بحث بعنوان
المواجهة الجنائية للتداول غير المشروع للبيانات الخاصة

إعداد الباحث

محمود عبدالله محمد سنوسي

باحث دكتوراه بقسم القانون الجنائي

كلية الحقوق – جامعة أسيوط

المواجهة الجنائية للتداول غير المشروع للبيانات الخاصة

المقدمة:

الحمد لله رب العالمين، والصلاة والسلام على سيدنا محمد – الصادق الوعد الأمين – وعلى اهل بيته – الطيبين الطاهرين – اللهم لا علم لنا الا ما علمتنا انك انت العليم الحكيم، اللهم علمنا بما ينفعنا وانفعنا بما علمتنا وذدنا علما، اللهم ارنا الحق حقا وارزقنا اتباعه، وأرنا الباطل باطلا وارزقنا اجتنابه، واجعلنا ممن يستمعون القول فيتبعون أحسنه، وأدخلنا برحمتك في عبادك الصالحين.

التعريف بموضوع الدراسة وأهميته:

تتجلى أهمية هذه الدراسة في الاعتبارات التي يفرضها التقدم التكنولوجي الكبير وتطوّر وسائل التواصل الاجتماعي والاتصالات المتنوعة، إضافةً إلى اتساع نطاق التواصل العالمي والاعتماد المتزايد على إرسال جميع أنواع البيانات والمعلومات عبر الإنترنت، ومن خلال هذا التطور، تم جمع هذه البيانات ومعالجتها، مما ينتج عنه تكوين مؤشرات ضخمة من المعلومات، ولهذا السبب، يصبح ضرورياً وضع نظام قانوني لحماية البيانات الخاصة من المخاطر المحتملة لمعالجة تلك البيانات، ويهدف هذا النظام القانوني إلى توفير إطار يحدد كيفية المواجهة الجنائية للتداول غير المشروع للبيانات الخاصة[1].

كما شغل الحق في حماية البيانات الخاصة حيزا هامًا على الصعيد

[1] **أنظر د. فتحي محمد عبدالسلام الفقي**، معالجة البيانات الشخصية عبر المواقع الإلكترونية والعلاقة التعاقدية الناشئة عنها دراسة مقارنه، دار مصر، القاهرة، ٢٠٢٣، الطبعة الأولى، ص ٧.

القانوني، فبادر المشرع بتكريسه وضمان الحماية اللازمة له على المستويين الدولي والداخلي، حيث كفلت المواثيق الدولية والتشريعات الوطنية المختلفة الحماية اللازمة للبيانات الخاصة، فكان هناك اهتماما واضحا على المستوى الدولي، بواسطة اللائحة الأوروبية لحماية البيانات العامة (GDBR) حيث منح المشرعون داخل التكتل الأوروبي لحماية الخصوصية وسرية البيانات الخاصة بالأفراد أهمية كبيرة، كونها جزء لا يتجزأ من الأمن القومي الأوروبي والأمن الداخلي للدول الأعضاء، ومن أجل ذلك تم تطبيق اللائحة الأوروبية لحماية البيانات العامة (GDBR) في ٢٥ مايو ٢٠١٨ على جميع الدول الأعضاء في الاتحاد الأوروبي[١].

كما نشاهد في الوقت الراهن أن الكثير من تعاملات الأفراد اليومية أصبحت تتم من خلال بياناتهم الخاصة، التي يتم تخزينها ومعالجتها بطريقة يسهل استحضارها، فكثير من الجهات والشركات تقدم علي انشاء قواعد للبيانات خاصة بعملائها بحيث يتم استحضارها وقت الحاجة اليها، وعلى الرغم من تعدد المزايا والآثار الايجابية للتعامل من خلال البيانات الخاصة، الا أن التجارب أثبتت تعرض الكثير منها بعد معالجتها للكثير من الانتهاكات والاختراقات حيث أساء البعض استخدامها سواء اثناء عملية المعالجة أو التخزين أو النقل، بحيث أصبحت الخصوصية التي كان يتمتع بها الأفراد من قبل أكثر عرضة للعديد من المخاطر، مما جعل نطاق الحياة الخاصة أكثر ضيقا نتيجة انتشار التكنولوجيا الحديثة، فوسائل تقنية المعلومات المستخدمة في الوقت الراهن أصبحت تشكل خطرا وتهديدا صارخا على الحياة الخاصة بالأفراد وحرياتهم، وذلك لما أثبتته من قدرتها

[١] **د. باسم محمد فاضل مدبولي**، المسئولية المدنية عن أضرار معالجة البيانات الرقمية، دراسة مقارنه، في ضوء اللائحة الأوروبية العامة (٦٧٩) لسنة ٢٠١٦ والقانون المصري ١٥١ لسنة ٢٠٢٠، دار الفكر الجامعي، الإسكندرية، ٢٠٢٣، ص٩.

الفائقة على ترجمة حياة الفرد خلال ثوان معدودة بعدما كانت محجوبة عن رؤية الآخرين[1].

اشكالية البحث:

تكمن اشكالية البحث في كمية البيانات الخاصة الهائلة الساكنة في الانترنت، والتي تمثل خطرا داهما على خصوصية أصحابها، سيما وأن هذا العصر هو عصر التكنولوجيا، وخاصة بعد ظهور نظرية التسويق المباشر التي تقوم على أساس انشاء دعاية خاصة لكل عميل اعتمادا على ما يتم تجميعه من معلومات عنه – هذه المعلومات هي البيانات الخاصة لهذا العميل – وهذا ما أدى الى أن تصبح لهذه البيانات الخاصة قيمة مادية، ومن ثم ظهور تجارة البيانات الخاصة، حيث أن البيانات الخاصة عند معالجتها أثناء الجمع أو التخزين أو النقل، تتعرض للعديد من المخاطر التي تنتهك خصوصية تلك البيانات، بالإضافة الي انتشار الوسائل الالكترونية التي سهلت السبل لذلك مع ضعف الوازع الأخلاقي أو غياب القاعدة القانونية التي تعمل على حماية تلك البيانات، مما أدى الى تدخل المشرع في كثير من البلدان لوضع اطار قانوني يحكم معالجة البيانات الخاصة، بحيث تكون هذه المعالجة ظاهرة ويعلم بها من تخصه هذه البيانات، فضلا عن حقه في الاعتراض عليها[2].

كما تعد ظاهرة التداول غير المشروع للبيانات الخاصة من الظواهر

---

[1] **د. عمرو طه بدوي محمد**، التنظيم القانوني لمعالجة البيانات الشخصية، دراسة تطبيقية علي معالجة تسجيلات المراقبة البصرية، دار النهضة العربية، القاهرة، ٢٠٢٠، ص١٠.

[2] **د. سامح عبدالواحد التهامي**، ضوابط معالجة البيانات الشخصية، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية ، المجلد ٣ ، العدد ٩ ، ٢٠١٥ ، ص.

الخطيرة التي تواجه المجتمعات الحديثة، حيث تؤدي إلى انتهاك خصوصية الأفراد وتعريضهم لمخاطر عديدة، مثل الابتزاز والتهديد والتمييز.

ونظرًا لخطورة هذه الظاهرة، فقد حرصت العديد من الدول على مواجهتها من خلال التشريعات الجنائية، وذلك من خلال تجريم التداول غير المشروع للبيانات الخاصة وتوقيع عقوبات رادعة على مرتكبيها.

غير أن مسألة المواجهة الجنائية لظاهرة التداول غير المشروع للبيانات الخاصة ليست بتلك الدرجة من السهولة التي قد تكمن عند الباحثين أو المهتمين، وإنما تثير عدة مشكلات قانونيه يجب أن يتناولها اي تنظيم قانوني.

تساؤلات البحث:

يثير هذا البحث العديد من التساؤلات يتمثل أهمها فيما يلي:

١- ماهية البيانات الخاصة ؟

٢- ماهي مخاطر تداول البيانات الخاصة ؟

٣- الموقف الفقهي والتشريعي من التداول غير المشروع للبيانات الخاصة؟

أهداف البحث:

اذا كانت هناك أسباب عدة دفعتنا الي اختيار موضوع الدراسة، الا أن هناك مجموعة من الأهداف نسعى الي تحقيقها من خلالها وهي على النحو التالي:

أولا: التعرف على ماهية البيانات الخاصة.

ثانيا: التعرف على مخاطر تداول البيانات الخاصة.

ثالثا: التعرف على الموقف الفقهي والتشريعي من التداول غير المشروع للبيانات الخاصة.

نطاق البحث:

يهدف هذا البحث الى التعرض للمواجهة الجنائية لظاهرة التداول غير المشروع للبيانات الخاصة من خلال ما ورد في التشريعات المصرية والتشريعات المقارنة التي وردت في هذا الشأن للعمل على بيان أوجه القصور أو الضعف التي شابت تلك التشريعات للعمل على تحسينها وتلافي أوجه القصور أو الضعف.

منهجية البحث:

اقتضت ضرورة البحث اتباع المنهج الاستقرائي التحليلي المقارن، ويتجلى الاعتماد على **المنهج الاستقرائي** من خلال تتبع التشريعات التي وردت بالمسألة محل الدراسة، مع رصد تلك التشريعات وتحليل نصوصها من خلال **المنهج التحليلي**، وأخيرا عقد المقارنة بين التشريع المصري والفرنسي، نظراً لتأثر كلا منهما بالآخر، مع الاحتكام الى بعض المبادئ الدولية التي تحمى الحق في الخصوصية من خلال **المنهج المقارن**.

تقسيم البحث:

وسنقوم بتقسيم هذا البحث وذلك على النحو التالي:

المبحث التمهيدي: ماهية البيانات الخاصة.

المبحث الأول: مخاطر نقل وتداول البيانات الخاصة.

المبحث الثاني: الموقف الفقهي والتشريعي من التداول غير المشروع للبيانات الخاصة.

المبحث التمهيدي

ماهية البيانات الخاصة

يعد فهم طبيعة وأهمية البيانات الخاصة والتعامل معها بشكل صحيح ومسؤول أمرًا بالغ الأهمية في العصر الحالي، حيث تتطلب هذه البيانات معالجة وتداولًا يتماشى مع التشريعات والأنظمة المعمول بها لضمان حماية حقوق الأفراد والحفاظ على الخصوصية الشخصية، وهو ما نود بيانه من خلال النقاط التالية:

أولا: التعريف اللغوي:

البيانات في اللغة: جمع كلمة بيان، والبيان يأتي في اللغة على عدة معان منها[1]:

أ- الوضوح والظهور: يقال بان الشيء بيانا، أي: اتضح وظهر[2].

ب- الفصاحة: ابداء المقصود بلفظ ومنطق فصيح، يقال فلانا أبين من فلان، أي أفصح منه، ومنه قوله تعالى: {خَلَقَ الإِنْسَانَ. عَلَّمَهُ الْبَيَانَ}[3].

ج – البلاغ: يقال في هذا الأمر بلاغ كفاية، وبلاغ يعلن للناس، أي بيان يعلن لهم

د- الدليل والحجة: يقال من ادعى شيئا فعليه البيان، أي: فعليه الدليل

---

[1] **د. أحمد مختار عبد الحميد عمر (ت ١٤٢٤ هـ)** وآخرين، معجم اللغة العربية المعاصرة، عالم الكتب، الطبعة الأولى، ١٤٢٩ هـ – ٢٠٠٨ م، جـ ١، ص ٢٧٥.

[2] **عبد الرحمن بن حسن حَبَنَّكَة الميداني الدمشقي (ت ١٤٢٥هـ)**، البلاغة العربية، دار القلم، دمشق، الدار الشامية، بيروت، الطبعة الأولى، ١٤١٦ هـ – ١٩٩٦ م، جـ ٢، ص ١٢٥.

[3] سورة الرحمن، الآيات (٣، ٤).

والحجة، ومنه قوله تعالى: {هَذَا بَيَانٌ لِلنَّاسِ}[1].

ثانيا: التعريف التشريعي:

أما بالنسبة لتعريف البيانات الخاصة، فقد حسمت الدول التي نظمت حماية البيانات الخاصة هذا التعريف بنص قانوني، اذ لا يخلو أي قانون متعلق بحماية البيانات الخاصة من تعريف لهذا المفهوم، وقد يكون السبب وراء هذا التوجه، الطابع الفني التقني لمصطلح البيانات الخاصة، ما يجعل هذا التعريف ذو طابع وظيفي يرتبط بمقتضيات وأهداف القانون ذاته.

ومن بين هذه التعريفات ما يلي:

١ – التشريع المصري:

عرف المشرع المصري البيانات الخاصة وذلك في المادة الأولي من القانون رقم ١٧٥ لسنة ٢٠١٨ م الخاص بشأن مكافحة جرائم تقنية المعلومات ، بأنها : " أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده ، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخري [2].

وفي المادة (١) من قانون حماية البيانات الشخصية بأنها: "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر، عن طريق الربط بينها وبين بيانات أخرى، كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد

[1] سورة آل عمران، من الآية (١٣٨).

٢ انظر القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات – المنشور في الجريدة الرسمية المصرية – العدد ٣٢ مكرر (ج) الموافق ١٤ اغسطس سنة ٢٠١٨

الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية "[1].

ومن خلال النص السابق نجد أن المشرع المصري وضع تعريفًا لمفهوم البيانات الخاصة وفقًا للقانون المصري لحماية البيانات الخاصة، ويُعرف في المادة (١) من هذا القانون البيانات الخاصة على أنها أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده مباشرة أو غير مباشرة، سواءً كان ذلك عبر الربط بينها وبين معلومات أخرى.

وتشمل هذه البيانات الخاصة مجموعة واسعة من المعلومات، مثل الأسماء والأصوات والصور والأرقام التعريفية، بالإضافة إلى البيانات التي يمكن أن تحدد الهوية عبر الإنترنت، وتُشدد على أن هذه البيانات تشمل أيضًا معلومات حساسة تتعلق بالهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية.

والهدف من هذا التعريف هو تحديد نطاق البيانات التي يجب أن تكون محمية والتأكيد على التزام الجهات المختصة باتخاذ سياسات وإجراءات لحماية هذه البيانات وضمان عدم استخدامها بشكل غير قانوني أو غير أخلاقي، ويعتبر هذا النهج جزءًا من الجهود الرامية إلى تعزيز حقوق الأفراد في الحفاظ على خصوصيتهم وسلامة بياناتهم الخاصة.

٢- التشريع الفرنسي:

في ظل تطور وسائل الاتصال الحديثة تطور مفهوم البيانات الخاصة وتعددت صورها ، وأدي ذلك إلي اهتمام المشرع الفرنسي لحماية هذه البيانات من أي معالجة غير قانونية [1].

[1] – القانون المصرى رقم ١٥١ لسنة ٢٠٢٠ م بشان حماية البيانات الشخصية.

وقد عرف المشرع الفرنسي البيانات الخاصة في ضوء القانون رقم ٨٠١ لسنة ٢٠٠٤ الخاص بحماية البيانات الشخصية في المادة الثانية منه بأنه: " يعتبر بيانا شخصيا أي معلومات تتعلق بشخص طبيعي معروف هويته أو يمكن التعرف علي هويته سواء بشكل مباشر أو غير مباشر ، أو يمكن تحديد هويته بالرجوع إلي الاسم ورقم تعريفه الشخصي وبيانات الموقع ؛ والمعروف عبر الانترنت لواحد أو أكثر من العناصر المحددة الخاصة بالهوية الشخصية أو الفسيولوجية أو الجنسية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"[٢].

أما البيانات الخاصة الحساسة : فهي البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية ، أو بيانات القياسات الحيوية " البيوميترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية ، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الخاصة الحساسة.

---

١ القانون الفرنسي في مجال حماية البيانات الشخصية يشكل نموذجًا رائدًا في هذا المجال، حيث أنشئ منذ عام ١٩٧٨ وتم تعديله وتحديثه بصفة دورية لمواكبة التطورات التكنولوجية والقضايا القانونية المتعلقة بالخصوصية والأمان، ويعد قانون المعلوماتية والحريات الفرنسي رقم (٧٨-١٧) من القوانين الرئيسية التي وضعت الأسس لحماية البيانات الشخصية في فرنسا وفي أوروبا بشكل عام.

أنظر **د. أحمد رجب سيد صميدة**، التنظيم القانوني للحق في الخصوصية المسكن – الاتصالات الخاصة – البيانات الشخصية في القانون الفرنسي والأمريكي والمصري وفقاً لآخر التعديلات التشريعية، دار النهضة العربية، القاهرة، ٢٠٢٢، ص ٢٦١.

2 Loi n° 2004-801 du 6 août 2004 relative è la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 5 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, J.O, 7 août 2004.

وقد نصت المادة الثامنة من قانون المعلوماتية والحريات الفرنسي المعدل رقم (٧٨ – ١٧) لسنة ١٩٧٨ ، علي أن الأصول العنصرية ، أو العرقية ، أو الآراء السياسية ، أو الفلسفية ، أو الدينية ، أو الانتماءات النقابية للأشخاص ، أو المتعلقة بالصحة ، أو حياتهم الجنسية تعد بيانات حساسة. [١]

ويمكننا الوصول لهوية شخص عن طريق بيانات شخصية مثل اللقب ، تاريخ الميلاد ، محل الإقامة ، الصورة أو رقم التليفون أو لوحة بيانات أو أي رقم هوية ؛ كما أنه يمكن الوصول لهوية الشخص عن طريق الإيميل، إذا كان يظهر به الاسم أو اللقب ، أو من خلال الغير، مثل مورد خدمة الوصول ، إذا كان يسمح بالكشف عن هوية الشخص الذي يتستر وراء اسم مستعار، فيفصح عن ملفات الصوت ، البصمات الوراثية أو الحركية، أو أي بيان بيومتري آخر [٢].

وقد أدانت اللجنة القومية للمعلوماتية والحريات في ٣ من يناير سنة ٢٠١٤ شركة " جوجل " وقامت بتغريمها بمبلغ وقدره ١٥٠٠٠٠ يورو ،

---

1 Article 8 "Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique".

Modifié par LOI n°2018-493 du 20 juin 2018 - art. 8

٢ **د. عثمان بكر عثمان،** المسئولية عن الاعتداء علي البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، مجلة كلية الحقوق، جامعة طنطا، العدد ٣٣، الجزء ٤، ص ٩.

وذلك لأن هذه الشركة قامت بتجميع بيانات مستخدميها ، وإن كانوا غير معلومين الهوية ؛ إلا أن تكامل هذه البيانات مع نظام الخصوصية الجديد ، يسمح بالوصول إلي الشخص من خلال الرجوع لمقوم أو مجموعة مقوماته ؛ وهو ما يعد خرقا للالتزام المنصوص عليه بقانون ٦ من يناير سنة ١٩٧٨ . [١]

ويقصد بالبيانات الخاصة في المادة الثانية من قانون المعلوماتية والحريات الفرنسي رقم ٧٨ لسنة ١٩٧٨ والمعدل بأحكام القانون الصادر في ٣٠ يناير سنة ٢٠٠٢ بأنها :- "كل معلومة متعلقة بشخص طبيعي محدد أو يمكن تحديده مباشرة بواسطة رقم معين أو بواسطة عنصر أو أكثر خاص به"[٢].

وأيضا عرف النظام الأوروبي العام لحماية البيانات الشخصية رقم (٦٧٩) لسنة ٢٠١٦ م GDPR البيانات الخاصة بأنها : "بيانات شخصية ناشئة عن معالجة تقنية أو فنية خاصة تتعلق بالخصائص الجسدية أو

---

١ **د. جبالي أبو هشيمة،** حماية البيانات الشخصية في البيئة الرقمية دراسة مقارنة بين القانون الفرنسي ومشروع القانون المصري، مؤتمر العصر الرقمي واشكالياته القانونية، كلية الحقوق – جامعة أسيوط، ابريل ٢٠١٦، ص ٤ .

3 Article 2 : "Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne".

Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004

الفسيولوجية أو السلوكية للشخص الطبيعي والتي تمكننا من تحديد هويته من خلال صورة الوجه أو البيانات الخاصة ببصمات الأصابع "[1].

٣ – التشريع التونسي:

عرف المشرع التونسي البيانات الخاصة في الفصل (٤) من قانون حماية المعطيات الشخصية بانها: "كل البيانات مهما كان مصدرها أو شكلها، والتي تجعل شخصا طبيعيا معرفا أو قابلا للتعريف، بطريقة مباشرة أو غير مباشرة، باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانونا"[2].

ثالثا: التعريف الفقهي للبيانات الخاصة:

تعددت التعاريف الفقهية التي تعرف البيانات الخاصة فمنهم من يرى بأنها: " الحقائق التي يتم تجميعها بواسطة الملاحظة أو القياس عن أحداث أو ظواهر أو بيانات، ، بحيث يمكن إعادة استخدامها أو تمثيلها في صورة مفردة او مجمعة، ، لإنتاج معلومات مفيدة يمكن استخدامها، وهذه البيانات بصورتها الأصلية قد لا تكون مفيدة، وليس لها أي دلالات دون معالجة".

بينما يرى آخر بأنها: البيانات التي تتعلق بشخص معين، ولا يشترط فيها أن تكون متعلقة بالحياة الخاصة به، وانما يكفي أن تتعلق بالحياة المهنية أو بحياته العامة أو انتماءاته السياسية أو النقابية [3].

---

[1] **د. نصر رمضان سعدالله الحربي**، التعويض عن الأضرار الناجمة عن الاعتداء علي البيانات الأساسية لمستخدمي مواقع التواصل الاجتماعي في ضوء القانون ١٥١ لسنة ٢٠٢٠ – دراسة مقارنة، مجلة كلية الشريعة والقانون، طنطا، العدد ٣٦ ، الجزء الثالث، ص ٤٣٩.

[2] **د. فتحي محمد عبدالسلام الفقي**، مرجع سابق، ص ١٨.

[3] **د. غانم محمد غانم**، دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، القاهرة، ٢٠١٣، ط ١، ص ٩٩.

في حين قسم آخر البيانات الي بيانات شخصية وبيانات متعلقة بالحياة الخاصة. ويعرف البيانات الخاصة بأنها تلك البيانات التي تتعلق بالشخص ذاته وتدخل في كيانه كإنسان مثل الاسم والعنوان ورقم الهاتف، ومعلوماته المتعلقة بحياته المهنية أو العامة أو السياسية. وأما البيانات المتعلقة بالحياة الخاصة فهي التي تتعلق بسمعة الأفراد واعتبارهم، مثل حالة الشخص الصحية أو أصوله العنصرية أو سوابقه القضائية[1].

ولذلك يمكننا القول بان البيانات الخاصة هي كل المعلومات المتعلقة بشخص طبيعي محدد، أو يمكن تحديده من خلال الرجوع إلى رقم هويته أو واحد أو أكثر من العوامل المحددة لهويته المادية او الفسيولوجية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية أو تلك المتعلقة برسم ميوله واتجاهاته السياسية ومعتقداته الدينية وجنسيته وهوايته.

وعلى الرغم من أن التشريعات المتعددة والمتعلقة بحماية البيانات قد استخدمت مصطلح البيانات الشخصية، إلا أنني قد فضلت استخدام مصطلح البيانات الخاصة حيث أنه أقرب إلى الخصوصية والتي تفترض قدرا من الكتمان والتخفي، وبذلك مصطلح البيانات الخاصة هو الأقرب في حماية بعض مظاهر حياة الفرد الخاصة والمحافظة على سريتها بما يصون سمعته ومعطيات حياته التي يحرص على عدم التدخل فيها[2].

إضافة إلى أن مصطلح البيانات الشخصية إنما يقصر نطاق الحماية

---

[1] **د. محمود أحمد طه**، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، ٢٠١٣، ص ٥٩.

[2] **د. ياسر محمد لمعي**، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، مجلة روح القوانين، العدد ٢٧، يناير ٢٠٢٢، ص ١١.

فقط على البيانات الشخصية الخاصة بالأشخاص الطبيعيين، ومن ثم فالبيانات الخاصة بالشخص المعنوي مستبعدة من نطاق الحماية القانونية[1].

المبحث الأول

مخاطر نقل وتداول البيانات الخاصة

إذا كان التقدم العلمي والتطور التكنولوجي قد فتح آفاقا ضخمة أمام تقدم الإنسانية وتحقيق مستوى أفضل ومتقدم للحياة، إلا أنه ألقى بظلاله على الحقوق والحريات الشخصية؛ حيث أدت هذه التطورات إلى ظهور أجهزة ومعدات حديثة سهلت انتهاك خصوصية الفرد وتسللت داخله واستحال الإنسان معها إلى مجموعة من البيانات مسجلة في بنوك المعلومات.

حيث إن كمية البيانات الخاصة الهائلة الساكنة في الانترنت، والتي تمثل خطراً داهماً على خصوصية أصحابها، سيما وأن هذا العصر هو عصر التكنولوجيا، وخاصة بعد ظهور نظرية التسويق المباشر التي تقوم على أساس انشاء دعاية خاصة لكل عميل اعتماداً على ما يتم تجميعه من معلومات عنه – هذه المعلومات هي البيانات الخاصة لهذا العميل – وهذا ما أدى إلى أن تصبح لهذه البيانات الخاصة قيمة مادية، ومن ثم ظهور تجارة البيانات الخاصة ، حيث أن البيانات الخاصة عند معالجتها أثناء الجمع أو التحزين أو النقل، تتعرض للعديد من المخاطر التي تنتهك خصوصية تلك البيانات، بالإضافة إلى انتشار الوسائل الإلكترونية التي سهلت السبل لذلك مع ضعف الوازع الأخلاقي أو غياب القاعدة القانونية التي تعمل على حماية تلك البيانات، مما أدى الى تدخل المشرع في كثير

[1] **د. حسن عبد الحميد وآخرين**، دراسة نقدية لقانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مركز بحوث القانون والتكنولوجيا، ٢٠٢٠، ص ٣٣.

من البلدان لوضع إطار قانوني يحكم معالجة البيانات الخاصة ، بحيث تكون هذه المعالجة ظاهرة ويعلم بها من تخصه هذه البيانات، فضلاً عن حقه في الاعتراض عليها[1].

والبيانات الخاصة قد لحقت التطور الذي شهدته شبكة الإنترنت؛ فلم تعد تقتصر البيانات الخاصة على البيانات التقليدية كالإسم واللقب والعنوان البريدي بل اتسعت هذه البيانات وتنوعت لتشمل صورة الشخص وصوته؛ كما أنها تضمنت بعض البيانات المتعلقة بالشخص ذاته من حيث قدرته المالية وسلوكياته وعادته وميوله وأذواقه؛ والأكثر من ذلك كله البيانات التي تتعلق بجسم الإنسان "البيانات البيوميترية"[2].

وبناء عليه سوف نبحث مخاطر معالجة البيانات الخاصة من خلال النقاط التالية:

اولا: المخاطر المتعلقة بتجميع البيانات الخاصة:

يقصد بتجميع البيانات الخاصة ، كل عمل من أعمال الجمع والترتيب لعناصر البيانات الخاصة لأحد الأشخاص، وإدراجها على بطاقة معلومات لذات الشخص سواء كانت هذه البطاقة ورقية أو الكترونية.

وإذا كان تجميع البيانات الخاصة وترتيبها بهذه الكيفية، أمرا لازما لتنفيذ معالجة البيانات، فإن معالجة البيانات لا تخلو في كثير من الأحيان من بعض المخاطر المتمثلة في خطر التعدي على الحقوق والحريات

[1] **د. سامح عبدالواحد التهامي** ، مرجع سابق، ص ٣٩٨ .

[2] **د. باسم محمد فاضل مدبولي** ، المسئولية المدنية عن أضرار معالجة البيانات الرقمية ، دراسة مقارنه ، في ضوء اللائحة الأوروبية العامة (٦٧٩) لسنة ٢٠١٦ والقانون المصري ١٥١ لسنة ٢٠٢٠ ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٢٣ ، ص ٢٣ .

الفردية للأشخاص المعنيين بهذه البيانات، أو انتهاك حرمة حياتهم الشخصية، على ضوء قيام الكثير من المؤسسات الحكومية والشركات الشخصية بتجميع بيانات عديدة ومفصلة عن المتعاملين معها كتلك التي تتعلق بالوضع المادي والصحي والتعليمي والعائلي والاتجاهات الاجتماعية وغيرها، مما يفتح الباب على مصراعيه لإساءة استخدامها أو توجيهها توجيها منحرفا أو خاطئا أو لمراقبة الأفراد والحكم عليهم حكما خفيا من واقع سجلات البيانات الخاصة المخزنة[1].

أضف إلى أن ربط الأجهزة الإلكترونية بعضها البعض بواسطة جهاز مركزي أو عبر شبكات عامة للاتصال يؤدي إلى تبادل المعلومات والبيانات الخاصة للأفراد فيما بين الأنظمة المعلوماتية، ومن ثم التوصل الى بيانات ومعلومات جديدة عن الأشخاص[2]، كما يمكن في وقتنا الحاضر تجميع البيانات الخاصة دون علم الأشخاص المعنيين بها، وذلك بفضل وسائل التكنولوجيا الحديثة ولاسيما الانترنت، والتي يمكن من خلالها تجميع البيانات الخاصة للمستخدمين وتخزينها عن طريق رسائل الكوكيز[3]، أو تقنية تحديد الهوية باستخدام موجات الراديو أو برامج التتبع بحيث يتم جمع هذه

---

[1] **د. هشام محمد فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة ، ١٩٩٢ ، ص١٧٩ وما بعدها .

[2] **د. محمود عبدالرحمن** ، التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية ، العدد التاسع السنة الثالثة ، مارس ٢٠١٥ ، ص١٠٩.

د . هشام محمد فريد رستم ، مرجع سابق، ص١٧٩ وما بعدها .

[3] الكوكيز عبارة عن ملفات نصية تضعها معظم مواقع الويب على القرص الصلب الخاص بالمتصفح (الزائر) ، عند زيارته لهذه المواقع ، بغرض جمع بعض المعلومات عن المستخدم ، تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة اليها ، ومكمن الخطورة في هذه الملفات انه من الممكن استغلالها في انتهاك خصوصية المستخدمين وجمع معلومات عنهم خلال تصفحهم لمواقع الويب المختلفة .

المعلومات ومعالجتها بسرعة فائقة، بالإضافة إلى ما تقوم به مواقع التجارة الإلكترونية على شبكة الإنترنت، حيث تطلب الشركات من المستخدمين تعبئة نماذج خاصة تحتوي في جنباتها الاستفسار عن بعض المعلومات على سبيل المثال: اسم المستخدم، وعنوان عمله ومنزله ورقم هاتفه وبريده الالكتروني ومكان اقامته ودخله الشهري أو السنوي. . . إلخ، أما الموقع الذي يتم فيه دفع ثمن المبيعات فإنه يطلب رقم بطاقة ائتمان المشتري ونوعها وتاريخ انتهائها[1].

بالإضافة الى ما تقوم به شبكات التواصل الاجتماعي من تجميع أكبر قدر من المعلومات عن مستخدميها حيث أصبحت هذه الشبكات بمثابة مستودع للمعلومات والتي من خلالها يتنازل المرء طواعية عن بياناته الشخصية للتسجيل في هذه المواقع، ومن ثم الحصول على حساب خاص به، ووفقا للسياسات الخصوصية التي لا يقرأها عادة المستخدم قد يكون هناك تنازل صريح للفرد عن بياناته، فضلا عما يقوم به الشخص بشكل يومي من إفصاح عن حياته الشخصية، وحالته المزاجية، وأراءه السياسية وغيرها مما يعد معلومات لا يجوز للغير الاطلاع عليها إلا بموافقة صاحب هذه البيانات وعدم قراءة سياسات الخصوصية ينجم عنه استغلال البيانات الخاصة لمستخدمي هذه الشبكات[2].

وفيما يتعلق بمجال البحث العلمي، يمكن أن يمثل تجميع البيانات

---

[1] Mallorie Wozny , Exploitation des données personnelles : raison commerciale, raison d'état et opportunités , mémoire , université de lyon , faculté de droit , 2017 , p.23 .

[2] **د. دينا عبدالعزيز فهمي** ، المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي ، مجلة كلية الحقوق، جامعة طنطا ، ٢٠١٧ ، ص ١٥ .

الخاصة شكل آخر لإساءة استخدامها، وبيان لذلك عند إجراء المرء للاختبارات عموما والاختبارات الجينية عبر الانترنت على وجه خاص، تقوم المعامل بتجميع العديد من البيانات الخاصة، التي يمكن استخدامها لبحوث خاصة أو في أغراض غير التي جمعت لها أو نقلها لجهات بحثية أخرى، كما أن الأشخاص المعنيين لن يستطيعوا معارضة استخدام بياناتهم التي أدلوا بها بمجرد الحصول على النتائج المطلوبة، وحتى لو مارس هؤلاء الأشخاص حقهم في الاعتراض على معالجة بياناتهم في أغراض البحث العلمي فلن يكون اعتراضهم محل اعتبار يذكر في ظل عدم خضوع البحوث العلمية لأي تقييم أخلاقي[1].

ثانيا: المخاطر المتعلقة باستخدام البيانات الخاصة:

يقصد باستخدام البيانات الخاصة: أن يقتصر توظيف البيانات المجمعة على غايات المعالجة، بحيث لا يتجاوز استخدام البيانات الخاصة حدود الأهداف المعلنة[2].

وعلى غرار المخاطر المرتبطة بجمع البيانات الخاصة، هناك أيضا مخاطر كثيرة ومتنوعة تحيط باستخدام هذه البيانات، بعض منها يرجع الى نتائج معالجة البيانات ذاتها، والبعض الآخر يرتبط بأهداف المعالجة، والبعض الثالث ينشأ من جراء تدفقها عبر شبكة الانترنت، وأخيرا قد تنتج عن تسويق هذه البيانات، وذلك على النحو التالي:

---

[1] **CORALIE DUMAS** , LE DROIT DE LA PERSONNALITE ET LES RESEAUX SOCIAUX , MEMOIRE , faculté de droit , université de MONTPELLIER , 2015 , p.14 .

[2] **د. نهلا عبد القادر المومني** ، الجرائم المعلوماتية ، دار الثقافة للنشر والتوزيع ، عمان ، ٢٠٠٨ ، ص ١٦٧ .

١ – المخاطر المتعلقة بنتائج معالجة البيانات الخاصة:

قد تكون معرفة نتائج معالجة البيانات الخاصة شاقة في بعض الحالات المرتبطة بالبحث العلمي عموما والبحوث الوراثية خاصة أو أن معرفة نتائجها من شأنه أن يعرض الأشخاص المعنيين بها لقدر أكبر من المخاطر. لذلك اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنسا الأبحاث المتعلقة بالوراثة، ولا سيما المرتبطة بالهوس الذهني أو الفصام، هي على قدر كبير من الحساسية، وبالتالي فان معالجة البيانات الخاصة في اطار البحوث الجينية قد تعرض الشخص المعني بالبيانات وأقاربه أيضا لأخطار جسيمة، وذلك برفض المجتمع لهم، اذا ما تم الكشف عن هذه البيانات، وما تحمله من نتائج وتشير إلى مرض وراثي لدى أصحابها ولذلك يجب استخدام الاختبارات الجينية التي تسمح باكتشاف المعلومات الجينية في ظل ظروف دقيقة جدا[1].

٢ – المخاطر المرتبطة بالهدف من معالجة البيانات الخاصة:

وبخصوص المخاطر المرتبطة بالهدف من معالجة البيانات الخاصة، فهي لا تتعرض لمشروعية الغرض من معالجة البيانات الخاصة وإنما لاحتمالات إساءة استخدام البيانات في غير الهدف المشروع، والذي على أساسه تم جمعها، أو إعادة استخدام هذه البيانات. فاليوم هناك اتجاه قوي نحو عدم تحديد أهداف معالجة البيانات الخاصة بدقة وبصورة مسبقة، ولا سيما في المجالات الطبية، وغالبا ما يكون الهدف إنشاء نظام معلوماتي على درجة من التأمين، وفيما بعد يتم تحديد الأهداف، وهو ما يمثل الخطر الأساسي من معالجة البيانات الخاصة؛ نظرا لانتفاء الهدف من المعالجة

[1] **Melle FAGET Marie** ,Les réseaux sociaux en ligne et la vie privé , Mémoire , faculté de droit , université Paris II , 2009 , p.33 .

وعدم تحديده بصورة واضحة لا لبس فيها، الأمر الذي يضفي على هذه المعالجة صفة عدم المشروعية[1].

كذلك أيضا فإن غموض أهداف المعالجة أو وسعها من جانب المسئول عنها، والذي يلتزم بإعلانها الى اللجنة الوطنية للمعلوماتية والحريات، يعطيه مساحة كبيرة للمناورة، كما أن ربط المعالجة بالعديد من الأهداف يصبح معها من المستحيل الحكم على مشروعية هذه المعالجة، مما لا يعطي الأشخاص المعنيين ضمانة حقيقية على بياناتهم محل المعالجة[2].

٣ – المخاطر الناجمة من جراء تدفق البيانات عبر الانترنت:

لقد أتاحت تكنولوجيا الاتصالات عبر الحدود، للأفراد أن يعطوا بياناتهم ومعلوماتهم لجهات داخلية وخارجية وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر إساءة استخدام هذه البيانات خاصة في الدول التي لا تتوافر فيها مستويات الحماية القانونية للبيانات الخاصة. وقد لا تخدم القوانين الوطنية هذا الفرض، كما أن تضمينها نصوصا بشأن السيطرة على نقل البيانات قد لا يكون فعالاً في ظل غياب التنسيق وضمان أن يكون نقل البيانات محكوما باتفاقات تكفل حمايتها أو تضمن توفير حماية مماثلة في

---

[1] **Farid BOUGUETTAYA** , LA PROTECTION DES DONNEES PERSONNELLES EN DROIT COMMUNAUTAIRE , MEMOIRE, UNIVERSITE DE MONTPELLIER I , FACULTE DE DROIT – IDEDH , 2006, p.60.

[2] **د. محمود إبراهيم الغازي** ، الحماية الجنائية للخصوصية والتجارة الإلكترونية ، مكتبة الوفاء القانونية ، الإسكندرية ، ٢٠١٤ ، ص ٢٠ ، ٢١.

الدول المنقول لها البيانات[1].

وتتسع المخاطر مع نشوء ملاجئ آمنة لا تقيد عمليات المعالجة بأي قيد ولا تتوافر عندها أي قيود على جمع ومعالجة البيانات، ومن ثم تهرب اليها مؤسسات الأعمال في بيئة الإنترنت للإفلات من القيود القانونية على معالجة البيانات الخاصة[2].

٤ – المخاطر الناشئة عن تسويق البيانات الخاصة:

لا شك أن المخاطر الناجمة من تجارة البيانات الخاصة هي الأكثر خطورة في وقتنا الحاضر بعد أن أصبحت المعلومات والبيانات الخاصة – المسجلة لدى العديد من الجهات مثل شركات الهاتف والمصارف– تمثل تجارة رائجة تتداولها شركات التسويق المحترفة في الأسواق المتعددة، فسهولة جمع البيانات الخاصة وانخفاض تكاليفها في أغلب المجالات أغرى الكثير على التخصص في جمع ومعالجة وبيع المعنيين بهذه البيانات حيث تصبح بيانات هؤلاء الأشخاص وخصوصياتهم سلعة تباع وتشترى لمن يملك الثمن وبغض النظر على موافقتهم أو رفضهم.

كما يرتبط هذا الجانب–أيضا – بشيوع استخدام الأفراد لخدمات مجتمع المعلومات مثل: محركات البحث أو مواقع التجارة الإلكترونية أو الشبكات الاجتماعية، فالخدمات التي تقدمها هذه المواقع أو الشبكات والتي يبدو أنها مجانية لها في الواقع بعد اقتصادي، ألا وهو تسييل البيانات الخاصة

---

[1] Commission nationale de l'informatique et des libertés (CNIL), « La publicité ciblée en ligne », Communication présentée en séance plénière le 5 février 2009, Paris, p 4.

[2] **د. مروة زين العابدين صالح** ، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني ، مركز الدراسات العربية ، القاهرة ، ٢٠١٦ ، ص٣٢٣ .

لمستخدميها مقابل منحهم حق الولوج المجاني.

ثالثا: المخاطر المتعلقة بحوسبة البيانات الخاصة:

يقصد بحوسبة البيانات عموما، تحويل المعلومات والبيانات الخاصة إلى بيانات إلكترونية بواسطة تسجيلها على دعامات ممغنطة، في صورة نبضات كهربائية، عن طريق استخدام الحاسوب، بحيث لا تقرأ إلا من خلاله، وهو ما يسمح بإمكانية تخزينها أو نقلها أو دمجها، وغير ذلك من الاستخدامات التي لا تزال غير معروفة، وجعل استخدامها أسهل إذا لزم الأمر، وبالتالي تحسين معالجتها[1].

ونود ان نلفت الانتباه إلى أن الإنسان قد عرف جمع ومعالجة البيانات الخاصة قبل ظهور التقنيات الحديثة لحوسبة البيانات، إلا أن ممارسته لأنشطة جمع ومعالجة هذه البيانات كانت تمارس في نطاق محدود للغاية.

وفيما يتعلق بالمخاطر التي قد تنجم عن حوسبة البيانات الخاصة، فإن استخدام الحواسيب في معالجة هذه البيانات، ترتب عليه زيادة في حجم المخاطر، التي يتعرض لها الأشخاص المعنيون بهذه البيانات، بالنظر الى امكانيات الحواسيب الهائلة في جمع البيانات وقدرتها على اعدادها وتجهيزها، بالإضافة إلى سهولة نقلها عبر الشبكات المركزية أو من خلال شبكة الإنترنت[2].

كذلك يصاحب عملية نقل البيانات الخاصة عبر هذه الشبكات بعض

---

[1] **د. علي جعفر**، جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة، دراسة مقارنة ، منشورات زين الحقوقية ، بيروت ، ٢٠١٣ ، ص ٤٠٨ وما بعدها.

[2] **د. منى تركي الموسوي** ، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة ، مجلة كلية بغداد للعلوم الاقتصادية ، ٢٠١٣ ، ص ١٠ .

المخاطر، والتي تتعلق بعدم قدرة شبكات الاتصال على توفير الأمان المطلق لسرية ما ينقل عبرها من بيانات، وامكانية استخدامها عن بعد في الحصول على المعلومات بصورة غير مشروعة، حيث لم تحد وسائل الأمان التقني من هذه المخاطر على الرغم من تطورها[1].

أضف الى هذا أن مسألة تأمين النظام المعلوماتي ليست بمنأى عن كل خطر، بالنظر إلى سهولة التسلل إلى هذه الأنظمة، أو تعرضها لهجمات تهدف إلى تقويضها من أجل الوصول الى البيانات، وهي من الأخطار القائمة، والتي تهدد النظام المعلوماتي بأكمله.

كذلك، فإن عدم كفاءة نظم تأمين البيانات، أو انعدامها، قد يترتب عليه انتهاك حقوق الأشخاص المعنيين بالبيانات، التي تحويها هذه النظم، بصورة مباشرة؛ لأن اختراق النظام المعلوماتي يسمح للفاعل بالاطلاع على البيانات التي يحويها النظام أو إدخال تعديلات عليها أو حذفها أو نسخها لحسابه الشخصي ومعالجتها مرة أخرى، أو بيعها أو استخدامها لأهداف غير مشروعة. وتتضح الخطورة وبشكل مضاعف إذا ما كان النظام المعلوماتي يحوي بيانات لا يجوز جمعها أو معالجتها بداية إلا برضاء الشخص المعني بالبيانات كالبيانات الحساسة[2].

[1] **د. مروة زين العابدين صالح** ، مرجع سابق، ص٣٢٣ .

[2] **د. حسين سليم محمد سليم** ، الحماية الجنائية للبيانات الشخصية المعالجة آليا: دراسة مقارنة ، مجلة العلوم القانونية والاقتصادية ، جامعة عين شمس، كلية الحقوق، ٢٠٢٠، ص ٤٥ .

المبحث الثاني

الموقف الفقهي والتشريعي من التداول غير المشروع للبيانات الخاصة

أصبحت البيانات الخاصة اليوم محلاً لاقتصاد جديد وهو الإتجار بها من قبل الجهات التي تقوم بجمعها وتجلب المال لهذه الجهات ؛ حيث إن كل منشأة تقوم بتبادل البيانات التي جمعتها مع منشآت أخري وذلك بهدف الوصول إلي بيانات متكاملة عن كل فرد.

ويتمثل الخطر هنا أن الفرد قد يقوم بمنح بعض البيانات لجهة معينة يري 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 أخري قد قام بتقديمها قبل ذلك لجهة أخري ، مما يؤدي إلي إمكانية رسم صورة متكاملة له.

و نقل هذه البيانات أصبح أمر سهل الآن مع استخدام شبكة المعلومات ، حيث يتم تكوين شبكة بين الحاسبات التي تتضمن قواعد بيانات لعدة جهات ، فيكون انتقال هذه البيانات بين تلك الحاسبات سهلا جدا ، ودون الحاجة لتدخل بشري.

فسهولة جمع البيانات الخاصة ومعالجتها وانخفاض تكاليفها أدى إلى قيام كثير من المنشآت التجارية المتخصصة في جمع وبيع هذه البيانات الخاصة إلى الجهات التي تريدها ؛ بل إن هناك كثيراً من الشركات التي

قامت ببيع البيانات الخاصة التي كانت في حوزتها بعد إفلاسها وتصفيتها وخروجها من السوق [1].

ويعتبر تجميع البيانات الخاصة- دون علم صاحب هذه البيانات- عمل غير مشروع؛ حيث يجب أن يتم تجميع البيانات الخاصة لأغراض مشروعة ومحددة ومعلنة للشخص المعني كما جاء بالقانون رقم ١٥١ لسنة ٢٠٢٠ الخاص بحماية البيانات الشخصية.

ويجب أن يتم تجميع البيانات الخاصة لأغراض محددة ومشروعة ، وذلك طبقاً للمادة (٦) من قانون حماية البيانات الشخصية وأن يكون الهدف منها تحقيق مصلحة مشروعة.

وتعد البيانات الخاصة منجم ذهب للقائمين علي الدعاية والاعلانات عبر شبكة الإنترنت؛ والسيرة المهنية (بروفيل) للعميل هدف يسعى إليه المعلنين كافة، فيبيع المشغل – في إطار هذه المعاملة – بيانات المستخدمين الخاصة الذين يترددون علي موقعة إلى شركات الإعلان ثم تقوم الشركات الاعلانية بإعداد قواعد بيانات تصنف من خلالها تحديد احتياجات المستخدمين ورغباتهم.

ويتمثل الخطر الأكبر اليوم في جمع البيانات الخاصة للمستخدمين عن طريق المستخدم نفسه من خلال استضافته على شبكات التواصل الاجتماعي (فيس بوك – ماي سباس) لأن هذه المواقع تدعو المستخدم بأن يدلي بنفسه ببياناته طواعية وذلك من أجل الاشتراك في هذه المواقع وهي معلومات خاصة كثيرة محددة وكاملة .

---

١ د. **سامح عبد الواحد التهامي،** نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها ، دراسة في القانون الاماراتي، مجلة البحوث القانونية والاقتصادية، العدد ٦٧، ديسمبر ٢٠١٨، ص ٤٠٤.

والواقع أن الشخص يدلي ببياناته بموافقته دون وعي منه لما يترتب على ذلك من إعادة استعمال هذه البيانات علاوة علي ذلك أن هذه البيانات تفهرس وتنشر وتستثمر دون تمكين صاحب البيانات من ممارسة حقوقه عليها [1].

وعلى حد تعبير أحد المؤلفين " إذا لم تؤد خدمة علي شبكة الإنترنت فإنك لن تكون مستهلكاً وإنما المنتج المباع" فشبكة (فيس بوك) كانت تبيع السيرة المهنية (بروفيل) للمشترك مقابل خمس دولارات لشركات التسويق عبر الإنترنت[2].

وقد اتخذت هذه النظرية تطبيقاً حديثاً وذلك مع زيادة عدد مستخدمي شبكات التواصل الاجتماعي أو شبكة الإنترنت بصفة عامة حيث اتجهت معظم الشركات التجارية إلى إنشاء مواقع لها على الإنترنت هذه المواقع تسمح لها بتجميع البيانات الخاصة لمستخدمي الإنترنت وتقدم عروض خاصة لهم عبر الشبكة وهو ما أصبح يسمى بالتسويق الإلكتروني[3].

فالمواقع والشبكات الاجتماعية تقدم خدمات مبتكرة ومجانية في الغالب لكن في مقابل الاستغلال التجاري للبيانات الخاصة.

وقد قضت محكمة النقض الفرنسية أن بيع السيرة المهنية (بروفيل) للعميل للمعلنين يمثل جمع بيانات خاصة عن المستخدمين وهو عمل غير مشروع ولذا نجد أن اللجنة القومية للمعلوماتية والحريات قد طلبت من موقع (فيس بوك) إعلام كامل عن ملفات مستخدميها ونادت بضرورة أن يكون

---

١ **د. عثمان بكر عثمان**، مرجع سابق، ص ١٨.

2 Chiffre proposé dans un article publié sur le site les échosofr : C.vincent, "La ruée vers l' ordes données personnelles" , Mars , 2013

٣ **د. سامح عبد الواحد التهامي**، مرجع سابق، ص ٤٠٠.

المستخدم على دراية بنشر معلومات مرتبطة بحياته الخاصة وآراءه السياسية والدينية[1].

والحقيقة أن أسلوب استغلال السيرة المهنية (بروفيل) للعميل لصالح المعلنين يتسم بالغموض. كما ان مدة حفظ بيانات مستخدم هذه الشبكة غير واضح وقد كان أهم الانتقادات هو أن (فيس بوك) يمكن أن يحتفظ ببيانات مستخدمين بعد إلغاء اشتراكهم.

والواقع أن بيع البيانات لا يقتصر على شبكات التواصل الاجتماعي بل يمتد ليشمل أيضاً محركات البحث فشركة جوجل والتي تسيطر على اكثر من ٨٠% من نشاط البحث في السوق الأوروبي استطاعت بحيله ما الحصول على بيانات مستخدميها والتي من المحتمل أن تستخدمها بعد ذلك لأغراض تجارية[2].

مما تقدم تبين لنا انه يجب أن يكون تجميع البيانات الخاصة لسبب مشروع وواضح أما إذا كان تجميع البيانات الخاصة لأغراض تجارية فهذا يعد عملاً غير مشروع؛ فتجميع العناوين البريدية لبعض الأشخاص بهدف بيع هذه العناوين لشركات الدعاية والإعلان يعد هدفاً غير مشروع لتجميع البيانات[3].

وتتضح هنا أهمية وجود تشريعات خاصة لحماية البيانات الخاصة للأفراد من الاستغلال والإتجار فيها لأغراض تجارية لما يمثله ذلك من

---

1 Cass. Crim, 14 Mars 2006, no 05 – 83 . 423, FP + F, Fabrice H.C/ Min. Public, Juris. Data no 2006 – 032892 , note LEPAGE.

2 Luc Crynbaum, Caroline le Goffic, Lydia Morlet – Haidara. no 1050, P.734.

3 Kassem Hala, l'internauteet son droit à être laissé tranquille, mémoire de D–E–A informatique et droit, fac de droit, univ Montpellier I, 2003, et disponible sur www.droit.ntic.com.P41,42.

انتهاك لخصوصية وسرية بيانات الفرد. فضلاً عن التسبب في إزعاجه عند استقباله سيلاً من الرسائل التسويقية والعروض الترويجية بصفة مستمرة وفي أوقات غير مناسبة أو حين تكون تلك الرسائل غير ملائمة لشخصه مطالباً الجهات المعنية بالعمل على رصد أنشطة الشركات التي تجمع البيانات الخاصة أو تبيعها لآخرين لأغراض تسويقية بصورة غير قانونية [1].

ومن خلال مطالعتنا للتشريع المصري والمقارن من أجل البحث عن المواجهة الجنائية التي أقامتها التشريعات الجنائية لمواجهة ظاهرة التداول غير المشروع للبيانات الخاصة، وجدنا أن المشرع تناول تلك الظاهرة تحت مسميات متعددة لعمل من أهمها:

اولا: نقل البيانات الخاصة بطريقة تنافي الغرض من جمعها:

تعتبر الخصوصية والبيانات الخاصة مرتبطتان ارتباطًا وثيقًا، حيث تنبثق البيانات الخاصة من مفهوم الخصوصية. لهذا السبب، تسعى جميع الأنظمة القانونية لحماية الحق في الخصوصية، وبالأخص البيانات الخاصة، من خلال قوانين دولية وإقليمية، بالإضافة إلى التشريعات الوطنية.

حيث نصت المادة الثانية عشرة من الإعلان العالمي لحقوق الإنسان على أنه "لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة، أو في شؤون أسرته، أو مسكنه، أو مراسلاته، ولا لحملات تمس شرفه وسمعته. ولكل شخص حق في أن يحميه القانون من مثل هذا التدخل أو تلك الحملات" [2].

---

١ د. **عثمان بكر عثمان**، مرجع سابق، ص ١٩.

[2] اعتمدت الجمعية العامة للأمم المتحدة الإعلان العالمي لحقوق الإنسان في باريس بتاريخ ١٠ كانون الأول/ديسمبر ١٩٤٨ بموجب القرار ٢١٧ ألف، واعتبرته معيارًا مشتركًا ينبغي أن تسعى جميع الشعوب والأمم لتحقيقه.

وجاء العهد الدولي للحقوق المدنية والسياسية ليتابع نهج الإعلان العالمي لحقوق الإنسان، حيث نص في المادة السابعة عشر منه على ما يلي: " لا يجوز تعريض أي شخص بشكل تعسفي أو غير قانوني للتدخل في خصوصياته، أو شؤون أسرته، أو منزله، أو مراسلاته، كما لا يجوز تعريضه لحملات غير قانونية تمس شرفه أو سمعته". ومن حق كل شخص أن يحميه القانون من مثل هذا التدخل أو المساس [1]. وتبنت الجمعية العامة للأمم المتحدة توصيات المؤتمر الدولي الأول لحقوق الإنسان، الذي عقد في طهران عام ١٩٦٨. حيث أظهرت التوصيات خطورة الحاسبات الإلكترونية على الحياة الخاصة، وأكدت على ضرورة تطوير آليات دولية وإقليمية لحمايتها [2].

وفي ١٤ كانون الأول/ديسمبر ١٩٩٠، اعتمدت الجمعية العامة للأمم المتحدة القرار رقم ٤٥/٩٥، الذي تضمن المبادئ التوجيهية لتنظيم ملفات البيانات الشخصية المخزنة على الحاسبات الإلكترونية. تناولت هذه المبادئ مسائل الحماية عبر نطاق واسع يشمل جميع الجهات المعنية بجمع البيانات ومعالجتها، سواء كانت بيانات عامة أم خاصة. وقد دعت المبادئ إلى توسيع نطاق التطبيق ليشمل الأشخاص المعنويين بالإضافة إلى الأشخاص الطبيعيين، وغطت المسائل على المستويين الوطني والدولي. فعلى المستوى الوطني، شددت المبادئ على ضرورة إقرار قوانين محددة واستثناءات، وتعيين سلطات رقابية وتطبيق العقوبات الجزائية. أما على المستوى الدولي،

---

[1] العهد الدولي للحقوق المدنية والسياسية صدر في ١٦ ديسمبر ١٩٦٦ وبدأ تنفيذه في مارس ١٩٦٧. وافقت جمهورية مصر العربية عليه بموجب قرار رئيس الجمهورية رقم ٥٣٦ لسنة ١٩٨١.

[2] **يونس خالد عرب**، جرائم الحاسوب (دراسة مقارنة)، رسالة ماجستير، الجامعة الأردنية، ١٩٩٤، ص. ١٢٥.

فقد وضعت أسسًا لمبادئ تدفق البيانات عبر الحدود وأكدت على قابلية تطبيق المبادئ على المنظمات الدولية الحكومية وغير الحكومية.

ايضا شملت المبادئ التي يجب على الدول إدراجها في قوانينها: مبدأ المشروعية والنزاهة، الذي يمنع جمع ومعالجة البيانات الخاصة بطرق غير نزيهة أو غير مشروعة، ويشدد على ضرورة استخدام البيانات بما يتماشى مع أهداف ميثاق الأمم المتحدة ومبادئه. كما نصت المبادئ على مبدأ صحة البيانات، الذي يفرض على معالجي البيانات التحقق من دقتها وملاءمتها للغرض المخصص لها. ينص مبدأ تحديد الغاية على وجوب الإعلان المسبق عن الهدف من جمع البيانات ومعالجتها، بحيث يكون الهدف مشروعًا ومحددًا، مما يسمح بمراقبة عدم الانحراف عن الغاية المعلنة واحترام حق الشخص في الموافقة على استخدام بياناته، وضمان محو البيانات بعد تحقيق الهدف.

أيضًا، ينص مبدأ وصول الأشخاص المعنيين إلى الملفات على حق الأفراد في الاطلاع على بياناتهم والتصرف فيها، وطلب تصحيحها أو محوها دون تكبدهم أي تكلفة غير مبررة. كما يشدد مبدأ عدم التمييز على عدم جواز التمييز العنصري بناءً على بيانات شخصية تتعلق بالعرق أو الأثنية أو اللون أو الميول الجنسية أو الآراء السياسية أو المعتقدات الدينية والفلسفية أو العضوية النقابية والمهنية. وأخيرًا، ينص مبدأ الأمن على ضرورة اتخاذ التدابير المناسبة لمنع فقدان البيانات أو تلفها أو تسربها أو الاطلاع عليها نتيجة عوامل طبيعية أو تصرفات بشرية غير مشروعة مثل الدخول غير المصرح به إلى الأنظمة أو استخدامها بشكل غير آمن [1].

[1] د. **منى الأشقر جبور**، د. **محمود جبور**، البيانات الشخصية والقوانين العربية، الهم الامني وحقوق الافراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، ٢٠١٨ ، ص ٥٣، ٥٢.

في تطور ملحوظ لتعزيز حماية البيانات الشخصية، أعربت الدول الأعضاء في الأمم المتحدة والجهات المعنية الأخرى عن قلقها من الأثر السلبي للممارسات الرقابية على حقوق الإنسان. وفي هذا السياق، اعتمدت الجمعية العامة للأمم المتحدة في كانون الأول/ديسمبر ٢٠١٣، دون تصويت، القرار رقم ٦٨/١٦٧ بشأن الحق في الخصوصية في العصر الرقمي. أكد هذا القرار، الذي قدمته ٥٧ دولة عضوًا، على ضرورة حماية حقوق الأفراد حتى خارج الفضاء الإلكتروني. دعت الجمعية العامة في قرارها جميع الدول إلى احترام وحماية الحق في الخصوصية في الاتصالات الرقمية، وطالبتها بمراجعة إجراءاتها وممارساتها وتشريعاتها المتعلقة بمراقبة واعتراض وجمع البيانات الشخصية. كما شددت على ضرورة أن تلتزم الدول بتنفيذ التزاماتها بموجب القانون الدولي لحقوق الإنسان بشكل كامل وفعّال.

وبناء على القرار رقم ٦٨/١٦٧ الصادر عن الجمعية العامة، طلب القرار من المفوض السامي لحقوق الإنسان إعداد تقرير حول حماية وتعزيز الحق في الخصوصية في ظل التطور التكنولوجي. كان من المقرر تسليم هذا التقرير إلى مجلس حقوق الإنسان والجمعية العامة في ٣٠ حزيران/يونيو ٢٠١٤. وقد أُنجز التقرير، الذي حمل عنوان "الحق في الخصوصية في العصر الرقمي"، ويعتبر ذا قيمة قانونية خاصة نظرًا لاعتماده على ممارسات الدول المتعلقة بهذا الموضوع[١].

وقد تضمن التقرير الذي أعده المفوض السامي لحقوق الإنسان التأكيد على حق جميع الأفراد في الحماية من الهجمات والتدخلات. أشار التقرير إلى عدم كفاية تطبيق الحق في الخصوصية والحاجة الملحة إلى اتخاذ

[١] د. **خالد حسن أحمد**، الحق في خصوصية البيانات الشخصية بين الحماية القانونية والتحديات التقنية: دراسة مقارنة، دار الكتب والدراسات العربية، القاهرة، ٢٠٢٠، ص. ١٠١.

تدابير ملموسة لحمايته، بما في ذلك التصدي بشكل شامل للوصول غير المأذون به إلى البيانات الشخصية والمراقبة المكثفة. دعا التقرير إلى اتخاذ إجراءات عاجلة لوقف ممارسات المراقبة وحماية الأفراد من انتهاك حقوقهم في الخصوصية. كما شدد على أن أي قيد على الحق في الخصوصية يجب أن يستند إلى قوانين واضحة وشفافة، وأن يقتصر على ما هو ضروري لحماية المصلحة العامة في أي مجتمع ديمقراطي. يجب أن تكون المراقبة التي تقوم بها الدولة متناسبة وعادلة، ومتوافقة مع القواعد والمعايير الدولية، وخاضعة لأحكام القانون، مع تحديد ضمانات كافية وفعالة لمنع إساءة الاستخدام [1].

وعقب صدور الإعلان العالمي لحقوق الإنسان، شهدت الاتفاقيات الإقليمية تقدمًا ملحوظًا في مجال حقوق الإنسان، خاصة في الأقاليم التي تشترك في تراث مشترك ولديها آليات لتنفيذها بفعالية. يعتبر الاتحاد الأوروبي من أبرز المنظمات الإقليمية التي اهتمت بحماية البيانات الشخصية. بدأ اهتمام الاتحاد الأوروبي بحماية البيانات في عام ١٩٩٥ مع إصدار القواعد الإرشادية، وفي ٢٧ أبريل ٢٠١٦، أقر البرلمان الأوروبي القواعد الأوروبية لحماية الأشخاص الطبيعيين من المعالجة الرقمية للبيانات الشخصية والتدفق الحر للمعلومات. دخل التشريع الأوروبي الموحد لحماية البيانات الشخصية، المعروف بالقواعد العامة لحماية البيانات، حيز التنفيذ في مايو ٢٠١٨، بهدف تحقيق انسجام بين القوانين الأوروبية عبر توحيد التشريعات لتعزيز الشفافية ودعم حقوق الأفراد ونمو الاقتصاد الرقمي، وهو

[1] د. **هشام مسعودي**، حماية وتعزيز الحق في الخصوصية في العصر الرقمي: قراءة في تقرير مفوضية الأمم المتحدة لحقوق الإنسان في دورته ٢٨، مجلة الحقوق والعلوم السياسية، جامعة عباس لغرور خنشلة، الجزائر، العدد ١، أبريل ٢٠٢٢، المجلد ٩، ص. ١٦٣.

ملزم لكافة دول الاتحاد [1].

تنص المبادئ التوجيهية للاتحاد الأوروبي في المادة (٦) على مجموعة من الالتزامات التي يجب أن تلتزم بها الدول الأعضاء أثناء معالجة البيانات الشخصية بطرق آلية، وهي كالتالي:

أ- يجب معالجة البيانات بطريقة عادلة وقانونية.

ب- يجب جمع البيانات لأغراض محددة وواضحة وشرعية، ولا يمكن معالجتها بعد ذلك بطرق تتعارض مع تلك الأغراض. يجوز استخدام المعالجة الآلية للبيانات لأغراض تاريخية أو إحصائية أو علمية، بشرط أن تكون هذه الأغراض غير متعارضة وأن تقدم الدول الأعضاء الضمانات المناسبة.

ج- يجب أن تكون المعالجة الآلية للبيانات كافية وغير زائدة ومرتبطة بالأغراض التي جمعت من أجلها أو عولجت لأجلها.

د- يجب أن تكون المعالجة الآلية للبيانات دقيقة، وعند الضرورة، يجب اتخاذ جميع الخطوات اللازمة لضمان تصحيح البيانات غير الدقيقة أو غير الكاملة بالنسبة للأغراض التي جمعت وعولجت من أجلها.

هـ - يجب أن تُحفظ البيانات التي تم معالجتها آلياً بطريقة تسمح بالتعرف على صاحب البيانات لمدة لا تتجاوز الغرض الذي جُمعت البيانات من أجله أو الذي عولجت من أجله. ويجب على الدول الأعضاء وضع الضمانات المناسبة للبيانات المخزنة لفترات أطول لاستخدامات تاريخية أو إحصائية أو علمية.

---

[1] د. **منى الأشقر جبور**، د. **محمود جبور**، البيانات الشخصية والقوانين العربية: الهم الامني وحقوق الافراد، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، ٢٠١٨ ، ص ٥٥.

كما يمكن القول إن الجهود التي بذلتها المنظمات الدولية والإقليمية كانت لها تأثير كبير في صياغة النظام القانوني لحماية خصوصية البيانات الخاصة على الصعيد الدولي. وقد تميز القانون الأوروبي في هذا المجال من خلال اللائحة العامة لحماية البيانات بالاتحاد الأوروبي، التي تُعد قانونًا نموذجيًا للعديد من التشريعات الوطنية داخل الاتحاد الأوروبي وخارجه.

وفي التشريعات الوطنية، تقوم قوانين حماية البيانات الخاصة بفرض التزامات على المعالجين، من أهمها ضرورة تحديد الغرض من معالجة البيانات مسبقًا، ويهدف ذلك إلى تقييد معالجة البيانات الخاصة بما يتناسب مع الغاية التي جمعت لأجلها، وتبقى هذه الغاية هي المعيار الذي يحكم ويحدد كل إجراء من إجراءات معالجة البيانات التي تقوم بها الجهة المعالجة.

وتُشدد القوانين على أن جمع البيانات الخاصة يجب أن يكون لأغراض مشروعة، ويجب تحديد تلك المصالح المشروعة، وضرورة أن تكون المعالجة ضرورية لتحقيق تلك الغاية، ويجب أيضًا مراعاة مبدأ التناسب بين مصالح الفرد وحقوقه وحرياته، وبين الغرض الذي تمت المعالجة لأجله، والذي يجب تحديده بوضوح أثناء الموافقة التي يصدرها صاحب البيانات على معالجة بياناته.

لذلك؛ جرم قانون العقوبات الفرنسي الأفعال التي تمثل تغيير للغرض من جمع البيانات بقوله: "يعاقب كل شخص يمتلك بيانات شخصية أثناء تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة، بتغيير هذه البيانات من غرضها على النحو المحدد في النص التشريعي أو اللائحة التنظيمية أو قرار اللجنة الوطنية، أو موافقته بالمعالجة الآلية، أو بالإعلان

المسبق لتنفيذ هذه المعالجة ..."[1].

السلوك الإجرامي في هذه الحالة يتجلى في تغيير الغرض الذي جمعت من أجله البيانات، مما يعني الانحراف عن الغاية الأساسية لعملية المعالجة، في هذا السياق، يحدث أن تقوم جهة المعالجة بجمع بيانات الأفراد بشكل شرعي، وباستئذانهم وموافقتهم على إجراء عمليات المعالجة على بياناتهم، ثم تستخدم هذه البيانات في أغراض لم يتم الاتفاق عليها مسبقًا، سواء كانت هذه الأغراض مشروعة أو غير مشروعة.

لذلك، يُعتبر نشر العناوين البريدية المرتبطة بالموظفين من قبل الشركة، وخارج سياق العمل، عملية معالجة غير مشروعة للبيانات الشخصية، ولا تتماشى مع الهدف الأساسي لجمع هذه العناوين البريدية، والذي كان في الأساس لتبادل المعلومات بين الموظفين في إطار العمل داخل الشركة[2].

أيضًا، يُعتبر جمع البيانات الخاصة لأغراض تنبؤيه عملية معالجة

---

[1] Art. 226-21: Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004

[2] Tribunal de grande instance de Paris 3ème chambre, 2ème section 25 avril 2003.

غير مشروعة، كما تم التأكيد عليه في قرار المحامي العام في القضية Ligue des droits humains v Conseil des ministre لسنة ٢٠٢٢، حيث أشار إلى التحديات في تحقيق التوازن بين حقوق الفرد والمصلحة العامة أثناء جمع البيانات الخاصة، يتساءل عن كيفية تحقيق هذا التوازن، خاصةً في ظل تطور التقنيات الرقمية التي تمكن من جمع وتخزين ومعالجة وتحليل كميات هائلة من البيانات الخاصة لأغراض تنبؤيه. فإذا كان الهدف هو تعزيز وحماية المصالح الأساسية للمجتمع، ومكافحة الإرهاب والجريمة، خصوصًا الجرائم الخطيرة، فينبغي أن يتم تحقيق التوازن بين هذه المصالح وحقوق الأفراد، ويتطلب ذلك تطبيق الضمانات الكافية لضمان عدم انتهاك حقوق الفرد وحماية بياناته الخاصة، بما في ذلك منع أي تجاوزات تتعلق بمعالجة تلك البيانات[1].

وفيما يتعلق بالركن المعنوي لهذه الجريمة، فإنه يلزم توافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم الجاني أن إجراء المعالجة الذي يقوم به يتم لأغراض منافية للغرض الأصلي الذي جمعت البيانات لأجله، ويقوم بذلك دون علم صاحبها وموافقته، وتتجه إرادته إلى إتيان هذا الفعل وتحقيق نتيجته.

وبناء عليه، عاقب المشرع الفرنسي كل من ارتكب هذا الفعل، بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠٠٠٠ يورو.

أما المشرع المصري فقد نصت المادة رقم ٣٨ من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ على أنه: "يعاقب بغرامة لا تقل عن ثلاثمائة ألف جنيه ولا تجاوز ثلاثة ملايين جنيه ، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في القانون"، والتي من بينها الالتزام أثناء

[1] Conclusions de l'avocat général M. G. Pitruzzella, présentées le 27 janvier 2022.

المعالجة بالغرض المحدد مسبقاً من المعالجة[1].

ثانيا: إفشاء البيانات الخاصة إلى غير ذي صفة قانونية:

تنص المادة ٣٦ من قانون حماية البيانات الشخصية المصري على معاقبة كل حائز أو متحكم أو معالج للبيانات الشخصية جمع أو عالج أو أفشى أو أتاح أو تداول بيانات شخصية معالجة إلكترونياً، بأي وسيلة من الوسائل، دون تصريح قانوني بذلك، أو بدون موافقة صاحبها[2].

أما قانون العقوبات الفرنسي، فقد تضمنت المادة ٢٢٦/ ٢٢ عقاب كل شخص يقوم أثناء نقله أو معالجته أو تصنيفه أو بأي شكل من أشكال المعالجة، بالإفصاح عن تلك البيانات للغير من غير ذي الصفة القانونية لتلقي تلك البيانات، وترتب على ذلك انتهاك لاعتبار صاحب البيانات وتعدي على حرمة حياته الخاصة، وتم ذلك دون موافقة أو تصريح من الشخص المعني بالبيانات[3].

---

[1] ووفقا للمادة (٤/ ٧) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ فإنه يجب على المتحكم ، محو البيانات الخاصة لديه فور انقضاء الغرض المحدد منها ، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض ، فيجب ألا تبقي في صورة تسمح بتحديد الشخص المعني بالبيانات.

[2] نصت المادة (٣٦) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ على أنه: "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات . وتكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه ، أو بإحدى هاتين العقوبتين ، إذا ارتكب ذلك مقابل الحصول علي منفعة مادية أو أدبية ، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر .

[3] Art. 226-22: Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet

ويتمثل الركن المادي في هذه الجريمة بفعل الإفشاء أو الإفصاح، والإفصاح يعني كشف معلومات يُحافظ صاحبها على سريتها، أو يرغب في تقييدها لعدد محدود من الأشخاص، ومن المرتبطات البارزة لقبول الإفصاح لعدد محدود من الأشخاص هو الاعتبار الشخصي للمعلومات وتأثيرها على حياة الفرد، حيث يتعلق الأمر بقرارات حيوية قد تؤثر بشكل كبير في مصيره، وينتج عن الإفشاء غالبًا أضرار على المستوى الشخصي، مثل السمعة أو الكرامة أو الأمور المالية أو النفسية لصاحب المعلومات[1].

وفيما يتعلق بالركن المعنوي فإنه يلزم توافر القصد الجنائي العام بعنصريه العلم والإرادة؛ بأن يعلم الجاني أن فعل التسجيل أو المعالجة أو الفهرسة يترتب عليه إفشاء لبيانات خاصة، ويقوم بذلك دون علم صاحبها

---

de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 euros d'amende lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Modifié par Loi n°2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004

[1] أنظر **محمد فتحي ابراهيم**، تجريم الاعتداء على المعلومة الإلكترونية ذات الطابع الشخصي بين الواقع والمأمول، مجلة الفقه والقانون، العدد ٦٤، ٢٠١٨م، ص١٩.

وموافقته، وتتجه إرادته إلى إتيان هذا الفعل وتحقق النتيجة[1].

وساوى المشرع الفرنسي بين القصد الجنائي والخطأ غير العمدي، مع اختلافه في تقرير العقوبة بينهما، فقد عاقب المشرع الفرنسي بالسجن خمس سنوات وبغرامة ٣٠٠ ألف يورو في حالة العمد، وبالسجن ثلاث سنوات وبغرامة ١٠٠ ألف يورو في حال ارتكاب سلوك الإفشاء عن طريق الإهمال وعدم الاحتياط أي بطريق الخطأ.

وبشأن قانون المعاملات الإلكترونية الكويتي في المادة (٣٥) منه حظر الاستخدام غير المصرح به، حيث ينص قانون المعاملات الإلكترونية الكويتي على حظر استخدام البيانات الشخصية لأغراض غير تلك التي جُمعت من أجلها، مما يعني أن أي معالجة للبيانات يجب أن تكون متوافقة مع الأغراض الأصلية التي جُمعت من أجلها.

وعاقب قانون العقوبات الفرنسي بموجب المادة ٢٢٦-٢٢/ ١ على حالة الإفشاء أو نقل البيانات الخاصة محل المعالجة إلى دولة لا تنتمي إلى الاتحاد الأوروبي أو إلى منظمة دولية، حيث تمثل انتهاك للفصل الخامس من اللائحة الأوروبية لحماية البيانات الصادرة بتاريخ ٢٠١٦/٦٧٩ للبرلمان الأوروبي، والمجلس بتاريخ ٢٧ أبريل ٢٠١٦ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الخاصة وحرية حركة هذه البيانات وإلغاء التوجيه ٩٥/٤٦ EC حيث تعاقب المواد رقم ١١٢ إلى ١١٤ من القانون رقم ١٧ – ٧٨ الصادر في ٦ يناير ١٩٧٨ بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠

[1] أنظر **د. محمود نجيب حسني،** شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي دار النهضة العربية، القاهرة، ٢٠١٨، ص ٧٥١- ٧٥٢.

ألف يورو[1].

وعاقب المشرع المصري على تلك الجريمة بالغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه. وتشدد العقوبة لتصبح الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه، ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكبت هذه الجريمة مقابل الحصول على منفعة مادية أو معنوية، أو ارتكبت بقصد تعريض صاحب البيانات للخطر[2].

ومن خلال النصوص السابقة يتبين لنا، فيما يتعلق بجريمة تغيير غرض جمع البيانات، ينص قانون العقوبات الفرنسي على معاقبة كل من يغير الغرض الأصلي لجمع البيانات الشخصية بعقوبات تشمل السجن لمدة تصل إلى خمس سنوات وغرامة قدرها ٣٠٠,٠٠٠ يورو. يتجلى السلوك الإجرامي هنا في استخدام البيانات لغير الأغراض التي جُمعت من أجلها، سواء كانت

[1] Art. 226-22-1: " e fait de procéder ou de faire procéder à un transfert de données à caractère personnel faisant l'objet ou destinées à faire l'objet d'un traitement vers un Etat n'appartenant pas à l'Union européenne ou à une organisation internationale en violation du chapitre V du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/ CE, ou des articles 112 à 114 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

Modifié par Ordonnance n°2018-1125 du 12 décembre 2018 - art. 13.

[2] أنظر المادة ٣٦ من قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م.

الأغـراض مشـروعة أو غيـر مشـروعة. كـذلك، فـإن الإفشـاء عـن البيانـات خـارج سياق الاستخدام الأصلي يُعتبر معالجة غير مشروعة.

وفـي المقابـل، يـنص قـانون حمايـة البيانـات الشخصـية المصـري (رقـم ١٥١ لسـنة ٢٠٢٠) علـى معاقبـة المـتحكم أو المعـالج الـذي لا يلتـزم بـالأغراض المحـددة مسـبقاً بعقوبـات تشـمل غرامـة تتـراوح بـين ٣٠٠,٠٠٠ و٣,٠٠٠,٠٠٠ جنيه.

أمـا بشـأن إفشـاء البيانـات، يـنص قـانون العقوبـات الفرنسـي فـي المـادة ٢٢٦-٢٢ علـى معاقبـة كـل مـن يفشـي بيانـات شخصـية بـدون تصـريح قـانوني بعقوبـات تصـل إلـى خمـس سـنوات سـجن وغرامـة ٣٠٠,٠٠٠ يـورو، مـع تمييـز بـين القصـد الجنـائي والخطـأ غيـر العمـدي. و**فـي المقابـل**، يعاقـب قـانون حمايـة البيانـات المصـري (المـادة ٣٦) علـى الإفشـاء غيـر المصـرح بـه للبيانـات الشخصـية بغرامـة لا تقـل عـن ١٠٠,٠٠٠ جنيـه ولا تتجـاوز مليـون جنيـه، مـع تشـديد العقوبـة إذا كانـت الجريمـة ارتُكبـت مقابـل منفعـة ماديـة أو معنويـة أو تعريض صاحب البيانات للخطر.

فـالمفهوم الأساسـي للطريقـة المشـروعة فـي معالجـة البيانـات الشخصـية هـو أن أي إجـراء يتخـذ بشـأن البيانـات يجـب أن يكـون قانونيًـا وموافِقًـا للغـرض الـذي جُمعـت البيانـات مـن أجلـه، يتضـح أن **المشـرع الفرنسـي** يشـدد علـى ضـرورة إبـلاغ الأفـراد بـأي إجـراء يتعلـق بمعالجـة بيانـاتهم لضـمان أن هـذا الإجـراء يُعتبـر مشـروعًا. بمعنـى آخـر، يجـب أن يكـون هنـاك شـفافية كاملـة تجاه الأفراد حول كيفية معالجة بياناتهم.

والشـرط الـذي يـنص علـى ضـرورة أن تتماشـى معالجـة البيانـات الخاصـة مـع الهـدف الأصـلي مـن جمعهـا يعنـي أن البيانـات لا يمكـن اسـتخدامها لأغـراض تتجـاوز تلـك التـي تـم جمعهـا مـن أجلهـا. الهـدف هـو ضـمان أن

عملية المعالجة لا تخرج عن نطاق الهدف الذي جُمعت البيانات لأجله، مما يحافظ على نزاهة العملية ويمنع الاستغلال غير المبرر للبيانات، وذلك على النحو التالي:

- **عند تقديم بيانات خاصة إلى جهة معينة**، مثلًا، طلب بيانات من عميل لتقديم خدمة محددة، يجب أن تقتصر معالجة هذه البيانات على تحقيق هذا الهدف المحدد فقط. أي استخدام للبيانات لأغراض أخرى يُعتبر غير مشروع.
- **إذا استخدمت البيانات الخاصة** لأغراض مختلفة عن تلك التي جُمعت لأجلها، مثل استخدام بيانات العملاء لأغراض تسويقية غير متفق عليها مسبقًا، فإن هذا يعد استخدامًا غير مبرر للبيانات.

ويظهر أهمية هذا الشرط:

- **الحد من الاستخدام غير المبرر:** هذا الشرط مهم لأنه يحد من إمكانية استخدام البيانات الشخصية بشكل غير مبرر ويشدد على أن البيانات تُستخدم فقط لتحقيق الأغراض التي جُمعت من أجلها.
- **الامتثال للأغراض المحددة:** يحافظ هذا الشرط على الانسجام بين الغرض الأصلي لجمع البيانات والإجراءات التي يتم اتخاذها بشأنها بعد جمعها.

الخاتمة

انتهيتُ بفضل الله وبعونه من إتمام هذه الدراسة التي بذلت فيها جهد المقل في محاولة نقل فكرة خطورة ظاهرة التداول غير المشروع للبيانات الخاصة، وقد ظهر جليا أن ظاهرة التداول غير المشروع للبيانات الخاصة أصبحت تشكل تحديًا جنائيًا خطيرًا يتطلب استجابة فورية وفعالة من القوانين والتشريعات، وتتضمن هذه الظاهرة مجموعة متنوعة من الانتهاكات والاعتداءات على خصوصية الأفراد وحقوقهم، مما يستدعي اتخاذ تدابير رادعة للحد منها ومعاقبة المرتكبين.

وقد أمكن لنا في نهاية تلك الدراسة الخروج بمجموعة من النتائج والتوصيات، نوردها فيما يلي:

أولا: نتائج الدراسة:

١ – تعد حماية خصوصية الحياة الشخصية، وبخاصة البيانات الخاصة للأفراد، أحد أبرز الحقوق التي تضمنتها التشريعات المحلية والدولية، وتزداد أهميتها في ظل التطور التكنولوجي الحديث وانتشار الرقمنة.

٢ – تتنوع البيانات الخاصة المحمية، وتشمل جميع أنواع البيانات التي يمكن استخدامها لتحديد الأفراد مباشرة أو غير مباشرة، سواء كانت حساسة أو خاصة بالشخص نفسه، وتستثني البيانات الإحصائية والتي تتعلق بالأمن القومي من حالات الإفصاح.

٣ – يجب توازن الحقوق المتعارضة وإعطاء الأولوية للحقوق بحسب الأولويات والضروريات الشرعية، مثل حماية المصلحة العامة والأمن القومي وحقوق الآخرين.

٤ – يجب على جهة المعالجة اتباع الشروط والضوابط المطلوبة عند تجميع ومعالجة البيانات، بما في ذلك الحصول على موافقة صريحة من

صاحب البيانات واستخدامها وفقًا للأغراض المعتمدة وعدم الاحتفاظ بها لفترات طويلة.

٥ – تُلزم التشريعات المعنية بحماية البيانات الخاصة بتمكين صاحب البيانات من ممارسة حقوقه على بياناته، مع تنظيم هذه الحقوق بما في ذلك الحق في العلم والوصول والتصحيح والمحو والنسيان والاعتراض.

٦ – تُجرم التشريعات الجنائية سلوكيات الاعتداء على البيانات الخاصة، سواء في مراحل جمعها أو معالجتها أو إفصاحها، بما في ذلك الاستغلال غير المشروع لها أو التهديد به.

٧ – تتنوع أشكال السلوك الإجرامي في جرائم الاعتداء على البيانات الخاصة، سواء كانت إيجابية أو سلبية.

٨ – يتطلب ارتكاب جرائم الاعتداء على البيانات الخاصة وجود قصد جنائي عمدي، ومع ذلك، تُعاقب بعض التشريعات على ارتكاب تلك الجرائم حتى في حالات الإهمال أو الخطأ.

٩ – يختلف نوع العقوبات الجنائية التي تُفرض على المعتدين على البيانات الخاصة، بحسب نوع وخطورة الجرائم المرتكبة.

ثانيا: توصيات الدراسة:

بناءً على النتائج التي تم التوصل إليها في الدراسة، تم اقتراح مجموعة من التوصيات، وهي كالتالي:

١ – بناء على ما توصلنا إليه من التفرقة بين مصطلح البيانات الخاصة والبيانات الشخصية وأن مصطلح البيانات الشخصية لا يشمل البيانات الخاصة بالشخص المعنوي، ونظرا لما تمثله الأشخاص الاعتبارية من أهمية يجب على المشرع أن يوسع نطاق الحماية لتشمل كلا من الشخص الطبيعي والشخص المعنوي على حد سواء.

٢ – نوصي المشرع بتوسيع نطاق الحماية لتشمل كلا من البيانات المدونة ورقيا والبيانات الالكترونية على حد سواء.

٣ – نوصي في الحالات التي يفرض فيها القانون التزامًا قانونيًا على الجهة المعالجة دون الحاجة إلى موافقة الفرد المعني بالبيانات، بتبصير الفرد بنوع هذا الالتزام وغرضه ومصدره القانوني.

٤ – يجب أن يشمل التشريع المصري جرائم الاعتداء على البيانات الخاصة، حتى في حالات الخطأ والإهمال غير العمدي، لضمان عدم تفادي المسؤولية الجنائية بحجة الإهمال.

٥ – عند تحديد الاستثناءات المتعلقة بالبيانات الخاصة التي يمكن إتاحتها دون الحصول على موافقة الفرد، يجب أن تُخضع لتقييم المصلحة والضرر، وأن يكون للمصلحة المترتبة عن الإفصاح الأولوية على الضرر المحتمل.

٦ – ينبغي على الجهات المعنية ووسائل الإعلام تبصير الأفراد بأهمية حماية بياناتهم الخاصة وحقوقهم المتعلقة بها.

٧ – يجب على الأفراد التأكد وقراءة الشروط المطلوبة قبل الدخول إلى مواقع أو تطبيقات إلكترونية.

٨ – ينبغي أن تتضمن التشريعات نصوصًا صريحة ودقيقة تنظم ممارسة حقوق الأفراد على بياناتهم دون إبطاء أو تأخير.

٩ – يجب أن تتضمن التشريعات عقوبات صارمة لمواقع الإنترنت ومواقع التواصل الاجتماعي التي تخالف سياسات حماية البيانات الخاصة.

١٠ – ينبغي تشديد العقوبات في حالات إفشاء البيانات الخاصة التي يمكن أن تضر بالنظام العام أو الأمن القومي.

١١ – يجب أن تميز العقوبات بين الاختلال بحماية البيانات الخاصة حسب ما إذا كان الفعل عمدًا أم غير عمد.

قائمة أهم المراجع

أولا: قائمة المراجع باللغة العربية:

١. **د. أحمد رجب سيد صميدة،** التنظيم القانوني للحق في الخصوصية: المسكن – الاتصالات الخاصة – البيانات الشخصية في القانون الفرنسي والأمريكي والمصري وفقاً لآخر التعديلات التشريعية، دار النهضة العربية، القاهرة، ٢٠٢٢.

٢. **د. أحمد مختار عبد الحميد عمر (ت ١٤٢٤ هـ)** وآخرين، معجم اللغة العربية المعاصرة، عالم الكتب، الطبعة الأولى، ١٤٢٩ هـ – ٢٠٠٨ م، جـ ١.

٣. **د. باسم محمد فاضل مدبولي** ، المسئولية المدنية عن أضرار معالجة البيانات الرقمية ، دراسة مقارنه ، في ضوء اللائحة الأوروبية العامة (٦٧٩) لسنة ٢٠١٦ والقانون المصري ١٥١ لسنة ٢٠٢٠ ، دار الفكر الجامعي ، الإسكندرية ، ٢٠٢٣.

٤. **د. جبالي أبو هشيمة،** حماية البيانات الشخصية في البيئة الرقمية دراسة مقارنة بين القانون الفرنسي ومشروع القانون المصري، مؤتمر العصر الرقمي واشكالياته القانونية، كلية الحقوق – جامعة أسيوط، ابريل ٢٠١٦.

٥. **د. حسن عبد الحميد وآخرين،** دراسة نقدية لقانون حماية البيانات الشخصية رقم (١٥١) لسنة ٢٠٢٠، مركز بحوث القانون والتكنولوجيا، ٢٠٢٠.

٦. **د. حسين سليم محمد سليم** ، الحماية الجنائية للبيانات الشخصية المعالجة آليا: دراسة مقارنة ، مجلة العلوم القانونية الاقتصادية ، جامعة عين شمس – كلية الحقوق ، ٢٠٢٠.

٧. **د. دينا عبدالعزيز فهمي** ، المسئولية الجنائية الناشئة عن إساءة استخدام مواقع التواصل الاجتماعي ، مجلة كلية الحقوق، جامعة طنطا ، ٢٠١٧.

٨. **د. سامح عبد الواحد التهامي،** نطاق الحماية القانونية للبيانات الشخصية والمسؤولية التقصيرية عن معالجتها – دراسة في القانون الاماراتي، مجلة البحوث القانونية والاقتصادية، العدد ٦٧، ديسمبر ٢٠١٨.

٩. **د. سامح عبدالواحد التهامي** ، ضوابط معالجة البيانات الشخصية ، دراسة مقارنة بين القانون الفرنسي والقانون الكويتي ، مجلة كلية القانون الكويتية العالمية ، المجلد ٣ ، العدد ٩ ، ٢٠١٥.

١٠. **د. عبد الرحمن بن حسن حَبَنَّكَة الميداني الدمشقي (ت ١٤٢٥هـ)،** البلاغة العربية، دار القلم، دمشق، الدار الشامية، بيروت، الطبعة الأولى، ١٤١٦ هـ – ١٩٩٦ م.

١١. **د. عثمان بكر عثمان،** المسئولية عن الاعتداء علي البيانات الشخصية لمستخدمي شبكات التواصل الاجتماعي، مجلة كلية الحقوق، جامعة طنطا، العدد ٣٣، الجزء ٤.

١٢. **د. علي جعفر،** جرائم تكنولوجيا المعلومات الحديثة الواقعة على الأشخاص والحكومة– دراسة مقارنة ، منشورات زين الحقوقية ، بيروت ، ٢٠١٣.

١٣. **د. عمرو طه بدوي محمد،** التنظيم القانوني لمعالجة البيانات الشخصية، دراسة تطبيقية علي معالجة تسجيلات المراقبة البصرية، دار النهضة العربية، القاهرة، ٢٠٢٠.

١٤. **د. غانم محمد غانم،** دور قانون العقوبات في مكافحة جرائم الكمبيوتر والانترنت، دار الفكر والقانون، القاهرة، ٢٠١٣.

١٥. **د. فتحي محمد عبدالسلام الفقي،** معالجة البيانات الشخصية عبر المواقع الإلكترونية والعلاقة التعاقدية الناشئة عنها دراسة مقارنه، دار مصر، القاهرة، ٢٠٢٣.

١٦. **د. محمد فتحي ابراهيم،** تجريم الاعتداء على المعلومة الإلكترونية ذات الطابع الشخصي بين الواقع والمأمول، مجلة الفقه والقانون، العدد ٦٤، ٢٠١٨م.

١٧. **د. محمود إبراهيم الغازي** ، الحماية الجنائية للخصوصية والتجارة الإلكترونية ، مكتبة الوفاء القانونية ، الإسكندرية ، ٢٠١٤.

١٨. **د. محمود أحمد طه**، المواجهة التشريعية لجرائم الكمبيوتر والانترنت، دار الفكر والقانون، ٢٠١٣.

١٩. **د. محمود عبدالرحمن** ، التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية ، العدد التاسع السنة الثالثة ، مارس ٢٠١٥.

٢٠. **د. محمود نجيب حسني**، شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي دار النهضة العربية، القاهرة، ٢٠١٨.

٢١. **د. مروة زين العابدين صالح** ، الحماية القانونية الدولية للبيانات الشخصية عبر الانترنت بين القانون الدولي الاتفاقي والقانون الوطني ، مركز الدراسات العربية ، القاهرة، ٢٠١٦.

٢٢. **د. منى تركي الموسوي**، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة ، مجلة كلية بغداد للعلوم الاقتصادية ، ٢٠١٣ ع١٠ .

٢٣. **د. نصر رمضان سعدالله الحربي**، التعويض عن الأضرار الناجمة عن الاعتداء علي البيانات الأساسية لمستخدمي مواقع التواصل الاجتماعي في ضوء القانون ١٥١ لسنة ٢٠٢٠ – دراسة مقارنة، مجلة كلية الشريعة والقانون، طنطا، العدد ٣٦.

٢٤. **د. نهلا عبد القادر المومني**، الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، عمان، ٢٠٠٨.

٢٥. **د. هشام محمد فريد رستم**، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ١٩٩٢.

٢٦. **د. ياسر محمد لمعي**، السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، مجلة روح القوانين، العدد ٢٧، يناير ٢٠٢٢.

ثانيا: قائمة المراجع باللغة الأجنبية:

1. Commission nationale de l'informatique et des libertés (CNIL), « La publicité ciblée en ligne », Communication présentée en séance plénière le 5 février 2009, Paris.

2. **CORALIE DUMAS** , LE DROIT DE LA PERSONNALITE ET LES RESEAUX SOCIAUX , MEMOIRE , faculté de droit , université de MONTPELLIER , 2015.

3. **Farid BOUGUETTAYA** , LA PROTECTION DES DONNEES PERSONNELLES EN DROIT COMMUNAUTAIRE , MEMOIRE, UNIVERSITE DE MONTPELLIER I , FACULTE DE DROIT – IDEDH , 2006.

4. Luc Crynbaum, Caroline le Goffic, Lydia Morlet – Haidara. no 1050.

5. Mallorie Wozny , Exploitation des données personnelles : raison commerciale, raison d'état et opportunités , mémoire , université de lyon , faculté de droit , 2017.

6. **Melle FAGET Marie** ,Les réseaux sociaux en ligne et la vie privé , Mémoire , faculté de droit , université Paris II , 2009.