جمهورية مصر العربية
جامعه المنصورة
كليه الحقوق
قسم القانون الجنائي

الحماية الجنائية لجمع وتخزين بيانات غير صحيحة او بطريقة غير مشروعة

بحث من رسالة دكتوراه في القانون الجنائي بعنوان

الحماية الجنائية للبيانات الشخصية

اعداد الباحثة

رنا أبو المعاطي محمد الدكرورى

تحت إشراف/

الأستاذ الدكتور	الدكتور
تامـــر محمـد صالـــح	**أحمد فاروق أحمد زاهر**
أستاذ ورئيس قسم القانون الجنائي	مدرس القانون الجنائي –قسم القانون الجنائي
ووكيل الكلية السابق لشئون الدراسات العليا والبحوث الاسبق	كلية الحقوق – جامعة المنصورة
كلية الحقوق – جامعة المنصورة	

المقدمة:

يعد الحق في الخصوصية اليوم، من الحقوق الدستورية الأساسية الملازمة للشخص الطبيعي بصفته الإنسانية كأصل عام، فهو أساس بنيان كل مجتمع سليم، ويعد من الحقوق السابقة على وجود الدولة ذاتها، لذلك حظيت الحياة الخاصة للأفراد بحماية دستورية وقانونية كبيرة في دول العالم قاطبة، وشهدت السنوات الأخيرة استجابة تشريعية على مستويات مختلفة لدواعي هذه الحماية، وسايرها القضاء بتجاوب ملحوظ مؤيداً من الفقه لما للحياة الخاصة للأفراد من أهمية قصوى على كيان الفرد والمجتمع معاً.

وتشكل البيانات الشخصية او الاسمية مظهرا من مظاهر الحق في حرمة الحياة الخاصة، فالبيانات الشخصية تحتوي على اسرار الشخص فتعكس شخصيته، لذلك فان المساس بسرية هذه البيانات يعد انتهاكا لحرمة الحياة الخاصة التي يكفلها الدستور، وهذا الامر يقتضي ان يكون التعامل في هذه البيانات والاطلاع عليها قاصرا على اصحابها والمتعاقدين معهم بحكم الوظيفة ولا يجوز للغير الاطلاع عليها او التعامل فيها. وفي ظل التوسع في النظم المعلوماتية وشبكات الانترنت، تزداد اهمية وضع التشريعات والضوابط التي تكفل حماية بيانات المتعاملين فيها.

والحقيقة أن استخدام وسائل التقنية الحديثة والعالية في ميدان جمع ومعالجة البيانات الشخصية، من قبل الدولة أو القطاع الخاص قد عمق التناقضات الحادة التي برزت منذ القدم بين حق الأفراد في الحياة الخاصة، وموجبات الاطلاع على شؤون الأفراد، وتتمثل هذه التناقضات بأربعة معالم رئيسية: –

أولا: التناقض بين حق الحياة الخاصة وحق الدولة في الاطلاع على شؤون الأفراد والذي عمقه تزايد تدخل الدولة في شؤون الأفراد باطلاعها على المعلومات الشخصية الخاصة بالفرد لأغراض تتناقض مع صونها واحترامها.

ثانيا: التناقض بين حق الفرد في الاحتفاظ بسريته، ومصلحته بكشف حياته الخاصة ليتمتع بثمار هذا الكشف في حالة استعمال المعلومات المعطاة طوعا لأغراض غير التي أعطيت لأجلها.

ثالثا: التناقض بين حق الحياة الخاصة، والحق في جمع المعلومات لغايات البحث العلمي أو حرية البحث العلمي.

رابعا: التناقض بين الحق في الحياة الخاصة وبين حرية الصحافة وتبادل المعلومات هذه التناقضات –كما بينا آنفا –برزت منذ القدم بين حق الفرد في حماية حياته الخاصة، وبين موجبات الاطلاع على شؤون الفرد، بما فيها تلك التي تقع ضمن نطاق حياته الخاصة[١].

هذا وقد أكد الخبراء على أن استخدام شبكة الإنترنت يجعل حياة الفرد كالكتاب المفتوح، على الرغم من أن هناك من أسرار الحياة الخاصة ما قد تقتضي الظروف أو المصلحة العامة عدم الكشف عنها، والاحتفاظ بها في مكان أمين للرجوع اليه عند الاقتضاء، كتسجيل مرض ألم به، أو رقما لحسابه في البنك، أو دعوى قضائية كان طرفا فيها، أو حكما قضائيا صدر له أو ضده ... الخ[٢]. وغير ذلك من المعلومات اللصيقة بالشخصية، وقد يكون هذا المكان الأمين أرشيف جهة حكومية أو سجلات جهة خاصة كطبيب أو محامي أو محاسب ... الخ[٣].

فيجب على من يطلع على هذه الأسرار الخاصة بحكم وظيفته أن يمتنع عن إفشائها ولو بعد انتهاء خدمته وزوال صفته، ما لم يكن ذكرها مقصودا به فقط منع ارتكاب جناية أو جنحة.

وهكذا فبعد أن كانت هذه المعلومات أو البيانات في ظل الطرق التقليدية لا يطلع عليها إلا صاحب الشأن نفسه بإتباع إجراءات معينة، أصبح بإمكان أي شخص يمتلك قدرا لا بأس به من الإمكانيات التقنية أن يصل لهذه البيانات أو المعلومات، مما يؤدي إلى انتهاك حرمة الحياة الخاصة بالشخص الذي تتعلق به هذه المعلومات أو البيانات.

---

[١] حيدر غازي فيصل، الحق في الخصوصية وحماية البيانات، مجلة كلية الحقوق، جامعة النهرين، المجلد ٨, العدد ٢, ٢٠٠٨، ص ٢٩٤.

[٢] الشحات ابراهيم محمد منصور، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر الجامعي، مصر, ٢٠١١. ص ٨١.

[٣] محمد حسين منصور، المسؤولية الإلكترونية، منشأة المعارف، الإسكندرية، ٢٠٠٦ ، ص ٣٠.

والمثال الواضح على صحة ذلك –كما ذكرنا سابقا –هو ما أكده بعض الخبراء حول استخدام شبكة الإنترنت بجعلها حياة الفرد كالكتاب المفتوح، إذ أكدوا إمكانية متابعة ومراقبة المواقع التي قد يزورها الشخص على هذه الشبكة.

هذا وقد أدى الاستخدام غير المشروع للبيانات الشخصية واتساع الاعتداء على حق الأفراد في الحياة الخاصة إلى تحريك الجهود الدولية والإقليمية والوطنية لإيجاد قواعد من شأنها حماية الحق في الحياة الخاصة، وبالضرورة إيجاد التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشخصية، وكفالة حماية هذه البيانات من مخاطر الاستخدام غير المشروع لتقنيات معالجتها إذ يقول ((Bowie . Rebertm)) أن ما يهدد الجنس البشري ليس حربا نووية، بل جهاز كمبيوتر مستقل[٤].

وتثير هذه المخاطر مسألة الأهمية الاستثنائية للحماية القانونية – إلى جانب الحماية التقنية – للبيانات الشخصية ، ومن العوامل الرئيسة في الدفع نحو وجوب توفير حماية تشريعية وسن قوانين في هذا الحقل، أنه وقبل اختراع الحاسوب، فأن حماية الأشخاص كانت تتم بواسطة النصوص الجنائية التي تحمي الأسرار التقليدية (كحماية الملفات الطبية أو الأسرار المهنية) وعلى الرغم من ذلك فأن هذه النصوص التقليدية لحماية شرف الإنسان وحياته الخاصة لا تغطى إلا جانبا من الحقوق الشخصية وبعيدة عن حمايته من مخاطر جمع وتخزين ونقل المعلومات في بيئة الوسائل التقنية الجديدة .

وجدير بالذكر أنه في أطار تكنولوجيا المعلومات تبرز خطورة التهديد المعلوماتي للحياة الخاصة بشكل أساس في إساءة استخدام المعلومات والبيانات المتعلقة بالأفراد، إذ تتسم صور الاعتداء على الحياة الخاصة بصعوبة حصرها، وذلك لكونها تتطور نتيجة تطور تكنولوجيا المعلومات باستمرار، إلا أننا يمكن أن نشير إلى أبرز الانتهاكات التي قد تطال حق الأفراد في حرمة حياتهم الخاصة. والتي يمكن اجمالها فيما يلي: –

١) استخدام بيانات شخصية غير صحيحة.

٢) جمع وتخزين بيانات شخصية صحيحة، ولكن على نحو غير مشروع جنائيا.

---

[٤] حيدر غازي فيصل ، مرجع ساق ذكره، ص ٢٩٦

٣) مخالفة القواعد الشكلية المنظمة لجمع ومعالجة ونشر البيانات ذات الطبيعة الشخصية التي تدخل في نطاق الحماية التشريعية لخصوصية المعلومات.

٤) الافشاء غير المشروع للبيانات الشخصية واساءة استخدامها.

٥) الاتلاف غير المشروع للسجلات والدفاتر الخاصة بالبيانات والمعلومات.

فالصور السابق ذكرها ينتهجها الجاني في محاولته المساس بالحياة الخاصة لاحد الافراد وذلك بالتسلل إلى النظام المعلوماتي والاطلاع على ما به من معلومات تخص أحد الافراد واستخدام هذه المعلومات سواء كانت صحيحة أو غير صحيحة عن طريق التلاعب بها أو محوها، وقد يكون هذا الجاني مرخصا له الدخول إلى هذا النظام أو غير مرخص له، أو أن يقوم بجمع البيانات الشخصية الخاصة بالمجني عليه لاستخدامها لأغراض شخصية أو يقوم بإفشاء هذه المعلومات ويسيء استخدامها.

وقد سرد المشرع المصري صور الاعتداء على البيانات الشخصية من خلال مشروع قانون وزارة الاتصالات وتكنولوجيا المعلومات الخاص بإتاحة البيانات والمعلومات لسنة ٢٠١٢ ويتضمن الباب السابع من القانون الجرائم المتعلقة بالبيانات والمعلومات، وتنص المادة «٤١» على: مع عدم الإخلال بأية عقوبة أشد وردت في أي قانون آخر، يعاقب بالحبس لمدة لا تقل عن شهر وبغرامة لا تقل عن ١٥ ألف جنيه ولا تزيد عن ٥٠ ألف جنيه أو بإحدى هاتين العقوبتين كل من ارتكب فعلاً أو أكثر من الأفعال الآتية:

١. إتاحة البيانات المطلوبة على غير النحو المتفق عليه.

٢. الامتناع، دون مبرر، حال كونه مختصاً، بعد مضى ثمانية أيام من إنذاره على يد محضر عن تقديم البيانات المطلوبة منه.

٣. التراخي دون مبرر، في تقديم البيانات أو المعلومات المطلوبة بعد الميعاد الوارد في إشعار الرد.

٤. الإتلاف العمدي للسجلات والدفاتر الخاصة بالبيانات والمعلومات لدى إحدى الجهات.

٥. إتاحة بيانات، أو معلومات مغلوطة أو مكذوبة أو ناقصة.

٦. إتاحة بيانات أو معلومات خاصة، في غير الأحوال المرخص بها قانوناً.

٧. الحول دون الحصول على بيان أو معلومة مطلوبة، دون وجه حق.

٨. كشف عن أي معلومات مستثناة من الإتاحة وفقا للقانون.

٩. الامتناع عن تنفيذ قرارات المجلس.

فضلا عن تعريفه لخرق وانتهاك البيانات الشخصية في قانون حماية البيانات الشخصية المصري رقم ١٥١ لعام ٢٠٢٠: بأنه كل دخول غير مرخص به إلى بيانات شخصية أو وصول غير مشروع لها، أو أي عملية غير مشروعة لنسخ أو إرسال أو توزيع أو تبادل أو نقل أو تداول يهدف إلى الكشف أو الإفصاح عن البيانات الشخصية أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها[٥] .

وتفصيل ذلك على النحو الاتي:

مشكلة الدراسة:

وتتمحور الإشكالية الرئيسة في بيان كيفية تحقيق الحماية الجنائية لحق الافراد في حماية البيانات الشخصية وتجريم مظاهر العدوان عليها مثل: جمع وتخزين بيانات غير صحيحة او بطريقة غير مشروعة، وتحديد العقوبات الملائمة لهذه التصرفات ومدى كفاية النصوص الواردة في قانون العقوبات لصون هذا الحق مع الاقتداء بالتشريعات الاجنبية بهدف الوصول الى سبل حماية البيانات الشخصية في التشريع المصري.

تساؤلات الدراسة:

البحث في هذا الموضوع يطرح عددا من التساؤلات المهمة نوجزها بما يأتي:

١) ما هي المخاطر التي تهدد حياتنا الخاصة بوجه عام وخصوصية البيانات والمعلومات على الإنترنت؟

٢) ماهية صور انتهاك خصوصية البيانات الشخصية، والعقوبات المقررة لها؟

---

[٥] الجريد الرسمية, العدد ٢٨, مكرر (هـ), مرجع سبق ذكره.

٣) هل القانون وحده كافٍ لحماية خصوصية المعلومات؟ أم لابد من تكاتف الاستراتيجيات التنظيمية والوسائل التقنية لحماية المعلومات الخاصة من خطر الانتهاك وفقدان الثقة بالإنترنت؟

أهمية الدراسة:

تتركز أهمية البحث حول كونه محاولة متواضعة من الباحث لتسليط الضوء على خصوصية الإنسان في ميدان المعلوماتية وصورها وأساليب انتهاكها وقوانين حمايتها وأساليب الحماية الموضوعية والإجرائية بدءاً من اهتمام الأسرة الدولية بصون الخصوصية عبر الوسائط الإلكترونية، مروراً بالقوانين المقارنة الأجنبية والعربية.

ومن ثم، يعد موضوع الاعتداء على البيانات الشخصية من الموضوعات الهامة التي باتت الحاجة إلى دراستها دراسة جيدة ومتأنية من قبل الباحثين ودارسي القانون من الأمور الضرورية والملحة في الوقت الراهن، وهو الأمر الذي دفعنا إلى إجراء دراستنا المتواضعة في هذا المجال القانوني الخصب.

منهج الدراسة:

يعتمد الباحث منهج الدراسة القائم على الوصف والتحليل المقارن للسياسة التشريعية المتعلقة بالحماية الجنائية بجمع وتخزين البيانات الشخصية بصورة غير مشروعة في كل من القانون الجنائي المصري وبعض الدول التي سبقت مصر في تبني التشريعات المتعلقة بالحماية الجنائية للبيانات الشخصية، وذلك من خلال الوقوف على النصوص القانونية المختلفة والاحكام القضائية والآراء الفقهية المختلفة لإبراز الحجج والاسانيد المختلفة المتعلقة بموضوع الدراسة.

خطه الدراسة:

نظرا لأهمية موضوع الحماية الجنائية البيانات الشخصية كأحد أهم حقوق الإنسان، سيتم تناوله من خلال مبحثين: اما المبحث الأول فهو يتناول جريمة استخدام بيانات شخصية غير

صحيحة، بينما يتناول المبحث الثاني جريمة جمع وتخزين بيانات شخصية صحيحة على نحو غير مشروع جنائيا

المبحث الاول

استخدام بيانات شخصية غير صحيحة

تعني الخصوصية المعلوماتية": حق الأفراد أو المجموعات أو المؤسسات أن يحددوا لأنفسهم، متى وكيف أو إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل للآخرين". كما يمكن تعريفها بأنها حق الفرد في أن يضبط عملية جمع المعلومات الشخصية عنه، وعملية معالجتها آلياً، وحفظها، وتوزيعها، واستخدامها في صنع القرار الخاص به أو المؤثر فيه، ويكون للشخص الحق في الدخول إلى هذه المعلومات، والحق في الاطلاع عليها، وتصحيحها، إذا كانت غير صحيحة، ومحوها إذا كانت محظورة[٦].

وفي ظل انتشار أجهزة الحاسب الآلي والانترنت, أصبح التعدي على البيانات الشخصية مسألة واردة وليست مستحيلة. وإذا أضفنا إلى ذلك احتمال الخطأ في عمل الآلة، وصعوبة تصحيح المعلومة، فضلاً عن إمكان تحويرها أصلاً لتضاعف الخطر الذي يهدد حياة الإنسان الخاصة بسبب النظام الآلي لمعالجة المعلومات. فالبيانات الشخصية المتصلة بالحياة الخاصة للفرد أو عائلته غالباً ما يقدمها الشخص بنفسه، أو قد تتوصل الهيئات إليها بوسيلة أو بأخرى، وتهديد المساس بالحياة قد يثور إذا أفشيت هذه المعلومات دون رضاء منه، أو نشرت بإحدى طرائق العلانية دون موافقته، سواء أكانت هذه المعلومات على شكل خبر أو تعليق أو صورة, وتكون متصلة بأسرار حياته الخاصة أو العائلية ولو كانت صحيحة.

---

[٦] محمد عبد المحسن المقاطع: حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، الكويت من دون ناشر ١٩٩٢ص.

١. التلاعب في البيانات الشخصية أو محوها من قبل اشخاص غير مصرح لهم بذلك ويقترن هذا التلاعب أو المحو –عادة – بتحقق مصالح مادية للجناة إلى جانب انتهاك السرية وحرمة الحياة الخاصة.

ومن الامثلة الواقعية لاستخدام هذا الاسلوب كما يذكر Sieber حالة شركة (Data TR.W Credit Company) الامريكية إذ تختص هذه الشركة بتزويد عملائها من البنوك والمتاجر الكبرى وغيرهم بالمعلومات الكافية عن المركز الائتماني لدى شخص تريد هذه الجهات التعامل معه ، الامر الذي دفع بستة عاملين في هذه الشركة إلى الاتصال بالأفراد والمؤسسات ذوي المركز الائتماني السيء حتى يحصلوا على مقابل لهم، مقابل تعديل البيانات الخاصة بهم، وبذلك تورط الكثير من عملاء هذه الشركة في تعاملات تجارية ومالية مع افراد لا يتمتعون بمركز ائتماني جيد [٧].

ومن تلك الامثلة[٨]: "قيام شخص يعمل في شركة مقرها كازاخستان باختراق النظام المعلوماتي العائد لشركة تعمل في ولاية نيويورك الأمريكية تقوم بتزويد الأخبار والمعلومات المالية إلى كافة أرجاء العالم، من خلال الدخول إلى البريد الإلكتروني الخاص بمدير الشركة ومدير الأمن فيها، الأمر الذي مكنه من الحصول على معلومات بالغة السرية، بعد ذلك قام بإرسال عدد من الرسائل الإلكترونية إلى مدير الشركة لإخباره بأن النظام المعلوماتي الخاص بالشركة قد تم اختراقه، وطالب بمبلغ وقدره مائتي ألف دولار مقابل عدم قيامه بنشر واقعة اختراق النظام المعلوماتي الخاص بالشركة وهو أمر لو تحقق فإنه سيضر بسمعة الشركة، وسيلحق بها خسائر مالية كبيرة، تم توجيه ست تهم إليه من بينها التآمر لإتلاف البيانات المخزنة وهي الجريمة التي يعاقب عليها بمقتضى المادة الثالثة من القانون الامريكي لإساءة استخدام الحاسوب لعام ١٩٩٠، وقد جاء في حيثيات الحكم أن إرسال بريد إلكتروني بطريقة يفهم منها أنه مرسل من شخص ما إلا أنه في الواقع تم إرساله من شخص اخر، الأمر الذي أدى إلى جعل جهاز الحاسوب يسجل معلومات غير صحيحة أضرت بشكل واضح بمصداقية البيانات المخزنة في الحاسوب، بناء على ذلك فإن هذا التصرف يدخل ضمن نطاق المادة ٢/٣/ج من

---

[7] UNITED NATIONS OFFICE ON DRUGS AND CRIME, Comprehensive Study on Cybercrime, new yourk , 2013.

[٨] محمود احمد عبابنة, جرائم الحاسوب وأبعادها الدولية, دار الثقافة والنشر والتوزيع, ٢٠٠٩, ص ١٠٦.

القانون باعتبار أن المعلومات هي بيانات بدون أدنى شك، كما قضت المحكمة بأن إدخال بيانات غير صحيحة إلى النظام المعلوماتي من خلال التظاهر بأنه صاحب البريد الإلكتروني مع أنه في الواقع ليس كذلك، يفسد عمل الحاسوب، ويعتبر تعديلا لمحتوياته من المعلومات، ويرى الفقه أن قرار المحكمة يشير بكل وضوح إلى أن نص المادة الثالثة يتطلب قصدا جرميا ذا طبيعة مزدوجة، اتجاه الإرادة نحو تعديل محتويات الحاسوب والمعلومات المخزنة فيه، وانصراف الإرادة نحو الإضرار بمصداقية المعلومات، إلا أنه عندما يتطلب الأمر أن يترتب على تعديل المعلومات الإضرار بمصداقيتها، فإن كلا القصدين يتداخلان ليصبح القصد المتمثل بإرادة تسجيل معلومات غير صحيحة في الحاسوب يعني أن الإرادة الجرمية قد اتجهت حتما نحو الإضرار بمصداقية البيانات.

ويشير البعض الى ان التعديل او التغيير غير المشروع للمعلومات والبرامج يتم عن طريق استخدام إحدى وظائف الحاسب الآلي هو احدي صور السلوك أو النشاط الإجرامي انتهاك الخصوصية المعلوماتية وحتى تقوم جنحة التلاعب لا بد من توافر ركنيها المادي والمعنوي

الفرع الأول: الركن المادي:

ويرِد النشاط الإجرامي في هذه الجريمة على محل محدد هو البيانات أي المعلومات المعالجة آليا، وليست المعلومات في حد ذاتها، أي تلك البيانات التي يحتويها وتعتبر جزءا منه، وبناء عليه، لا تقع الجريمة على مجرد المعلومات التي لم يتم إدخالها بعد إلى النظام أو تلك التي دخلت ولكن لم يتخذ حيالها إجراءات المعالجة الآلية، ويرى جانب من الفقه أن المعلومات التي هي في طريق المعالجة، حتى ولو لم تكن المعالجة الآلية قد بدأت، تكون محلا لجريمة التلاعب[٩].

ولا يشترط أن تقع صور الفعل الإجرامي المشكل لجريمة التلاعب على البيانات بشكل مباشر، إذ من الممكن أن يتحقق ذلك بشكل غير مباشر سواء عن بعد أو بواسطة شخص ثالث.

---

[٩] عبد القادر القهوجي شرح قانون العقوبات، القسم العام، المسؤولية الجنائية والجزاء الجنائي، منشورات الحلبي الحقوقية، بيروت، لبنان) , ٢٠٠٩, ص ١٣٢.

الفرع الثاني: الركن المعنوي:

ان جريمة التلاعب في المعطيات جريمة عمدية تقوم بالقصد الجنائي العام، لذا يجب لقيامها أن تتجه إرادة الجاني إلى فعل الإدخال أو المحو أو التعديل، كما يجب أن يعلم الجاني بأن نشاطه الإجرامي يترتب عليه التلاعب في البيانات، ويعلم أيضا بأن لا حق له في القيام بذلك، وأنه يعتدي على صاحب الحق والسيطرة على تلك المعطيات أو أنه يقوم بأفعاله دون موافقته.

وتعاقب مادة ٣-٣٢٣ قانون العقوبات الفرنسي بالحبس إلى خمس سنوات وبالغرامة المالية ب: ٧٥٠٠٠ يورو جريمة التلاعب بالبيانات وجريمة إعاقة أو التسبب في تحريف تشغيل نظام معالجة البيانات.

٢. استخدام بيانات شخصية غير حقيقية بواسطة الأشخاص المصرح لهم قانونا. حيث يكون الاهمال في الغالب هو السبب وراء عملية جمع أو معالجة أو نشر البيانات الشخصية غير الصحيحة بواسطة الأشخاص المسموح لهم قانونا مع امكانية حدوث ذلك بصورة عمدية. فضلا عن ادخال بيانات أو معلومات وهمية: إذْ يمكن بهذه الوسيلة أن يستولى المعتدي على بيانات شخصية غالباً ما تتعلق بعناصر الذمة المالية بغية تحقيق أموال لنفسه.

وفي التشريع الجزائري, تعد جريمة التعامل في معطيات غير مشروعة جريمة عمدية، بنص م ٣٩٤مكرر" ٢عمدا وعن طريق الغش"، يلزم لتوافرها القصد الجنائي العام بعنصريه العلم والإرادة، علم الفاعل بأنه يتعامل في معطيات غير مشروعة، وانصراف إرادته رغم ذلك لارتكاب النشاط الإجرامي[١٠].

ويرى البعض أن المشرع يتطلب إلى جانب القصد العام قصدا خاصا يتمثل في نية الإعداد أو التمهيد لاستعمال هذه المعطيات، وهذا بالنسبة للصورة الأولى لهذه الجريمة المنصوص عليها في الفقرة الأولى من م ٣٩٤مكرر" تجريم تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية

[١٠] محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, رسالة ماجستير غير منشورة, كلية الحقوق, جامعة الاسكندرية, ٢٠٠٦, ص٢١١.

للمعطيات"، وهذا يتوافق مع مبادئ العدالة وما جاءت به اتفاقية بودابست في هذا الشأن، أما بالنسبة للصورة الثانية المنصوص عليها في الفقرة الثانية من المادة سالفة الذكر فإن استعمال المشرع لمصطلح "لأي غرض كان" يقطع الطريق أمام أي تأويل، ويوضح بجلاء أن المشرع لا يتطلب بالنسبة لهذه الجريمة "حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في القسم المتعلق بالمساس بأنظمة المعالجة الآلية للمعطيات" سوى القصد الجنائي العام، ولا يتطلب قصدا جنائيا خاصا

أما المشرع الفرنسي فلم يستعمل لفظ "عمدا وعن طريق الغش"، وإنما أورد لفظا آخر هو "مسوغ شرعي"، مما يجعل الركن المعنوي بالنسبة لهذه الجريمة مقتصرا على القصد الجنائي العام وحده فقط، دون القصد الخاص.

وتشير المادة ٢ من قانون حماية البيانات الشخصية المصري الى الشخص المعنى بالبيانات يكون له الحقوق الآتية:

١) العلم بالبيانات الشخصية الخاصة به الموجودة لدى أى حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.
٢) العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.
٣) التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية

كما يؤكد البند ٢ من المادة ٤ على ضرورة التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها.

كما تنص المادة ١٨٨ على: يعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرين ألف جنيه أو بإحدى هاتين العقوبتين، كل من نشر بسوء قصد أخبارا أو بيانات أو إشاعات كاذبة أو أوراقا مصطنعة أو مزورة أو منسوبة كذبا إلى الغير، إذا كان من شأن ذلك تكدير السلم العام أو إثارة الفزع بين الناس أو إلحاق الضرر بالمصلحة العامة[١١].

[١١] تامر محمد صالح, الحماية الجنائية للحق في المعلومات الرسمية (دراسة مقارنة) مجلة القانون والاقتصاد, العدد ٩٢ , ٢٠١٩, ص ٦٧٩.

المبحث الثاني

جمع وتخزين بيانات شخصية صحيحة على نحو غير مشروع جنائيا

يتمثل فعل الانتهاك للحق في الحياة الخاصة للأفراد في عملية جمع وتخزين بيانات صحيحة عنهم، لكن على نحو غير مشروع وغير قانوني، ويستمد هذا الجمع أو التخزين صفته غير المشروعة، أما من الاساليب غير المشروعة المستخدمة للحصول على هذه البيانات والمعلومات، أو طبيعة مضمونها[١٢].

أ- عدم مشروعية اساليب وطرق جمع أو تخزين البيانات والمعلومات: ومن بين تلك الاساليب ما يلي:

١. التقاط الارتجاجات التي تحدثها الاصوات في الجدران الاسمنتية للحجرات وترجمتها ومعالجتها بحاسب ألي مزود ببرنامج خاص لترجمتها إلى كلمات وعبارات.
٢. مراقبة أو اعتراض والتقاط وتفريغ الرسائل المتبادلة عن طريق البريد الإلكتروني.
٣. توصيل اسلاك بطريقة خفية إلى الحاسب الالي الذي تخزن داخله البيانات المطلوب الاستيلاء عليها.
٤. التوصل بطريق غير مشروع إلى ملفات بيانات تخص الآخرين.

ب- عدم مشروعية مضمون البيانات التي تم جمعها أو تخزينها:

البيانات والمعلومات ذات الطبيعة الشخصية متعددة ومتنوعة، نظرا لطبيعة مضمونها. فهي جريمة تقع في المراحل الأولى من المعالجة تتكون عناصرها من سلوك إجرامي يتضمن فعل الجمع للمعطيات وأن تستعمل طرق غير مشروعة في ذلك بالإضافة الى القصد الجنائي.

ويقصد بعملية الجمع أن يتمكن الجاني من الحصول على معطيات لشخص واحد أو لعدة أشخاص، إذ تعتبر هذه العملية إحدى أبسط أشكال الاعتداء على البيانات الشخصية، كما تعتبر إحدى مراحل المعالجة لتلك البيانات والتي تعرف المعالجة بأنها " كل عملية أو مجموعة عمليات ... مثل الجمع أو التسجيل...."، لذلك فالجمع هو عملية الإلمام المسبق بالبيانات وتنظيمها من أجل استعمالها فيما بعد". وعملية الجمع يمكن أن ترد على عدة معطيات مختلفة

---

[١٢] نهلا عبد القادر، الجرائم المعلوماتية, دار الثقافة, الاردن, ٢٠١٠ ، ص ١٧٤

تخص شخص واحد مثل رقم هاتفه، وعنوانه الإلكتروني واسمه....، كما يمكن أن تكون البيانات نفسها لكن تخص عدة أشخاص، كعملية جمع البريد الإلكتروني لعدة أشخاص.

المطلب الأولى

تجميع البيانات الشخصية

يتعامل الإنسان في حياته اليومية مع كثير من الجهات التي تطلب منه أن يدلي ببعض البيانات الشخصية، سواء كانت هذه الجهات جهات خاصة مثل الشركات والفنادق والمستشفيات والبنوك...إلخ أو جهات تابعة للدولة مثل الجهات الإدارية التي يتعامل معها الإنسان بصورة أو بأخرى.

فكثير من الجهات الحكومية أو الخاصة تجمع عن الأفراد بيانات عديدة ومفصلة في أثناء تعامل هؤلاء الأفراد معهم، هذه البيانات قد تتعلق بالوضع العائلي أو المادي أو الوظيفي أو التعليمي أو الصحي .....إلخ.

ومما لا شك فيه أن تجميع هذه البيانات قد يكون مهما لسير العمل بالنسبة إلى هذه الجهات، وخاصة بالنسبة إلى الجهات الإدارية التابعة للدولة " إذ إن طلب هذه البيانات الشخصية يكون مهما لتقديم الخدمة التي يطلبها هذا الفرد على خير وجه.

ويتمثل الخطر الأكبر في قيام الجهات الخاصة بتجميع البيانات الشخصية مثل الشركات التجارية والفنادق والمستشفيات والبنوك...إلخ. فالجهات الخاصة لا تقتصر فقط على تجميع البيانات الضرورية لتقديم خدماتها للفرد، بل إنها في كثير من الأحوال تتعدى ذلك إلى تجميع البيانات كثر من اللازم.

ولكن ما سبب اهتمام الجهات الخاصة بتجميع البيانات الشخصية للأفراد بهذه الصورة؟ . السبب في ذلك هو تطبيق هذه الجهات لنظرية حديثة في التسويق هي " نظرية التسويق المباشر " [١٣] .

تقوم هذه النظرية على أساس أن تهتم المنشاة التجارية بكل فرد من عملائها على حدة وتقوم بتسويق منتجاتها لكل عميل على حدة على حسب ذوقه الخاص وبمقتضى ذلك تقوم المنشاة

---

[13] Thierry LEONARD, E-Marketing et protection des données à caractère personnel, Etude disponible sur, la date de mise en ligne est:23/5/2000, P 3.

بجمع كبر عدد من البيانات الشخصية الممكنة عن هذا العميل، سواء من حيث اسمه، عنوانه، رقم الهاتف، عنوان البريد الإلكتروني ...إلخ، وأيضا عن المنتجات التي يفضل العميل شراءها من الشركة حتى يتسنى تعرف ذوق العميل [١٤] .

فهذه النظرية الحديثة في التسويق تقوم على أساس إدارة علاقات المنشاة مع العملاء على أساس معرفة احتياجات العملاء وسلوكهم، بهدف الاقتراب أكثر من العميل وتعرفه عن قرب" مما يتيح تقديم منتج أو خدمة متلائمة معه هو شخصيا، أو تقديم عروض تجارية خاصة لكل عميل، أو عمل دعاية خاصة لكل عميل على حدة.

وحتى تستطيع المنشأة التجارية الاقتراب من العملاء، فإن الأمر يقتضي جمع بيانات شخصية عن كل عميل، وتجمع تلك البيانات في كل مرة يتم التعامل فيها بين العميل والمنشاة، حيث يتم تسجيل ما قام العميل بشرائه وما يفضله من منتجات، هذا، بالإضافة للبيانات الأخرى الخاصة برقم الهاتف وعنوان المسكن وعنوان البريد الإلكتروني...إلخ[١٥]. بل إن بعض المنشآت التجارية تقوم بمنح منتجات أو خدمات مجانية للعملاء وذلك بهدف واحد هو جمع بيانات شخصية عن هؤلاء العملاء.

وقد اتخذت هذه النظرية تطبيقا حديثا، وذلك مع زيادة عدد مستخدمي شبكة الإنترنت، إذ اتجهت معظم الشركات التجارية إلى إنشاء مواقع لها على الإنترنت، هذه المواقع تسمح لها بتجميع البيانات الشخصية لمستخدمي الإنترنت وتقديم عروض خاصة لهم عبر الشبكة، وهو ما أصبح يسمى ب " التسويق الإلكتروني ".

ويتم تجميع البيانات الشخصية عبر شبكة الإنترنت عن طريق تقنية تسمى (كوكيز) ، وهي ملف يقوم الموقع الخاص بالمنشاة التجارية بزرعه على القرص الصلب للكمبيوتر الخاص بمستخدم الإنترنت عند زيارته لهذا الموقع ، هذا الملف يمكن أن يتم فيه تخزين العديد من المعلومات عن مستخدم الإنترنت مثل المواقع التي يقوم بزيارتها والمنتجات التي يفضل شراءها، بالإضافة إلى اسمه وعنوانه ورقم الهاتف ورقم بطاقة الائتمان وعنوان البريد

---

[14] Ibid, p 3.
[15] Ibid, p 5.

الإلكتروني الخاص به، وأي بيانات أخرى يقوم مستخدم الإنترنت بكتابتها في أثناء قيامه بالتجول على الشبكة [١٦] .

يقوم هذا الملف بإرسال هذه المعلومات إلى الموقع الخاص بالمنشاة التجارية، التي تستطيع باستخدام هذه البيانات أن تقوم بإرسال عرو ض تجارية ودعائية خاصة لمستخدم الإنترنت تتناسب مع ميوله وذوقه، ويتم إرسال هذه العروض عبر البريد الإلكتروني.

وتقوم الجريمة سواء تم الجمع يدويا أي جمعها في ملفات أو سجلات ورقية مثلا، أو تم بطريق آلي أي باستعمال الأجهزة المعلوماتية، يكون الجمع في جهاز معلوماتي عن طريق انتقاء البيانات وادراجها في سجلات أو ملفات رقمية، كما قد يتم جمعها من وثائق ورقية موجودة مسبقا أو عن طريق مساءلة في شكل استطلاع للشخص المعني مباشرة أو إعطاءه وثيقة أسئلة يجيب عنها كتابة، كما يمكن الحصول عليها من استطلاع لدى الغير كما لو كان هذا الغير مسؤولا على الشخص المعني؟.

ولقيام الجريمة يجب أن تكون البيانات موضوع الجمع هي بيانات شخصية، وقد اعتبرت البيانات الشخصية هي: " كل معلومة بغض النظر عن دعامتها، متعلقة بشخص معرف أو قابل للتعرف عليه بصفة مباشرة أو غير مبشرة، لا سيما بالرجوع إلى رقم التعريف أو عنصر أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"، وبالتالي فالبيانات الشخصية هي تلك المعلومات المحصل عليها، والتي تؤدي إلى التعرف إلى شخص ما بشكل مباشر أو غير مباشر كاللجوء الى رقم تسجيل معين كرقم الهاتف أو رقم تسجيل السيارة أو رقم تسجيل الضمان الاجتماعي أو الضريبي"، فقد قضي بأن رقم الهاتف يعتبر من البيانات الشخصية التي يمكن عن طريقها التعرف على الشخص الطبيعي صاحب الرقم، بل ذكر المشرع أيضا المعلومات تلك المتعلقة بعناصر من الهوية الفيزيولوجية والنفسية والاقتصادية والثقافية وكذا الاجتماعية، وهذا التوسع في مفهوم البيانات الشخصية لإزالة الإشكال الذي كان يطرح حول التمييز بين مصطلح البيانات الشخصية والبيانات الإسمية، إذ أن هذا الأخير هو المصطلح الذي استعمله المشرع الفرنسي عند صدور قانون المعلوماتية في سنة ١٩٧٨، ثم تخلى عنه عندما

---

[١٦] يونس عرب، مرجع سبق ذكره , ص ٩.

نقل النصوص العقابية إلى قانون العقوبات في المواد من ١٦—٢٢٦ الى ٣٠—٢٢٦ ليتبنى مصطلح البيانات الشخصية"، متأثرا بموقف الفقه الذي اعتبر أن البيانات إسمية أو شخصية فهي تحمل نفس المفهوم، بحيث تتضمن كل المعلومات المتعلقة بالفرد سواء كانت مرتبطة بحياته الخاصة أو المهنية أو توجهاته الفكرية والثقافية والسياسية، فقد اعتبرت اللجنة الوطنية للمعلوماتية والحريات في فرنسا أن القيام باختبار الصحة النفسية يعتبر جمعا لبيانات ذات طابع شخصي، وفي المقابل لم يعتبر القضاء هناك نتائج سبر الآراء متعلقة بإحدى الشخصيات حول موقف الرأي العام منه في وقت معين بأنها معطيات شخصية".

والخطر يتمثل هنا في أن الفرد قد يقوم بمنح بعض البيانات لجهة معينة يرى أنها بيانات ضرورية لتقديم الخدمة له" أي يعطيها بيانات في حدود الضرورة، ويعتقد أن هذه البيانات لا تسمح برسم صورة كاملة عنه، ولكنه لا يعلم أن هذه البيانات سوف يتم تكملتها ببيانات أخرى قد قام بتقديمها قبل ذلك لجهة أخرى؛ مما يؤدي إلى إمكانية رسم صورة متكاملة له.

ونقل هذه البيانات أصبح سهلا الآن مع استخدام الشبكات، حيث يتم تكوين شبكة بين الحاسبات التي تتضمن قواعد بيانات لعدة جهات، فيكون انتقال هذه البيانات بين تلك الحاسبات سهلا جدا، ودون حاجة لتدخل بشري. بل إن الأخطر من ذلك، أن البيانات الشخصية أصبحت اليوم محلا لاقتصاد جديد، ومحلا للإتجار بها من قبل الجهات التي تقوم بجمعها، وتجلب المال لهذه الجهات. فسهولة جمع البيانات الشخصية ومعالجتها وانخفاض تكاليفها أدى إلى قيام كثير من المنشآت التجارية إلى التخصص في جمع وبيع هذه البيانات الشخصية إلى الجهات التي تريدها، بل إن هناك كثيرا من الشركات التي قامت ببيع البيانات الشخصية التي كانت في حوزتها بعد إفلاسها وتصفيتها وخروجها من السوق.

يستوجب القانون لقيام جريمة الجمع غير المشروع للمعطيات، أن تستعمل في ذلك طرق تدليسية أو غير نزيهة أو غير مشروعة، وهو السلوك الإجرامي الذي يجب توافره لقيامها، إذ وردت هذه العبارات بنفس الشكل الذي وردت في المادة ١٦—٢٢٦ من قانون العقوبات الفرنسي وقبلها في المادة ٢٥ من قانون المعلوماتية لسنة ١٩٧٨، وقد اعتبر الفقه آنذاك أن

عبارات "بطريقة تدليسية أو غير نزيهة أو غير مشروعة" تفتقد الدقة والوضوح التي يقتضيها مبدأ الشرعية، لذا فهي تمنح سلطة واسعة للقاضي الجزائي في تفسيرها".

إذ أن مصطلح "الطريقة غير المشروعة" تكفي وحدها لتتضمن الوسائل التدليسية وغير النزيهة لجمع المعلومة، يضاف إليها كل أشكال الاختلاس من الوثائق أو السجلات الرقمية، أو الحصول عليها عن طريق الدخول غير المشروع للأنظمة المعلوماتية.

ومن ثم تقع جريمة التخزين غير المشروع للبيانات الشخصية، متى تم ذلك دون رضاء صاحبها أو لاستخدامها لأغراض غير المخصصة لها. وتتحقق هذه الجريمة على رأي في الفقه الجنائي حتى وان كانت الحكومات هي من قامت بأفعال التخزين للبيانات الشخصية ما دامت هذه الافعال قد حصلت دون سند في القانون أو في غير الحالات التي يصرح بها القانون او دون امر قضائي، ألا ان التخزين يعد مشروعا متى تم وفقا للقانون او انه من مقتضيات الصالح العام كما هو الحال في الدول التي تطبق اعمال الحكومات االلكترونية بموجب قوانين نافذة.

وفيما يتعلق بصفة عدم المشروعية التي تلحق أفعال الجمع والتخزين، فقد يكون مصدرها اساليب الحصول على البيانات أو مضمون وطبيعة هذه البيانات. واما اركان جريمة التخزين غير المشروع فأن الركن الاول هو محل أو موضوع الجريمة والذي يتمثل بالبيانات الشخصية، اما الركن المادي لها فيتمثل بالحفظ او التخزين للبيانات الشخصية على نحو غير مشروع إما بانتهاج احدى الوسائل أو الطرق غير المشروعة ذات الطبيعة التقنية، أو معالجة بيانات يحظر القانون معالجتها، أو لأي سبب من أسباب عدم المشروعية سندا للنص القانوني المجرم لهذا السلوك.

اما فيما يتعلق بالركن المعنوي للجريمة فأنه يتخذ صورة القصد الجنائي الذي يقوم على عنصري العلم والإرادة، إذ يجب أن يعلم الجاني بالطبيعة الشخصية لهذه البيانات وبعدم مشروعية تخزينها، وان تتجه اردته الى حفظها او تخزينها خلافا لأحكام القانون.

وقد ادرك المشرع المصري خطورة هذا, ومن ثم فقد تناوله من خلال قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات, بالمواد ٢٤, ٢٥, ٢٦, لكل من يصطنع بريدا إلكترونيا أو موقعا أو حسابا خاصا ونسبه زورا إلى شخص طبيعي أو اعتباري, او ارسال

العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارا أو صورا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة, بكل من الحبس والغرامة.

كما يشترط القانون المصري لحماية البيانات الشخصية لعام ٢٠٢٠ عدة اشتراطات عند تجميع البيانات في المادة)٣:(يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها. توافر الشروط الآتية:

١) أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني
٢) أن تكون صحيحة وسليمة ومؤمنة
٣) أن تعالج بطريقة مشروعة وملائمة، للأغراض التي تم تجميعها من أجلها
٤) ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها

وتحدد اللائحة التنفيذية لهذا القانون السياسَاتٌ والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات.

المطلب الثاني

فقد البيانات الشخصية وسرقتها

إن القيام بجمع البيانات الشخصية وعمل قواعد بيانات لها أدى إلى إمكانية فقد هذه البيانات أو إلى إمكانية الوصول إلى قواعد البيانات وسرقة ما تحتويه من بيانات شخصية.

ان البيانات الشخصية الموجودة في قواعد البيانات على كمبيوتر متصل بشبكة تكون هدفا سهلا " للقراصنة " الذين يقومون بالدخول إلى قواعد البيانات وسرقة هذه البيانات الشخصية واستخدامها استخداما غير مشروع أو على الأقل بيعها لجهات أخرى.

فالقرصنة على النظم المعلوماتية أمر شائع نتيجة ضعف تأمين تلك النظم في بعض الأحيان، وهو الأمر الممكن حدوثه مع النظم التي تتضمن قواعد بيانات شخصية. وهناك حوادث قرصنة على نظم قواعد بيانات شخصية قد حدثت بالفعل:

فقد اعترفت دار النشر (lex– nexis) في عام ٢٠٠٥ بسرقة البيانات الشخصية لنحو ٣٢ لف مشترك ، وذلك من قاعدة البيانات الخاصة بها [١٧].

كما أعلنت إحدى المؤسسات المالية الأمريكية أن هناك عملية قرصنة معلوماتية قد حدثت على قواعد البيانات الخاصة بها" مما أدى إلى سرقة ما يزيد على ٤٠ مليون رقم كارت بنكي لعملاء المؤسسة [١٨] .

بالإضافة إلى القرصنة المعلوماتية فإنه من الممكن سرقة الكمبيوتر الذي توجد عليه قواعد البيانات الشخصية، وهذا ما حدث مع إحدى المستشفيات في الولايات المتحدة الأمريكية، حيث تم سرقة جهازي كمبيوتر عليهما بيانات صحية، وأرقام التأمين الصحي لنحو ١٨٥ للف مريض. كذلك تم سرقة كمبيوتر محمول في إحدى الجامعات الأمريكية " مما أدى إلى سرقة بيانات شخصية خاصة بمائة ألف طالب.

وبجانب سرقة البيانات الشخصية أو القرصنة المعلوماتية لها، من الممكن أن تفقد الجهة التي لديها قواعد البيانات الشخصية، هذه البيانات نتيجة لخطأ من جانب أحد العاملين بها، ولعل أشهر حادث هو فقد إدارة الضرائب البريطانية عام ٢٠٠٧ لقرصي كمبيوتر يتضمنان بيانات شخصية تخص ٢٥ مليون شخص[١٩].

---

[١٧] سامح التهامي, مرجع سبق ذكره, ص ٤٠٤.

[١٨] المرجع السابق, ص ٤٠٥.

[19] Eric Pfanner, Data Leak in Britain Affects 25 Million, the newyork times journal , noline nov, 22, 2007. https://www.nytimes.com/2007/11/22/world/europe/22data.html

وفي واقعة أخرى في الولايات المتحدة الأمريكية، أعلن بنك أمريكا، ثالث أكبر بنك في الولايات المتحدة، عن فقد بيانات شخصية تتعلق بنحو ١,٢ مليون عميل [٢٠] .

وفي فرنسا فقدت إحدى الشركات (Touche &Deloitte) في عام ٢٠٠٦ أسطوانة عليها البيانات الشخصية لتسعة آلاف عامل فيها [٢١].

بل إن الإحصائيات تشير إلى أنه في ٢٠٠٧ فقد نحو ١٦٢ مليون ملف يحتوي على بيانات شخصية، وذلك بالمقارنة ب ٤٩ مليون ملف في عام ٢٠٠٥.

ومن ثم، فإن من المخاطر التي يمكن أن تتعرض لها البيانات الشخصية خطر فقد تلك البيانات من قبل الجهة التي قامت بتجميعها أو سرقتها من تلك الجهة، أو الوصول إلى قواعد البيانات الشخصية والحصول عليها.

أما طريقة التدليس تعني استعمال كل وسائل الخداع والاحتيال، بما فيها الكذب على الشخص المعني بالتأثير على إرادته إلى درجة أن يقتنع بصحة ما يدعيه الجاني، وبالتالي يقدم معلومات ذات طابع شخصي يستغلها الجاني في جمعها.

مما لا شك فيه أن المعلومات وإن كانت تثير إشكالا يتمثل في مدى اعتبارها من الأموال التي يمكن سرقتها[٢٢]، إلا أنه من المسلم فيه أن هذه المعلومات ابتداء يمكن أن تترجم إلى قيم مالية نظرا لقابليتها للاستغلال مقارنة بالبرامج التي هي نوع من الإبداع الذهني والفكري، وبما أن البرامج عبارة عن أسلوب ينظم العمل والمعالجة، فإن استخدام هذا الأسلوب بصورة غير مصرح بها من قبل مالكها أو حائزها الشرعي يشكل اعتداء على حقوق الاستغلال المالي

أما عن موقف بعض التشريعات الغربية، فلم يرد في قانون العقوبات الفرنسي الجديد ما يشير إلى جريمة سرقة المعلومات، عندما تناول في المادة (٣٢٣) بفقراتها المعالجة الالية للبيانات،

---

[٢٠] سامح التهامي, مرجع سبق ذكره, ص ٤٠٥.

[٢١] المرجع السابق, ص ٤٠٥.

[٢٢] أثير جدل فقهي وقضائي حول ما إذا كانت المعلومات صالحة أن تكون محل سرقة . نشير في بداية الأمر إلى أن الاتجاه الذي كان سائدا في تحديد مدى انطباق وصف المال على الأشياء كان يعتمد على الصفة المادية في الأشياء لاعتبارها مالا. هذا الرأي يدافع عنه جانب من الفقه الذي يعتمد في تحليله على كون الأموال غير المادية هي أموال غير مجسدة ومن ثم فإن المعلومة وحدها تكون غير قابلة للسرقة إن كانت منفصلة عن سندها المادي. إلا أن التطورات التي حدثت في العقود الماضية والتي مازالت مستمرة للآن في مجال تكنولوجيا المعلومات جعلتها تنتشر بصورة كبيرة في كافة المجالات والمعاملات مما أدى في بعض الأحيان إلى ارتفاع قيمتها عن قيمة الأموال المادية، هذا التطور أدى بالفقه الحديث إلى البحث عن معيار آخر غير معيار مادية المال، حيث تم اللجوء إلى معيار القيمة الاقتصادية للشيء. إذ لا يعتبر الشيء مالا بالنظر إلى كيانه المادي الملموس وإنما بالنظر إلى قيمته الاقتصادية. ووفقا لهذا الاتجاه يمكن إصباغ صفة المال على المكونات المعنوية للنظام المعلوماتي على أساس ما تتمتع به من قيمة اقتصادية.

وكأن في هذا إشارة إلى سريان القواعد العامة للسرقة على سرقة المعلومات من جانب المشرع[٢٣].

أما في الولايات المتحدة الأمريكية، صدر قانون حماية البنية التحتية للمعلومات الذي عدل في القانون رقم (١٨) المتعلق بالغش والاحتيال المرتبط بالكمبيوتر، وينظم القانون رقم (١٨) الجرائم المرتبطة بالحاسب الالي، فالمادة (١٠٢٩) تتعلق بالاحتيال والنشاطات المتعلقة بالاتصال مع أدوات الاتصال، والمادة (١٠٣٠) تتعلق بالاحتيال المرتبط بالكمبيوتر، والمادة (١٣٦٢) التي تتعلق بخطوط الاتصال والمحطات والأنظمة، والمادة (٢٥١١) التي تتعلق باعتراض وإفشاء المعلومات بعد الاطلاع عليها من خلال الأسلاك، والمادة (٢٧٠١) التي تتعلق بالنشاطات غير القانونية تجاه الاتصالات المخزنة[٢٤].

وبشأن موقف بعض التشريعات الغربية، ففي الولايات المتحدة الأمريكية لا تثور مشكلة بهذا الخصوص، لأن القانون رقم (١٨) المتعلق بجرائم الحاسب الالي يعالج هذه المسألة، أما في فرنسا، فإن قانون العقوبات الفرنسي الصادر عام ١٩٩٣م نظم هذه المسألة أيضا، ونص في المادة (٣٢٣/٣) كل من يدخل بطريقة مخادعة لمعطيات داخل نظام المعالجة الالية أو من يحذف أو يعدل بطريقة مخادعة معطيات موجودة في النظام، فإنه يعاقب بالسجن لمده" ثلاث سنوات وغرامة قيمتها ثلاثمائة ألف فرنك فرنسي".

أنماط سرقة المال المعلوماتي المعنوي:

تعد البيانات والمعلومات اللامادية المخزنة في قواعد البيانات والمتبادلة عبر خطوط شبكة الانترنت، هدف الجاني وغايته، فاذا ما اختلست تلك المعلومات بطريقة ما، فإن ذلك يمثل اعتداء على المال المعلوماتي، وسببا لقيام وصف السرقة أو الاحتيال أو خيانة الأمانة وذلك حسب طبيعة الاختلاس ونية الجاني.

وقد تدارك المشرع المصري ذلك في قانون مكافحة جرائم تقنية المعلومات رقم (١٨٥) لسنة ٢٠١٨, بشأن الجرائم المرتكبة من مدير الموقع والمسئولين عن ادارته, او كل من أنشا أو أدار أو استخدم موقعا أو حسابا خاصا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل

---

[٢٣] هدى قشقوش, جرائم الحاسب الالكتروني في التشريع المقارن, دار النهضة العربية, القاهرة, ١٩٩٢, ص ١٦٤.
[٢٤] محمد سامي شوا, ثورة المعلومات وانعكاساتها على قانون العقوبات , دار النهضة العربية, القاهرة , ١٩٩٤.

ارتكاب جريمة معاقب عليها قانوناً. او اخفاء أو العبث بالأدلة الرقمية لإحدى الجرائم المنصوص عليها في هذا القانون والتي وقعت على موقع أو حساب أو بريد إلكتروني بقصد إعاقة عمل الجهات الرسمية المختصة بكل من الحبس والغرامة[٢٥].

ويشترط المشرع المصري في القانون رقم ١٥١ لحماية البيانات الشخصية في مادة)٧:(والمتعلقة بالإخطار اثناء معالجة البيانات بما يلي: يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق، أو انتهاك للبيّانات الشخصية لديه بإبلاغ المركز خلال (اثنتين وسبعين ساعة. وفى حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فورياً ٠ وعلى المركز وفى جميع الأحوال إخطار جهات الأمن القومي بالواقعة فورا كما يلتزم بموافاة المركز خلال اثنتين وسبعين ساعة من تاريخ علمه بما يأتي[٢٦]:

١) وصف طبيعة الخرق أو الانتهاك، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها.
٢) بيانات مسئول حماية البيانات الشخصية لديه
٣) الآثار المحتملة لحادث الخرق أو الانتهاك
٤) وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية
٥) توثيق أي خرق أو انتهاك للبيانات الشخصية والإجراءات التصحيحية المتخذة لمواجهته
٦) أي وثائق أو معلومات أو بيانات يطلبها المركز
٧) وفى جميع الأحوال يجب على المتحكم والمعالج، بحسب الأحوال إخطار الشخص المعنى بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات

وتحدد اللائحة التنفيذية لهذا القانون الإجراءات الخاصة بالإبلاغ والإخطار.

---

[٢٥] الجريدة الرسمية - العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨, قانون رقم ١٧٥ لسنة ٢٠١٨, في شأن مكافحة جرائم تقنية المعلومات, المواد ٢٧, ٢٨ , ٢٩.

[٢٦] الجريد الرسمية, العدد ٢٨, مكرر (هـ), مرجع سبق ذكره.

الخاتمة:

تتعلق هذه الدراسة بالحماية الجنائية للبيانات الشخصية باعتباره أحد حقوق الإنسان التي تشكل جيلا جديدا من الحقوق والحريات، وقد وجدت هذه الحماية أساسها في الكثير من المواثيق الدولية، والتشريعات الوطنية؛ كونه حقا يمكن أفراد المجتمع من ممارسة بقية حقوقهم. وتعتبر البيانات الشخصية محل الحماية الجنائية، وتتضمن البيانات، والمعلومات الخاصة بالأفراد الطبيعيين وليس الأشخاص المعنويين.

وقد اتخذت هذه الحماية وسائل عدة هي تجريم جمع ومعالجة البيانات بطرق غير مشروعة، اتاحة معلومات مغلوطة، واتلاف المعلومات سواء اكان الاتلاف ماديا، أم معنويا. وتحقق الحماية فاعليتها من خلال العقوبات الجنائية التي يتم توقيعها على الجناة –شخص طبيعي، اعتباري –سواء اتخذت شكل العقوبة السالبة للحرية، أم الغرامة، والواقع أن هذه السلوكيات المجرمة قد ترتكب بحسن نية فلا يتم مساءلة مرتكبيها، وإذا ما انتفى حسن النية، فقد تشكل جريمة أخرى فنكون أمام تعدد معنوي تطبق فيه العقوبة الأشد.

النتائج:

كشف تناول هذا الموضوع عن عدد من النتائج أهمها:

١) الحق في حماية البيانات الشخصية، أحد الحقوق الهامة في الوقت الراهن، أقرته الكثير من القواعد الدولية، والتشريعات الوطنية، فأصبح حقا عالميا.
٢) تمتع أفراد المجتمع بهذا الحق لا يتوقف فقط على وجود تشريع يعترف به، وينظمه، وإنما يؤخذ في الاعتبار الرغبة السياسية والمجتمعة في ممارسة هذا الحق بشكل فعال؛ لذا تختلف ممارسته من بلدا الى اخر، بل من إدارة إلى اخرى داخل البلد الواحد.
٣) حماية وتنظيم استخدام البيانات الشخصية يرتبط بشكل وثيق بحماية الحق الدستوري في الخصوصية، ومن ثم فإن التشريعات التي تنظم استخدام البيانات الشخصية هي من القوانين المكملة للدستور.

٤) يرتبط قانون حماية البيانات الشخصية رقم ١٥١ لعام ٢٠٢٠ ارتباطا وثيقا بالدفاع عن الحق في الخصوصية، ويمكن اعتباره وسيلة من وسائل العودة لحماية الخصوصية.

لا شك ان تعزيز الخصوصية وحماية البيانات هي جزء من الحل، ومن ثم فان القانون المعني بحماية البيانات الشخصية خطوة هامة في هذا الطريق ولكنه يحتاج الى الاخذ بعين الاعتبار ما يلي:

١) ان يتم تعيين اعضاء سلطة حماية البيانات بما يضمن استقلاليتها، ويؤمن لها القدرة على اتخاذ القرار بحرية تامة.
٢) ضرورة الاخذ بما هو بما هو معمول به في التشريع الأوروبي, الذي يشدد علي دور هذه السلطة في حماية الأشخاص الطبيعيين من تجاوزات السلطات العامة وممارسات الشركات الكبرى, وتفقدهم السيطرة على حياتهم الخاصة.
٣) ضبط نطاق تطبيق القانون وفقا لمعالجة البيانات , حيث باتت بيانات الأشخاص الاعتبارية تحظى بأهمية بالغة في الوقت الحاضر قد تفوق أهمية بيانات الشخص الطبيعي، وهو ما يحتاج لإفراد حماية خاصة بها.
٤) توسع القانون في البيانات المستبعدة من نطاق تطبيق القانون مما يؤدي الى خروج عدد كبير من البيانات من نطاق التطبيق وخاصة بيانات البنك المركزي حيث يجب إدراجها لما فيها من خطورة إن لم تشمل بالحماية.
٥) لم يبين القانون الاختصاص القضائي بالمنازعات الناشئة عن هذا القانون، كالاعتراض على عمليات الجمع والمعالجة، أو المطالبة بالتعويض وغيرها، ومن ثم من المفروض أن تخضع أيضاً لاختصاص المحاكم الاقتصادية.

٦) لم تفرد اللائحة تعريفا خاصا بالبيانات الشخصية الحساسة, ومن ثم يجب تعديل تعريف البيانات الحساسة بإضافة إحالة للائحة التنفيذية لتقوم بتعريف البيانات التي تم تصنيفها على أنها بيانات شخصية حساسة في هذه المادة

٧) تعديل القانون بإضافة تعريفات دقيقة لتلك الأفعال التي تعد من قبيل المعالجة في القانون، أو تعديله بإضافة إحالة إلى اللائحة التنفيذية لتقوم بذلك ليترك مجال لأفعال أخرى ربما يخلقها التطور المستمر في التعامل مع البيانات.

٨) ضرورة التنسيق على كل من المستويين المحلي والدولي، بما يؤمن الانسجام بين قوانين الحماية، ويضمن التدفق الحر للبيانات بين الحدود في إطار من الحماية.

٩) ضرورة تعزيز الشفافية وارساء قواعد الحوكمة الرشيدة في مجال نشر وتبادل البيانات، في إطار من الحفاظ على الخصوصية وسرية البيانات.

١٠) يجب نشر ثقافة قانونية وحقوقية وتقنية تهدف إلى تعريف وتوعية الأفراد بها، عن طريق الحملات التواصلية والإعلامية بجميع أشكالها التقليدية والمتطورة للوصول إلى جميع فئات المجتمع.

المراجع:

أولا: المراجع العربية:

١) د. اسامة عبدالله قايد، الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، القاهرة، ١٩٨٨.

٢) د. امير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجيود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، ط ١ ، مكتبة الوفاء القانونية ، الإسكندرية ، ٢٠١١ ، ص٢٨٥.

٣) د. تامر محمد صالح, الحماية الجنائية للحق في المعلومات الرسمية (دراسة مقارنة) مجلة القانون والاقتصاد, العدد ٩٢ , ٢٠١٩, ص ٦٧٩.

٤) د. حيدر غازي فيصل، الحق في الخصوصية وحماية البيانات، مجلة كلية الحقوق, جامعة النهرين, المجلد ٨, العدد ٢, ٢٠٠٨, ص ٢٩٤.

٥) د. سامح عبد الواحد, الحماية القانونية للبيانات الشخصية, دراسة القانون الفرنسي, القسم الاول, مجلة الحقوق, الكويت, ٢٠١١.

٦) د. سامية عبد الرزاق خلف ، التعدي على حرمة الحياة الخاصة باستخدام التكنولوجيا الحديثة (دراسة مقارنة) مجلة الدراسات القانونية, ع ٢٥, ٢٠١٠ ، ص١١٥

٧) د. سليم عبد الله الجبوري ، الحماية القانونية لمعلومات شبكة الانترنت، منشورات الحلبي الحقوقية –بيروت– ط ١، ٢٠١١ .

٨) د. الشحات ابراهيم محمد منصور ، الجرائم الالكترونية في الشريعة الاسلامية والقوانين الوضعية، دار الفكر الجامعي, مصر, ٢٠١١.

٩) د. غنام محمد غنام, الحماية الادارية والجنائية للأفراد عند تجميع بياناتهم الشخصية في اجهزة الكمبيوتر, مجلة الامن والقانون, الامارات, مج ١١, ع ٣, ٢٠٠٣ , ص ١٠٥.

١٠) د. محمود احمد عبابنة, جرائم الحاسوب وأبعادها الدولية, دار الثقافة والنشر والتوزيع, ٢٠٠٩, ص ١٠٦.

١١) د. محمد حسين منصور، المسؤولية الإلكترونية، منشأة المعارف ، الإسكندرية ، ٢٠٠٦.

١٢) د. محمد خليفة، الحماية الجنائية لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, رسالة ماجستير غير منشورة, كلية الحقوق, جامعة الاسكندرية, ٢٠٠٦.
١٣) د. محمد سامي شوا, ثورة المعلومات وانعكاساتها على قانون العقوبات , دار النهضة العربية, القاهرة , ١٩٩٤.
١٤) د. محمد عبيد الكعبي ، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الأنترنت (دراسة مقارنة) ، ط٢ ، دار النهضة العربية ، القاهرة ، ٢٠٠٩ .
١٥) د. محمد عبد المحسن المقاطع: حماية الحياة الخاصة للأفراد وضماناتها في مواجهة الحاسوب الآلي، الكويت من دون ناشر ١٩٩٢ص.
١٦) د. نهلا عبد القادر، الجرائم المعلوماتية, دار الثقافة, الاردن, ٢٠١٠ .
١٧) د. هدى قشقوش, جرائم الحاسب الالكتروني في التشريع المقارن, دار النهضة العربية, القاهرة, ١٩٩٢,
١٨) د. يونس عرب, المخاطر التي تهدد الخصوصية وخصوصية المعلومات في العصر الرقمي، مقال منشور بتاريخ ٦ نوفمبر ٢٠٠٦.

القوانين:

١) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨, قانون رقم ١٧٥ لسنة ٢٠١٨, في شأن مكافحة جرائم تقنية المعلومات, المواد ٢٧, ٢٨ , ٢٩.
٢) الجريد الرسمية, العدد ٢٨, مكرر (هـــ), قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية.

ثانيا: **المراجع الاجنبية**:

1) Eric Pfanner, Data Leak In Britain Affects 25 Million, The Newyork Times Journal , Noline Nov, 22, 2007. Https://Www.Nytimes.Com/2007/11/22/World/Europe/22data.Html
2) Thierry Leonard, E-Marketing Et Protection Des Données À Caractère Personnel, Etude Disponible Sur, La Date De Mise En Ligne Est:23/5/2000, P 3.
3) United Nations Office On Drugs And Crime, Comprehensive Study On Cybercrime, New Yourk , 2013.