاملة الأغراض التي من أجلها تم جمعها أو معالجتها، وأن يتم مسح البيانات أو تصحيحها.
- أن يتم الاحتفاظ بها في الشكل الذي يسمح بتحديد الأشخاص المتعلقة بها البيانات الشخصية لمدة لا تتجاوز المدة اللازمة للأغراض التي يتم جمعها ومعالجتها من أجلها.

---

(1) X.Linant, de bellefonds, L'informatique et le droit,2e ed,1985,p.2.

كذلك تقضى المادة السابعة من ذات القانون المعدل في ٦ أغسطس ٢٠٠٤، بأنه يجب لمعالجة البيانات الشخصية ضرورة الحصول على موافقة من الشخص المعني أو توافر أحد الشروط التالية:

- احترام الالتزام القانوني المفروض على المسئول عن المعالجة للبيانات الشخصية؛
- حماية حياة الشخص المُعنى.
- تنفيذ مهمة مرفق عام المخولة للمسئول عن المعالجة أو المستفيد منها.
- تنفيذا، سواء لعقد موضوع البيانات يكون الشخص المعني طرفا فيه، أو لاتخاذ إجراءات سابقة علي التعاقد تتعلق بالشخص المعني بالبيانات الشخصية.
- تحقيق المنفعة المشروعة عن طريق المسئول عن البيانات أو المستفيد منها، مع مراعاة عدم تجاهل مصالح أو الحقوق والحريات الأساسية للشخص المعني بمتابعتها.

كما وضع المشرع الفرنسي تنظيما خاصا لبيانات فئات معينة بمقتضى المواد الثامنة والتاسعة والعاشرة من ذات القانون السابق. حيث حظر القانون تجميع أو بحث البيانات الشخصية التي تكشف، على نحو مباشر أو غير مباشر، إذا استندت على الأصل العرقي أو الجنسي أو الآراء السياسية أو الدينية أو الفلسفية أو الانتماء النقابي للأشخاص، أو التي تتعلق بالصحة أو الحياة الجنسية للشخص المُعنى، ما لم يصدر قرار من مجلس الدولة بعد أخذ رأي اللجنة الوطنية للمعلومات والحريات[1]. بيد أنه يستثنى من هذا الحظر الحالات الآتية [2]:

(١) الفقرة الأولي من نص المادة الثامنة من القانون الصادر في ٦ يناير ١٩٧٨ المعدل في ٦ أغسطس ٢٠٠٤ بشأن معالجة البيانات الشخصية.

(٢) الفقرة الثانية من نص المادة الثامنة من القانون الصادر في ٦ يناير ١٩٧٨ المعدل في ٦ أغسطس ٢٠٠٤ بشأن معالجة البيانات الشخصية.

- المعالجات التي يقدم فيها الشخص المعني موافقته الصريحة، عدا الحالات التي ينص فيها القانون على أن الحظر المشار إليه سابقا لا يمكن التنازل عنه بموافقة الشخص المعني.
- المعالجات اللازمة للحفاظ على حياة الإنسان، في حالة أن هذا الشخص لا يستطيع إعطاء موافقته بسبب عجزه القانوني أو الاستحالة المادية.
- المعالجات التي تنفذها جمعية أو منظمة أخرى فلسفية أو سياسية أو دينية أو نقابية لا تهدف للربح.
- المعالجات التي تنطوي على البيانات الشخصية التي صدرت على الملأ من قبل صاحب البيانات.
- المعالجات اللازمة للإثبات، وممارسة أو الدفاع عن الحقوق القضائية.
- المعالجات اللازمة للطب الوقائي والتشخيص الطبي، وتوفير الرعاية أو العلاج أو إدارة الخدمات الصحية وتنفيذها من قبل عضو في المهن الصحية أو من جانب شخص آخر عليه التزام بالحفاظ على السرية المهنية المنصوص عليها في المادة ٢٢٦-١٣ من قانون العقوبات.

كما تقضي المادة التاسعة من أحكام قانون ٦ يناير ١٩٧٨ بأن معالجة البيانات الشخصية المتعلقة بالجرائم، والإدانات والتدابير الأمنية يمكن تنفيذها من قبل:

١- المحاكم والسلطات العامة والأشخاص المعنوية التي تتولى إدارة مرفق عام، التي تتصرف في حدود الصلاحيات القانونية.

٢- موظفي المحاكم، في إطار التزامهم بتنفيذ المهام الموكلة لهم من قبل القانون.

٣- الأشخاص الاعتبارية المشار إليها في المواد L.321-1 وL.331-1 من قانون

الملكية الفكرية، التي تتصرف بموجب الحقوق التي يديرونها أو نيابة عن ضحايا انتهاكات حقوق الإنسان المنصوص عليها في الكتاب الأول والثاني والثالث من هذا القانون من أجل ضمان الدفاع عن هذه الحقوق.

كما تقتضي المادة العاشرة بأنه لا يجوز أن تتضمن معالجة البيانات الشخصية الآلية أي قرار قضائي ينطوي على تقييم سلوك الشخص والذي يهدف إلى تقييم جوانب شخصيته. وأي قرار قضائي أخر يتضمن آثار قانونية صدرت في مواجهة شخص لا يمكن الاعتماد عليها فقط كأساس للمعالجة الآلية للبيانات الشخصية بهدف التعريف على الملف الشخصي للشخص المعني أو لتقييم بعض جوانب شخصيته. كما يجب ألا تؤخذ القرارات التي تصدر في إطار إبرام أو تنفيذ عقد كأساس وحيد للمعالجة الآلية للبيانات الشخصية، وذلك في حالة كون الشخص المعني قد تمكن من تقديم ملاحظاته، وعدم كفايتها لتلبية متطلبات الشخص المعني[1].

ثانيا: دور التشريعات العربية:

أما على مستوي التشريعات العربية، فقد قامت بعض الدول بإصدار تشريعات تتضمن حماية البيانات الشخصية، كدولة الإمارات العربية المتحدة التي أصدرت قانون حماية البيانات الشخصية المعدل عام ٢٠٠٧، حيث يضمن " قانون حماية البيانات"، بصيغته النهائية التي تم التوصل إليها بعد مراعاة التوصيات والمشورة العامة على مسودة القانون، حماية جميع البيانات الشخصية، بما فيها البيانات الحساسة ونقل وتداول البيانات، ويتفق القانون الجديد مع أحكام وقوانين وتوجيهات الاتحاد الأوروبي، وكذلك إرشادات منظمة التنمية والتعاون الاقتصادي (OECD).

(١) د. شريف خاطر، المرجع السابق، ص٥٥.

وفي تونس صدر قانون أساسي رقم ٦٣ لعام ٢٠٠٤ لحماية المعطيات الأساسية، وبموجبه يحظر جمع البيانات الشخصية إلا في أغراض مشروعة ومحددة وواضحة، واشترط القانون وجوب اخذ موافقة الشخص المعني بالأمر، وأناط القانون إلي الهيئة الوطنية لحماية المعطيات الشخصية منح تصاريح الحصول علي البيانات، كما اشترط القانون أن تكون البيانات المجمعة لتحقيق مصلحة حيوية للشخص المعني بالأمر أو لأغراض علمية ثابتة، وتطلب لإجراء عملية معالجة البيانات الشخصية ضرورة استخراج تصريح مسبق يودع بمقر الهيئة الوطنية لحماية المعطيات الشخصية. وأوجب القانون إعلام الأشخاص الذين تم جمع المعطيات عنهم مسبقاً بطلب كتابي متضمن علي نوع المعطيات الشخصية المراد معالجتها، وأهداف تلك المعالجة، ومدة حفظ المعطيات الشخصية، واسم الشخص الطبيعي أو المعنوي المستفيد من المعطيات، واسم المسئول عن المعالجة، ونص القانون علي عقوبات ماسة بالحرية وغرامات مالية، فقرر السجن لمن يفشي البيانات إلي بلاد أجنبية في حال أن تكون متعلقة بالأمن العام أو بالمصالح الحيوية للبلاد التونسية، وأيضاً لمن تعمد إحالة المعطيات الشخصية لتحقيق منفعة شخصية أو لغيره بغرض إلحاق الضرر بالشخص المعني بالأمر.

وفي المغرب صدر قانون "حماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي" في ٢٠٠٩، حيث وضع القانون إجراءات للحفاظ علي سرية المعطيات للأشخاص، وأوجب القيام بإجراءات تقنية وتنظيمية ملائمة لحماية المعطيات ذات الطابع الشخصي من الإتلاف أو الإذاعة، بالإضافة إلى حمايتها من أي شكل من أشكال المعالجة غير المشروعة. ويشترط القانون الحصول إذن مسبق من اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي لمعالجة المعطيات، ويمنح هذا الإذن بناء علي موافقة الشخص المعني. كما يعطي القانون للشخص المعني الحق في

الحصول علي تأكيد بأن المعطيات ذات الطابع الشخصي المتعلقة به تعالج أو لا تعالج، كما يحق للشخص المعني أن يتقدم بطلب للمسئول عن المعالجة لتصحيح المعطيات أو محوها. وأيضا حظر علي المسئول عن المعالجة نقل البيانات إلي دولة أجنبية، إلا إذا كانت هذه الدولة تضمن مستوي حماية كاف للحياة الشخصية وللحريات والحقوق الأساسية للأشخاص، وتعد اللجنة الوطنية قائمة الدول المتوفر فيها تلك المعايير وذلك بعد إجراء تقييم كافي لبيان مستوى الحماية الذي تضمنه دولة معينة، وإجراءات الأمن التي تطبق فيها، واستثني القانون نقل المعطيات ذات الطابع الشخصي إلى دولة لا تتوفر فيها الشروط السابقة في حال الموافقة الصريحة للشخص الذي تخصه المعطيات، أو في الحالات التالية:

أ- إذا كان النقل ضرورياً من أجل المحافظة على حياة الشخص المعني، أو المحافظة على المصلحة العامة، أو تنفيذاً لإجراء متعلق بتعاون قضائي دولي، أو الوقاية من إصابات مرضية.

ب- إذا كان النقل يتم تنفيذ لاتفاق ثنائي أو متعدد الأطراف يكون المغرب عضواً فيه.

ت- بناء علي إذن صريح ومعلل للجنة الوطنية.

وفي عمان والكويت أيضا صدرت تشريعات تنظم حماية البيانات الشخصية. بينما خلا التشريع المصري إلى وقت إعداد تلك الدراسة من أي قانون خاص لحماية الخصوصية المعلوماتية، بالرغم من تأكيد بعض المواد الدستورية على الحق في الخصوصية[1]، والتي تحدثت بصورة غير مباشرة عن الأنشطة الإلكترونية إلا أن ذلك

(١) حرص الدستور المصري الصادر عام ٢٠١٤ على التأكيد على حرمة الحياة الخاصة للموطنين، والنص على أن سريتها مكفولة للجميع. وأنه لا يجوز مصادرة المراسلات البريدية والبرقية =

حتى الآن لم ينتج عنه قانون فعلي، باستثناء مشروع قانون لمراقبة مواقع التواصل الاجتماعي والجرائم الالكترونية، مازالت السلطات المختصة في مرحلة دراسته والإعداد له.

وعلى الرغم من عدم إيلاء المشرع المصري أهمية لوجود قانون خاص معني بحماية البيانات الشخصية، فبمراجعة القوانين المصرية يتضح وجود نصوص قانونية تجرم إفشاء البيانات الشخصية، حيث سلك المشرع إلي تشديد العقوبة لمن يفشي سر خصوصي أؤتمن عليه بحكم وظيفته كالأطباء والجراحين والقوابل يعاقب بالحبس مدة لا تزيد علي ستة أشهر. في هذا الاتجاه نصت المادة (٩) من قانون٢٦٠ لسنة ١٩٦٠ في شأن الأحوال المدنية المعدل بالقانون رقم ١١ لسنة ١٩٦٥ والقانون رقم ١٥٨

=

والالكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال؛ ولا مراقبتها، ولا الاطلاع عليها إلا لمدة محددة، وفي الأحوال التي يبينها القانون، وبأمر قضائي مسبب. وفيما يخص الحصول على المعلومات فقد ورد أنه" حق تكفله الدولة مواطن؛ بما لا يمس حرمة الحياة الخاصة، وحقوق الآخرين، ولا يتعارض مع الأمن القومي". وأكدت المحكمة الدستورية العليا على أن "ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها، وينبغي دوماً – ولاعتبار مشروع – ألا يقتحمها أحد ضماناً لسريتها، وصوناً لحرمتها، ودفعاً لمحاولة التلصص عليها، أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التي بلغ تطورها حداً مذهلاً، وكان لتنامي قدراتها علي الاختراق أثراً بعيداً علي الناس جميعهم حتي في أدق شئونهم، بل وببياناتهم الشخصية التي غدا الاطلاع عليها، وتجميعها نهباً لأعينها ولآذانها، وكثيراً ما ألحق النفاذ إليها الحرج أو الضرر بأصحابها، وهذه المناطق من خواص الحياة ودخائلها، تصون مصلحتين قد تبدوان منفصلتين، إلا أنهما تتكاملان، ذلك أنهما تتعلقان بوجه عام بنطاق المسائل الشخصية التي ينبغي كتمانها، وكذلك نطاق استقلال كل فرد ببعض قراراته الهامة التي تكون- بالنظر إلي خصائصها وآثارها- أكثر اتصالاً بمصيره وتأثيراً في أوضاع الحياة التي اختار أنماطها، وتبلور هذه المناطق جميعها- التي يلوذ الفرد بها، مطمئناً لحرمتها ليهجع إليها بعيداً عن أشكال الرقابة وأدواتها- الحق في أن تكون للحياة الخاصة تخومها بما يرعي الروابط الحميمة في نطاقها، ولئن كانت بعض الوثائق الدستورية لا تقرر هذا الحق بنص صريح فيها إلا أن البعض يعتبره من أشمل الحقوق وأوسعها، وهو كذلك أعمقها اتصالاً بالقيم التي تدعو إليها الأمم المتحضرة". قضية رقم ٢٣ لسنة ١٦ قضائية المحكمة الدستورية العليا متاح عبر الرابط التالي:

http://hrlibrary.umn.edu/arabic/Egypt-SCC-SC/Egypt-SCC-23-Y16.htm

لسنة ١٩٨٠ على أن البيانات التي تحويها سجلات الأحوال المدنية تعتبر سرية ولما كانت هذه البيانات سراً فإن إفشائها من قبل الموظف يوقعه تحت طائلة القانون والمساءلة بموجب أحكام قانون العقوبات. كما قرر المشرع معاقبة كل من أخل بسرية البيانات الإحصائية أو أفشى بياناً من البيانات الفردية أو سرا من أسرار الصناعة أو التجارة أو غير ذلك من أساليب العمل التي يكون قد اطلع عليها بمناسبة عمله بالحبس. كما حرص المشرع على سرية بيانات العملاء البنكية، فحظر الإطلاع والإفشاء بغير المقرر للأشخاص والجهات المسموح لها وفقاً لأحكام القانون، و يمتد الحظر حتى بعد زوال العلاقة بين العميل والبنك ويسري الحظر على جميع الأشخاص والجهات بما في ذلك الجهات التي يخولها القانون سلطة الإطلاع أو الحصول علي الأوراق أو البيانات المحظورة إفشاء سريتها طبقاً لأحكام قانون سرية الحسابات بالبنوك، ويظل هذا الحظر قائماً حتى ولو انتهت العلاقة بين العميل والبنك لأي سبب من الأسباب. كما تنص المادة الثانية : ".....وفي جميع الأحوال لا يجوز الكشف عن شخصية صاحب الحسابات أو الوديعة المرقمة إلا بإذن كتابي منه أو من أحد ورثته أو من أحد الموصي لهم بكل أو بعض هذه الأموال أو من النائب القانوني أو الوكيل المفوض في ذلك أو بناء علي حكم قضائي واجب النفاذ أو حكم محكمين نهائي . كما نصت المادة الخامسة علي انه "يحظر علي رؤساء وأعضاء مجالس إدارة البنوك ومديريها أو العاملين بها إعطاء أو كشف أية معلومات أو بيانات عن عملاء البنوك أو حساباتهم أو ودائعهم أو الأمانات أو الخزائن الخاصة بهم أو معاملاتهم في شأنها تمكين الغير من الإطلاع عليها في غير الحالات المرخص بها بمقتضى أحكام القانون"، ويسري هذا الحظر على كل من يطلع بحكم مهنته أو وظيفته أو عمله بطريق غير مباشر على البيانات والمعلومات المشار إليها[1].

(١) راجع قانون سرية الحسابات في البنوك رقم ٢٠٥ لسنة ١٩٩٠.

كما حرص المشرع على حماية بيانات الطفل؛ فقد قرر تغريم من ينشر بيانات تخص هوية طفل معرض للخطر، حيث نصت المادة ١١٦ مكرر (ب) من قانون الطفل ١٢ لسنة ١٩٩٦:"مع عدم الإخلال بأي عقوبة أشد ينص عليها في قانون آخر، يعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين ألف جنيه كل من نشر أو أذاع بأحد أجهزة الإعلام أي معلومات أو بيانات، أو أي رسوم أو صور تتعلق بهوية الطفل حال عرض أمره على الجهات المعنية بالأطفال المعرضين للخطر أو المخالفين للقانون".

كما حظر القانون إفشاء من اتصل علمه بحكم عمله إفشاء بيانات ومعلومات متعلقة بالتوقيع الإلكتروني، ففرض المشرع على تلك البيانات السرية وقرر توقيع الغرامة لمن يخالف ذلك، كما اشترط المشرع نشر الحكم لمن يثبت ضده مخالفة القانون على أن ينشر في جريدتين واسعتي الانتشار وذلك علي نفقة من صدر ضده الحكم بالإدانة(١).

وبرغم تلك النصوص القانونية المتفرقة التي تعالج بعض مظاهر الحق في الخصوصية في مجالات محددة، إلى أننا نحث المشرع المصري بضرورة الإسراع لمعالجة ذلك النقص التشريعي حيال حماية البيانات الشخصية من خلال إصدار قانون ينظم طرق جمع البيانات من خلال الوسائل المشروعة، ويحدد كيفية الحفاظ عليها، وطرق معالجتها وضوابط المعالجة، ويكفل الحماية القانونية اللازمة لمنع التعدي عليها.

(١) راجع قانون التوقيع الالكتروني المصري رقم ١٥ لعام ٢٠١٤.

المطلب الثاني

مدى ملائمة قوانين معالجة البيانات الشخصية لضمان الحماية عبر وسائل الاتصال والتواصل

بينا أن مطلع السبعينيات كان النواة لانطلاق وتيرة الاهتمام الدولي والوطني بحماية الخصوصية من مخاطر التكنولوجيا الحديثة، بمظاهرها المستحدثة في مجالات الاتصال والتواصل، الأمر الذي انطلقت منه مفاهيم حماية البيانات الخاصة من مخاطر التقنية، انتهاء بوضع العديد من القواعد التي يمكن أن نطلق عليها الشرعة الدولية لحماية البيانات، أو دستور خصوصية المعلومات الشخصية في العصر الرقمي.

حاولت الدول من خلال تلك القواعد السابقة تكريس مفهوم خصوصية المعلومات، وإقامة التوازن بين هذا الحق وبين الحق في تدفق المعلومات عبر الحدود من ناحية، وبين الحاجة لتوظيف التكنولوجيا في الأنشطة الإدارية والخدمية والإنتاجية من ناحية أخرى، مما اقتضى ضرورة وضع معيار توازن مقبول، باعتبار أن الخصوصية في حقيقتها قيد على حق الوصول للمعلومات.

ولا شك أن تطبيق معيار التوازن بين حقان متعارضان في طبيعتهم أمر تشوبه بعض الصعوبات، إذ ثمة تناقضات متعددة تسبب هذه الإشكالية، ومن صور ذلك:

١- التناقض بين حرمة الحياة الخاصة للأفراد، وبين حق الدولة في الاطلاع على شئون الأفراد من أجل حماية مقتضيات الصالح العام، ولكن على نحو يتناقض مع صون حياته الخاصة واحترامها.

٢- التناقض بين حق الفرد في الحفاظ على سريته، ومصلحته في كشف حياته الخاصة ليتمتع بثمار هذا الكشف.

٣- التناقض بين الحياة الشخصية وبين الحق في جمع المعلومات لغايات البحث العلمي.

٤- التناقض بين الحق في الحياة الخاصة وحرية الصحافة وتبادل المعلومات.

ومن ثم فإن القواعد السابقة التي وضعت من أجل حماية معالجة البيانات الشخصية قد تبدو قاصرة عن توفير حماية كاملة للبيانات الشخصية. فإذا كانت الجهود التنظيمية، الإدارية، والتشريعية السابقة قد سعت إلى إقامة التوازن بين هذه الحقوق المتعارضة فإن استخدام التقنية في ميدان جمع ومعالجة البيانات، قد خلق واقعا صعبا هدد معيار التوازن، وعمق حدة التناقضات السابقة، فمن غير المقبول التفريط في حماية خصوصية البيانات الشخصية بذريعة الحق في الوصول إلى المعلومات.

من ناحية ثانية، وفيما يخص حماية البيانات الشخصية عبر وسائل الاتصال الحديثة ومواقع التواصل، فلا تبدو ثمة حماية توفرها القوانين السابقة، فالمعلومات الشخصية عن الشخص التي يشاركها مع أشخاص أخريين عبر وسائل التواصل الاجتماعي لغايات شخصية تكون خارج دائرة الحماية بموجب القوانين الأوروبية المتعلقة بالبيانات الشخصية. حيث أعدت هذه القوانين لحماية الأفراد من معالجة البيانات من قبل الحكومات والشركات التجارية، وليس لتقليص الاتصالات بين الأفراد وتقييد نقل المعلومات بينهم، ومن ثم فلا تحمي هذه القوانين الفرد من نفسه ولا ممن يتعامل معهم[1].

(1) Lothar Determann, Social Media Privacy: A Dozen Myths and Facts, 2012 STANFORD TECHNOLOGY LAW REVIEW. 7 , p 3. http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf

وفقا لذلك فإن البيانات والمعلومات التي يضعها مستخدم وسائل التواصل على صفحته الشخصية لا تكون محمية بموجب قوانين معالجة البيانات، إلا إذا عمدت الجهات المسئولة عن إدارة مواقع التواصل إلى معالجة مجموع تلك البيانات التي تخص المستخدمين والتصرف فيها. فهنا فقط يكون للمستخدم حق الاعتراض لأسباب مشروعة على معالجة بياناته الشخصية، ما لم يكن قد وافق على ذلك، أو كان القانون يجيز ذلك. كما يكون له الحق في الاطلاع على بياناته المعالجة وعلى غايات المعالجة ومصدر البيانات والأشخاص المرسلة إليهم، وله حق طلب تصحيح بياناته الشخصية وتحديثها ومحوها وإكمالها حال اتضح له عدم صحتها، أو عدم توافقها مع مقتضيات المعالجة.

كما أن مقاربة الولايات المتحدة بشأن مفهوم البيانات الشخصية وتنظيم معالجتها وسبل حمايتها، تبدو مقاربة ليبرالية، قائمة على تفضيل حرية التعبير عن الرأي، ولا توفر سوى حماية قاصرة للبيانات الشخصية، والتي تعتبرها من قبل المعلومات العامة أو الأموال ضمن نطاق التجارة. فالخصوصية محمية بوجه الأشخاص العاملين بالقطاع العام وليس بوجه أشخاص القطاع الخاص إلا على نحو ضعيف على أساس قواعد المسئولية التقصيرية المدنية، ويترك للسوق تنظيم ذاته بذاته، وبالتالي على المستخدم اختيار المشغل بالاستناد إلى التوازن الذي يرغب في إقامته بين الخدمة المقدمة له والبيانات الشخصية المقدمة منه كمقابل لما يحصل عليه من خدمات[1]. ويضيق نطاق حماية البيانات الشخصية في الولايات الأمريكية فقط لبعض المخاطر القاهرة الخاصة ومن خلال قوانين حماية المستهلك، وبعض النصوص المتفرقة، ومنها

(1) Guillaume Florimond, Droit et Internet, De la logique internationaliste à la logique réaliste, Bibliothèque des thèses, Editions Mare & martin, 2016, p 347.

القوانين المتعلقة بالإبلاغ عن خرق البيانات، ذلك على خلاف القوانين الأوروبية التي لا تميز بين المخاطر الخاصة والصناعات وأنواع البيانات في نطاق حماية البيانات الشخصية. دفع ذلك الاختلاف بالمفوضية الأوروبية إلى عقد اتفاق مع الإدارة الأمريكية في عام ٢٠١٦ سمي "Privacy Shield" يسمح باحترام الحقوق الأساسية للمواطنين الأوربيين عند معالجة بياناتهم الشخصية في الولايات المتحدة[١]. حيث يعطي هذا الاتفاق بعض الموطنين الأوربيين المتواجدين على أرض الولايات المتحدة الحقوق المنصوص عليها في التوجيه الرئاسي حول الحياة الخاصة الصادر عام ٢٠١٤، والمنصوص عليها كذلك بالقانون الأمريكي لعام ١٩٧٤ جول الخصوصية المسمي"Privacy act "، والذي يعطي المواطنين الأمريكيين حق الاطلاع والطعن أو الاعتراض على ما يجمعه الأمن الوطني من معلومات، وذلك حال استخدام بياناتهم الشخصية بوجه غير مشروع، بالنظر إلى أن البيانات الشخصية المجمعة في أوروبا من قبل وسائل التواصل الاجتماعي الأمريكية يتم تخزينها في الولايات المتحدة للاستعانة بها عند الحاجة.

كما يبدو ضعف حماية القوانين الأوروبية للبيانات الشخصية من خلال مطالعة حكم محكمة العدل الأوروبية في عام ٢٠٠٣ الذي اعتبر منع تصدير البيانات الشخصية لا ينطبق على المواقع الإلكترونية، كما اعتبر أن وضع بيانات شخصية على موقع إلكتروني مستضاف ضمن الاتحاد الأوروبي لا يشكل نقلا لتلك البيانات، ولو أمكن الوصول إليها عبر الانترنت من قبل أشخاص ينتمون لدول أخرى[٢].

(1) Garance Mathias, Données personnelles: votre conformité, Janvier 2017, p. 5. http://www.avocats-mathias.com

(2) Cour de justice des communautés européennes, cité dans: Fabrice Mattatia, Internet et les réseaux sociaux, que dit la loi? Eyrolles, 2ème édition, 2016, p 64.

وفي عام ٢٠٠٩ ، أصدرت المحكمة الأوروبية لحقوق الإنسان حكمها بأن المعلومات في حال السماح بإيصالها لمعارفه من الجمهور من قبل الشخص المعني ذاته، فإنها تفقد صفة السرية، وتصبح متاحة بحرية[1]. الأمر الذي يعني أن قيام الشخص بنشر بياناته على وسائل التواصل الاجتماعي من شأنه أن يضعف حقه في حماية حياته الخاصة.

ويؤخذ على هذا الحكم الأخير أنه نفي عن البيانات الشخصية وصف السرية لمجرد نشرها بمعرفة الشخص المعني ولو كان النشر لطائفة محددة من معارفه أو أصدقائه، الأمر غير الصحيح ، إذ يجب تقدير مدى رغبة المستخدم في إفشاء بياناته من عدمه في ضوء إعدادات الخصوصية المطبقة منه على هذه البيانات عبر وسائل التواصل، فإن قيدها المستخدم في دائرة مجموعة خاصة من المستخدمين فقط، فلا يعتبر أنه أفشاها أو أنه يسمح ضمنيا بجعلها بيانات عامة متاحة للجميع.

أيضا يبدو ضعف الحماية من إقرار التوجيه الأوربي رقم ٥٨ لسنة ٢٠٠٢، المتعلق بمعالجة البيانات الشخصية وحماية الحياة الخاصة في قطاع الاتصالات الإلكترونية، لحق الشركات في وضع الكعكات على حواسب المستخدمين لأهداف مشروعة، بعد اطلاع المستخدمين بشكل واضح ومحدد على هذه الأهداف، وعلى ماهية المعلومات المنزلة على حواسبهم، وإن كان من حق المستخدم أن يطالب بمنع وضع هذه الكعكات. ومع النقد الشديد لهذا التوجه فرض الاتحاد الأوروبي على الشركات بموجب التعديل الحاصل في عام ٢٠٠٩ ضرورة الحصول على الموافقة المسبقة للمستخدمين قبل وضع الكعكات على حواسبهم لأغراض تجارية وتسويقية.

---

(1) Cour Européenne des droits de l'homme, 23 juillet 2009 n° 12268/03, Hachette Filipacchi Associés (Ici Paris) c/ France.

كذا فرض التوجيه الأوروبي على الدول الأعضاء ضرورة تضمين التشريعات الوطنية قواعد تضمن سرية الاتصالات ومعلومات حركة البيانات من خلال شبكة الاتصالات العامة، بحيث يمتنع على أي شخص غير المستخدم الاستماع أو اعتراض أو تخزين الاتصالات ومعلومات حركة البيانات أو مراقبتها دون موافقة المستخدم، إلا إذا كان الشخص المذكور مصرح له بموجب القانون لضرورات الأمن والدفاع الوطني، أو لملاحقة الجرائم أو لردعها. ولكن لا يُمنع التخزين التقني الضروري لسير الاتصال دون التعرض لسرية البيانات.

ورغم كل التوصيات السابقة فما زالت انتهاكات خصوصية البيانات ظاهرة منتشرة، حيث لا تحترم المواقع الإلكترونية التي تجمع بيانات شخصية إلا بالحد الأدنى من التوصيات السابقة، أثناء معالجتها للبيانات الشخصية، فهذه المواقع تعرف غايات المعالجة بشكل عام وواسع، مع حفظ حقها بهامش معين لجهة تعديل غايات المعالجة ولو ضمن إطار الغايات العامة المعلن عنها سابقا.

المبحث الثاني
وسائل مواجهة الاعتداءات على البيانات الشخصية
في عصر التواصل والاتصال

نعرض في هذا المبحث للضمانات المتاحة أمام صاحب البيانات الشخصية لتوقي حدوث أية أضرار تلحق به نتيجة الاعتداء على بياناته ومعلوماته الشخصية، كإجراءات وقائية، لا تتطلب انتظار وقوع الضرر حتى يبدأ المعتدى على بياناته بالمطالبة بالحماية، كما نعرض أيضا للحماية المدنية التي توفرها قواعد المسئولية المدنية، حال وقوع الأضرار التي تترتب على انتهاك خصوصية البيانات الشخصية للأفراد، وذلك من خلال ما يلي :

المطلب الأول: الحماية الوقائية للبيانات الشخصية من مخاطر تقنيات الاتصال الحديثة.

المطلب الثاني: المسئولية المدنية عن الأضرار التي تسببها تقنيات الاتصال الحديثة.

المطلب الأول
الحماية الوقائية للبيانات الشخصية من مخاطر تقنيات الاتصال الحديثة

لمواجهة الاعتداءات المختلفة التي تقع على البيانات الشخصية، سواء أكانت بالتجسس أو السرقة أو التحايل أو التدمير والإتلاف أو بأي من صور الاعتداء التي

تعرضنا لها سابقاً؛ فقد اتخذت وسائل فنية (الفرع الأول)، وأخرى إدارية (الفرع الثاني) من شأنها توفير حماية وقائية للبيانات الشخصية من مخاطر الاعتداء.

الفرع الأول

الوسائل الفنية لمواجهة الاعتداءات على البيانات الشخصية

نتيجة التطور المستمر لطرق وأساليب الاعتداء على البيانات الشخصية، فكان لزاماً أن تتطور في مقابلها وسائل وطرق فنية للحماية، ومن هنا حرص المسئولين عن أنظمة الاتصال ومواقع التواصل الحديثة على الاهتمام بأمنها وحمايتها من كافة المخاطر المحتملة. تلك الحماية الفنية يمكن تحقيقها من خلال استخدام كلمة السر ضد الاختراقات التي انتشرت بوسائل التقنية الحديثة، ومن خلال تشفير البيانات. وذلك على النحو التالي:

أولا: استخدام كلمة السر ضد الاختراقات:

سبق أن بينا دور التطور التكنولوجي في مجال المعلومات في ظهور العديد من صور التعدي على البيانات الشخصية الخاصة للأفراد عبر مواقع التواصل الاجتماعي، أو عبر البريد الإلكتروني، بغرض التطفل أو الاطلاع غير المشروع. الأمر الذي جعل حق الأفراد في التحكم بدقة معلوماتهم أو منع الدخول لحساباتهم محلا للخطر المحدق، حيث أصبحت عملية الدخول في استطاعة أي شخص عبر شبكات الإنترنت.

لمواجهة ذلك عمد المسؤليين عن أنظمة الاتصال والتواصل الحديثة إلى إنشاء نظام حماية وقائية يعتمد على إنشاء المستخدم لكلمة سر لا يعرفها أحداً سواه، بحيث لا يتمكن غيره من الدخول لحسابه عبر البريد الإلكتروني أو عبر وسائل التواصل الاجتماعي، ومن ثم العبث ببياناته أو القيام بانتهاكها.

في ضوء ذلك اهتم الباحثين والمختصين بشفرات الكمبيوتر وأجهزة الاتصال باستخدام تقنيات جديدة لكلمات سر قوية يصعب اختراقها أو الوصول إليها، حيث اتجهت بعض الشركات وعلى رأسها شركة "مايكروسوفت" العملاقة لاستبدال كلمات السر التقليدية بأشكال من الصور التي تكون أسهل في الحفظ وأصعب في الاختراق. وتتنوع كلمات السر المستخدمة ما بين الأحرف أو الأرقام أو الرموز.

بيد أن تلك الوسيلة الفنية وكأثر للتطور التقني باتت غير كافية لمواجهة خطر الاختراق، حيث يتمكن "الهاكرز" حاليا من معرفتها أو الوصول إليها بسهولة.

ثانيا: تشفير البيانات:

يعرف التشفير بأنه عملية تحويل البيانات إلى شفرات غير مفهومة – تبدو غير ذات معنى- من أجل منع الأشخاص غير المرخص لهم من الاطلاع على البيانات أو حتى فهمها، ومن ثم تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة.

ومن المؤكد أن بيئة الإنترنت أصبحت المجال الأضخم لنقل البيانات والمعلومات، لذا كان من الضروري العمل على نقل البيانات الحساسة التي تخص المعاملات المالية بصيغة مشفرة من أجل الحفاظ على سريتها وتأمينها من عبث المتطفلين والمخربين والمعتديين.

وتعتمد قوة وفعالية التشفير على عاملين أساسيين، الخوارزمية، وطول المفتاح مقدرا بالبت (Bet)، ويعاد فك التشفير عبر إعادة تحويل البيانات إلى صيغتها الأصلية، وذلك باستخدام المفتاح المناسب لفك الشفرة. وينقسم نظام التشفير إلى نوعيين:

النوع الأول: التشفير المتماثل (التناظري)

وهو نوع من التشفير الذي يفتحه مفتاح واحد متعارف عليه يطلق عليه المفتاح السري، بحيث يستخدم كل من المرسل والمستقبل المفتاح السري ذاته في تشفير الرسالة أو البيانات المتداولة وفكها. ويتفق الطرفان في البداية على عبارة المرور (passphrase) التي سيتم استخدامها.

وبعد استقبال الرسالة المشفرة، يستخدم المستقبل عبارة المرور نفسها من أجل فك شفرة النص المشفر[١]. بيد أن عملية تبادل المفتاح السري يصاحبها عدم الأمان، مما أدى لتراجع استخدام هذا النوع من التشفير واعتباره من ذكريات الماضي.

النوع الثاني: التشفير اللامتماثل (المفتاح العام)

يعتبر هذا النظام أكثر أمنا من سابقه، فعوضا عن استخدام مفتاح واحد يتبادله الطرفان، يستخدم التشفير اللامثماثل مفتاحين اثنين تربط بينهما علاقة، أحدهما مفتاحا عاما، والآخر مفتاحا خاصا، بحيث يكون المفتاح الخاص معروفا لدى جهة واحدة فقط أو شخص واحد فقط، وهو المرسل، يستخدم لتشفير البيانات ولفك تشفيرها، أما المفتاح العام فيكون معروفا لدى أكثر من شخص أو جهة ، ويستطيع المفتاح العام فك شفرة الرسالة التي شفرها المفتاح الخاص.

بيد أنه يؤخذ على هذا النظام من التشفير بطئه إذ أن جلسة التشفير وجلسة فك التشفير يجب أن تكونا متزامنتين تقريبا[٢].

---

(١) م. حسام شوقي: حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠٠٣، ص٩٨ وما بعدها.

(٢) م. حسام شوقي: المرجع السابق، ص ١٠٠.

وحاليا أصبح هناك مجموعة من المعايير المتبعة في أنظمة التشفير المتفق عليها على مستوى العالم منها ANSIX وهو نظام طورته لجنة خاصة كانت تابعة لمؤسسة المعايير الأمريكية الوطنية بهدف توفير الحماية اللازمة للصناعات المصرفية، وبشكل خاص لحماية الرقم الشخصي السري PIN ومعالجة الشيكات والتحويل الإلكتروني للأموال والبيانات.

وعلى الرغم من أن نظام التشفير هدفه منع الاطلاع على محتويات الرسالة وتأمين خصوصياتها، إلا أن إمكانية العبث بمضمون الرسالة مازال قائماً، حيث بدا قصور التشفير كوسيلة للأمان التقني، وبدت الحاجة ماسة للبحث عن أنظمة بديلة تحقق الحماية؛ فظهر نظام البصمة الإلكترونية للرسائل، وأعقبه ظهور تقنية الغفلية، أو ما أطلق عليه " أجهزة معاودة الإرسال بشكل مغفل"، والذي أعد من أجل توفير حماية فاعلة من التهديد الدائم على خصوصية وأمن المستخدمين، خاصة في مجال الحق في احترام سرية الاتصالات، وتبادل البيانات عبر الشبكة، حيث تتيح هذه الوسيلة الحماية للمستخدمين في سرية اتصالاتهم، وغالبا ما تؤتي تلك الوسيلة ثمارها في منتديات المناقشة، والمجموعات الإخبارية التي تتضمن بيانات أو معلومات يحرص أصحابها على التستر عليها لأسباب شخصية. فتحول دون قيام الغير بجمع أو تحليل أو استغلال بيانات شخصية دون رضاء صاحبها أو موافقته الصريحة. وكعادة البشر في استغلال الجوانب السلبية للأنظمة على حساب جوانبها الإيجابية، فقد استغل بعض المستخدمين تلك الخاصية استغلالاً غير مشروع عبر شبكة الإنترنت في إرسال رسائل تحريضية أو تشهيرية.

لهذا السبب ظهر بروتوكول الإنترنت، الذي بمقتضاه استوجب عنونة البيانات في الشبكة يمكن من خلالها معرفة الموزع الذي استعمله المستخدم للاتصال بالمواقع الأخرى الموصولة بشبكة الإنترنت(١).

ولن ندخل في عمق التفصيلات التقنية للحماية، حتى لا نخرج كثيرا عن الإطار القانوني. بيد أننا نتساءل عن إلزامية الحماية التقنية، وهل استعمالها شرطاً لإضفاء الحماية القانونية؟

نتفق مع غالبية الفقه القانوني في أن الحماية الفنية أو وضع نظام أمني فني لحماية شبكات الاتصال، يعد إجراءً ضروريا، باعتبار أن القانون يجُرم الاعتداء على نظم الأمن المتضمنة أو المندمجة في النظام المعلوماتي، فمن باب أولى عدم العقاب على فعل لم يتخذ صاحبه وسائل الحيطة اللازمة، كما أن توافر الحماية يكون من شأنه إقامة الدليل على خطورة وسوء نية القائم بالاعتداء الإلكتروني، ومن ثم الأخذ بها كقرينة في مجال الإثبات (٢).

الفرع الثاني

الوسائل الإدارية لمواجهة الاعتداءات على البيانات الشخصية

بينا فيما سبق، أن قوانين معالجة البيانات، أعطت الحرية لكل فرد في الاطلاع على المعلومات حيث يشاء وفي أي وقت، غير أنها أوردت بعض القيود المتعلقة

(١) م. حسام شوقي: المرجع السابق، ص١٠٥. ولمزيد من التفصيلات راجع الموقع التالي: http//www.dejanews.com

(٢) د. علي عبد الله القهوجي، الحماية الجنائية، للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، مايو ٢٠٠٨؛ د. عبد الفتاح بيومي حجازي، الحماية الفنية والجنائية لنظام الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣، ص٤١.

بطبيعة ومضمون هذه المعلومات، إذ يجب أن تخلو مادة المعلومة من أي مسخ للهوية والثقافة الإنسانية للشعوب، أو ما يشكل اعتداءات على الحريات الشخصية. دفع ذلك بعض الدول لفرض قيوداً لمواجهة الاعتداء على الحياة الشخصية للأفراد، ومن ذلك الرقابة على البيانات والمعلومات الشخصية في الحاسبات الإلكترونية، والضوابط والإجراءات الإدارية على البيانات الشخصية.

أولا: الرقابة على البيانات الشخصية:

أصبحت بياناتنا الشخصية تملأ مختلف وسائل الاتصال والتواصل الحديثة الفردية منها والاجتماعية عبر أدواتها المختلفة سواء أكانت حواسب آلية أو أجهزة اتصال محمولة، وحفاظا على هذه البيانات من الاعتداء، وضعت الجهات الإدارية بعض الضمانات للرقابة على هذه المعلومات، تتراوح ما بين ضمانات إدارية، وضمانات قضائية.

١- **الضمانات الإدارية:**

أنشئت فرنسا لجنة مستقلة خاصة (اللجنة الوطنية للمعلومات والحريات) يناط بها الإشراف على توافر احترام القواعد المقررة لحماية الحرية الشخصية من إساءة استخدام البيانات الشخصية، والعمل على تحسين هذه القواعد بما يتلاءم والخبرة والتطور الفني، وأحيط أعضاء هذه اللجنة بجميع الضمانات التي تكفل استقرارها.

وتضم اللجنة مختلف التخصصات من الفقهاء والقانونيين، وعلماء الإعلام، لكي لا يكون اختصاصها محل نزاع من حيث القانون والأساليب الفنية، والأنشطة التي تقوم بها هذه اللجنة تتضمن اتخاذ القرارات وممارسة الرقابة على البيانات، كما يجوز للحكومة أن تفوض جزء من سلطاتها التنظيمية إلى هذه اللجنة.

وتقوم اللجنة بدور الهيئة الاستشارية، إذ يمكنها أن تقترح على الحكومة بعض الآراء التي ترى اللجنة بأنها كفيلة بالتشريع والتنظيم، كما يمكن لها أن تصدر عددا من القرارات الفردية تحت رقابة القضاء.

ويتعين على اللجنة إخطار كل الأشخاص المعنية والمسئولين عن المعالجات للبيانات ذات الطبيعة الشخصية بحقوقهم والتزاماتهم المنصوص عليها في القانون، وتلتزم اللجنة بالنسبة للبطاقات الآلية التي يتم إنشاؤها بقرار لائحي بنشر هذا القرار في الجريدة الرسمية، على أن يتضمن النشر بيانات عن الجهة المعالجة من أجل التوجه إليها للاطلاع على البيانات وطوائف البيانات المسجلة. كما يجب على اللجنة أن تسهر على احترام المعالجات التي يكون محلها بيانات شخصية لأحكام القانون(١).

كما تمارس اللجنة دور الرقابة السابقة على إنشاء المعالجات للبيانات الشخصية التي تقوم بها الأشخاص المعنوية العامة أو الخاصة التي تتولى إدارة مرفق عام من خلال سلطتها في إعطاء الإذن أو التصريح بإنشاء المعالجات للبطاقات ذات الطبيعة الشخصية، كما تتلقي اللجنة الإخطارات البسيطة بشأن المعالجات التي تتضمن اعتداء على البيانات الشخصية التي يحميها القانون(٢).

وتطلع اللجنة على التطورات في تكنولوجيا المعلومات، وتعلن عند الاقتضاء، عن تقديرها للنتائج المترتبة على ممارسة هذه التطورات على الحقوق والحريات، ومن ثم تقترح على الحكومة الإجراءات التشريعية واللائحية المناسبة لحماية الحريات في

(1) V.Jean-paul costa, « La transparence administrative », Regards sur l'Actualité septembre- octobre 1998, P.37-44.

(٢) د. شريف خاطر، المرجع السابق، ص ١٠٨.

مواجهة تلك التطورات. كما يمكن لها أن تقدم مساعدات بشأن حماية البيانات متى طلبت منها الجهات الإدارية ذلك.

كما تملك اللجنة سلطة الرقابة اللاحقة على المعالجات التي تمت، فتقوم بالتحري والتحقيق من تلقاء نفسها حال خروج أي معالجة للبيانات عن أحكام القانون

ولعبت الولايات المتحدة الأمريكية دورا حاسما في مسائل خصوصية البيانات على الصعيد العالمي ليس فقط بسبب وزنها ومكانتها الدولية، ولكن أيضا لهيمنتها الواسعة المتمثلة في الشركات التي تقدم خدمات الإنترنت، حيث تتخذ معظم شركات التزويد بخدمات الإنترنت التي أصبح لها نفوذ عالمي من الولايات المتحدة مقرا لها – مثل (جوجل – الفيسبوك – ياهو – يوتيوب- توتير- وويكيبيديا)، لذا كان للولايات المتحدة تاريخ طويل في مضمار توفير الحماية للخصوصية[١]، حيث وجدت وسيلتان لحماية سرية المعلومات في نظم الحاسبات الإلكترونية: إحداهما فنية (تكنولوجية) والثانية إجرائية توفر حماية أمنية وإشراف رقابي إداري على البيانات.

وأنشأ الكونجرس الأمريكي البنك القومي للمعلومات لكي يتولى رقابة البيانات الشخصية، وإن كان دوره محكوما بأمرين: الأول اللوائح التي تحظر إنشاء البيانات والمعلومات الشخصية، والثاني: أن يكون هناك ميثاق لائحي لا يسمح بإصدار أي بيانات خاصة بصفة فردية[٢].

---

(١) الحماية القانونية للبيانات الشخصية في العصر الرقمي- دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير- إعداد توبي مندل (Toby mendel) وأندرو بوديفات ( ) Andrew puddephatt ، سلسلة اليونسكو بشأن حرية الإنترنت،ص٨٧. متاح على الموقع التالي: https://books.google.com.bh/books .

(٢) شمس الدين إبراهيم أحمد، المرجع السابق، ص١٦٦، وما بعدها.

وقد اعترف القانون الأمريكي لأكثر من قرن بالضرر الناتج عن انتهاك الخصوصية، والذي يمنح الحق في مقاضاة الجهات الخاصة والعامة. وثمة أربع إجراءات قانونية مكفولة بشأن الخصوصية فيما يتعلق بحالة التدخل غير المبرر في عزلة الفرد، واستغلال الاسم أو الشبه، والدعاية التي تروج للفرد شهرة كاذبة والدعاية غير المعقولة لحياة المرء الخاصة. ويضع قانون الخصوصية لسنة ١٩٧٤ نظاما لحماية البيانات، ولكن ينحصر على السلطات العامة فقط، أما الهيئات الخاصة فلها في معظم الأحيان حرية وضع معايير الخصوصية الخاصة بها، وفي كثير من النواحي تتشابه قيم ومبادئ حماية البيانات الأساسية التي يقوم عليها قانون الخصوصية لتلك التي تضمنها توجيه الاتحاد الأوروبي لحماية البيانات، وإن اختلفت في نطاق التطبيق.

كما أنه يوجد بالولايات المتحدة الأمريكية عدد كبير من البرامج النظامية في الولايات المتحدة؛ فينص قانون خصوصية الاتصالات الإلكترونية لسنة ١٩٨٦ (ECPA) والذي طبق تشريعات التصنت التقليدية في عصر الانترنت على الحماية للاتصالات الإلكترونية، وينقسم إلى ثلاثة أجزاء أو أبواب وهي قانون التنصت، وقانون الاتصالات المخزنة، وقانون سجل أرقام الاتصال، حيث يضمن الباب الأول سرية الاتصالات أثناء نقلها، ويضمن الباب الثاني سرية الاتصالات المخزنة، بينما يحظر الثالث تعقب الرسائل الصادرة والواردة. بيد أن قانون الأمن الوطني لعام ٢٠٠٢ ما لبث أن أضعف من نطاق الحماية وفقا للأبواب السابقة لا سيما من خلال توسيع صلاحيات الاعتراض لأغراض الأمن وتنفيذ القانون.

في عام ١٩٩٤ اعتمدت الولايات المتحدة قانون حماية خصوصية السائق استجابة لبيع سجلات السيارات، بما فيها من الكثير من البيانات الشخصية الحساسة مثل أرقام الهاتف والعناوين والتفاصيل الشخصية والمعلومات الطبية، التي تسببت في

مقتل إحدى الممثلات الشهيرات. كما يجرم أيضا قانون سجلات التليفون وحماية الخصوصية لسنة ٢٠٠٦ استخدام ذريعة كاذبة للحصول على بيع أو شراء السجلات الهاتفية الشخصية، كما يشترط قانون حماية خصوصية الأطفال على الإنترنت لسنة ٢٠٠٠ (COPPA) موافقة أولياء الأمور قبل جمع معلومات الأطفال دون سن ١٢ عام، كما يشترط على المواقع ضرورة وضع سياسات خصوصية، ومن ثم العمل على أساس نهج يقوم على التنظيم الذاتي.

وإلى الآن رفضت الولايات المتحدة الأمريكية اعتماد قواعد الاحتفاظ بالبيانات على غرار قواعد الاحتفاظ المنصوص عليها في التوجيه الأوروبي، وإن كانت قد اقترحت مشاريع قوانين تسمح بالاحتفاظ بالبيانات الشخصية مثل قانون منع الانترنت من تسهيل استغلال البالغين لشباب اليوم لسنة ٢٠٠٩، والذي تم اقتراحه لكنه لم يعتمد؛ حيث كان هذا القانون سيسمح لمقدمي خدمات الاتصالات الاحتفاظ لمدة لا تقل عن سنتين بكافة السجلات أو المعلومات الأخرى المتعلقة بهوية أي مستخدم(١).

وفي مصر وتحديدا في عام ٢٠٠٢ قررت وزارة الداخلية إنشاء إدارة لمكافحة الجرائم المعلوماتية، أطلقت عليها اسم إدارة مباحث مكافحة جرائم الحاسبات وشبكات المعلومات، تكون وظيفتها متابعة ورصد وضبط الجرائم الإلكترونية المستحدثة، وكل أشكال الاعتداءات على شبكات المعلومات وقواعد البيانات، وجرائم التخريب والفيروسات والاختراقات التي يكون الكمبيوتر عنصرا في ارتكابها.

---

(١) الحماية القانونية للبيانات الشخصية في العصر الرقمي- دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير- إعداد توبي مندل (Toby mendel) وأندرو بوديفات ( ) Andrew puddephatt ، سلسلة اليونسكو بشأن حرية الإنترنت ٨٨، ٨٩. متاح على الموقع التالي: https://books.google.com.bh/books .

٢- **الضمانات القضائية**:

منح المشرع الفرنسي للجنة الوطنية للمعلومات والحريات سلطة توجيه الإنذار والتحذير للمسئول عن المعالجة للبيانات، حال عدم احترامه لأحكام قانون ٦ يناير ١٩٧٨، وقد استخدمت اللجنة تلك السلطات في العديد من الحالات، حيث قامت اللجنة بتوجيه الإنذار عام ١٩٨٤ لبعض منظمات الإسكان المنخفض HLM بسبب قيامها باستخدام بطاقات المستأجرين لأغراض سياسية، كما قامت بتوجيه إنذارات أيضا في ذات العام إلى شركة كهرباء فرنسا وشركة غاز فرنسا لعدم اتخاذها الاحتياطات الضرورية للحفاظ على البيانات المدرجة ببطاقات موظفيها، الأمر الذي أدي إلى استغلال تلك البيانات من جانب أنصار الحزب الشيوعي في الدعاية النقابية، وفي العام ١٩٩٠ وجهت اللجنة إنذارا إلى رئيس المجلس الإقليمي لنقابة الأطباء عقب استخدام بطاقات الأطباء لإرسال دعوات لهم لطلب المشاركة في مظاهرة سياسية.

ونرى من جانبنا ضعف تلك السلطة القضائية التي منحها المشرع الفرنسي للجنة المذكورة، فلا تملك اللجنة سوى توجيه الإنذار حال مخالفة أحكام القانون، فضلا عن أن سلطتها في إخطار النيابة العامة مقيد بضرورة كون الاعتداء على البيانات يمثل جريمة جنائية، وبالتالي لا تملك اللجنة سلطة توجيه أية أوامر للجهة الإدارية المخالفة، أو توقيع جزاءات على المخالفين لأحكام القانون.

لذا فنرى أن ضعف تلك الضمانة القضائية كان مبررا لما قام به المشرع الفرنسي من تعديل لنص المادة ٤٥ من القانون الصادر في ٦ يناير ١٩٧٨، بمقتضي القانون الصادر في ٢٩ مارس ٢٠١١، والذي وسع بمقتضاه نطاق السلطات القضائية للجنة الوطنية للمعلومات والحريات، حيث أضاف لها بعض الصلاحيات التي تمكنها من توجيه تحذيرات للمسئول عن معالجة البيانات الشخصية حال عدم التزامه أحكام

القانون، ويكون لهذا التحذير صفة الجزاء[١]. ويمكن لرئيس اللجنة أن يوجه إنذارا للمسئول عن المعالجات بضرورة احترام القانون والتوقف عن المخالفات خلال مدة يحددها، ويكون للإنذار الموجه من اللجنة صفة الجزاء أيضا.

ومن جانبنا نرى أنه، بالنظر إلى استقرار الرأي على إسباغ وصف الجزاء على التحذير والإنذار التي توجهه اللجنة المذكورة؛ فإنه يجب على اللجنة بالمقابل أن تراعي حقوق الدفاع وضماناته لمن يوجه إليه الاتهام بمخالفة أحكام قانون ٦ يناير لسنة ١٩٧٨.

وإذا لم تحترم الجهة المخالفة الإنذار الموجه إليها، بل استمرت في ارتكاب اعتداءاتها، فقد أعطى القانون الصادر في ٢٩ مارس ٢٠٠١، للجنة سلطة توقيع بعض الجزاءات الآتية [٢]:

١- توقيع غرامة مالية تختلف بحسب جسامة المخالفة وخطورة الاعتداء علي البيانات، بحيث لا تتجاوز قيمة الغرامة في المرة الأولى ١٥٠ ألف يورو، وفي حال تكرار المخالفة خلال الخمس سنوات التالية على تاريخ وقوع المخالفة الأولى تضاعف الغرامة، بحيث لا تتجاوز ٣٠٠ ألف يورو، ويكون قرار توقيع الغرامة من قبل اللجنة نهائيا، لا يجوز الطعن عليه أو التظلم منه.

---

(1) l'Article 45 de la loi du 6 janvier 1978, Modifié par la loi n° 2011-334 du 29-03-2011 art 8.

(٢) من الجدير بالذكر أن تلك السلطة الممنوحة للجنة الوطنية للمعلومات والحريات في توقيع الجزاءات، يمكن تطبيقها في مواجهة عمليات المعالجة التي تتم كلها أو جزء منها على الإقليم الفرنسي، وكذلك في مواجهة المسئول عن المعالجات التي تتم على إقليم دولة أخرى تكون عضوا في الاتحاد الأوروبي. أنظر نص المادة ٤٨ من قانون ٦ يناير ١٩٧٨، المعدل بمقتضى قانون ٢٩ مارس ٢٠١١.

بيد أنه يلاحظ أن السلطة القضائية للجنة المذكورة تظل قاصرة، حيث أن المشرع استثنى الحالة التي تتم فيها المعالجات بواسطة الدولة، حيث لا تملك اللجنة فرض جزاءات مالية على الدولة ولو ثبت حدوث اعتداء على البيانات أو مخالفة الدولة لأحكام قانون ٦ يناير ١٩٧٨.

٢- يكون للجنة المذكورة أن تصدر أمراً بوقف المعالجات التي تتضمن اعتداءً على البيانات أو حال مخالفة أحكام نص المادة ٢٢ من القانون.

وإذا ما نتج عن تنفيذ المعالجة أو استغلال البيانات الشخصية أي اعتداء على الحقوق والحريات، فيكون للجنة بعد إتباع الإجراءات الحضورية، أن تلجأ لإصدار بعض الإجراءات المستعجلة التي تتمثل في إصدار قرار بوقف تنفيذ المعالجة لمدة لا تتجاوز ٣ أشهر، باستثناء المعالجات التي تقوم بها الدولة، كما يحق لها بعد القيام بتحذير المخالف أن تصدر قراراً بغلق بعض البيانات الشخصية المعالجة لمدة ٣ أشهر[١].

وإذا اتضح للجنة خطورة الاعتداء الواقع على البيانات الشخصية؛ كان من حق رئيس اللجنة أن يطلب بالطريق المستعجل من القاضي المختص اتخاذ كافة الإجراءات الضرورية مع توقيع غرامة تهديدية لوقف الاعتداء [٢].

(1) l'Article 45 de la loi du 6 janvier 1978, Modifié par la loi n° 2011-334 du 29-03-2011 art 8 : I, II.

(2) l'Article 45 de la loi du 6 janvier 1978, Modifié par la loi n° 2011-334 du 29-03-2011 art 8 : III.

وغالبا ما تلجأ اللجنة الوطنية للمعلومات والحريات إلى إعلان قراراتها الصادرة بتوقيع أي من الجزاءات السابقة في الصحف والمجلات إضفاءً للشفافية في توقيع الجزاء(١).

ثانيا: الضوابط والإجراءات الإدارية لحماية البيانات في مجال الاتصالات:

تطورت شبكات الاتصالات في العالم كله تطورا سريعا كأثر للثورة المعلوماتية التي اجتاحت العالم، حيث أصبحت شبكات الاتصال والتواصل وسيلة هامة لسريان المعلومات وتبادل البيانات عبر إرسال وتسلم الرسائل من خلال البريد الإلكتروني وتطبيقات التواصل عبر شبكة الانترنت والاتصالات السمعية والبصرية عبر الهاتف المحمول. ومع وجود مبدأ حرية تداول المعلومات وتبادل البيانات، كان لابد من فرض رقابة على الشبكات ووسائل الاتصال تضمن احترام الخصوصية المعلوماتية.

أطلق على هذه الرقابة في فرنسا اصطلاح الرقابة الأمنية، وقد حدد المشرع حالاتها على سبيل المثال لا الحصر وذلك في المادة الثالثة من قانون ١٠ يوليو عام ١٩٩١ بشأن حرية المراسلات، والتي قصر المشرع من خلالها حق الرقابة على الحالات التي يكون هدفها الحصول على معلومات تتعلق بمسائل الأمن القومي والمحافظة على المركز العلمي والاقتصادي لفرنسا ولمكافحة الإرهاب والجريمة المنظمة. وأنشأ القانون المذكور لجنة تسمى باللجنة القومية لمراقبة التسجيلات الأمنية تختص بمراقبة صحة الإجراءات الخاصة بالمراقبة الأمنية التي قد تتم بشأن المراسلات والاتصالات التي تتم بطريق الانترنت(٢).

---

(١) د. شريف خاطر، المرجع السابق، ص ١٤٠.

(٢) د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، ٢٠٠٢، ص ٧٩.

كذلك فقد أنشأت فرنسا المجلس الأعلى للاتصالات السمعية والبصرية (C.S.A) وأوكلت إليه مهمة ضمان ممارسة حرية الاتصالات، من خلال رقابة المحتوى المعلوماتي للخدمة السمعية والبصرية، والتنبيه على حاملي تراخيص استغلال أحد المرافق السمعية والبصرية إلى ضرورة احترام الالتزامات المفروضة عليهم بواسطة القوانين واللوائح.

وهناك أيضا المجلس الأعلى للتقنيات (C.S.T) التي تمتزج فيها شبكات الاتصال بوسائل المعلوماتية، وهو مجلس استشاري لدى وزير الاتصالات السلكية واللاسلكية، أنشأ تطبيقا للقرار بقانون رقم ٢٧٤-٩٣ الصادر في ٢٥ فبراير ١٩٩٣، من أجل صياغة التوصيات ذات الطبيعة الأدبية لحماية الشباب من الخدمات التي تقدمها الاتصالات التي تمتزج فيها طرق المعلوماتية بوسائل الاتصالات السلكية واللاسلكية والمسموعة، فضلا عن دورها في الاهتمام بالعلاقة التي تربط بين القائمين على الشبكات ومستخدميها [1].

وفي أمريكا، تفجرت موجة من الجدل بشأن حق المديرين داخل الشركات والمؤسسات المختلفة في مراقبة البريد الإلكتروني الصادر والوارد من وإلى الموظفين الذين يعملون تحت إشرافهم، وذلك عقب الإعلان عن نتائج الدراسة التي أجرتها جمعية إدارة الموارد البشرية الأمريكية بالتعاون مع مجموعة ويست جروب، والتي أظهرت أن حوالي ٧٤% من الموظفين المسئولين على الموارد البشرية في شركاتهم يراقبون العاملين في الشركة، ويتمكنون من التعرف على أنواع مواقع الإنترنت التي يزورها الموظفين، ويطلعوا على مضمون الرسائل التي تصدر عبر نظمها الإلكترونية، تفاديا لانخفاض إنتاجية العمل وللتعرف على التصرفات غير اللائقة.

(١) د. شمس الدين إبراهيم أحمد، المرجع السابق، ص ١٧٠-١٧١.

فور الإعلان عن النتائج السابقة أعرب الموظفين عن عدم رضائهم، واعتبروا أن مراقبة بريدهم الإلكتروني، ومكالماتهم واتصالاتهم تمثل اعتداءا صارخا على حقهم في الخصوصية.

لذا بدت الحاجة الماسة لإيجاد هيئة مستقلة تكون لها سلطات واسعة بما يكفل لها ممارسة دورا إشرافيا ورقابيا، يكون لها القدرة على إيجاد التوافق بين أنظمة المعالجة وضمان حقوق الأفراد، والتي من بينها وأهمها الحق في حرمة خصوصية المستخدمين، بحيث تعتبر هذه الهيئة بمثابة صمام الأمان ضد الانتهاكات التي يحتمل أن تقع من جانب السلطات.

وقام المشرع الأمريكي بفرض حماية قانونية لخصوصية الأفراد أثناء عمليات الاتصال وتبادل المعلومات، وذلك بإصداره لقانون خصوصية الاتصالات الإلكترونية لعام ١٩٨٦، ويحظر هذا القانون حجز أو بث الاتصالات الإلكترونية الخاصة، حيث يجرم الدخول غير المشروع للاتصالات الإلكترونية المخزنة والمبثوثة عبر البريد الإلكتروني ومواقع التواصل، واعتبر الدخول غير المأذون لأي من هذه الحسابات بمثابة انتهاك لقانون خصوصية الاتصالات.

كما تقدم النائب الأمريكي مايكل روجرز بمشروع قانون مشاركة وحماية المعلومات الرقمية، الذي يعرف اختصارا باسم سيسبا (CISPA)، وسانده في ذلك ١١١ نائبا، وتم تمرير المشروع لمجلس النواب في ٢٦ ابريل ٢٠١٢، لكن لم يصادق عليها مجلس الشيوخ الأمريكي، وتم نقض وثيقة المشروع لافتقارها للسرية، وعدم حماية الحريات المدنية، وفي فبراير من عام ٢٠١٣ أعاد البيت الأبيض تقديم الوثيقة ومررها في ١٨ ابريل ٢٠١٣.

وانتقدت سيسبا من قبل دعاة خصوصية الإنترنت والحريات المدنية، على أساس أن سيسبا تحتوي قيودا قليلة حول كيفية وفترة مراقبة الحكومة لتصفح أي فرد للمعلومات على الإنترنت. إضافة إلى ذلك، الخوف من أن تستعمله السلطات الجديدة للتجسس على الناس بدلا من متابعة المخترقين الأشرار. وبالمقابل لقيت سيسبا الاستحسان من الشركات ومجموعات الضغط مثل مايكروسفت، فيس بوك، أي تي أند تي، أي بي إم، آبل، غرفة التجارة الأمريكية، التي تنظر إليها كوسيلة بسيطة وفعالة لمشاركة المعلومات المهمة حول تهديدات الإنترنت مع الحكومة.

المطلب الثاني

المسئولية المدنية عن الأضرار المتحققة بفعل وسائل الاتصال والتواصل الحديثة

بالنظر لكون الحصول على التعويض اللازم للأضرار التي سببتها مخاطر وسائل الاتصال والتواصل الحديثة لا يتحقق إلا من خلال رفع دعوى المسئولية المدنية. فإننا نتعرض لدراسة هذه الدعوى من خلال تقسيم هذا المبحث الي ثلاث مطالب، نخص الأول لدراسة شروط تحقق المسئولية المدنية عن الأضرار التي تسببها وسائل الاتصال والتواصل الحديثة، بينما يتعرض المطلب الثاني لأطراف دعوى المسئولية المدنية، ويناقش المطلب الثالث آثار دعوى المسئولية المدنية عن أضرار وسائل الاتصال والتواصل الحديثة.

الفرع الأول

شروط تحقق المسئولية المدنية عن الأضرار الناشئة بفعل استخدام وسائل الاتصال والتواصل الحديثة

وفقا للقاعدة التقليدية في مجال المسئولية المدنية فإن كل خطأ سبب الضرر للغير يلزم محدثه بالتعويض[١]، بيد أنه بالنظر لخصوصية المجال الذي تستخدم من خلاله وسائل الاتصال والتواصل، وهو بلا شك مجال تقني معقد، الأمر الذي يثير التساؤل حول مدي ملائمة الشروط التقليدية للمسئولية المدنية لانعقاد المسئولية المدنية في هذا المجال

أولا: مدي ملائمة اشتراط الخطأ لتحقق المسئولية المدنية في مجال الاتصال والتواصل:

يمكن تعريف الخطأ في مجال شبكات الاتصال والتواصل بأنه" كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح يرتبط بالمعالجة الآلية للبيانات أو نقلها أو انتهاكها"[٢]، كما يمكن تعريفه بأنه عمل غير قانوني يستخدم فيه الحاسب الآلي كأداة أو كموضوع للاعتداء على البيانات الشخصية للمستخدمين[٣].

وبالتالي فإن الخطأ هنا ينصب علي كل فعل غير مشروع يمثل اعتداءً على

(١) أنظر نص المادة ١٦٣ من القانون المدني المصري، يقابلها نص المادة ٢٥٦ من القانون المدني الأردني، والمادة ١٥٨ من القانون المدني البحريني.

(٢) د.محمد الشوا، ثورة المعلومات وانعكاسها علي قانون العقوبات، دار النهضة العربية، الطبعة الثانية، القاهرة، ٢٠٠٠ ،ص٧.

(٣) د. ذياب موسي البداينة،جرائم الحاسب والانترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، جامعة نايف للعلوم الأمنية، الرياض، ١٤٢٠ هـ، ص١٠٢.

البيانات في انسيابها وتدفقها بما تمثله من أموال أو أصول أو أسرار أو معلومات شخصية.

وأصبحت هذه المعلومات والبيانات جديرة بالحماية القانونية في العصر الحديث باعتبارها مالا قابلا للتملك أو الاستغلال، على أساس قيمته الاقتصادية، وليس على أساس كيانه المادي، أيا كان الوسط المادي الذي يتضمنها، فهي تخول صاحبها ميزتين أساسيتين: تتمثل الأولى في حقه في ضمان سرية معلوماته وبياناته الشخصية، بينما تتمثل الثانية في طلب التعويض عن الأضرار التي تترتب علي أي عمل غير مشروع يتعلق بها.

ولا شك إن وقوع الخطأ كشرط أولي لتحقق المسئولية يتطلب وجود بيئة رقمية وجهاز كمبيوتر واتصال بشبكة الانترنت، ثم قيام المعتدي بتجهيز الكمبيوتر لكي يحقق له مكنة الاعتداء، فيقوم بتحميله برامج فيروسات تمهيدا لبثها، لكي تساعده في انتهاك الخصوصية، وقد يقوم بإعداد صفحات تحمل في طياتها مواد مخلة بالآداب يرسلها للمضرور، بغية خداعه للدخول إليها ومن ثم إمكانية سرقة بياناته وبيانات حسابه[1]. ومن الطرق التي تستخدم في الاعتداء علي الخصوصية والتصنت على المحادثات التي تتم عبر مواقع التواصل الاجتماعي استخدام برنامج معين يقوم بفتح نافذة على جهاز المضرور، يمكن من خلالها الاستماع إلى جميع المحادثات، والاطلاع على كافة المراسلات الصادرة والواردة إلى حساب المضرور، والتمكن من قراءة بياناته الشخصية.

(١) في مجال تكنولوجيا المعلومات، لا شك أن شراء برامج الاختراق، ومعدات فك الشفرات وكلمات المرور، وحيازة صور إباحية أو غيرها يمثل جريمة جنائية يعاقب عليها القانون.

بينما يتمثل خطأ بنك المعلومات، في وجود تقصير في مسلك بنك المعلومات، ما كان ليقع فيه بنك يقظ وجد في نفس الظروف الخارجية التي أحاطت بالبنك المسئول، نتيجة تقصيره في القيام بواجب الحيطة والحذر في أدائه للعمل الذي يقوم به.

وعلى ذلك يتوافر الخطأ في جانب القائم بتجميع البيانات عند ثبوت تقصيره في التزام الأصول الفنية والمهنية أثناء قيامه بعملية التخزين أو الحفظ للمعلومات. ومن الأصول الفنية التي يجب على المسئول إتباعها:

- ضرورة توافر الخبرة الدقيقة في كل عمليات تشغيل الحاسوب، ابتداء من عملية التجميع وانتهاء بعملية التخزين، وأي خلل يقع في إحدى هذه العمليات يعتبر خروجا عن الأصول الواجبة الإتباع.
- ضرورة توافر التقنية العالية لدى القائمين على عمليات تجميع البيانات، وتوعيتهم بالمسئولية الملقاة على عاتقهم في المحافظة على كافة المعلومات والبيانات المتعلقة بالحياة الخاصة التي تتصل بعلمهم، والحيلولة دون وصول المتطفلين إليها، وعدم وضعها في التداول بدون إذن صاحبها.

ثانيا: معيار توافر الخطأ عن انتهاك البيانات الشخصية:

بالنظر إلى أن التقني هو شخص مهني متميز، وبالتالي فالعناية التي يجب أن يبذلها في هذا المجال هي عناية من نوع خاص، تتمثل في ضرورة أن يبذل أقصى ما بوسعه للحفاظ على سرية البيانات الشخصية، باعتباره متخصصا ومتمكن من تقنيات الحماية التي تمنع الغير من التعدي على البيانات الشخصية.

ونرى من جانبنا أن التقني مطالب بأن يبذل درجة كبيرة من العناية للحيلولة دون التعرض لبيانات المستخدمين الشخصية، الأمر الذي يعني أن المعيار الذي يطالب به التقني هو معيار المهني اليقظ، فأي خطأ في إيراد أي معلومة ولو كانت بسيطة أو

تقديم للبيانات مع عدم وجود التزام بالسرية يعتبر خطأ يوجب المسئولية بمجرد قيام دلالة قاطعة وثابتة بأن عمل التقني يتنافي مع أصول وقواعد المهنة.

وبالتالي يتحقق الخطأ في مجال البيانات الشخصية من خلال القيام بأي تجميع أو تخزين للمعلومات دون إخطار صاحبها، وفي ظل انعدام نظام أمني كفيل باحترام كامل لسرية البيانات، فإن تداول البيانات وانسيابها عبر شبكة الانترنت، وسهولة الحصول عليها بصورة غير مشروعة، وكذلك التنافس الحاد بين شركات الاتصال المرتبط بنظام الحاسوب للوصول إلى بيانات الأفراد ورصد خصوصياتهم، تعد من صور الخطأ الأكثر شيوعا(١).

ثالثا: صعوبات إثبات الخطأ عبر مواقع الاتصال والتواصل:

بيد أن ضرورة إثبات الخطأ من قبل المضرور في هذا المجال التقني المعقد قد تشوبه بعض الصعوبات التي تفرزها خصوصية الخطأ من قبل المعتدين على البيانات الشخصية والمعلومات عبر وسائل الاتصال والتواصل الحديثة، ويمكن إرجاع هذه الصعوبات للأسباب الآتية:

١- **سرعة ارتكاب الخطأ وخفاؤه:**

حيث أن الاعتداء علي الخصوصية وسرقة البيانات أو نشرها لا يستلزم سوي جزء من الثانية يقوم فيها المعتدي بالضغط علي زر أو مفتاح علي جهاز الكمبيوتر أو هاتفه النقال، بل إن الخطأ بالنظر لخصوصية محل الاعتداء قد لا يستلزم لارتكابه الوجود المادي للمعتدي أمام الأجهزة بل قد يقوم ببت وضبط بعض البرامج التي

(١) د.محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٣، ص٣٦٣.

تساعده على الاعتداء على البيانات والمعلومات أو نشرها من تلقاء نفسها، ومن ثم قد يستطيع نفي خطأه بإثبات وجوده في مكان ما وقت وقوع الاعتداء [1].

٢- **خصوصية محل ارتكاب الخطأ**:

حيث يتم الاعتداء على البيانات الشخصية والمعلومات وانتهاك خصوصية المضرور عبر عالم افتراضي من خلال بيئة المعلومات والبيانات الآلية، مما يعني صعوبة التعامل معها، حيث يلزم توافر معرفة تقنية وفنية لاكتشاف الاعتداء وتحديده، الأمر الذي يفتقده غالبية رواد مواقع التواصل الاجتماعي أو سائل الاتصال ذات التكنولوجية المعقدة.

٣- **تعدد وتواطؤ مرتكبي الخطأ**:

لعل أكثر ما تتميز به جرائم المعلومات عبر مواقع الاتصال والتواصل الحديثة هو تضامن بعض المتخصصين في البرمجة والتعامل مع البيانات، بحيث يمكن أن يكون هناك شخص هو الذي قام بالدور الفني للاعتداء، وآخر من محيط المضرور أو خارجه هو الذي قام بالاستخدام غير المشروع للبيانات، وآخر هو الذي غطى عملية التلاعب بالبيانات وتم تحويل المكاسب على حسابه. الأمر الذي يُصعب مهمة المضرور في تحديد شخصية مرتكب الخطأ.

٤- **تنفيذ الخطأ عن بعد**:

حيث تساعد خصوصية المجتمع الافتراضي لرواد الوسائل التكنولوجية الحديثة للاتصال على سهولة الاتصال عبر الشبكة العنكبوتية بين أشخاص ينتمون لدول متفرقة، ومن ثم قد يكون المعتدي مقيما بدولة بعيدة عن مكان وجود المضرور.

---

(١) د. علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، مطابع جاد للأوفست، الرياض، ١٤٢٦هـ. ص ٦٣.

٥- **عدم وضح الاعتداء وصعوبة إثباته**:

في كثير من الأحيان قد لا يعلم المضرور بحدوث الاعتداء إلا إذا كان الاعتداء له أثار مالية كسرقة بعض البيانات الشخصية للحسابات البنكية ومن ثم الحصول على أموال المتضرر، أو حينما يفكر المعتدي في ابتزاز المضرور للحصول منه على مبالغ نظير عدم نشر صوره أو بياناته الشخصية، كما أن الاعتداء هنا يتميز عن الاعتداء التقليدي، حيث يستطيع المعتدي محو أدلة الاعتداء وتدميرها في ثوان محدودة(١).

وفي إطار تلك الصعوبات التي تحيط بعملية إثبات الخطأ في هذا المجال التقني المعقد، وتؤدي لتعذر الوقوف على شخصية الهاكرز المعتدي أو المستخدم الأخر المنتهك لخصوصية البيانات، وبالتالي حرمان المضرور من تعويض الأضرار التي أصابته بسبب الاعتداء علي بياناته الشخصية، فإننا نقترح قيام المسئولية المدنية عن أضرار مواقع الاتصال والتواصل في حال تعذر تحديد شخصية المعتدي الحقيقية والحصول منه علي مبلغ التعويض، علي أساس الخطأ في الحراسة، حيث قد يوفر ذلك أمامنا شخصا مسئولا عن تعويض تلك الأضرار، إذا ما ثبت تقصيره في القيام بواجب الحراسة والرقابة.

ولاشك أن واجب الحراسة أو الرقابة يُلقي علي عاتق مالك موقع التواصل الاجتماعي أو مديره، وعلى عاتق وسطاء الانترنت، وعلى عاتق مصممي تقنيات الاتصال، حيث يعدون في حكم المنتج للأشياء غير الحية، باعتبار أن شبكة الانترنت في طبيعتها كيان غير حي، له مُبتكر ومسئول عن إدارته.

---

(١) دعت هذه الخصوصية للجرائم التي يتم وقوعها عبر الشبكة العنكبوتية، إلى قيام بعض الدول بإنشاء محاكم إلكترونية للبت في هذه الجرائم ، مثل المحكمة الإلكترونية بدبي بالإمارات العربية المتحدة. راجع في ذلك د. نبيل عبد المنعم جاد، جرائم الحاسب الآلي، مركز أبحاث شرطة دبي، ١٩٩٩، ص٢٥.

رابعا: الخطأ في الحراسة أساسا للمسئولية المدنية في مجال شبكات الاتصال والتواصل:

نظرا لشيوع استعمال مواقع التواصل الاجتماعي في مجال الاتصال وتبادل المعلومات، حيث أدي تطور المجتمعات الحديثة والرفاهية التي وصلت إليها في هذا المجال، إلى اعتماد الإنسان في نشاطه وجوانب تواصله الاجتماعي على شبكة الانترنت بصورة كبيرة، ممّا زاد في عدد الأشخاص الذين يتعرضون لآذاها بشكل كبير، وهو ما يجعل المسؤولية المدنية عن هذا المجال تطرح بشكل جدي، لاسيما مع خطورة الأضرار التي صارت تُلحقها وصعوبة إثبات الخطأ في جانب محدثها.

ونتيجة لكون القواعد العامة في الإثبات قد تبدو قاصرة عن أن توفر الحماية المطلوبة للمتضررين من فعل هذه المواقع، لعدم مقدرتهم على إقامة الدليل على الخطأ؛ إذ إن سبب الحادث يبقى غالبًا مجهولاً، وإن أمكن معرفة السبب فقد يتعذر تحديد المسئول الفعلي عنه، مما يحول دون إمكانية حصول المضرور على التعويض. فهل نجد في نظرية المسئولية الشيئية علاجا وافيا، فهي مسئولية لا تقوم على افتراض الخطأ، وإنما تقوم على مجرد ملكية الشيء الذي أحدث الضرر، وتجعل المالك مسئولاً عن مخاطر ملكه، وذلك على أساس تحمل تبعة المخاطر؟؟

فمن خلال مطالعة نصوص القانون المدني المصري يتضح أن نص المادة ١٧٨ من القانون المدني المصري لم يجعل المسئولية مفترضة بشأن جميع الأشياء غير الحية، وإنما قصر المسئولية المفترضة على الأشياء التي تتطلب حراستها عناية خاصة، سواء لطبيعتها أم بالنظر للظروف والملابسات التي تجعلها مصدرًا لخطر يلزم له عناية خاصة، الأمر المتحقق في مجال شبكات الانترنت ووسائل الاتصال والتواصل الحديثة.

ويمكن الأخذ في ذلك بنظرية الحراسة القانونية، التي تربط الحراسة بحق الملكية لشخص على الشيء الذي أحدث الضرر، فحارس الشيء هو من له حق الملكية.

والحارس هو من تكون له سلطة قانونية على الشيء يستمدها من حق عيني على الشيء أو من حق شخصي متعلق به، ومصدر هذه السلطة يكون العقد أو نص القانون أو الإرادة المنفردة(١).

وإعمالاً لتلك النظرية، فإن المسئول عن الفعل الضار لوسائل الاتصال والتواصل هو من يملك السيطرة الفعلية والقانونية على طريقة تداول البيانات عبر الشبكة، أي من يملكها. ومع ذلك يثور تساؤل آخر حول من يعتبر المالك في مجال وسائل الاتصال والتواصل: هل هو منشئ الموقع ومديره ومالكه الذي يملك وحدة براءة اختراعه؟ أم هو المستخدم العادي الذي انتقلت إليه ملكية الحساب علي هذا الموقع بمجرد التسجيل والاشتراك؟

وفقًا للمجرى العادي للأمور، فإن المستخدم العادي، على الرغم من تسجيله واشتراكه في مواقع التواصل، واعتباره بذلك الحائز المادي للحساب عبر صفحات التواصل الاجتماعي مثلا، ومن ثم صاحب جميع السلطات عليه بمجرد تسلمه لكلمة المرور أو الرقم السري للدخول، إلا أنه الطرف الذي لحقه الضرر، ومن ثم فإن المسئول عن الفعل الضار الذي أحدث انتهاكا للبيانات الشخصية يتوقف تحديده على ما إذا كان مرجع الضرر خطأ فني أم خطأ إداري، ففي الحالة الأولى تقع المسئولية على عاتق مورد البيانات أو متعهد الإيواء، كما يعتبر تقصير وإهمال المسئول الفني عن

(١) د. أحمد شوقي عبد الرحمن، مسئولية المتبوع باعتباره حارسًا، دار الفكر العربي، القاهرة، ١٩٩٨، ص٥٨.

الصيانة سببا لتحقق مسئوليته، وعلى صعيد اختراق قواعد السرية وانتهاك خصوصية البيانات الشخصية الخاصة فإن المسئولية تنعقد للمستخدم المعتدي، أما في الحالة الثانية وحال ثبوت التقصير في اتخاذ الاحتياطات التقنية اللازمة فإن المسئول هو مالك الموقع أو مديره أو وسيط الشبكة الذي يتولي السلطة الفعلية لإدارة حسابات مواقع التواصل والاتصال.

بيد أن التحديد السابق يؤدي بنا لبعض الإشكاليات القانونية، حيث أن إمكانية تحديد عناصر المسئولية وفقا لهذا التحديد أمراً غاية في الصعوبة، فحتى لو تمكنا من تحديد طبيعة الأخطار وتقدير الأضرار المترتبة عنها، فإن تحديد المسئول عن انتهاك الخصوصية من بين جميع الأشخاص السابقين ليس بالأمر السهل، فأي منهم تكون له صفة الحارس الذي يمكن الرجوع عليه بالتعويض حال انتهاك خصوصية البيانات الشخصية عبر بنوك المعلومات ووسائل الاتصال والتواصل الحديثة، وهو ما نحاول مناقشته فيما يلي:

- **تحديد الحارس المسئول(في حالة تعدد الحراس)**:

يتعدد حراس الشيء في أحد فرضين: أولهما هو فرض تجزئة الحراسة الذي يتولى فيه الحراسة على الشيء مالك الموقع أو مديره بوصفه حارسًا للتكوين والمالك أو مورد البيانات ومتعهد الإيواء وهما من تنتقل إليهما سلطات الرقابة والتوجيه باعتبار أيا منهما حارسًا للاستعمال. أما الفرض الثاني فهو فرض تعدد الحراس في نطاق حراسة التكوين ذاتها.

الفرض الأول: **افتراض مسئولية منشيء المواقع في الفرض الخاص بتجزئة الحراسة**:

مما لا جدال فيه أن نظرية تجزئة الحراسة قد نشأت في الأصل بغرض تخفيف مسئولية الحارس غير المالك الذي عهد إليه بالشيء للاستخدام المؤقت، دون أن تكون

لـه أي سـلطة فعليـة فيمـا يخـص مكونـاتـه الداخليـة؛ حيـث أثقلـت المـادة ١/١٣٨٤ مـن القـانون المـدني الفرنـسي كاهـل المالـك المؤسـس للموقـع (المنـتج) باعتبـاره حارسًـا للتكوين ومسئولاً عن عيوب مُنتَجه وما ينتج عنه من أضرار[١].

وفيما يخص مجال الخصوصية عبر وسائل الاتصال والتواصل الحديثة نرى أن تعيين مالك الموقع الإلكتروني ومنشئه حارسًا للتكوين وتحمله وحده المسئولية حال انتهاك البيانات الشخصية للمستخدم فيه من الإجحاف والعنت به؛ حيث لا يستطيع في كثير من الأحيان أن يتلافى التدخل الضار لغيره من وسطاء الانترنت، كما أن هذا القول يتنافى مع ما حددته محكمة النقض من تعريف الحارس، حيث ربطت بين الحراسة وبين ما للشخص من سلطات فعلية على الشيء محل الحراسة.

وبخصوص ذلك يثور التساؤل بشأن تحديد الحارس الذي يرجع الضرر إلى خطئه، هل هو حارس التكوين (مالك الموقع ومؤسسه- منشئ بنوك المعلومات) أم حارس الاستعمال (مورد المعلومات -ومتعهدي الإيواء- ووسطاء الشبكة)؟

لا شك أنه في الحالة التي تبدو فيها عيوب اختراق الخصوصية عبر الموقع الإلكتروني ظاهرة أو يسهل استخلاصها من ظروف الحال، بحيث يسهل إرجاع التعرض للبيانات إما إلى العيب التقني الداخلي لوسائل الأمان للموقع أو التطبيق الإلكتروني، وبناء عليه يسهل إثبات خطأ مالكه أو مؤسسه باعتباره حارسًا للتكوين، أو إرجاع سبب الاختراق إلى المسلك الخارجي المتمثل في إدارة نقل وتبادل المعلومات[٢]، وبالتالي إسناد الخطأ لتقصير من يتولى حراسة الاستعمال.

---

(1) Art. (1384/1) du Code Civil français.

(2) Goldman (B.), La détermination du gardien responsable du fait des choses inanimées, thèse, Lyon, 1945, p.12.

بينما تبدو الصعوبة في الحالة التي يتعذر فيها تحديد سبب انتهاك البيانات أو الوسيلة التي تم من خلالها اختراق الموقع أو التطبيق، ومن ثم صعوبة تحديد الحارس المسئول. فقد يكون المخرج البديهي، على رأي البعض، هو رفع الدعوى على الحارسين معًا وترك الأمر للقضاء للفصل فيه في ظل الخبرة الفنية[1]. إلا أنه لا يخفي علينا ما يمكن أن يترتب على هذا الرأي من نتائج قد يكون من أشدها إيلامًا بالمضرور رافع الدعوى أن ترفض دعواه على الحارسين معًا، فضلاً عما قد يمثله ذلك من تكلفة مادية وجهد مضاعف مما قد يضر بمصلحة المضرور رافع الدعوي. لذا يمكن القول بأن مصلحة المضرور تقتضي أن تبقى مسئولية مالك الموقع الالكتروني أو مؤسسه مفترضة بوصفه حارسًا للتكوين حتى في الحالات التي تنجم فيها الأضرار عن التقصير في رقابة سرية تبادل المعلومات، باعتباره الأقدر على الرقابة والإشراف على الموقع الإلكتروني، أو حتى في الحالات التي يتعذر فيها تحديد سبب أو وسيلة انتهاك خصوصية البيانات.

وفي خصوص وسائل الاتصال والتواصل الحديثة كمواقع التواصل الاجتماعي يفرض تساؤل هام نفسه في إطار العرض، وهو من يكون المسئول عن انتهاك خصوصية البيانات الشخصية في الحالة التي تكون فيها سلطة الاستعمال قد انتقلت إلى المستخدم الذي يملك وحده كلمة السر، ويكون له السلطة الفعلية في الدخول لحسابه والخروج منه وتعبئته بما يشاء من بيانات شخصية وصورا خاصة؟؛ حيث لا يكون المستخدم علي دراية بالتكوين التقني للموقع ووسائل التعامل مع أي اختراق قد يتعرض له من الهاكرز أو من وسطاء الشبكة، وفي هذا الفرض أيضًا ينعدم الإدعاء

(١) د. حسن جميعي، مسئولية المنتج عن الأضرار التي تسببها منتجاته المعيبة، دار النهضة العربية، القاهرة، ٢٠٠٠، ص١٥٩.

بأن المالك أو المؤسس للموقع يباشر سلطة فعلية على مكوناته، وبهذا فإن التعامل مع التقنيات الفنية للموقع الإلكتروني تخرج عن سيطرة المستخدم لجهله بالنواحي التقنية والفنية، وهو في ذات الوقت يخرج عن السيطرة الفعلية المباشرة للمالك، فأي من الطرفين يكون من الأولى أن تنسب إليه حراسة التكوين، ومن ثم يتحمل مسئولية انتهاك الموقع ومسئولية التعدي على البيانات؟، وإذا كان المعيار هو القدرة على درء الضرر ومقاومة أي محاولة للاختراق، فأيهما هو الأقدر على ذلك: المالك أو المؤسس الذي كان بمقدوره منع اختراق الموقع من البداية عبر اتخاذه لاحتياطات الأمان الملائمة التي تصد محاولات الاختراق، أم المستخدم صاحب الحساب الذي انتقلت إليه السلطات الفعلية على الحساب أو التطبيق، ولكن لا يملك من الإمكانات الفنية سوى الانصياع لتعليمات مؤسس الموقع ومديريه الذين أولاهم ثقته؟

عمليًا إذا ما استطاع المالك أو المؤسس للموقع الإلكتروني الإفلات من المسئولية بحجة أنه لم يكن حارسًا للتكوين، فيكون من الظلم البين إلقاء تبعة هذه المسئولية على كاهل المستخدم وحده الذي لا يعرف شيئًا عن التقنيات الفنية لطرق تشغيل الموقع ولتفصيلات نقل البيانات عبر الشبكة، والذي يكون هو نفسه ضحية لاختراق حسابه ومن ثم انتهاك بياناته.

ونرجح أن يظل مالك الموقع أو مؤسسه محتفظاً بحراسة التكوين أو الإنشاء لموقعه الإلكتروني باعتباره الأكثر دراية بثغرات الأمان للموقع وسبل معالجتها، على الرغم من قيام المستخدم بممارسة السلطة الفعلية على حسابه عبر كلمة السر التي يحوزها.

وفي الحالة التي يعهد فيها مالك الموقع الإلكتروني أو مؤسسه إلى شخصا أخر يتولى إدارة الموقع الإلكتروني، وثبوت التقصير في جانب مدير الموقع سواء أكان هو

من انتهك خصوصية البيانات، أو أدي تقصيره في الإدارة المناسبة للموقع الإلكتروني إلى تسهيل عمليات الاختراق من قبل الهاكرز، فيمكن أيضا الرجوع على المالك وفقا لقواعد مسئولية المتبوع عن فعل تابعه إذا توافرت شروطها.

الفرض الثاني: تحديد حارس التكوين في الفرض الخاص بتعدد وسطاء الشبكة:

بما أن التخصص هو سمة العصر الحديث، بحيث أصبح التعامل مع التقنيات الحديثة في مجال الاتصال والتواصل تحتاج إلى نوعا من التخصص في التكوين والإدارة والصيانة والبرمجة، حيث لم يعد متصورًا الآن أن ينفرد شخص واحد بإدارة عمليات الاتصال ونقل المعلومات عبر شبكة الانترنت. فمن المؤكد أن هناك متخصصين في ابتكار تطبيقات التواصل، وهناك متخصصين في إنشاء تقنيات الإرسال، ومتخصصين في الإدارة، ومتخصصين في التطوير، ومتخصصين في الإشراف على عمليات نقل البيانات، ومتخصصين في الصيانة ومعالجة الأعطال.

وبناء على ذلك، إذا حدثت أي من صور انتهاك البيانات السابق التعرض لها على الموقع الإلكتروني، أو عبر وسيلة التواصل الاجتماعي، أو أي من تطبيقات التواصل الحديثة نتيجة وجود خلل في تقنيات نقل وتبادل المعلومات والبيانات، فيثور التساؤل عمن يعتبر حارسًا لهذا التكوين، ويلتزم بناء على ذلك بتعويض الضرر الناشئ عن انتهاك البيانات أو التعدي على خصوصيتها؟؟

لن تكون هناك ثمة مشكلة في تلك الحالة إذا أمكن تحديد جزئية الخلل التي سهلت التعدي. فقد يكون مرجع الخلل لعيب في تقنية إنشاء الموقع ذاته، حيث تنعقد مسئولية المالك أو المؤسس نفسه، أو يرجع الخلل لعيب في تقنيات الإرسال، فتتحقق مسئولية وسيط الشبكة، أو خلل في رقابة وتأمين نقل وتبادل البيانات، فتنعقد مسئولية متعهد الإيواء.

ولكن تثور الصعوبة في الفرض الذي لا يمكن فيه تحديد الجزء الذي أدى تعيبه إلى حدوث التعدي. حيث نقترح الرجوع على جميع الأشخاص الذين تثبت لهم صفة حارس التكوين للموقع على سبيل التضامم. وحال تعذر الرجوع على هؤلاء الأشخاص مجتمعين بالنظر لضعف الإمكانات الفنية والمادية للمستخدم المعتدى على بياناته، وبالنظر إلى أن محل الاعتداء وهو الشبكة الدولية للانترنت التي يكون منشئيها ووسطاءها منتمون لدول متعددة مما يُصعِب على المضرور فرص الرجوع عليهم مجتمعين، فيمكن رفع الدعوى هنا على مالك الموقع أو مؤسسه الذي تكون شخصيته ومحل إقامته غالبا محددة، باعتباره الحارس الظاهر أمام المستخدمين للمواقع والتطبيقات الإلكترونية.

خامسا: تيسير إثبات مسئولية مالك الموقع أو مؤسسه من خلال افتراض علاقة السببية:

بمجرد أن يثبت أن ثمة خلل في وظائف الأمان بالموقع الإلكتروني كان السبب في انتهاك خصوصية البيانات الشخصية للمستخدم، فإنه يجب على القضاء أن يفترض مباشرة مسئولية مالك الموقع ومؤسسه على أساس الخطأ في الحراسة وفقا لقواعد المسئولية الشيئية قياساً على تبني القضاء الفرنسي اتجاها يفترض مباشرة مسئولية المنتج باعتباره حارسًا للتكوين في مجال المنتجات، وأنه يتعين عليه إذا أراد أن يدفع مسئوليته أن يثبت السبب الأجنبي.

ويعتبر مسلك القضاء بشأن إثبات علاقة السببية في مجال حراسة التكوين للمواقع الإلكترونية متوافقًا مع المبادئ الأساسية الحاكمة لمسئولية الحراسة عن الأشياء، حيث إنه وقد وقع الضرر والتعدي على البيانات بسبب الخلل في أي من تقنيات الموقع الإلكتروني، فإن المستخدم المضرور يجب ألا يقع على عاتقه إقامة

الدليل على علاقة السببية بين ما لحقه من ضرر نتيجة انتهاك بياناته وبين خلل الموقع أو خطأ المؤسس المالك[١].

بيد أنه يجب التنويه إلى أنه بالرغم من القرينة القضائية التي نطالب بتوفيرها للمستخدم المعتدى على بياناته الشخصية أسوة بالقرينة التي يقيمها القضاء لصالح المضرور من فعل المنتجات المعيبة، فإن المالك أو المؤسس أو المدير أو وسيط الشبكة يمكنه أن يدفع مسئوليته إذا أثبت اتخاذه لكافة وسائل الاحتياط والأمان اللازمة للحيلولة دون اختراق موقعه أو تطبيقه الإلكتروني، وأن عمليات الاختراق التي حدثت مرجعها خطأ المستخدم نفسه الذي سهل للغير الدخول لحسابه عبر اختيار كلمة سر ضعيفة يسهل اختراقها، أو عبر نشر بياناته وجعلها مباحة الاطلاع للعامة، أو حال إثباته للسبب الأجنبي.

الفرع الثاني

الضرر

يلزم ثانيا لتحقق المسئولية المدنية عن الأضرار التي تلحق بالبيانات الشخصية عبر وسائل الاتصال والتواصل الاجتماعي حدوث ضرر لبعض الأشخاص الذين يرتادوا هذه الوسائل. فما هو المقصود بهذا الضرر وما هي شروطه؟

أولا: المقصود بالضرر وصوره:

يعرف الضرر عامة بأنه" الإخلال بحق أو بمصلحة ذات قيمة مالية للمضرور"[٢]، كما يعرف أيضا بأنه" ما يصيب الشخص في حق من حقوقه أو

(١) د. حسن جميعي، المرجع السابق، ص١٦٩.
(٢) عبد الرزاق السنهوري، الوسيط في المسئولية المدنية، ج١ ف٥٧١، ص٨٥٦.

بمصلحة مشروعة له "[١]. وأصبح المستقر عليه أنه طالما كانت المصلحة مشروعة، فيستوي بعد ذلك أن تتعلق بسلامة جسده أو بعاطفته أو بماله أو بحريته أو بشرفه أو في أي مصلحة يحرص عليها الإنسان.

وينقسم الضرر عامة إلى ضرر مادي يصيب الذمة المالية للمضرور، وضرر معنوي يتمثل في المعاناة والآلام التي تصيب عاطفة المضرور وشعوره. ولم يعد هناك خلافا في الفقه على شمول التعويض المستحق لكلا النوعين من الضرر.

ولا شك في تحقق كلا النوعان من الضرر للمعتدى على خصوصياته وعلى بياناته الشخصية عبر مواقع الاتصال الإلكتروني أو مواقع التواصل الاجتماعي، فالدخول إلى صفحات رواد مواقع التواصل الإلكترونية بما فيها من معلومات وبيانات سرية يتم بسرعة وسهولة، ويكون الضرر الناجم عن الكشف والاطلاع على البيانات الشخصية والأمور السرية بمثابة انتهاك لخصوصية صاحب الحساب أو البريد الإلكتروني، الأمر الذي قد يلحق به العديد من الأضرار المادية الناتجة عن بث معلوماته وبياناته عبر الشبكة، حيث يكون هناك عدد غير محدود من المطلعين عليها، مما يصيبه بأضرار بالغة على صعيد سوق العمل نتيجة رفض التعامل معه، أو عدم الموافقة على طلب دخوله في مناقصه أو مسابقة بسبب ما نشر عنه من بيانات ومعلومات، وقد يتمثل الضرر المادي في خسارته لبعض أمواله نتيجة سرقة كلمات مروره السرية لحساباته البنكية والحصول على أموال من حساباته[٢].

(١) د. سليمان مرقس، الوافي في شرح القانون المدني، الفعل الضار، الجزء الثالث، ص١٣٣.

(٢) د.منصور بن صالح السلمي، المسئولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٠، ص١٠٣.

كما يتمثل الضرر الأدبي الناجم عن انتهاك الخصوصية والاعتداء على بياناته الشخصية في انتهاك حرمة الحياة الخاصة لرواد مواقع التواصل الاجتماعي، وما يستتبعه ذلك من المساس بسمعة الشخص الاجتماعية ونشر معلوماته وأسراره الخاصة، بما قد ينطوي عليه من إهانه وتجريح وفضح لأسراره وصوره العائلية أو الخاصة أو لمعلوماته الصحية أو الاجتماعية[1].

ثانيا : **شروط الضرر**:

يلزم في الضرر الذي يوجب التعويض ضرورة أن يكون محققا، أي أن يكون قد وقع بالفعل، أو أن وقوعه بالمستقبل أمر حتمي، وهو ما يتوافر بلا أدنى شك في الضرر المعلوماتي الناشئ عن الاعتداء على الخصوصية عبر مواقع التواصل الاجتماعي، فهو دوما محقق، حيث أن الضرر الاحتمالي غير متصور على صعيد انتهاك الخصوصية والسرية المعلوماتية، فمجرد الاعتداء على البيانات والإطلاع على الأسرار الشخصية لصاحب الحساب هو في حد ذاته ضررا محققا، بصرف النظر عن الأضرار اللاحقة التي تتبع الاعتداء.

(١) في سياق ذلك وفي عام ٢٠١٤ أيدت محكمة استئناف عمان قرارا صادرا عن محكمة بداية حقوق عمان، بتعويض المشتكي مبلغ ١٢٥٠٠ دينار، يدفعها المدعي عليه بعد قيامه بنشر صورة زوجة المدعي عارية عبر موقع التواصل الاجتماعي "فيسبوك"، مما أدي إلي تطليق هذه الزوجة وإصابتها بالضرر المعنوي الجسيم، كما قضت المحكمة للمدعي بمبلغ ١٠ ألاف دينار بدلا لأضرار معنوية لحقت به حيث أثر ذلك علي سمعته وشرفه ومركزه المالي مما اضطره لترك وظيفته ومغادرة محل عمله بالإمارات. أنظر مقالة منشورة بعنوان الجرائم الإلكترونية عبر الفيسبوك: الأدلة والثغرات والتعويض عبر الموقع الالكتروني التالي:
https://www.7iber.com/society/facebook-cyber-crimes

كما يلزم ثانيا في الضرر أن يمس مصلحة مشروعة للمضرور، الأمر المتحقق أيضا بالنسبة للاعتداء الذي يتعرض له صاحب الحساب عبر وسائل الاتصال الإلكتروني ومواقع التواصل الاجتماعي، حيث أن خصوصياته وحرمة بياناته الشخصية والسرية والحفاظ عليها، تعتبر من أهم المصالح المشروعة لرواد هذه المواقع التي يجب أن توفر لها الحماية القانونية.

ويلزم في الضرر ثالثا أن يكون مباشرًا، فالضرر المباشر وحده هو الذي يمكن التعويض عنه في مجال المسئولية المدنية، ويكون الضرر مباشرا إذا كان نتيجة طبيعية لفعل الاعتداء، ولم يكن في الإمكان تفادي حدوثه بجهد معقول، الأمر المتحقق أيضا في الضرر الناشئ عن التعدي على البيانات الشخصية عبر مواقع الانترنت.

الفرع الثالث

علاقة السببية

بالإضافة إلي الخطأ والضرر، يلزم توافر علاقة سببية بين الخطأ الذي من خلاله تم الاعتداء على البيانات الشخصية وخصوصية معلومات صاحب الحساب عبر مواقع التواصل وبين الضرر المادي أو الأدبي الذي لحقه.

وفيما يتعلق بإثبات رابطة السببية، فيمكن القول بأنه وإن كان من الصعب على المضرور إقامة الدليل على الخطأ الذي تقوم عليه المسئولية، نظرا لصعوبة تفسير أو تمييز الخطأ أو تحديد مصدره أو وقت حدوثه بالنظر لتعدد مراحل تنفيذ الأمر الالكتروني بالاعتداء [1]، إلا أنه وبسهوله يمكن ربط الضرر المتحقق بهذا الخطأ، وإثبات رابطة السببية بينهم، فلا يوجد سبب أخر لنشر البيانات الشخصية بدون علم

(١) منصور بن صالح السلمي، المرجع السابق، ص١١١.

صاحبها أو استعمالها بدون سابق معرفة منه، إلا لوقوع اعتداء على خصوصية حسابه عبر مواقع الاتصال والتواصل، وإن ظلت مسألة تحديد هوية مرتكب الخطأ محل صعوبة، وبالتالي يمكن الرجوع على من تثبت له الحراسة كما سبق بيانه.

المطلب الثاني

دعوى المسئولية المدنية عن الاعتداء على البيانات الشخصية عبر وسائل الاتصال الحديثة

نعرض في هذا المطلب لتحديد أطراف الدعوى من خلال الفرع الأول، بينما يخصص الفرع الثاني لدراسة القانون واجب التطبيق والمحكمة المختصة بالدعوى، ويتناول الفرع الثالث دراسة أثر الدعوى.

الفرع الأول

أطراف دعوى المسئولية المدنية عن الاعتداء على البيانات الشخصية عبر وسائل التواصل الحديثة

لا شك أن أطراف كل دعوي هما المدعي، والمدعي عليه، بيد أنه أذا كان من اليسير تحديد المدعي رافع الدعوى، إلا أنه قد تقابلنا بعض الصعوبات في تحديد المدعي عليه المسئول عن الأضرار المتحققة عبر وسائل الاتصال الحديثة نتيجة الاعتداء. لذا نعرض لذلك من خلال ما يلي:

أولا: المدعي صاحب الدعوى

يحق للمضرور ذاته أن يقوم برفع دعوى المسئولية المدنية مطالبا بتعويض الأضرار التي لحقته جراء الاعتداء، كما يحق لورثته من بعده أن يحلو محل مورثهم في دعوى المسئولية المدنية.

- المضرور:

أدث الثورة التكنولوجية الهائلة التي اجتاحت وسائل الاتصال والتواصل إلى تعاظم عمليات نقل وتبادل المعلومات والبيانات الشخصية، وتسهيل تواصل الأفراد عبر استخدم بعض المواقع التي خصصت من أجل تشجيع التواصل الاجتماعي، وفتح المجال أمام الأشخاص كبار وصغار لامتلاك حسابات متعددة عبر المواقع الإلكترونية، وفي سابقة فريدة من نوعها فقد كان عدد المشتركين عبر مواقع التواصل الاجتماعي يتعدي الملايين من الأفراد، رغم مرور فترة زمنية قصيرة جدا على إنشاء تلك المواقع، وتتطلب هذه المواقع للاشتراك فيها وتملك صفحة شخصية من خلالها ضرورة إدراج المشترك لعدد كبير من البيانات عن الحالة الشخصية والاجتماعية وإدراج صورا شخصية تميز صفحته، ثم ما لبث الأمر أن تتطور وأتُيحت الإمكانات لتحميل البيانات الشخصية الأكثر خصوصية، والعثور علي العديد من الأصدقاء التي تربطهم بصاحب الحساب اتحاد في مجال الدراسة أو تقارب في المكان الإقليمي أو تشابه في الميول والهوايات، ثم سهلت عملية التواصل بعد ذلك عبر المحادثات الصوتية أو الكتابية، وتبادل إرسال الصور الشخصية، بل وأصبحت بعض المحادثات تتم عبر الصوت والصورة المباشرة بين أصحاب الحسابات. وزادت عدد التطبيقات التي يتم من خلالها المرور والإطلاع على البيانات الشخصية بكافة مظاهرها وبموافقة مسبقة مشوبة بنوع

من التدليس على المستخدم صاحب الحساب، كذلك فرض التطور ضرورة امتلاك كل فرد لبريد إلكتروني يكون بمثابة عنوانا محلا لمراسلاته وكافة معاملاته.

ترتب على ما سبق أن أصبح كل مستخدم لهذه المواقع عبر وسائل التواصل المتعددة عبر شبكات الإنترنت مهددا بانتهاك خصوصيته والاعتداء على بياناته الشخصية، كنتيجة لقصور هذه المواقع في توفير الحماية الفاعلة للبيانات والمعلومات المدرجة عليها لوجود ثغرات تقنية يتمكن من خلالها المعتدي الدخول لهذه الصفحات وانتهاك خصوصياتها وسرقة محتوياتها، واستغلال البيانات. ومن ثم يستطيع كل شخص يلحقه الضرر بسبب ذلك أن يقوم برفع دعوى المسئولية المدنية مطالبا بتعويض الأضرار التي لحقته جراء هذا الاعتداء.

- **ورثة المضرور**:

يثور التساؤل حول مدى أحقية الورثة في حال وفاة مورثهم في رفع دعوى المسئولية المدنية للمطالبة بالتعويض عن الأضرار التي لحقت مورثهم جراء الاعتداء على خصوصياته وبياناته الشخصية؟؟

لا شك أنه في هذه الحالة نفرق بين ما إذا كانت وفاة المضرور بعد مضي مدة من وقوع الاعتداء، أو فور وقوعها:

١- **وفاة المضرور بعد مضي فترة علي وقوع الاعتداء علي بياناته الشخصية وخصوصيته**:

في هذه الحالة إذا أقام المضرور دعواه أمام القضاء قبل وفاته، فإن لورثته أن يحلو محل مورثهم في الدعوى المدنية ويستمروا فيها باعتبار أن الحق في التعويض قد انتقل إليهم مع ذمة مورثهم، يستوي أن يكون الضرر ماديا أم أدبيا.

بيد أن التساؤل يطرح نفسه في الحالة التي يتوفى فيها المضرور دون أن يكون قد رفع دعوى بتعويض الضرر الناتج عن الاعتداء على بياناته الشخصية واختراق خصوصيته قبل وفاته؟

اتجه بعض الفقه إلى القول بأنه يحق للوارث الحلول محل مورثه في جميع حقوقه إلا إذا وجد نص بخلاف ذلك، حيث يحق للورثة المطالبة بتعويض الضرر سواء كان ماديا أم أدبيا، طالما أن الاعتداء الذي وقع علي المضرور لم يكن يمثل جريمة جنائية يتوقف رفعها علي شكوى المضرور، لأنه إذا توفي المضرور في مثل هذه الحالة وقبل رفع دعواه، كان ذلك بمثابة نزول عن دعواه الجنائية والمدنية، ومن ثم فلا تنتقل للورثة[1]. وهو ما قضت به المحكمة العليا بقولها" إذا توفي المضرور من الجريمة، فإن حقه في التعويض يعتبر جزءا من أمواله وينتقل ضمن تركته إلى ورثته، ويكون لهم حق رفع الدعوى المدنية التي كانت لمورثهم، أو حتى الحلول محله فيها إذا كان قد رفعها قبل وفاته" [2]. غير أن المشرع ما لبث أن قيد انتقال هذا الحق فيما يتعلق بالتعويض عن الضرر الأدبي بضرورة كون المضرور قد قام برفع الدعوي قبل وفاته، ثم ينتقل للورثة الحق في متابعة المطالبة بالتعويض عن الأضرار التي لحقت بمورثهم جراء الاعتداء.

ونرى أن هذا الاتجاه محل نظر، فكثير من جرائم الاعتداء على الخصوصية يكون لها جانب جنائي، فغالبا ما يقترن الاعتداء على البيانات الشخصية بجريمة ابتزاز، أو اختلاس أو سرقة، أو حتى جريمة سب وقذف باستخدام بعض البيانات

(١) د. أحمد شرف الدين، عناصر الضرر الجسدي وانتقال الحق في التعويض عنها إلي شخص أخر غير المضرور، بحث منشور بمجلة قضايا الدولة، ١٩٧٨، ص٨٢، وما بعدها.

(٢) قضاء المحكمة العليا في جلسة ١٦/٣/١٩٥٥، ٦٩، مشار إليه عند د.صدقي محمد أمين، التعويض عن الضرر ومدي انتقاله للورثة، الطبعة الأولي، ٢٠١٤، ص٣١٣.

والأسرار شديدة الخصوصية للمستخدم التي يتم الاطلاع عليها من خلال محادثته ومراسلاته عبر تلك المواقع الالكترونية، وبالتالي يكون موت صاحب الحساب المعتدى على بياناته دون أن يكون قد تقدم بشكوى، أو رفع دعوى يطالب فيها بوقف التعدي أو التعويض بمثابة العائق أمام الورثة لرفع دعوى مدنية لصالح مورثهم يطالبون فيها بتعويض الأضرار التي لحقت به نتيجة الاعتداء على بياناته أو نتيجة انتهاك خصوصياته.

٢- **وفاة المضرور فور وقوع الاعتداء على بياناته الشخصية**:

لا يجوز للورثة أن يرفعوا الدعوى الجنائية باعتبارهم ورثة تلقوا الحق عن مورثهم، لأن هذا الحق لم يدخل في ذمة المورث قبل وفاته، ومن ثم لا ينتقل للورثة، غير أن ذلك لا يمنع الورثة من رفع الدعوى المدنية إذا ما لحقهم ضرر مباشر نتيجة الاعتداء على بيانات مورثهم . وقد استقر القضاء الفرنسي على أن للورثة المطالبة بتعويض ما أصاب مورثهم قبل وفاته من أضرار شريطة أن يكون الضرر المادي قد نشأ مباشرة عن الاعتداء، وبالتالي عندما يباشر الورثة دعوى التعويض فإنما يقومون بذلك مقام المضرور(١).

وبالنظر لخصوصية مواقع الاتصال والتواصل الحديثة التي تظل صفحاتها وحساباتها قائمة عبر شبكة الانترنت برغم وفاة صاحبها، والتي لا يملك أحد من الورثة كلمات المرور اللازمة لإغلاقها، فإننا نتساءل بشأن الحالة التي يموت فيها صاحب الحساب بعد أن كان قد أدرج على حسابه بيانات وأسرار وصورا ومحادثات شخصية دارت بينه وبين بعض المشتركين عبر صفحات وسائل التواصل الاجتماعي أو عبر

(١) د.صدقي محمد أمين، المرجع السابق، ص٣١٥.

البريد الإلكتروني الخاص به، ثم يفاجأ الورثة بأن هناك انتهاك لصفحات وحسابات مورثهم وانتهاك لخصوصيته ونشر لبياناته الشخصية، فهل يحق لهم المطالبة بالتعويض عن الأضرار التي نشأت بفعل هذا الاعتداء؟

هنا وقع الاعتداء بعد وفاة صاحب الحساب، ومن ثم لم يصب صاحب الحساب أي ضرر محقق أثناء حياته، وبالتالي لا ينشأ له الحق في التعويض، حيث لا يمكن القول بأن الميت قد لحقه ثمة ضررا ماديا أو أدبيا جراء الاعتداء.

بيد أننا نرى أن بإمكان الورثة رفع دعوى تعويض عن الأضرار التي تلحق بهم عن طريق رفع دعوى مباشرة لتعويض الأضرار التي لحقتهم، خاصة إذا كانت البيانات والأمور الخاصة التي تم الاعتداء عليها على صفحات أو حسابات مورثهم مما يسئ لسمعة الورثة أو تؤثر عليهم ارتدادا. فقد تتأثر سمعة البنت وتتعرض لبعض الأضرار المادية أو الأدبية نتيجة الاعتداء على خصوصية أبيها أو نشر بيانات ومعلومات أو صور خاصة كانت على الحساب ومن شأنها تسئ لسمعة والدها ومن ثم تتأثر بها البنت عن طريق الارتداد، حيث يحق للبنت أن ترفع دعوى المسئولية المدنية لتعويض الأضرار المادية أو الأدبية التي تلحقها جراء هذا الاعتداء.

ثانيا: المدعى عليه

لا يمكن استخدام مواقع التواصل الاجتماعي أو حساباته إلا من خلال شبكة الانترنت، ويستلزم تدفق المعلومات والبيانات وسائر العمليات التي تنساب عبر الانترنت ومنها إنشاء وإدارة مواقع التواصل الاجتماعي المرور بمراحل متعددة ما بين إنتاجها وإنشائها ووصولها للمستخدم وتمكينه من فتح حساب له عبر الشبكة العنكبوتية، ومن هنا كان لابد من تضافر جهود عدة أشخاص تتنوع أدوارهم عبر النشاط الإلكتروني، بدءً من مورد منافذ الدخول إلى الانترنت الذي يتولي توفير وسائل

التقنية التي تساعد المستخدمين للدخول لصفحات الانترنت عامة، ومرورا بمقدم خدمات الإيواء على الانترنت الذي يتولى تخزين وحفظ البيانات والمعلومات لعملائه ويمدهم بالوسائل الفنية التي تمكنهم من الوصول لهذه البيانات واستخدامها، وهناك من يسمى بمورد المعلومات أو منتجها الذي يقوم ببث المعلومات والرسائل عبر حسابات الشبكة، كما أن هناك مدير أو منشئ لمواقع التواصل الاجتماعي عبر شبكة الانترنت مثل (الواتس آب- الفيسبوك – الإنستجرام- توتير.....).

وقد يقع الاعتداء على البيانات الشخصية للمستخدم أو انتهاك خصوصيته أو استغلال بياناته الشخصية وبيعها لبعض الشركات أو لبعض الأشخاص من أحد هؤلاء الأشخاص، وقد يقع الاعتداء واختراق الخصوصية من قبل مستخدم محترف للانترنت بمساعدة وعلم أحدهم، أو بدون مساعدتهم، أو دون علمهم . وفي حال كون المعتدي مستخدم عادي لمواقع التواصل، فقد يمكن التعرف عليه، ومن ثم مساءلته جنائيا أو مدنيا، وقد تحول خصوصية مواقع التواصل الحديثة بالنظر للطابع الفني المعقد لشبكة الانترنت باعتبارها شبكة عالمية لا تخضع لهيمنة أو سلطة دولة أو حكومة محددة دون إمكانية الوصول لشخص المعتدي أو تحديد مكانه. الأمر الذي يثير التساؤل عن الشخص الذي يتم مطالبته بتعويض الأضرار التي لحقت بالمضرور، فهل يمكن الرجوع علي وسطاء الانترنت بالتعويض، أم أن المسئول هو مدير أو منشئ موقع التواصل الذي وقع الاعتداء من خلاله؟

١- مسئولية وسطاء الانترنت عن تعويض الأضرار:

ينحصر دور وسطاء الانترنت في تقديم الوساطة الفنية، التي تمكن المستخدم من الدخول للشبكة والتجوال فيها والإطلاع على المعلومات التي تم نشرها عبر مواقع

الانترنت، بيد أنه رغم ذلك لا يخفي أهمية هذا الدور، الذي لولاه لما تمكن المستخدم من الاتصال بالموقع الالكتروني.

وقد ظهرت مسؤولية وسطاء الانترنت في بادئ الأمر من خلال البعد الجنائي الذي سيطر على الأذهان بسبب القضايا المتعلقة بحرمة الحياة الخاصة، حيث تدخل أفعال الوسطاء الخاطئة في أغلبها في نطاق التجريم، وفي إطار ذلك أصدر المشرع الفرنسي القانون رقم ٧١٩ لسنة ٢٠٠٠ المعدل للقانون ١٠٦٧ لسنة ١٩٨٦ بشأن حرية الاتصال، ومن خلال نص المادة ٨/٤٣ من هذا القانون قرر المشرع عدم قيام المسئولية الجنائية والمدنية للأشخاص المعنوية والطبيعية التي تقوم بمقابل أو بدون مقابل بالتخزين المباشر والدائم لتضع تحت تصرف الجمهور إشارات أو كتابات أو صور أو صوت أو رسائل أيا كانت طبيعتها، ولا تسأل عن محتوي هذه الخدمات إلا في حالتين:

الأولي: إذا تم أخطارها من قبل سلطة قضائية ولم يقم باتخاذ الإجراءات اللازمة لمنع وصول المحتوى للجمهور.

الثانية: إذا أخطره الغير بأن المادة التي يقوم بتخزينها غير مشروعة وتسبب له أضرار ولم يقم باتخاذ الإجراءات اللازمة لمنعها[1].

كما أوجبت الفقرة التاسعة من المادة ٤٣ أيضا على متعهد الإيواء أن يزود عملائه بالوسائل الفنية التي تسمح بتحديد هوية كل من يسهم في وضع مضمون

(١) قرر المجلس الدستوري بفرنسا عدم دستورية الحالة الثانية نظرا لتعارضها مع مبدأ الشرعية" لا جريمة ولا عقوبة إلا بنص"، لأن النص يعطي للأفراد سلطة تقدير شرعية العمل الأمر غير المبرر، حيث تم حذف الفقرة المذكورة. أنظر في ذلك د. طارق سرور، جرائم النشر والإعلام، الكتاب الأول، الأحكام الموضوعية، الطبعة الأولي، دار النهضة العربية ، القاهرة، ٢٠٠٤، ص١٩٩ وما بعدها.

المعلومات على الانترنت، وذلك حتى يمكن تحديد الشخص المسئول عن المعلومات غير المشروعة. بينما أشارت الفقرة العاشرة من ذات المادة إلى ضرورة الالتزام بالشروط الواردة في القوانين المنظمة للاتصال السمعي البصري ومنها أحكام القانون رقم ٦٢٥ لسنة ١٩٨٢ والمتعلق بقواعد تنظيم الاتصالات السمعية والبصرية، والتي أوجبت على متعهد الإيواء أن يحدد اسمه وموطنه، وإذا كان شخصا معنويا، فيجب تحديد اسم الشركة ومركزها واسم مديرها أو المسئول عنها، وتهدف هذه الإجراءات إلى تمكين الجمهور من معرفة بيانات كل شخص يساهم في بث معلومة أو إذاعة خدمة عن طريق أي وسيلة من وسائل الاتصال حتى يكون من السهل عليه توجيه دعوى المسئولية إلى الشخص المسئول عن الضرر.

ووفقا للفقرة ١١ لا يجوز أن يفرض على متعهد الإيواء التزام عام بمراقبة المعلومات التي يقوم بنقلها أو تخزينها، ولا التزام عام بالبحث عن الوقائع والظروف التي تكشف الأنشطة غير المشروعة، ولكن يتحمل متعهد الإيواء واجب التحقيق وفحص محتوى المعلومة المراد إيوائها ولا يكون مسئولا مدنيا إلا إذا علم بمحتوى المواقع أو تمادى على إبقاء الروابط رغم علمه بعدم مشروعية المعلومات والبيانات ولم يعمل على منع دخولها أو وصولها، فمناط المسئولية يكون علمه بالصفة غير المشروعة للمعلومات والبيانات التي يقوم بتخزينها أو نقلها [1].

وعلي ذات النهج سار المشرع الأوربي من خلال التوجيه الأوربي الخاص بالتجارة الإلكترونية الصادر في ١٧ يونيو عام ٢٠٠٠، حيث أقرت نصوص هذا التوجيه عدم التزام الوسطاء الفنيين برقابة مشروعية المعلومات والإعلانات التي تثبت

(١) د.عبد المهدي كاظم، المسئولية المدنية لوسطاء الانترنت، مجلة القادسية للقانون والعلوم السياسية، العدد الثاني، المجلد الثاني، ٢٠٠٩، ص٢٤٦.

عبر الموقع، وإنما فرضت عليهم أن يتصرفوا بشكل مناسب لمنع الوصول إلى المحتوى غير المشروع، كما أعفت الفقرة الأولي من المادة ١٢، مزود خدمة الانترنت من المسئولية عن الأعمال غير المشروعة التي يتضمنها الموقع إذا توافرت الشروط الآتية:

١- ألا يكون مصدر الضرر.

٢- ألا يكون قد اختار المرسل إليه الذي ينقل إليه المعلومات.

٣- ألا يختار المعلومات التي يقوم بنقلها أو يعدل فيها.

بينما تنص الفقرة الثانية على أن مزود الخدمة يتضمن تخزين مؤقت للمعلومات التي يقوم بنقلها، بيد أن هذا التخزين المؤقت لا يجعله مسئولا، ولا يجعل عمله يرقى إلى عمل متعهد الإيواء، ومن ثم لا يجب مساءلته[1].

غير أن عدم مسئولية مزود الخدمة عن مضمون المعلومات أو الخدمات التي تمر عبر أدواته الفنية، أمر مرهون باحتفاظه بكونه وسيطا بأدواته الفنية بين مستخدمي مواقع التواصل ومقدمي الخدمات والمعلومات، أما إذا تعدى هذا الدور، مما ارتقى به لمصاف المنتج أو المورد للمعلومات والبيانات والخدمات، انعقدت مسئوليته عن أي تعدي عن مضمون ومحتوى المعلومات والبيانات المدونة عبر صفحات التواصل، حيث أصبح بمكنته مراقبة المضمون والعلم بأي تعدي أو استغلال غير

(1) Directive 2000/31/CE du parlement Européen et du conseil du 8 juin 2000(relative à certains aspects juridiques des services de la société de l' information et notamment du commerce électronique, dans le marché intérieur(“ directive sur le commerce électronique”),Journal official des communautés européennes 178/117/7/2000.

مشروع لمضمونها[١]. ومن ثم يمكن تحقق مسئوليته على أساس الخطأ في الرقابة أو الحراسة كما سبق أن بينا.

وفي الصين حدث تطور هام عند اعتماد قانون المسئولية التقصيرية في ٢٦ ديسمبر ٢٠٠٩ الذي دخل النفاذ في ١ يوليو ٢٠١٠، حيث وضع مسئولية تقصيرية منفصلة تتعلق بالخصوصية، حيث أجاز للمعتدى على بياناته الرجوع بالتعويض عن الأضرار على مشغل موقع الإنترنت الذي يصبح على علم أو يتم إعلامه بانتهاك خصوصية مستخدم أخر أو المساس ببياناته الشخصية نتيجة لمحتوى يتم استضافته على موقعه الإلكتروني، حتى لو عجز عن إزالة هذا المحتوى، حيث يعتبر مسئولا بالتضامن والتكافل مع الشخص الذي نشر هذا المحتوى، ويجب عليه أن يبادر إلى إعطاء الطرف الذي لحقه الاعتداء على بياناته معلومات التسجيل الخاصة بالطرف المعتدي أو الذي قام بالنشر، فإن امتنع عن ذلك يصبح مسئولا عن المحتوى مسئولية مباشرة[٢].

وعلى مستوي التشريعات العربية يعد التشريع البحريني الأكثر تقدما، حيث كان الأسبق في تنظيم مسئولية مزودي الخدمة ووسيط الشبكة من خلال المادة ١٨، ١٩

---

(١) اتساقا مع هذا النهج قضت المحكمة العليا في مدينة نيويورك بمسئولية شركة prodigy عن مضمون الرسائل التي أرسلت عبر بريدها الالكتروني، وتضمنت معلومات وبيانات غير مشروعة، وذلك علي اعتبار أنها تقوم إلي جانب متعهد الوصول بدور مورد للمعلومات وكانت تملك وسائل الرقابة التي تسمح باستبعاد ومنع الرسائل غير المشروعة التي أرسلت عبر حسابها الالكتروني، وحيث ثبت تقصيرها، فيمكن مسألتها علي أساس الخطأ في واجب الحراسة أو الرقابة. راجع د. عبد المهدي كاظم، المرجع السابق، ص٢٣٤.

(٢) دراسة استقصائية عالمية حول خصوصية الإنترنت وحرية التعبير، إعداد توبي مندل (Toby mendel)وأندرو بوديفات (Andrew puddephatt) ، سلسلة اليونسكو بشأن حرية الإنترنت، متاح على الموقع التالي: https://books.google.com.bh/books .

من التشريع البحريني الصادر في ١٤ سبتمبر ٢٠٠٢ بشأن المعاملات الإلكترونية، والتي نفت المادة ١٩ منه المسئولية المدنية أو الجنائية لوسطاء الشبكة بشأن أي مادة خاصة بالغير وتكون في شكل سجلات، عندما يكون دوره مقصورا على مجرد التمكين من استخدام الشبكة، دون أن يكون هو المنشئ لتلك المادة، وذلك إذا كانت مسئوليته قائمة علي :

١- علم أو نشر أو إصدار أو توزيع هذه المواد بشكل سجلات إلكترونية أو أية بيانات تتضمنها هذه المواد.

٢- انتهاك أية حقوق قائمة بخصوص هذه المواد أو ما يتعلق بها.

كما يشترط المشرع لانتفاء مسئولية وسيط الشبكة ما يلي:

- عدم علمه بأنه ينشأ عن هذه المعلومات أية مسئولية مدنية أو جنائية.
- عدم علمه بأية وقائع أو ملابسات من شأنها أن تدل بحسب المجرى العادي للأمور، على قيام مسئوليته المدنية والجنائية.
- في حالة قيام وسيط الشبكة علي الفور- في حالة علمه بما تقدم- بإزالة المعلومات من أي نظام للمعلومات تحت سيطرته، ووقف توفير إمكانية الدخول على تلك المعلومات أو عرضها[١].

وبمفهوم المخالفة يتضح من النص أن مسئولية وسطاء الانترنت تتحقق عندما يكون دوره غير قاصر علي مجرد التمكين من استخدام الشبكة، وأيضا في الحالة التي

(١) راجع في ذلك المرسوم بقانون رقم (٢٨) لسنة ٢٠٠٢ بشأن المعاملات الإلكترونية في مملكة البحرين.

يكون فيها هو المنشئ للموقع الالكتروني الذي سبب الضرر، حيث يمكن تأسيس مسئوليته المدنية على أساس الخطأ في الحراسة والرقابة لتلك المواقع.

٢- مسئولية مالك أو مدير مواقع التواصل الالكتروني عن تعويض الضرر:

يمكن تعريف مالك أو مدير موقع التواصل الاجتماعي بأنه كل شخص طبيعي أو اعتباري يملك وسيلة إعلامية بمقتضاه يستطيع إنشاء وتأسيس مواقع للتواصل الاجتماعي، وذلك بعد حصوله على الترخيص أو الاعتماد اللازم.

ويحسب للقانون السوري تنظيمه لعملية امتلاك وإدارة موقع للتواصل من خلال نصه في المادة ٥ من قانون تنظيم التواصل على شبكة الانترنت ومكافحة الجريمة المعلوماتية، على ضرورة ذكر اسم صاحب الموقع الالكتروني وعنوانه وسجله التجاري في حال وجوده، وذلك حتى يمكن تحديد شخصية صاحب الموقع أو الصفحة الالكترونية، بما يمكن المضرورين من إقامة الدعوى في مواجهته والمطالبة بالتعويض(١).

كما حرص قانون مكافحة جرائم تقنية المعلومات الاتحادي الإماراتي رقم ٥ لسنة ٢٠١٢ على تجريم بعض الأفعال التي تتضمن إنشاء أو إدارة موقع تواصل اجتماعي بقصد تحقيق هدف أو أهداف غير مشروعة، كالترويج لأفكار من شأنها إثارة

(١) راجع الفقرة الأولي من نص المادة الخامسة من قانون تنظيم التواصل علي شبكة الانترنت ومكافحة الجريمة الالكترونية الصادر بالمرسوم التشريعي رقم ١٧ لسنة ٢٠١٢، والتي ورد نصها كالتالي" أ- على كل من يقدم خدمات التواصل علي الشبكة بالصفة الاحترافية أن يضع في موضع بارز في موقعه الالكتروني البيانات التالية: ١- اسم صاحب الموقع الالكتروني أو مقدم خدمات التواصل علي الشبكة وعنوانه، وسجله التجاري في حال وجوده ٢- اسم المدير المسئول في الموقع الالكتروني وعنوانه، ووسيلة وبيانات الاتصال به .٣- أي بيانات مطلوبة في أي قانون أخر، وبوجه خاص قانون الإعلام النافذ.٤- أي بيانات أخري تحددها التعليمات التنفيذية لهذا القانون".

الفتنة أو الطائفية أو الإضرار بالوحدة الوطنية، أو نشر معلومات أو رسوم أو أخبار من شأنها تعريض أمن وسلامة الدولة ومصالحها للخطر، أو لأجل الاتجار بالأسلحة النارية أو القطع الأثرية أو الفنية.

حيث جرم المشرع الإماراتي القيام بأي فعل إيجابي يتضمن إنشاء أحد الأشخاص لمنتدى على شبكة الإنترنت، وقام بالأعمال المادية اللازمة لذلك، كالولوج لشبكة الإنترنت وحجز مساحة على موقع الكتروني معين، والقيام بالبرمجيات وغيرها من الأعمال اللازمة للإنشاء والتأسيس، كما هو الحال بالنسبة لموقع التواصل الاجتماعي فيسبوك، كما يعد السلوك المادي لهذا الفعل متوافرا، في الحالة التي يقوم فيها مدير المجموعة في مواقع التواصل الاجتماعي بإنشاء مجموعة على أحد مواقع التواصل الاجتماعي بواسطة هاتفه النقال، كتأسيس مجموعة بواسطة نظام الواتس آب أو قيامه بتأسيس غرفة محادثة ودردشة على موقع بال توك.

ويؤخذ علي المشرع الإماراتي قصره الاهتمام بتجريم إدارة أو إنشاء موقع التواصل على بعض الجرائم التي تمس الصالح العام، وإغفاله الاهتمام بالجرائم وأفعال التعدي التي تلحق بالحياة الخاصة، خاصة في مجال التعدي على البيانات الشخصية للأفراد.

ومن ثم يمكن أن يكون المدعي عليه في دعوي المسئولية المدنية هو مالك، أو مدير، أو منشئ موقع التواصل الذي من خلاله تم الاعتداء علي الخصوصية وانتهاك حرمة البيانات الشخصية بدون رضاء من صاحبها، سواء تم التعدي بواسطته أو من قبل الغير ولكن بمساعدته الايجابية، أو نتيجة تقصيره في توفير درجة كافية من الأمان من أجل حماية بيانات وخصوصية أصحاب الحسابات عبر هذه المواقع، وفقا لقواعد المسئولية الشيئية على أساس الحراسة، كما تتحقق مسئوليته حتى ولو اقتصر دوره

علي إنشاء الموقع، بينما أحال مسألة إدارة الموقع لأشخاص أخرى، حيث تنعقد مسئوليته المدنية أيضا وفقا لقواعد مسئولية المتبوع عن أعمال تابعه إذا توافرات شروطها.

الفرع الثاني

القانون واجب التطبيق والمحكمة المختصة بدعوى المسئولية المدنية عن التعدي على البيانات الشخصية

غالبا ما تتضمن الشروط العامة لاستخدام وسائل الاتصال والتواصل الحديثة بندا يحدد القانون الواجب التطبيق والمحكمة المختصة بنظر النزاعات التي تنشأ بسبب استخدامها، كما يوجد شرطا مفادة اعتبار المستخدم قد وافق على ذلك بمجرد تسجيله لحساب عبر هذه الوسائل. لذا نتسائل عن مدى صحة وقانونية ذلك من خلال ما يلي:

أولا: القانون واجب التطبيق:

لا شك لدينا أنه بصرف النظر عن القانون الذي تحدده الشروط العامة للاستخدام، فإن مشكلة تحديد القانون واجب التطبيق ليست مسألة انعدام وإنما هي مسألة وفرة؛ إذ أنه بالنظر إلى عالمية شبكة الانترنت وتجاوزها الحدود الجغرافية لكافة دول العالم قد تفرض نوعا من التزاحم بين قوانين عدة دول[1]. وتعمل كل دولة على محاولة توسيع نطاق صلاحية قوانيها الوطنية لتشمل المحتوى الصادر خارج إقليمها الوطني، مع الأخذ في الاعتبار بأن ما قد يمثل أمرا قانونيا مشروعا في دولة معينة قد يمثل أمرا غير قانوني وغير مشروع في دولة أخرى.

(1) Michel Vivant, Cybermonde: Droit et droits des réseaux, JCP, 1996 II, n 43, p 407.

وفيما يخص الدعاوى المرفوعة في مجال وسائل التواصل الاجتماعي، يمكن للقاضي تطبيق القانون الوطني على منازعات المسئولية المدنية، متجاهلا ما تنص عليه الشروط العامة للاستخدام طالما أقيمت الدعوى أمام القضاء الوطنى لبلد المتضرر، حيث جرت العادة على اعتبار البند الوارد في الشروط العامة لوسائل التواصل من قبيل البند التعسفي خاصة عند تطبيقها على مستخدمين مقيمين خارج الولايات المتحدة باعتبار أن الشروط العامة تحيل إلى قانون دولة كاليفورنيا باعتبارها الدولة التي تتواجد فيها المقرات الرئيسية لشركات الاتصال والتواصل الحديثة، مما يمثل اجحافا بحق المستخدمين المتضررين من خارج الولايات المتحدة.

ويتضمن الإرشاد الأوروبي حول التجارة الإلكترونية مبدأ يقضي بأن مقدمي الخدمات يخضعون لقوانين بلادهم، مما دفع البعض بطلب التوسع في تطبيق المبدأ على مسئولية الوسطاء من أجل حماية المستخدمين والوسطاء أنفسهم، بدافع عدم مفاجأتهم بتطبيق قوانين أجنبية لا يعلمون عنها شيئا، مما قد يحد من حريتهم بالتعبير على الانترنت خوفا من التعرض للمسئولية[١].

وتعتبر أعمال التعدي على البيانات الشخصية عبر وسائل الاتصال والتواصل بمظاهرها السابقة من قبيل الأعمال غير القانونية المرتبة للمسئولية التقصيرية التي تخضع الدعوى الناشئة عنها لقانون مكان وقوع الفعل الضار أو مكان وقوع الضرر[٢].

(1) Cynthia Wong, James X. Dempsey, Mapping digital media, THE MEDIA AND LIABILITY FOR CONTENT ON THE INTERNET, May 2011, p 22. www.mappingdigitalmedia.org.

(2) Cassation, 1 ère chambre civile, 14/1/1997, n 94- 16861, Bull. Civ I, n 14.

وتنص المادة الرابعة من التوجيه الأوروبي لعام ١٩٩٥ حول معالجة البيانات الشخصية على أنه يطبق القانون الوطني الأوروبي في حال كان مركز المسئول عن المعالجة، أي الشخص الذي يحدد أهدافها ووسائلها، موجودا على أراضي الدولة. بينما جاء النظام الأوروبي الجديد لعام ٢٠١٦ حول البيانات الشخصية والذي سيطبق بدءا من تاريخ ٢٥/٥/٢٠١٨ والذي ألغي التوجيه السابق لعام ١٩٩٥، لينص في المادة الثالثة منه على تطبيقه على معالجة بيانات شخصية من قبل مسئول عنها يكون مركزه في الإتحاد الأوروبي، أو في حال تعلقها بسلع وخدمات لأشخاص في الإتحاد الأوروبي، أو تعلقت بمراقبة سلوكهم الحاصل ضمن الإتحاد الأوروبي.

وقضت محكمة العدل الأوروبية حديثا، وتحديدا بتاريخ ١٣/٥/٢٠١٦ بأن القانون الوطني الفرنسي هو الواجب التطبيق بالاستناد إلى تنزيل جوجل لكعكات على حواسب المستخدمين، حيث افترضت أن جوجل يقوم بمعالجة البيانات الشخصية على أرض أوروبية، كما اعتبرت أن جوجل تقيم على أرض أوروبية وفقا لوجود فروع متعددة له على الأراضي الأوربية [1].

يتضح مما سبق إمكان انعقاد الإختصاص بدعوى المسئولية المدنية لأحكام القانون الوطني لبلد المتضرر، أو لقانون مكان وقوع الاعتداء حال كان الاعتداء من قبل شخص أو أفراد ينتمون لنفس الدولة، كما يمكن للقاضي الوطني أن يطلب من وسيلة التواصل تقديم جميع عناصر الاثبات التي تحوزها للاستعانة بها في إطار التحقيقات القضائية القائمة

(1) Cour de justice de l'Union européenne, 13/5/2014, cité dans: Fabrice Mattatia, Internet et les réseaux sociaux, que dit la loi? Eyrolles, 2ème édition, 2016, p 70.

ثانيا: المحكمة المختصة بدعوى المسئولية المدنية

وفقا للشروط العامة للاستخدام تعقد وسائل التواصل الاجتماعي الاختصاص بنظر المنازعات الناشئة عبر وسائلها إلى محاكم سان فرانسيسكو، بيد أن محمكة العدل الأوروبية قد نصت في حكمها الصادر بتاريخ ٢٧/٥/٢٠٠٠ بأن البند المعطى للصلاحية الحصرية لمحكمة قد تكون بعيدة عن محل إقامة المتقاضي، هو بند تعسفي، يصعب من إمكانية مثول المتقاضي أمام القضاء للمطالبة بحقه [١].

وتعليقا على تمسك جهة الفيسبوك بإنعقاد الاختصاص للمحكمة التي تم اسناد الاختصاص إليها بموجب الشروط العامة للاستخدام؛ فقد صدر قرار محكمة الاستئناف في بو بفرنسا بتاريخ ٢٣/٣/٢٠١٢ يقضي بأن بند الصلاحية الوارد ضمن شروط الاستخدام العامة لفيسبوك لا يحتج به إلا قبل الطرف الذي علم به وقبله صراحة. وبما أن البند الوارد كان مستغرقا ضمن بنود كثيرة مكتوبة بخط صغير وباللغة الإنجليزية، فإنه يعتبر في حكم غير المكتوب، ويكون الضرر المزعوم اللاحق لإغلاق حساب المدعي المستخدم قد حصل على الإقليم الفرنسي، مما يجعل معه القضاء الفرنسي هو المختص بالنظر في الدعوى[٢].

يتضح من ذلك ميل القضاء لتسهيل عملية التقاضي على المستخدم الضعيف الذي يثقله الانتقال إلى المحكمة المحددة وفقا لشروط وسائل التواصل، ومن ثم قد تدفع

---

(1) European Court of Justice, 27 June 2000, Arrêt Océano Grupo, In Joined Cases C-240/98 to C-244/98. مشار إليه عند د. وسيم شفيق الحجار، المرجع السابق، ص ١٢٥.

(2) Cour d'appel de Pau, 1ère chambre, 23/3/2012, Sébatien R./Facebook, Légipresse 2012, n 294-03, p 280; Bérad F., Facebook: quand la Cour d'appel de Pau crée le buzz.., Gaz. Pal., 17/5/2012, p 11.

به تلك الصعوبات إلى التنازل عن حقه، وعدم رفع الدعوى، ومن ثم تكون المحكمة الوطنية لبلد المضرور هي الأقدر على الفصل في النزاع المعروض عليها خاصة فيما يتعلق بمسائل الاعتداء على البيانات الشخصية عبر مواقع التواصل والاتصال الحديثة.

الفرع الثالث

أثر دعوى المسئولية المدنية لمخاطر وسائل التواصل الاجتماعي

يتمثل هدف المسئولية المدنية في التعويض اللازم لجبر الأضرار المتحققة. بيد أن التعويض كأثر للمسئولية المدنية قد شهد تطورًا في الآونة الأخيرة فيما يتعلق بالأساس الذي يقدر بناءً عليه. ومما لم يعد خلافًا عليه أن التعويض قد يكون نقديًا أو عينيًا[1].

ونتعرض لدراسة قواعد تقدير التعويض عن الأضرار المتحققة بفعل وسائل التواصل الحديثة من خلال بيان أساس تقدير التعويض، وأنواع التعويض وطرق تقديره.

أولا: أساس تقدير التعويض

يدور التعويض، باعتباره جزاء للمسئولية المدنية، وجودًا وعدمًا مع الضرر. فالمسئولية يمكن أن تقام في بعض الحالات دون اللجوء إلى فكرة الخطأ، ولكنها لا تقوم إلا بالضرر. وبناءً عليه يعد الضرر أساس التعويض، ومناطه.

(١) د. إبراهيم الدسوقي أبو الليل، تعويض الضرر في المسئولية المدنية، دراسة تحليلية تأصيلية لتقدير التعويض، مطبوعات جامعة الكويت، ١٩٩٥، ص١٤.

فلما كان الضرر ركنًا من أركان المسئولية، فإنه يجب لتوافرها أن يترتب ضرر على الفعل الخاطئ الذي من خلال تم التعدي على البيانات الشخصية عبر موقع التواصل وانتهاك الحق في الخصوصية. فالحق في المطالبة بالتعويض ينشأ من الوقت الذي يصبح فيه الضرر محقق الوقوع، وليس من وقت وقوعه فعلاً، ولا من وقت حدوث الخطأ[١]. وإثبات وقوع الضرر إنما يقع على المدعي طبقًا لقاعدة البينة على من ادعى، وإن كانت هناك بعض الحالات الاستثنائية التي يكون الضرر فيها مفترضًا[٢]. وبناءً على ذلك، فعند وقوع الضرر وباقي الأركان الأخرى، فإن عناصر المسئولية تتوافر. ومتى تخلف الضرر عن الخطأ وتأخر فإن أركان المسئولية تكون ناقصة وغير متوافرة للحكم بالتعويض، أي أن المعول عليه في التعويض هو الضرر اللاحق بالمستخدم من خلال الاعتداء على بياناته.

ولا شك لدينا أن مجال شبكات الاتصال والتواصل بالنظر لحداثتها، وخصوصية مجال استخدامه عبر شبكة عنكبوتية إلكترونية معقدة، يصعب على المستخدم العادي فهم فحواها، وطرق أغوارها، يجعل من العسير التمسك بقواعد المسئولية التقليدية في ضرورة إثبات الخطأ، حيث عملية إثبات كيفية التعدي من خلال اختراق صفحات التواصل وحسابات البريد الالكتروني وملفات بنوك المعلومات، يحتاج إلى قدر من

(١) د. سمير عبد السميع الأودن، مسئولية الطبيب الجراح وطبيب التخدير، دار المعارف، الإسكندرية، ٢٠٠٤، ص٤٠٦.

(٢) يكون الضرر مفترضًا حيث توجد قرينة لصالح المضرور، هذه القرينة قد تكون مفروضة من المشرع أو بإرادة الطرفين. ومن أمثلة الأولى ما قررته المادة ١٢٨ من القانون المدني من أنه "لا يشترط لاستحقاق فوائد تأخير قانونية كانت أو اتفاقية أن يثبت الدائن ضررًا لحقه من هذا التأخير"؛ إذ تعفي هذه المادة الدائن من إثبات الضرر رغم كونه أساس التعويض. ومن أمثلة القرينة التي تنتج بإرادة الطرفين، ما يدرج عادة في العقود ويطلق عليه الشرط الجزائي. حيث يعتبر في حقيقة الأمر تعويضًا اتفاقيًا لا يلتزم فيه المدعي بإثبات الضرر.

التخصص بل والتخصص الدقيق في مجال البرمجة والالكترونيات، الأمر غير المتحقق غالبا للمستخدم العادي لمواقع التواصل الاجتماعي وسائر مواقع الاتصال الإلكترونية الأخرى المعبئة بالبيانات الشخصية للمستخدمين(١). ومن ثم فكيف يستطيع أن يثبت خطأ محددًا في خضم التعقد التقني المصاحب لشبكة الانترنت. وبناءً على ذلك، فإن الأوفق لمصلحة المستخدم العادي الذي أصابه الضرر أن يتحمل المعتدي إذا أمكن تحديد شخصيته تعويض الضرر وفقا للقاعدة العامة التي تقضي بإلزام محدث الضرر بالغير بضرورة تعويضه، كما يمكن الرجوع بالتعويض على وسطاء الشبكة إذا ثبت دورهم في تحقيق الضرر وانتفت بشأنهم حالات الإعفاء من المسئولية المحددة على النحو السابق، كما يمكن الرجوع على مالك أو مدير موقع التواصل أو منشئ ومدير بنك المعلومات، وتحميلهم مسئولية التعويض بمجرد حدوث الضرر، وذلك في الحالة يتعذر فيها إثبات الخطأ الفعلي في جانب المسئول شريطة قيام سببية مباشرة بين الضرر واستخدام مواقعهم بناء على قواعد المسئولية الموضوعية أو بناء على قواعد المسئولية الشيئية خاصة فيما يتعلق بالخطأ في الحراسة أو الرقابة.

ثانيا: أنواع التعويض وطرق تقديره

تختلف أنواع التعويض عن الضرر الذي يلحق المضرور باختلاف نوعه وما إذا كان الضرر ماديا أو أدبيا. ولا شك أن مبلغ التعويض يجب أن يشمل ما فات المضرور من كسب، وما حاق به من خسارة. هذا ويعتبر التعويض النقدي هو الأصل، أما التعويض العيني فالحكم به جوازي للقاضي.

(١) د. عايد رجا الخلايلة، المسئولية التقصيرية الالكترونية، المسئولية الناشئة عن استخدام الحاسوب والإنترنت، دار الثقافة، ٢٠٠٩، ص٤٨.

١- التعويض النقدي:

حيث يقدر القاضي التعويض بمبلغ من النقود، يكفي لجبر الضرر، حيث تنص المادة ٥٠ من القانون المدني المصري على أنه" لكل من وقع عليه اعتداء غير مشروع في حق من الحقوق الملازمة لشخصيته، أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من ضرر".

ومن ثم يحاول القاضي من خلال فرضه التعويض، جبر وإصلاح الأذى الذي أصاب المضرور بفعل وسائل الاتصال والتواصل الحديثة نتيجة الاعتداء على حرمة بياناته الشخصية وحرمة حياته الخاصة عبر هذه الوسائل.

ولا يثير التقدير النقدي أو المالي للتعويض عن الضرر المادي الذي لحق المضرور أي صعوبات، لأنه يكون عادة مقدر بقدر الضرر، الأمر الذي يمكن تحقيقه من خلال نص المادة١/٢٢١ من القانون المدني المصري يقابلها نص المادة ١٦١ من القانون المدني البحريني، والمادة ٢٨٨ من القانون المدني الأردني، التي تلزم القاضي بضرورة مراعاة أن يشمل التعويض مقدار الخسائر التي لحقت المضرور جراء التعدي، ومقدار ما فاته من كسب، شريطة أن يكون ذلك نتيجة طبيعية للاعتداء.

بيد أن الصعوبة تواجه القاضي عند تقديره لمبلغ التعويض النقدي عن الضرر الأدبي الذي لحق بالمضرور جراء المساس بخصوصياته، حيث قد تكون المصلحة الأدبية التي تم المساس بها لا تقبل التقدير بالنقود، أو على الأقل يتعذر تقدير مبلغ نقدي يوازيها أو يعادلها. غير أن الفقه قد اتفق على أهمية فرض التعويض النقدي عنها أيضا، على اعتبار أنها على الأقل تقدم ترضيه ولو بسيطة للمضرور.

وعلى ذلك يحاول القاضي الاجتهاد من أجل الوصول لتقدير التعويض بمبلغ يتناسب مع مقدار الأضرار وفقا للظروف الملابسة.

٢- التعويض العيني:

في مجال تعويض الأضرار التي تلحق بالمضرور عبر وسائل الاتصال الاتصال والتواصل الحديثة، قد يرى القاضي أن التعويض العيني يمكن أن يقدم ترضية مناسبة للمضرور، فيحكم به القاضي بناء على طلب من المضرور. حيث يهدف إلى إعادة الحال إلى ما كانت عليه قبل التعدي، أو إزالة الأثر الضار الذي ترتب على الاعتداء. ومن ثم قد يجد القاضي أن إمكانية إزالة أثر التعدي الذي وقع على البيانات الشخصية مازالت متاحة، ويحدث ذلك عندما يتمثل التعدي في سرقة بيانات المضرور أو صوره وبثها في مواقع إباحية، أو نشر هذه المعلومات بطريقة تسئ لصاحبها، أو استخدام بياناته وكلمات مروره في الحصول على أموال من حساباته البنكية، فيحكم القاضي بوقف التعدي، ثم إزالة هذه الصور والبيانات من هذه المواقع، ونشر تصحيح واعتذار يزيل الأثر الضار الذي رتبه التعدي، أو إعادة الأموال التي تم سحبها من حسابات المستخدم إليها مرة ثانية.

ويبقي أن نشير إلى أن التعويض هنا يكون مقياسه الضرر المباشر، ومن ثم التعويض في أية صورة كانت، تعويضا عينيا أو بمقابل، تعويضا نقديا أو غير نقدي، مقسطا أو إيرادا مدى الحياة، يقدر بمقدار الضرر المباشر الذي أحدثه الخطأ أو التعدي، سواء أكان الضرر ماديا أو أدبيا، وسواء كان متوقعا أو غير متوقع، وسواء كان حالا أو مستقبلا مادام أنه محقق.

الخاتمة

تناولنا بالدراسة خصوصية الحماية المدنية للمعلومات والبيانات الشخصية في مواجهة الثورة التكنولوجية لوسائل الاتصال والتواصل، حيث قسمت الدراسة لفصلين، تناول الفصل الأول منهما لأثر تكنولوجيا الاتصال والإعلام على خصوصية المعلومات الشخصية، وتعرض المبحث الأول للمفهوم القانوني للمعلومات الشخصية في ظلال الثورة المعلوماتية، بينما ناقش المبحث الثاني مظاهر الاعتداء على البيانات الشخصية عبر تكنولوجيا الإعلام والاتصال، وتناول الفصل الثاني بالدراسة لحماية البيانات الشخصية في عصر التقنيات الحديثة من خلال مبحثين تناول المبحث الأول قواعد حماية الخصوصية المعلوماتية للبيانات الشخصية عبر وسائل الاتصال والتواصل الحديثة من خلال التعرض لقواعد الحماية على المستوى الدولي والوطني، بينما جاء المبحث الثاني بعنوان وسائل مواجهة الاعتداءات على البيانات الشخصية في عصر الاتصال والتواصل متعرضا بالدراسة لوسائل الحماية الوقائية للبيانات الشخصية من مخاطر تقنيات الاتصال الحديثة في المطلب الأول، بينما تناول المطلب الثاني دراسة المسئولية المدنية عن الأضرار التي تسببها وسائل الاتصال الحديثة.

ومن خلال هذه الدراسة توصلنا إلى النتائج التالية:

١- يعد مبدأ حماية البيانات الشخصية للأفراد أمرا منبثقا من مبدأ الخصوصية، وتعد خصوصية البيانات الشخصية عبر مواقع التواصل الاتصال والتواصل الحديثة خاصة وعبر شبكة الانترنت عامةً من أحدث أنواع الخصوصية التي تكفل حق الفرد في توفير الحماية لبياناته ومعلوماته الشخصية، التي أفصح عنها طواعية عبر جميع مواقع الاتصال والتواصل.

٢- تمثل مفهوم البيانات الشخصية في تلك البيانات التي يمكن من خلالها تعريف الشخص تعريفًا محددا، أو تُمكن من الاستدلال عليه، وتشمل أيضا آراء الشخص ومعتقداته وتوجهاته العقائدية والسياسية كما سبق بيانه.

٣- انعكست الثورة التكنولوجية الهائلة في عالم الاتصال على تزايد أهمية بعض المواقع التي راج استخدامها من قبل الأفراد بشكل شبه دائم، وشبه لحظي، أطلق عليها مواقع التواصل الاجتماعي، والتي أضحت منبرا للأفراد للتعبير عن آرائهم، وحالتهم، وبياناتهم، ويمكن خلالها التعارف والتعامل والتواصل، بل أصبحت وسيلة للإعلان التجاري، ويمكن من خلالها البيع والشراء. تلك المواقع بالرغم من ايجابياتها الظاهرة، إلا أنه لابد من الحذر من سلبياتها، حيث يستخدمها البعض بصورة غير مشروعة تتضمن مساسا واعتداءً علي خصوصية الأفراد.

٤- نظرا لتزايد الإقبال علي التعامل والتفاعل بين الأفراد عبر مواقع الاتصال والتواصل الحديثة، أصبحت خصوصية البيانات الشخصية مهددة، وصارت بيانات رواد هذه المواقع مادة هامة جدا يتم استخدامها تجاريا في تنفيذ دعاية تسويقية لبعض الشركات والجهات التجارية، أو حتي يتم مراقبتها من قبل جهات حكومية، فضلا عن تعرضها للسرقة والاختراق من قبل محترفي التعامل بشبكة الانترنت (الهاكر)، ثم استخدامها في أغراض قد تكون غير مشروعة لتحقيق مكاسب غير شرعية.

٥- فرضت الأهمية التي استبغت بها مواقع الاتصال والتواصل ضرورة توفير الحماية القانونية للبيانات الشخصية التي تم إعلانها طواعية من خلالها، وعدم افتقادها الحماية لمجرد علانيتها أو الإفصاح عنها من قبل أصحابها، حيث إن الاستيلاء علي البيانات أو معالجتها بدون وجه حق، يمثل اختراقا لحماية هذه البيانات.

٦- في مواجهة الانتهاكات التي تتعرض لها البيانات الشخصية بكافة مظاهرها على النحو السابق، بدأت محاولات توفير الحماية للبيانات الشخصية ضد مخاطر تكنولوجيا الإعلام والاتصال، ودأب رجال القانون إلى البحث عن آليات وضمانات قانونية توفر الحماية الفاعلة، كما دأب التقنيين على محاولة توفير الحماية التقنية للبيانات الشخصية عبر سياسة الخصوصية على هذه المواقع.

٧- لا تمثل أنظمة حماية البيانات الشخصية الحالية أداة فعالة لمواجهة مخاطر الاعتداء على البيانات الشخصية، لكونها غير مجهزة للتعامل مع العدد الذي لا يحصى من التحديات التي تواجه الخصوصية من خلال الانترنت والتقدم التكنولوجي، والتي يتمثل أهمها في الانتشار الواسع وتعدد الوظائف في بيئة خدمات الاتصالات الإلكترونية، فضلا عن قدراتها التفاعلية، والطابع الدولي لمنتجي الشبكات والخدمات.

التوصيات:

١- بالنظر إلي الأهمية الدستورية للحق في الخصوصية ومنها البيانات الشخصية عبر مواقع الاتصال والتواصل، فيجب إلزام وسطاء الانترنت وملاك ومديري مواقع التواصل بوضع نظام يضمن التشفير وإخفاء الهوية القابل للعكس، من أجل توفير الحماية ضد الوصول لمحتوى البيانات والاتصالات.

٢- تشجيع التوجهات التكنولوجية بما يتفق مع تحسين وضع الأشخاص المحميين من الناحية القانونية، بما يتطلبه ذلك من توفير الأدوات اللازمة للامتثال بقواعد حماية البيانات، وتوفير قدر من الشفافية، يتمكن المستخدمون من السيطرة الكاملة على البيانات المرسلة والمستقبلة عبر صفحات المواقع الإلكترونية للاتصال والتواصل.

٣- ضرورة وضع ميثاق شرف، أو مدونة سلوك خاص بالإعلام الالكتروني عبر شبكات التواصل الاجتماعي يحدد الضوابط القانونية والأخلاقية لاستخدامها.

٤- إعداد قواعد قانونية لحماية بياناتنا وخصوصياتنا لمواجهة الثورة التكنولوجية في مجال الاتصال والتواصل بسلبياتها المتقدمة، تعادل قواعد حماية الخصوصية للمستهلك في العالم المادي.

٥- تحديد واجبات والتزامات قانونية علي عاتق مقدمي خدمات الانترنت ومديري مواقع التواصل والاتصال الحديثة تمكن من توفير الحماية اللازمة للبيانات

الشخصية، وتتيح اتخاذ الإجراءات اللازمة لمنع المنافسة والممارسات غير المشروعة. ومن ثم تحقق مسئوليتهم المدنية عند الإخلال بأي من هذه الالتزامات.

٦- نحث المشرع المصري بضرورة الإسراع لمعالجة ذلك النقص التشريعي حيال حماية البيانات الشخصية من خلال إصدار قانون ينظم طرق جمع البيانات من خلال الوسائل المشروعة، ويحدد كيفية الحفاظ عليها، وطرق معالجتها وضوابط المعالجة، ويكفل الحماية القانونية اللازمة لمنع التعدي عليها.

٧- حث المشرعين في الدول العربية علي تطوير قواعد المسئولية المدنية لكي تتمكن من مواجهة الآثار الضارة التي خلفها الجانب السلبي للثورة التكنولوجية الهائلة في مجال الاتصالات.

٨- عدم الاعتداد بالخطأ واجب الإثبات كأساس مطلق لاستحقاق التعويض عن الأضرار التي يسببها الاعتداء علي البيانات الشخصية عبر مواقع الاتصال والتواصل الحديثة.

٩- ضرورة اعتماد المشرع لقواعد خاصة من شأنها أن توفر الحماية للبريد الإلكتروني ولخصوصية البيانات والمراسلات الواردة والصادرة من خلاله، باعتباره أضحى أهم وأوسع طرق الاتصال والمراسلة حاليا.

١٠- إعمال قواعد المسئولية الشيئية خاصة ما يتعلق منها بجانب الخطأ في الحراسة، باعتباره حلا قانونيا أنسب يمكن من إسناد الخطأ إلى أشخاص محددة ومعروفة، حال عدم إمكان الوقوف على حقيقة شخص المعتدى.

قائمة المراجع

أولا: المراجع العربية:

١- د. إبراهيم الدسوقي أبو الليل، تعويض الضرر في المسئولية المدنية، دراسة تحليلية تأصيلية لتقدير التعويض، مطبوعات جامعة الكويت، ١٩٩٥.

٢- د. إبراهيم بن داود، د. أشرف شعت، الاطلاع على البريد الالكتروني بين متطلبات النظام العام والحق في سرية المراسلات، دفاتر السياسة والقانون، العدد ١٦، ٢٠١٧.

٣- د. أحمد خليفة الملط، الجرائم المعلوماتية، دار الفكر الجامعي، الطبعة الثانية، ٢٠٠٦.

٤- د. أحمد شرف الدين، عناصر الضرر الجسدي وانتقال الحق في التعويض عنها إلى شخص أخر غير المضرور، بحث منشور بمجلة قضايا الدولة، ١٩٧٨.

٥- د. أحمد شوقي عبد الرحمن، مسئولية المتبوع باعتباره حارسًا، دار الفكر العربي، القاهرة، ١٩٩٨.

٦- د. أحمد محمود مصطفى، جرائم الحاسب الآلية في التشريع المصري، دراسة مقارنة، رسالة دكتوراه، جامعة القاهرة، كلية الحقوق، ٢٠١٦.

٧- د. السيد حمد مرجان ، ثورة المعلومات والحق في بناء مجتمع معرفي بين سياسات السلطة وأخلاقيات المهنة، بحث منشور بمجلة الفكر القانوني والاقتصادي ـ كلية الحقوق – جامعة بنها، لأعمال مؤتمر " الجوانب القانونية والاقتصادية للانفتاح المعلوماتي- ثورة المعلومات المنعقد في ٣١ مايو ٢٠١١.

٨- د. جلال الدين الشيخ زيادة، العلاقة بين الإعلام التقليدي وشبكات التواصل الاجتماعي: الخصوصية والمهنية، دراسة مقارنة، بحث منشور ضمن أعمال مؤتمر وسائل التواصل الاجتماعي- التطبيقات والإشكاليات المنهجية- التي نظمته

كلية إدارة الأعمال – جامعة الأمام محمد بن سعود الإسلامية في الفترة من ١٠- ١١ مارس ،٢٠١٥.

٩- د. حسام الدين الأهواني ، الحق في احترام الحياة الخاصة، دار النهضة العربية، القاهرة، ١٩٧٨.

١٠- م. حسام شوقي: حماية وأمن المعلومات على الإنترنت، دار الكتب العلمية للنشر والتوزيع، القاهرة، ٢٠٠٣.

١١- د. حسن جميعي، مسئولية المنتج عن الأضرار التي تسببها منتجاته المعيبة، دار النهضة العربية، القاهرة، ٢٠٠٠.

١٢- د. خالد حامد مصطفي، المسئولية الجنائية لناشري الخدمات التقنية ومقدميها عن سوء استخدام شبكات التواصل، مجلة رؤى إستراتيجية- مركز الإمارات العربية للدراسات والبحوث، المجلد الأول، العدد الثاني، مارس ٢٠١٣.

١٣- د. خالد ممدوح ابراهيم، الجريمة الإلكترونية، الدار الجامعية، ٢٠٠٨.

١٤-د. ذياب موسي البداينة،جرائم الحاسب والانترنت، أبحاث الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، جامعة نايف للعلوم الأمنية، الرياض، ١٤٢٠.

١٥- د. سامح عبد الواحد، الحماية القانونية للبيانات الشخصية، مجلة الحقوق الكويتية، العدد الرابع ٢٠١١.

١٦- د. سليمان مرقس، الوافي في شرح القانون المدني، الفعل الضار، الجزء الثالث.

١٧- د. سمير عبد السميع الأودن، مسئولية الطبيب الجراح وطبيب التخدير، دار المعارف، الإسكندرية، ٢٠٠٤.

١٨- د. شريف خاطر، حماية الحق في الخصوصية المعلوماتية، مجلة كلية الحقوق - جامعة المنصورة للبحوث القانونية والاقتصادية، الجزء الثاني، العدد ٥٧، أبريل ٢٠١٥.

١٩- د. شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات على الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، الطبعة الأولى، دار النهضة العربية، القاهرة، ٢٠٠٥.

٢٠- د.صدقي محمد أمين، التعويض عن الضرر ومدي انتقاله للورثة، الطبعة الأولي، ٢٠١٤.

٢١- د. صلاح محمد دياب، الحماية القانونية للحياة الخاصة للعامل وضمانتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب القانونية، الإسكندرية، ٢٠١٠.

٢٢- د. طارق سرور، جرائم النشر والإعلام، الكتاب الأول، الأحكام الموضوعية، الطبعة الأولي، دار النهضة العربية ، القاهرة، ٢٠٠٤.

٢٣- د. عايد رجا الخلايلة، المسئولية التقصيرية الالكترونية، المسئولية الناشئة عن استخدام الحاسوب والإنترنت، دار الثقافة، ٢٠٠٩.

٢٤- د. عباس مصطفي صادق، الصحافة والكمبيوتر، الدار العربية للعلوم، بيروت، ٢٠٠٥.

٢٥- د. عبد الحميد نجاشي ، حدود التزام المشترك بحقوق الملكية الفكرية لمؤلف قاعدة البيانات على شبكة الانترنت. بحث منشور بمجلة الفكر القانوني والاقتصادي - كلية الحقوق – جامعة بنها، لأعمال مؤتمر " الجوانب القانونية والاقتصادية للانفتاح المعلوماتي- ثورة المعلومات المنعقد في ٣١ مايو ٢٠١١.

٢٦- د. عبد الفتاح بيومي حجازي، مكافحة جرائم المصارف الالكترونية، ورقة عمل ضمن ندوة المصارف الإلكترونية، الجمعية المصرية لقانون الإنترنت المنعقدة في ١٣ مايو ٢٠٠٧.

٢٧- د. عبد الفتاح بيومي حجازي، الحماية الفنية والجنائية لنظام الحكومة الإلكترونية، دار الفكر الجامعي، الإسكندرية، ٢٠٠٣.

٢٧- عبد الله بن ناصر بن أحمد العمري، رسالة ماجستير، كلية الدراسات العليا،جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٠.

٢٨- د. عبد المنعم أحمد سلطان، التقنيات المعلوماتية وأثرها على حماية الحياة الخاصة بين الفقه الإسلامي والقانون الوضعي، بحث منشور بمجلة الفكر القانوني والاقتصادي - كلية الحقوق – جامعة بنها، لأعمال مؤتمر " الجوانب القانونية والاقتصادية للانفتاح المعلوماتي- ثورة المعلومات المنعقد في ٣١ مايو ٢٠١١.

٢٩- د.عبد المهدي كاظم، المسئولية المدنية لوسطاء الانترنت، مجلة القادسية للقانون والعلوم السياسية، العدد الثاني، المجلد الثاني، ٢٠٠٩.

٣٠- د.عبد الهادي فوزي العوضي، الجوانب القانونية للبريد الالكتروني، دار النهضة العربية، القاهرة، بدون سنة نشر.

٣١- عرب يونس، الجزء الثاني، الخصوصية وأمن المعلومات في الأعمال اللاسلكية بواسطة الهاتف الخلوي، ورقة عمل مقدمة لمنتدى العمل الالكتروني، إتحاد المصارف العربية، عمان، ٢٠٠١.

٣٢- د. عفيفي كامل عفيفي، جرائم الكمبيوتر، منشورات الحلبي، بيروت، ٢٠٠٣.

٣٣- د. علي عبد الله القهوجي، الحماية الجنائية، للبيانات المعالجة إلكترونيا، بحث مقدم إلى مؤتمر القانون والكمبيوتر والإنترنت، جامعة الإمارات، مايو ٢٠٠٨.

34- د. علي بن هادي البشري، الجهود القانونية للحد من جرائم الحاسب الآلي، مطابع جاد للأوفست، الرياض، ١٤٢٦هـ.

٣٥- د. فريد جبور، حماية البيانات الشخصية، مقال منشور على الموقع الإلكتروني التالي:

https://lita-lb.org/archive/56-questions-answers-html

٣٦- د. فيصل على خالد فرحان المخلافى، المؤسسات الإعلامية في عصر تكنولوجيا المعلومات، دراسة لواقع المؤسسات الصحفية اليمنية،المكتب الجامعي الحديث، ٢٠٠٥.

٣٧- د.محمد الشوا، ثورة المعلومات وانعكاسها على قانون العقوبات، دار النهضة العربية، الطبعة الثانية، القاهرة، ٢٠٠٠.

٣٨- د.محمد حسين منصور، المسئولية الإلكترونية، دار الجامعة الجديدة، الإسكندرية، ٢٠٠٣.

٣٩- د.محمد بن عبد العزيز بن صالح، المسئولية الجنائية عن إساءة استخدام وسائل التواصل الاجتماعي الحديثة – دراسة تأصيلية تطبيقية- رسالة دكتوراه، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٤.

٤٠- د. محمد عبد المحسن المقاطع، حماية الحياة الخاصة للأفراد وضمانتها في مواجهة الحاسوب الآلي، الكويت، بدون ناشر،١٩٩٢.

٤١- د. مدحت رمضان، جرائم الاعتداء على الأشخاص والانترنت، دار النهضة العربية، ٢٠٠٢.

٤٢- د. مدحت محمد محمود، مفهوم وأهداف وخصائص شبكات التواصل الاجتماعي، بحث مقدم لمؤتمر ضوابط استخدام شبكات التواصل الاجتماعي في الإسلام، الجامعة الإسلامية، الرياض،٢٠١٦.

٤٣- د.منصور بن صالح السلمي، المسئولية المدنية لانتهاك الخصوصية في نظام مكافحة جرائم المعلوماتية السعودي، جامعة نايف للعلوم الأمنية، الرياض، ٢٠١٠.

٤٤- أ. مريم نريمان نومار، استخدام مواقع الشبكات الاجتماعية وتأثيره في العلاقات الاجتماعية- دراسة عينة من مستخدمي الفيسبوك بالجزائر، رسالة ماجستير، جامعة الحاج لخضير- باتنة،٢٠١١.

٤٥ - د. نبيل عبد المنعم جاد، جرائم الحاسب الآلي، مركز أبحاث شرطة دبي، ١٩٩٩.

٤٦ - د. نعيم مغبغب، مخاطر المعلوماتية والانترنت منشورات الحلبي القانونية، بيروت، الطبعة الثانية، ٢٠٠٨.

٤٧ - د. نهلا عبد القادر المومني ، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان ٢٠٠٨.

٤٨ - د. ليلي حسام الدين أحمد،:أثر التقدم في تكنولوجيا المعلومات على الخصائص النوعية والكمية للموارد البشرية، مؤلف من إصدارات المنظمة العربية للتنمية الإدارية،القاهرة، ٢٠١١.

٤٩ - د.وسيم شفيق الحجار، النظام القانوني لوسائل التواصل الاجتماعي، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، الطبعة الأولى، بيروت – لبنان، ٢٠١٧.

المراجع الانجليزية:

1- **Adrienne Felt, David Evans, Privacy Protection for Social Networking APIs, University of Virginia Charlottesville, VA, http://www.cs.virginia.edu/~evans/pubs/proxy/privacybyproxy.**

2- **Céline Castets -Renard, Droit de l'Internet: Droit français et européen, 2ème edition, Montchrestien, L'extenso éditions, 2012.**

3- **Christopher F. Spinelli, Social Media: No 'Friend' of Personal Privacy, The Elon Journal of Undergraduate Research in Communications, Vol 1, No 2, Fall 2010.**

4- David Beer: Social network (ing) sites…revisiting the story so far : A response to danah body & Nicole Ellison, Journal of computer – Mediated Communication, V.13 (2),P516-529. Janury 2008.

5- Lothar Determann, Social Media Privacy: A Dozen Myths and Facts, 2012 STANFORD TECHNOLOGY LAW REVIEW. 7 .

http://stlr.stanford.edu/pdf/determann-socialmediaprivacy.pdf

6- Michael SAX, data collection and privacy protection: An international perspective,on line at, 6 august,1999.

7- Nemone Franks, Social media and the law: A handbook for UK companies, January 2014,

http://www.linklaters.com/pdfs/mkt/london/TMT-Social-Media-Report

المراجع الفرنسية:

1- Cynthia Wong, James X. Dempsey, Mapping digital media, THE MEDIA AND LIABILITY FOR CONTENT ON THE INTERNET, May 2011. www.mappingdigitalmedia.org.

2- Flora Fischer, CIGREF, Marie-Noelle Gibon, Jean-Luc Raffaelli, Christophe Boutonnet, Economie des données personnelles, Les enjeux d'un business éthique, octobre 2015, CIGREF, Réseau de grandes enterprises.

http://www.cigref.fr/wp/wp-content/uploads/2015/11/CIGREF-Economie-donnees-perso-Enjeux-business-ethique-2015

3- Garance Mathias, Données personnelles: votre conformité, Janvier 2017.

4- Goldman (B.), La détermination du gardien responsable du fait des choses inanimées, thèse, Lyon, 1945.

5- Guillaume Florimond, Droit et Internet, De la logique internationaliste à la logique réaliste, Bibliothèque des thèses, Editions Mare & martin, 2016.

6- Michel Vivant, Cybermonde: Droit et droits des réseaux, JCP, 1996 II, n 43.

7- sophie LOUVEAUX, électronique et la protection de la vie privée, Art disponible sur : http://www.crid.be/pdf/crid/4710.pdf.

8- sulliman OMARJEE, le data mining Aspect juridiques de l'intelligence artificielle au regard de la protection des données personnelles, memoire,faculté de droit, université Montpellier,2001/2002, disponible sur: www.droit-ntic.com/pdf/Data_mining.pdf.

9- TGI Paris, 2Nov,2000. Note A .de senga,p. L.Rapp, secret des correspondences et couriers électroniques , D.2000.

10-V.Jean-paul costa, « La transparence administrative », Regards sur l'Actualité septembre- octobre 1998.

11-X.Linant, de bellefonds, L'informatique et le droit,2e ed,1985.