الحماية الجنائية للبيانات الشخصية المعالجة آليا

« دراسة مقارنة »

دكتـــــور

سليم محمد سليم حسين

مدرس القانون الجنائي

بالأكاديمية الحديثة

لعلوم الكمبيوتروتكنولوجيا الإدارة

بالمعادي

الملخص

يتصـدي هذا البحث بالدراسـة والتحليل لثلاثة جوانب يثيرها موضـوع الحماية الجنائية للبيانات الشخصية المعالجة آليا:

أول هذه الجوانبُ يتعلق بمفهوم البيانات الشخصية وما إذا كانت تقتصر علي بيانات التعريف المباشـر للأشـخاص أم تشـمل إلي جانب ذلك بيانات أخرى. وما هو المقصـود بمعالجة البيانات الشـخصـية ؟ وهل يقتضـي الحق في الخصـوصـية أن تمتد الحماية الجنائية لتشمل كافة صور معالجة البيانات الشخصية ؟

وثاني هذه الجوانب يتعلق بالضـوابط المقررة لحماية البيانات الشـخصـية، وهل يخضـــع المســـئول عن معالجتها لرقابة جهة إدارية ما بالدولة حتي نضـــمن التزامه بالقانون ؟ وإلي أي مدى يلتزم بضـــمان أمن البيانات وســـريتها ؟ وما هي المبادئ التوجيهية المتعلقة بمعالجة البيانات الشخصية التي يتعين علي المعالج احترامها ؟ وما هي الحقوق التي خولتها التشريعات المقارنة للشخص المعني والتي يستطيع ممارستها في مواجهة معالج البيانات ؟

ويتمثل الجانب الأخير في أوجه الحماية المقررة للبيانات الشـــخصـــية في التشـــريعات المقارنة. وهل اتفقت الدول في كيفية التحرك التشـــريعي لحماية البيانات الشـــخصـــية المعالجة آليا ومواجهة الأفعال المتعلقة بانتهاك هذه البيانات أو الاعتداء عليها ؟

Abstract

المقدمة

من المعلوم أن الحق في الخصوصية يعد أحد الحقوق اللصيقة بالإنسان [1]، ويشمل هذا الحق صورًا عديدة تتصل جميعها بأسرار الفرد وحياته الخاصة، وتنبع من حريته الشخصية. ولعل من أهم صور هذ الحق: حق الفرد في المحافظة علي أسراره الشخصية التي لا يجب أن يطلع عليها أحد إلا بإذنه، مثل السر المتعلق بحالته المالية، والوضع الصحي والاتجاهات الأخلاقية والسياسية، وحقه في اختيار الزوج، واجتماع شمل الأسرة ....، ..... والحق في حماية البيانات الشخصية الخاصة به كالصورة، والأرقام والعناوين الشخصية، والخصائص البيوميترية، ومراسلاته بصورها المختلفة.

---

[1] د/ أحمد فتحي سرور، الحماية الدستورية للحقوق والحريات، دار الشروق 2000، ص 33 وما بعدها.

وبالرغم من أن للخصوصية العديد من العناصر المستقلة القائمة بذاتها، إلا أنها ترتبط مع بعضها البعض وهي كالأتي: **أولها**، خصوصية المعلومات، وتتضمن القواعد التي تحكم جمع وإدارة البيانات الخاصة كمعلومات بطاقة الهوية والمعلومات المالية والسجلات الطبية والسجلات الحكومية، وهي المحل الذي يتصل بمفهوم حماية البيانات محل الدراسة. **وثانيها**، الخصوصية الجسدية، والتي تتعلق بالحماية الجسدية للأفراد ضد أية إجراءات ماسة بالنواحي المادية لأجسادهم كفحوص الجينات وفحص المخدرات وفحوص الحمض النووي. **وثالثها**، خصوصية الاتصالات، والتي تغطي سرية وخصوصية المراسلات الهاتفية والبريد الإلكتروني وغيرها من وسائل الاتصالات. وأخيرا، الخصوصية المكانية، والتي تتعلق بالقواعد المنظمة للدخول إلي المنازل وأماكن العمل أو الأماكن العامة، والتي تتضمن التفتيش والرقابة الإلكترونية والتأكد من بطاقات الهوية الشخصية.

ولمزيد من التفاصيل حول صور الخصوصية، انظر:

د/ محمد نصر محمد، المسئولية الجنائية لانتهاك الخصوصية المعلوماتية– دراسة مقارنة، مركز الدراسات العربية، الطبعة الأولي 2016، ص 24؛ د/ مروة زين العابدين صالح، الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مركز الدراسات العربية، الطبعة الأولي 2016، ص 57 وما بعدها.

وتندرج العناصر السابقة المشتقة من الحق في الخصوصية جميعها تحت مظلة حرمة الحياة الخاصة، وهي من الحقوق اللصيقة بالشخص باعتباره إنسانا يعيش داخل المجتمع. وقد كان للجهود الدولية العالمية منها والإقليمية دورًا بارزًا في توفير الحماية الفعالة للحق في حرمة الحياة الخاصة بصفة عامة والحق في الخصوصية بصفة خاصة باعتبارها عنصرا من عناصرها[1].

وإذا كان استخدام الحاسب الآلي كوسيلة لتخزين المعلومات عن جميع العاملين بالقطاعين العام والخاص هادفا إلي تنظيم العمل داخل المؤسسات، إلا أن هذا لا يمنع، ما لم يتدخل المشرع، من استعمال واستغلال هذه البيانات بطريقة غير مشروعة. كما أن جمع وتخزين المعلومات والبيانات عن الأشخاص عموما قد يتطلب مراجعة وتعديلا وتحديثا لها، وحظر استعمالها أو نقلها أو اطلاع الغير عليها إلا في إطار الضوابط التشريعية[2].

لذا فإن التدخل التشريعي لوضع حماية للبيانات الشخصية أصبح لازمًا في عصر تكنولوجيا المعلومات الذي أصبح معه من السهل اليسير تجميع وتخزين كم هائل من المعلومات عن الأشخاص وإمكانية نقلها وتعديلها وحذفها في أقل من ثانية. فلم يعد غلق النوافذ وبعد المسافات عائقا ضد الحصول أو الاطلاع علي الأسرار الخاصة بالأشخاص في ظل تدفق المعلومات والبيانات الشخصية وسهولة نقلها وإمكانية نسخها كبيانات رقمية ما لم يتم وضع ضوابط لحماية هذه البيانات.

---

(1) وحول الجهود الدولية والإقليمية لحماية خصوصية البيانات الشخصية، انظر :
د/ محمود سلامة، الحماية الدستورية والقضائية لخصوصية البيانات الشخصية للعامل، مطبعة أبناء وهبة حسان، الطبعة الأولي 2016، ص 181 وما بعدها؛ د/علاء محمود يس حراز، الحماية الجنائية للمعلومات المعالجة آليا، رسالة دكتوراة – حقوق عين شمس، 2015، ص 818 وما بعدها.

(2) د/ شريف يوسف خاطر، حماية الحق في الخصوصية المعلوماتية، دار الفكر والقانون 2015، ص 2.

أهمية الموضوع:

يكتسب الموضوع أهميته من كونه يناقش قضية في غاية الخطورة ألا وهي الحماية القانونية للبيانات الشخصية، حيث تعد البيانات الشخصية من أهم خصوصيات الإنسان التي لها حرمتها، والتي تحرص أغلب الدول علي توفير الحماية القانونية لها وصيانتها من أن تكون عرضة للافصاح أو التداول غير المبرر قانونًا أو أن يساء استغلالها.

وتأتي أهمية الموضوع في وقتنا الحالي نظرًا لشيوع ظاهرة الاتجار في البيانات الشخصية حيث أتاحت تكنولوجيا المعلومات والانفتاح علي صعيد الاتصالات قدرًا هائلا من المعلومات عن الاشخاص لم يكن متاحا من قبل وبالتالي يصبح من الطبيعي أن يظهر من يحاول استثمار هذه البيانات والمعلومات لأغراض تجارية دون الحصول علي الرضا الصريح من أصحاب هذه البيانات، إذ ترسل ملايين من الرسائل الدعائية والترويجية يوميًا عبر رسائل الهاتف والبريد الإلكتروني من دون موافقة المرسل إليه لتحقيق أرباح مادية.

ونظرًا لشيوع استخدام الأفراد والشركات لتكنولوجيا المعلومات مما أتاح الفرصة لجمع وتخزين ومعالجة البيانات الشخصية، وذلك بالتفاعل مع تقنيات الحاسب الآلي، وإتاحة وسائل تبادل المعلومات عبر شبكة الإنترنت والمتمثلة في برمجيات التصفح ودخول المواقع والبريد الإلكتروني، فضلًا عن قيام محتوي البيانات (IP) بالتعريف بهوية المرسل والمرسل إليه، أضف إلي مجموعات الأخبار، وغرف الدردشة والتي يكون معظمها مفتوحا أمام المستخدمين؛ فهي تحتوي علي بيانات شخصية يمكن تخزينها آليا علي العديد من الحاسبات بدون تدخل من المستخدم. بالإضافة إلي انتشار قواعد البيانات ومحركات البحث وتحليل السلوك والتصرفات الخاصة بالمستخدم علي شبكة الإنترنت وهو ما يلقي بظلاله علي الخصوصية وحماية البيانات الشخصية.

ويتضح الخطر الذي قد يمس البيانات الشخصية لدي قيام المستفيد بعمل اشتراك ما بالمواقع الإلكترونية، أو منتديات النقاش أو شبكات التواصل الاجتماعي أو حتي لدي إبرامه لعقود شراء عبر الإنترنت، حيث يضطر لتقديم بعض البيانات الخاصة به التي يقوم البعض باستغلالها لأغراض تجارية تسويقية أو حتي لأغراض غير مشروعة. وهو ما أدي في النهاية إلي ظهور تجارة البيانات الشخصية والتي تعد – وبحق– إحدى سَوْآتُ ثورة الاتصالات وتكنولوجيا المعلومات.

وهكذا أصبحت البيانات الشخصية – في مجتمعنا المصري والكثير من المجتمعات– محلا للتعامل بين الجهات التي تقوم بجمعها وتبادلها فيما بينها واستغلالها نظرًا لغياب التنظيم التشريعي لدينا بشأن البيانات الشخصية، وسهولة الحصول عليها في ظل التحول إلي مجتمع معلوماتي وزيادة حجم التعاملات الإلكترونية ووجود الشركات الأجنبية، وما يصاحب ذلك من نقل لبيانات العملاء الشخصية خارج الوطن دون وضوح لطبيعة نقل البيانات الشخصية للأفراد والغرض منه، والذي يتعارض بالقطع مع سياسات ومقومات الأمن المعلوماتي باعتباره من روافد الأمن الوطني.

وأمام هاتين الظاهرتين خالجت نفسي العديد من التساؤلات:

أولها: هل هناك علاقة بين ظهور وانتشار تجارة البيانات الشخصية وعدم وجود تنظيم قانوني بشان البيانات الشخصية ؟ وهل النظم القانونية التي تأخذ بنظام قانوني لحماية البيانات الشخصية تنعدم فيها هذه التجارة ؟ وهل النظم القانونية التي لا يوجد لديها تشريعات لحماية البيانات الشخصية تصير بيانات مواطنيها – في ظل ازدياد مجالات استخدام هذه البيانات – مستباحة ومحلا للاعتداء عليها أم يمكن حمايتها وفقا للقواعد العامة ؟

ثانيها: ما مدي مشروعية معالجة البيانات الشخصية ؟ أي هل معالجة البيانات الشخصية أمر مشروع يباح القيام به دون قيد أو شرط، أم أن هناك شروط يجب توافرها حتي تكون معالجة البيانات أمرًا مشروعًا ؟ وهل هناك التزامات علي

عاتق المسئول عن معالجة هذه البيانات فتجعل هذه المعالجة أمرًا ظاهرًا وليس خفيًا ؟ وهل هناك حقوق لمن يتم معالجة بياناته يمارسها في مواجهة القائم بمعالجة هذه البيانات ؟ هل تتسق هذه الحقوق مع الحماية المقررة لحماية الحق في حرمة الحياة الخاصة حتي نكفل للشخص المعني بالبيانات قدرًا من الأطمئنان علي صحة ما يتم معالجته من معلومات وبيانات ويضمن في الوقت نفسه جودتها وتحديثها لكي تطابق الواقع وتصحيحها إذا ما شابها الخطأ أو القصور ؟

ثالثها: هل العقوبات المقررة لمرتكبي جرائم الاعتداء علي حقوق الأشخاص خلال معالجة بياناتهم الشخصية تكفي لردع الجناة، ومن ثم القضاء علي استغلال البيانات الشخصية للأفراد في الدول التي لديها تشريعات لحماية هذا النوع من البيانات؟ وهل تستوعب النصوص التجريمية التقليدية القائمة – في الدول التي لم تسن بعد تشريعات لحماية البيانات – الاستخدام غير القانوني للبيانات الشخصية ؟

أو بمعني آخر هل تكفي القواعد العامة المتعلقة بحماية الحياة الخاصة في ظل غياب النصوص التشريعية التي تحمي البيانات الشخصية في النظام القانوني المصري في بسط حمايتها القانونية علي البيانات الشخصية للأفراد ؟

ولقد حاولت الإجابة علي هذه التساؤلات من خلال اختيار موضوع الدراسة « الحماية الجنائية للبيانات الشخصية المعالجة آليًا» إلاَّ أَنه يتعين علينا في سبيل الإجابة علي هذه التساؤلات المحورية أن نتصدى بالتحليل والدراسة لثلاثة جوانب رئيسية يثيرها الموضوع.

أولها يتعلق بمفهوم البيانات الشخصية حتي يمكن التمييز بينها وبين غيرها من المعلومات الشخصية، وهل تقتصر البيانات الشخصية علي بيانات التعريف المباشرة للأشخاص كالبيانات الاسمية والصورة أم تشمل إلي جانب ذلك بيانات التعريف غير المباشرة بالإضافة إلي البيانات الحساسة ؟

وما هو المقصود بمعالجة البيانات الشخصية ؟ وهل يقتضي الحق في الخصوصية أن تسري علي كافة صور معالجة البيانات الشخصية الحماية القانونية

؟ وما هي المخاطر التي قد تسببها معالجة البيانات الشخصية علي الحق العام في احترام الحياة الخاصة لهؤلاء الأشخاص ؟

ثانيها يتعلق بالضوابط القانونية المقررة لحماية البيانات الشخصية المعالجة، وهل يخضع المسئول عن معالجة البيانات الشخصية لرقابة جهة إدارية بالدولة لضمان التزامه بالقانون وتوفير مستوي ملائم لحماية أمن البيانات وضمان سريتها ؟ وهل يجوز أن يحتفظ الأخير بالبيانات الشخصية لمدة تزيد عن المدة اللازمة لتحقيق الغرض الذي من أجله تم جمع البيانات ؟ وهل يشترط الحصول علي موافقة الشخص المعني قبل الشروع في المعالجة ؟ وهل هناك مبادئ – توجيهية – متعلقة بمعالجة البيانات يتعين علي المسئول عن معالجة البيانات الشخصية احترامها ؟

ويتعلق الجانب الثالث بكيفية حماية البيانات الشخصية في التشريعات المقارنة، وهل اتفقت الدول في كيفية التحرك التشريعي لحماية البيانات الشخصية المعالجة آليا ومواجهة الأفعال المتعلقة بانتهاكها أو الاعتداء عليها ؟

لذلك رأيت تناول موضوع البحث من خلال بيان مضمون معالجة البيانات الشخصية، والضوابط القانونية المقررة لحماية البيانات الشخصية، ثم تسليط الضوء علي الحماية المقررة للبيانات الشخصية في التشريعات المقارنة.

منهج البحث:

لقد حاولت في هذا البحث اتباع منهج الدراسة التحليلية التأصيلية المقارنة التي تعتمد علي تحليل نصوص قانون حماية البيانات الفرنسي رقم 78–17 الصادر لسنة 1978 بشأن المعلوماتية والحريات وما أدخل عليه من تعديلات، وقانون العقوبات الفرنسي فيما يتعلق بالاعتداء علي حقوق الأشخاص المتعلقة بالمعالجة المعلوماتية، بالإضافة إلي الإشارة إلي التوجيه الأوربي رقم 95–46 الصادر لسنة 1995 بشأن حماية البيانات ذات الطابع الشخصي، والقوانين ذات الصلة بالموضوع. وهذا المنهج الذي يركز علي دراسة الواقع الفعلي لحماية البيانات الشخصية للأفراد

في القانون الفرنســـي لما له من فائدة علي مصـــرنا الحبيبة كنموذج يحتذي به عند البدء في وضع قانون لحماية البيانات الشخصية في مصر.

خطة البحث:

سنتناول دراسة موضوع الحماية القانونية للبيانات الشخصية المعالجة آليا من خلال ثلاثة فصول: نخصص الفصل الأول للوقوف علي مضمون البيانات الشخصية والمخاطر المتصلة بمعالجتها، والثاني لبيان الضوابط القانونية المقررة لحماية هذه البيانات، والثالث للوقوف علي كيفية حماية البيانات الشـــخصـــية في التشريعات المقارنة، وذلك علي النحو التالي:

الفصل الأول: مضمون معالجة البيانات الشخصية.

الفصل الثاني: الضوابط المقررة لحماية البيانات الشخصية.

الفصل الثالث: حماية البيانات الشخصية في التشريعات المقارنة.

بينما أخصص الخاتمة للوقوف علي النتائج التي أسفر عنها البحث وما تفرع عنها من توصيات.

الفصل الأول

مضمون معالجة البيانات الشخصية

لكي نتعرف علي جوهر معالجة البيانات الشخصية ينبغي أن نوضح مفهوم البيانات الشخصية (أولاً)، ثم نتحدث عن مفهوم معالجة البيانات الشخصية (ثانياً)، ثم نعقبه ببيان مخاطر معالجة هذا النوع من البيانات علي الحق في الخصوصية والذي ينبثق عنه حماية البيانات.

وبناء عليه سوف نتناول مضمون معالجة البيانات الشخصية في ثلاثة مباحث علي النحو التالي:

المبحث الأول: مفهوم البيانات الشخصية.

المبحث الثاني: مفهوم معالجة البيانات الشخصية.

المبحث الثالث: المخاطر المتعلقة بمعالجة البيانات.

المبحث الأول

مفهوم البيانات الشخصية

يعد كل من الحق في الخصوصية وحماية البيانات الشخصية أمرًا مقرًا ومعترفًا به في نصوص التشريعات الوطنية والدولية والأوروبية. كما أنَّ هذا الموضوع تم تكريسه وتبنيه من قبل المواقع الإلكترونية ذاتها عن طريق ما يسمى بالتنظيم الذاتي أو بسياسات الخصوصية لكن المشكلة قد تثور في تحديد مفهوم البيانات الشخصية، ذلك أن هنالك خلطًا بين مفهوم الحق في الخصوصية وبين مفهوم البيانات الشخصية. كما أنَّ المشكلة تثور لدى تحديد عناصر البيانات الشخصية ومدى الحماية المقررة لها وإطارها القانوني وهو محور دراستنا، فليس كل البيانات يمكن وصفها بالبيانات الشخصية وإدخالها بالتالي في نطاق الحماية الجنائية.

وعليه سوف نتناول مفهوم البيانات الشخصية في مطلبين علي النحو التالي:

المطلب الأول: تعريف البيانات الشخصية.

المطلب الثاني: عناصر البيانات الشخصية.

المطلب الأول
تعريف البيانات الشخصية

والواقع أن تعريف البيانات الشخصية ليس بالأمر العسير نظرًا لتعرض المشرع الفرنسي لهذه المسألة مرتين: **أولهما**، بالقانون رقم78-17 الخاص بالمعلوماتية والحريات والصادر في 6 يناير 1978[1]، **وثانيهما**، بالقانون رقم 2004-801 بشأن حماية الأشخاص الطبيعين بالنظر إلي معالجة البيانات ذات الطابع الشخصي والصادر في 6 أغسطس 2004 والمعدل للقانون سالف الذكر[2]، إذ تبني المشرع الفرنسي في نطاق تطبيق قانون 6 يناير 1978 مفهوما ضيقًا بشأن تحديد تعريف البيانات الشخصية أو البيانات الاسمية حيث نصت المادة الرابعة منه قبل تعديلها علي أنه يعد بيانًا شخصيًا: " كل البيانات، أيًا كان شكلها، التي تسمح بشكل مباشر أو غير مباشر بتحديد هوية الأشخاص الطبيعين المنطبقة عليهم، سواء تمت المعالجة من شخص طبيعي أو معنوي".

ولكن الفقه والقضاء الفرنسي تبني تفسيرًا واسعا لنص المادة الرابعة سالفة الذكر بما يسمح بدخول جميع أشكال البيانات الشخصية تحت نطاق هذا التعريف،

---

(1) LOI n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF. du 7 jan 1978, p. 227.

(2) LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF. du 7 août 2004, p. 14063.

وتجدر الإشارة إلي أن القانون الفرنسي رقم 78-17 بشأن المعلوماتية والحريات قد تعرض للتعديل عدة مرات، كان أخرها بمقتضي القانون رقم 2017-55 والصادر في 20 يناير 2017، بيد أن التعديل الوارد في القانون رقم 2004-801 يعد أهم التعديلات.

ومن ثم خضوعها للحماية القانونية[1]. كما عملت اللجنة المعنية باحترام أحكام قانون 6 يناير 1978 والتي أطلق عليها اللجنة الوطنية للمعلوماتية والحريات[2] CNIL علي تبني ذات المفهوم الواسع للبيانات الشخصية[3].

وفي ذات الاتجاه عرفت الاتفاقية الأوربية رقم 108 الصادرة عن مجلس أوروبا[4]، البيانات الشخصية بأنها: " كل معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد"[5]. وبعبارة قريبة من ذلك جاءت المادة 1/2 من التوجيه الأوربي رقم 95-46 بشأن حماية الأشخاص الطبيعين بالنظر إلي معالجة البيانات ذات الطابع الشخصي لتعرف البيانات الشخصية بشكل دقيق ومفصل بقولها: " البيانات الشخصية، هي كل معلومة تتعلق بشخص طبيعي محددة هويته أو يمكن تحديدها، ويعد الشخص محدد الهوية أو يمكن تحديد هويته سواء بطريقة مباشرة أو غير مباشرة لاسيما بالرجوع إلي رقمه الشخصي، أو واحد أو اكثر من العناصر الخاصة بتحديد هويته المادية والفيسولوجية والنفسية والاقتصادية أو الاجتماعية[6].

---

(1) ***V. Brffard WILLIAM***, Le système de traitment des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier I, 2003, p. 15.

(2) La Commission National de L'Informatique et libertés (ci- après CNIL).

(3) فالبيانات الشخصية لديها هي: " البيانات التي تسمح بطريق مباشر بالتعرف علي الشخص بواسطة اسمه أو لقبه علي سبيل المثال، وبطريق غير مباشر من خلال رقم الضمان الاجتماعي أو رقم التليفون .... الخ". وحول تفصيلات الموضوع، راجع:
CNIL, Délibération 80-10 du 1 er avril 1980 rapport annuel 1980. et ***CNIL***, 6 ème Rapport d'activité 1985, Doc.fr. Paris, 1986. p. 44 et s.

(4) وتتعلق هذه الاتفاقية بحماية الأشخاص في مواجهة المعالجة الآلية للبيانات ذات الطابع الشخصي، وقد تم توقيعها في 28 يناير 1981، ولم تدخل حيز التنفيذ إلا في الأول من أكتوبر 1985 بعدما صدقت عليها خمس دول، وقد صدقت عليها فرنسا في 19 أكتوبر 1982.

(5) ***Art. 2- Définition***: Aux fins de la present convention: (a) «données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);

(6) ***Art. 2/a, directive nº 95/46/CE***: " Toute information concernant une personne physique identifiée ou identitiable (personne concernée): est reputée identifiable une personne qui peut être identifiée, directement ou in directement, notamment par référence à un

ولما كانت أحكام التوجيهات الأوروبية ملزمة للدول الأعضـــاء في الاتحاد الأوروبي، وبـالتـالي يتعين عليهـا تعـديـل تشـــريعـاتهـا الـداخليـة بمـا يتواءم وأحكـام التوجيهات الصـادرة في الموضـوعات المختلفة، لذا تدخل المشـرع الفرنسـي بإصـدار القانون رقم 2004-801 ســـالف الذكر معدلًا أحكام القانون رقم 78-17 بشـــأن المعلوماتية والحريات وذلك ليتواءم وأحكام التوجيه الأوروبي رقم 95-46 الصـــادر لسنة 1995[1].

وهكذا أخذ المشـرع الفرنسـي بالمفهوم الواسـع للبيانات الشـخصـية بمقتضـي التعديل الوارد علي المادة الثانية ســـالفة الذكر بموجب القانون رقم 2004-801 الصادر في 6 أغسطس 2004 والتي أصبح نصها كالآتي: " تعتبر بيانات شخصية كل معلومة تتعلق بشـخص طبيعي محددة هويته أو قابلة للتحديد بطريقة مباشـرة أو غير مباشـرة، سـواء تم تحديد هويته بالرجوع إلي رقمه الشـخصـي أو عبر واحد أو أكثر من المعطيات التي تخصه"[2].

وبذلك تخلي المشـرع الفرنسـي عن المفهوم الضـيق للبيانات الشـخصـية الذي كان يقصـرها – فقط – علي تلك " المعلومات التي تسـمح بتحديد هوية الشـخص الطبيعي بطريقة مباشرة أو غير مباشرة" . لصالح المفهوم الواسع للبيانات الشخصية

numéro d'identification ou à ou plussieurs elements spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ».

(1) ومن قبل التشـريع البلجيكي لحماية البيانات ذات الطابع الشـخصـي والصـادر لسـنة 1992 والمعدل لسـنة 1998 والذي أخذ بالتعريف الوارد بالتوجيه الأوروبي بشـكل حرفي، حيث عرفها بأنها:" كل معلومة متعلقة بشـخص طبيعي محددة هويته أو يمكن تحديدها بطريقة مباشـرة أو غير مباشرة، ولاسيما بالرجوع إلي رقمه الشخصـي أو إلي أحد أو اكثر من العناصـر الخاصـة بتحديد هويته المادية والفيسولوجية والنفسية والاقتصادية أو الاجتماعية.

Art. 1er, § 1er nouveau de la loi belge du 8 décembre 1992.

(2) ***Art. 2/al, 2 Loi nº 78-17***: "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 ".

لتصـــبح وفق النص الجديد " كل معلومة تتعلق بشـــخص طبيعي طالما أن هذا الشخص محددة هويته، أو قابلة للتحديد بأية طريقة.

وبناء علي ذلك – وطبقًا للنص الجديد – فإن إمكانية تحديد الأشـــخاص الطبيعين من خلال بياناتهم لم تعد تقتصـــر علي فكرة التعريف المباشـــر بهم، عن طريق الاسم الشخصي أو اللقب، ولكن امتد مفهوم البيانات الشخصية ليشمل أي بيان خاص بالشـــخص الطبيعي يمكن من خلاله تحديد هويته، ولو بطريقة غير مباشرة، وهو ما يفهم من عبارة " وذلك بالرجوع إلي رقمه الشخصي أو عبر واحد أو أكثر من المعطيات التي تخصه "، وهي العبارة التي أتي بها النص الجديد، ولا يوجد لها مقابل في النص القديم.

والجدير بالذكر أن الحماية الجنائية للبيانات الشخصية تقتصر علي البيانات الشخصية الخاصة بالأشخاص الطبيعين[1]، ومن ثم تستبعد البيانات الخاصة بالاشـــخاص المعنويين من نطاق هذه الحماية [2]، وهو أمر واضـــح من التعريف السابق للبيانات الشخصية، وليس هناك اختلاف ايضًا بين القانون القديم والجديد في هذا الشأن، إذ تقتصر الحماية الجنائية علي البيانات الشخصية للشخص الطبيعي دون الشخص المعنوي.

---

(1) ***Voir. En ce sens, CE***, 3 juillet 2002, reproduit in CNIL, 23ème Rapport d'activité 2002, Doc.fr. Paris, 2003. pp. 397-399.

(2) وبالرغم من ذلك يمتد نطاق الحماية الجنائية ليشمل الممثلين القانونيين للأشخاص الاعتباريين والذين لهم الحق في التوقيع ويتم تحديدهم اســـميا، عند إنشـــاء هذه الكيانات. ولمزيد من التفاصيل حول شروط انطباق الحماية الجنائية علي هؤلاء:

Voir notamment, CNIL, Délibération n° 84-28 du 3 juillet 1984. et ***Frayssinet (J)***, A propos du droit d'accès des personnes morales, D. 21 mai 1992, n° 80, p. 253.

المطلب الثاني
عناصر البيانات الشخصية

إذا كان تعريف البيانات الشخصية ليس أمرًا عسيرًا إلا أن تعداد عناصر البيانات ذات الطابع الشخصي ليس بالأمر السهل نظرًا لصعوبة غلق دائرة البيانات الشخصية علي عناصر محددة في ظل ما نعيشه من ثورة في مجال الاتصالات وتكنولوجيا المعلومات. لذا كان المشرع الفرنسي أكثر إدراك وفهمًا للأمر فلم يحدد عناصر البيانات الشخصية وإنما ترك هذه المهمة للفقه والقضاء.

لما كان تحديد هوية الأشخاص هو جل اهتمامات التوجيه الأوروبي رقم 95-46 الخاص بحماية البيانات ذات الطابع الشخصي، كذلك هو صلب التشريع الفرنسي رقم 78-17 الخاص بالمعلوماتية والحريات وسبب وجوده. لذا أجمعت الدراسات التي أجريت علي خلفية كل من: « المعلومات الشخصية»[1] ،« البيانات والمعلومات الشخصية»[2] علي الكشف عن نوعين من الثوابت: أولهما، تحديد الأشخاص. وثانيهما، تحديد ورصد الأشخاص. وبناء عليه ارتبط مفهوم البيانات الشخصية بفكرة تحديد الهوية[3].

فتحديد هوية الأشخاص- إن صح التعبير- هو عملية يمكن أن تؤدي إلي توصيف للشخص، ومن ثم تفريده بما يجعل من الممكن تميزه عن غيره من الأشخاص الطبيعيين[4]. فبعد أن كان يتم تحديد هوية المرء من خلال الاسم أو الصورة (بيانات التعريف المباشر)، أصبح من الممكن تحديدها من خلال مجموعة من العناصر الأخري، مثل رقم الهوية، أو عبر واحد أو أكثر من العناصر الخاصة

---

(1) ***Frédérique LESAULNIER***, L'information nominative, Thèse , Paris II, 2005, p. 43.

(2) ***Marot (Pierre-Yves)***, Les données et informations à caractère personnel. Essai sur la notion et ses fonctions, Thèse, Université de Nantes, 2007, p. 71.

(3) ***Claudine GUERRIER,*** Les aspects techniques de la régulation des données personnelles : la question du numéro IP, in La régulation des données personnelles, LEGICOM n° 42 - 2009/1, p. 12.

(4) فيما يتعلق بتحديد هوية الأشخاص، راجع:
Jacqueline BOUSSON-PETIT, L'identité de la personne humaine. Étude de droit français et de droit comparé, Bruxelles, Bruylant, 2002.

بتحديد هوية الشخص المادية والفيسولوجية والنفسية والاقتصادية أو الاجتماعية[1] (بيانات التعريف غير المباشر). والتي صاغها المشرع الفرنسي بعبارة، واحد أو أكثر من المعطيات التي تخصه [2].

وبالرغم من اختلاف صياغة المادة الثانية من التوجيه الأوربي الصادر لسنة 1995 مقارنة بالمادة الثانية من قانون المعلوماتية والحريات المعدل لسنة 2004، إلا أنهما متقاربتان لبعضهم البعض[3]. ومن ثم فإن تحديد هوية الأشخاص – كما تشير النصوص– يمكن أن يكون عبر بيانات التعريف المباشر أو غير المباشر.

كما أن هناك نوع ثالث من البيانات يطلق عليه البيانات الحساسة، راعت كافة التشريعات الخاصة بحماية البيانات الشخصية توفير حماية قصوي لها؛ نظرًا لتعلقها بالمعلومات الأكثر خصوصية التي يحرص الأفراد علي حجبها عن الأخرين؛ لذا حظرت كافة التشريعات جمعها أو معالجتها إلا بعد موافقة السلطات المعنية أو بعد الحصول علي أذن صاحبها.

وبناء عليه سوف نتناول عناصر البيانات الشخصية في ثلاثة أفرع علي النحو التالي:

الفرع الأول: بيانات التعريف المباشر.

الفرع الثاني: بيانات التعريف غير المباشر.

الفرع الثالث: البيانات الحساسة.

---

(1) ***Directive 95/46/CE***, précité, article 2 (a).

(2) Loi Informatique et libertés modifiée, article 2 alinéa 2.

(3) ***Ibrahim COULIBALY***, La protection des données à caractère personnel dans le domaine de la recherche scientifique. Thèse, Université de Grenoble, 2011. p. 18.

الفرع الأول

بيانات التعريف المباشر

يقصد ببيانات التعريف المباشر Les données d'identification directe تلك البيانات الشـــائع اســـتخدامها في الأغراض التعليمية والتربوية ... إلخ. وتتألف من بيانات أبجدية رقمية كاللقب، والاسم الأول[1] ويضاف إليها الصورة [2] والصوت [3]. بما يجعل من السهولة التعرف علي أصحابها[4].

وبناء عليه سوف نتناول البيانات الاسمية والصورة والصوت باعتبارها من البيانات المباشرة، وذلك علي التفصيل الآتي:

أولاً: البيانات الاسمية:

يعد الاسم أحد أهم مميزات الشخصية الإنسانية والذي يميز كل شخص عن غيره، ويقصد بالاسم الشخصي أو الحقيقي أو الرسمي أو الأصلي ذلك الاسم الذي يطلق علي الشخص عند ولادته والمدون بالسجلات الرسمية الخاصة بواقعة الميلاد[5] ، ويتم ذكره في بطاقة تحقيق الشـخصـية، أو غيرها من الأوراق المتعلقة بالمعاملات الرسمية[6].

---

(1) ***Nathalie MELLET-POUJOL***, Protection de la vie privée et des données à caractère perssonnelle, , Février 2004, nº 59. p.21. Étude Disponible sur: http://eduscol.education.fr/chrgt/guideViePrivee.pdf

(2) وتشمل الصور الثابتة والمتحركة والفيديو.

(3) ***Nathalie MELLET-POUJOL***, Op. cit., p. 21.

(4) ***Ibrahim COULIBALY***, Th. préc., p. 19.

(5) إذ أوجب قانون الأحوال المدنية ذكر اسم المولود واسم أبيه ضمن البيانات الواجبة الإبلاغ عن واقعة الميلاد. المادة 18 من القانون رقم 260 لسنة 1960 الخاص بالأحوال المدنية المصري.

(6) د/ سهير منتصر، النظرية العامة للحق، بدون دار نشر، 2006، ص 66.

ويختلف تركيب اسم الإنسان باختلاف المجتمعات ، فمنها ما يعتد "بالاسم الأول" " واللقب" [1] كما هو الحال في المجتمعات الغربية، ومنا ما يعد بالاسم الأول ثم اسم الأب ثم الجد، وهو ما عليه الحال في مصر [2] والدول العربية.

وتجدر الإشارة إلي أن اسم الإنسان سواء كان اسمًا شخصيًا أو أسمًا مستعارًا أو اسم شهرَة، يعد من البيانات الشخصية، التي تخضع للحماية القانونية علي اعتبار أنه من البيانات التي تسمح بتحديد هوية الشخص بطريقة مباشرة[3].

ثانياً: الصورة والصوت:

مما لاشك فيه أن صورة الشخص سواء كانت صورة ثابتة أم صورة متحركة تعد من بيانات التعريف المباشر التي تسمح بتحديد هوية الشخص؛ لأنها انعكاس لشخصيته في مظهرها المادي والمعنوي، لذا تخضع للحماية القانونية في التشريع الفرنسي، كذلك الصوت[4]، فقد اعتبرتهما اللجنة الوطنية للمعلوماتية والحريات بفرنسا من قبيل بيانات التعريف المباشر للشخصية، وقد استندت اللجنة في ذلك إلي أن التكنولوجيا الرقمية الحديثة سمحت بمعالجة الصوت والصورة باستخدام الحاسب الآلي ووضعهما علي دعامة واحدة بجانب النص، ومن ثم اعتبارهما من البيانات الشخصية التي يمكن معالجتها بطريقة منفصلة ومستقلة بذاتها[5].

---

(1) اللقب عبارة عن اسم العائلة وهو الذي يميز الشخص عن غيره ويحدد انتمائه إلي أسرة معينة.

(2) فقد جرت العادة في مصر علي إضافة اسم الأب واسم الجد بجانب الاسم الشخصي، والاستغناء بذلك عن لقب العائلة.

(3) ***Xavier BIOY***, "L'identité de la personne devant le Conseil constitutionnel", Rev. FDC, n° 65, janv 2006. pp. 74-75.

(4) ***En se sens. Nathalie MELLET-POUJOL***, Op. cit., p. 21.

ولمزيد من التفاصيل بخصوص الصوت كأحد عناصر تحديد الهوية، راجع:

D. Huet-Weiller, La protection juridique de la voix humaine, Rev. RTD civ. 1982, p. 497; ***M. Serna,*** La voix et le contrat: le contrat sur la voix, CCC, septembre 2009, chron. 9, pp. 4-8. La voix comme élément d'identification directe des personnes fait, cependant, l'objet d'une contestation par certains scientifiques.

(5) ***CNIL***, Délibération 96-009 du 27 fevrier 1996, Délibération portant adoption du rapport intititule˝Les information personnelles issues de la voix et de l,image et la protection de la vie privee et des libertes fondamentales˝. Disponible sur: www.legifrance.gouv.fr.

كما تخضع صورة الشخص أيضًا لحماية قانونية من نوع خاص يعرف بحق الشخص علي صورته باعتبارها مظهر من مظاهر حق الفرد في الخصوصية[1]، كذلك الصوت[2]، ومن ثم فإن أي اعتداء علي صورة الشخص، يسمح لهذا الشخص بدفع هذا الاعتداء، إما عن طريق حماية البيانات الشخصية، أو بالحماية المقررة لحق الانسان علي صورته[3].

وتجدر الإشارة إلي أن اللجنة الوطنية للمعلوماتية والحريات قد اعتبرت الصوت والصورة بيانات شخصية حتي من قبل تعديل قانون المعلوماتية والحريات سنة 2004، وهو ما يعكس دورها في تطوير مفهوم البيانات الشخصية، وذلك من خلال هجرها المفهوم التقليدي للبيانات الشخصية، والأخذ بالمفهوم الحديث لهذه البيانات، مستندة في ذلك إلي التوجيه الأوربي الخاص بحماية البيانات الشخصية، الصادر لسنة 1995. حيث اعتبر هذا التوجيه صورة الشخص وصوته من قبيل البيانات الشخصية التي يمكن معالجتها.

V. Louise CADOUX, Voix, image et protection des données personnelles, Commission nationale de l'informatique et des libertés, La documentation francaise, 1996.

(1) انظر: د/ سعيد جبر، الحق في الصورة ، دار النهضة العربية، 1986، ص 127؛ د/ آدم عبد البديع آدم، الحق في حرمة الحياة الخاصة ومدي الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراة – حقوق القاهرة، 2000، ص 338 ما بعدها؛ د/ كاظم السيد عطية، الحماية الجنائية لحق المتهم في الخصوصية، دار النهضة العربية، 2007، ص 140 وما بعدها.

Voir aussi. KAYSER (P), « Le droit dit à l'image», Mélanges P. Roubier, Dalloz-Siery, 1961, p. 73; ***KAYSER (P)***, Les droits de la personnalité aspect théorique et pratique, Rev.trim.dr.civ. 1971, p. 66; ***ACQUARONE (D)***, L'ambiguïté du droit à l'image, D. 1985, chron. p.129**; *GAILLARD (E)***, La double nature du droit à l'image et ses conséquences en droit positife française, D. 1984, chron. p. 16.

كما أقر القضاء الفرنسي بدوره أيضًا طابع البيانات الشخصية علي الصور الفوتوغرافية المعروضة علي الإنترنت، وذلك بمناسبة المعالجة الالكترونية للبيانات عبر شبكة الانترنت والتي تتضمن الاستخلاص، والاستخدام، والاطلاع من خلال النقل، وكل شكل آخر متاح للبيانات ذات الطابع الشخصي.

***Voir par Example*. TGI** Paris, 3 sept 1997, Expertises n° 213, mars 1998, p. 79.

(2) ***V.*** TGI Paris, 3 déc. 1975, D. 1977, 211, note ***R. Lindon***, JCP 1978, II, 19002, note ***D. Bécourt***; TGI Paris, 11 juill. 1977, D. 1977, 700, note ***R. Lindon***; TGI Paris, mai 1982, D. 1983, 147, note ***R. Lindon***.

(3) TGI Paris, 21 jan 1972, J.C.P. 1972-1-375; TGI Paris, 25 oct. 1982. D. 1983-363, note ***Lindon***; TGI Toulouse, 15 jan. D. 1991, 600, note ***J. Ravanas***.

كذلك الأمر بالنسبة لصوت الشخص، فيعد بياناً شخصيًا يخضع لذات الحماية المقررة للبيانات الشخصية، باعتباره من ضمن العناصر الحديثة لمفهوم البيانات الشخصية والتي تسمح بتحديد الهوية[1].

الفرع الثاني
بيانات التعريف غير المباشرة

إذا كانت فئة البيانات المباشرة لا تثير أي صعوبة في تحديد هوية الأشخاص الذين تتصل بهم[2]. إلا أن بيانات التعريف غير المباشر Les données d'identification indirecte بالمقابل تثير صعوبات شتي: **أولها**، تتعلق بصعوبة وضع تصنيف شامل للمعلومات التي من شأنها التحقق من البيانات التي تؤدي إلي التعريف غير المباشر للأشخاص. **ثانيها**، قد تسمح المعلومات غير المباشرة في تحديد الهوية في حالات ولا تؤدي الغرض في حالات أخري، فمثلا، الاسم الشخصي واللقب لشخص ما يعيش في مكان متحضر مكتظ بالسكان ويحترم الخصوصية – عدم الكشف علي الهوية – بتحديد هذا الشخص، على العكس من ذلك، إذا كان الشخص يقيم في قرية بها عدد قليل من السكان سيصبح التعرف عليها ممكنا[3].

أما الجانب الثالث فيتعلق بعدم إمكانية هذه البيانات – بذاتها – الكشف عن هوية الشخص الذي تنطبق عليه، ولكن مع ارتباطها بغيرها من البيانات – وفي سياق معين – يمكن تحديد ذلك[4].

وتشمل بيانات التعريف غير المباشر التي هي بطبيعتها بيانات ذات طابع شخصي ولكنها أقل وضوحًا من سابقتها في التعريف بصاحب هذه البيانات العديد

---

(1) ***Nathalie MELLET-POUJOL***, Op. cit., p. 21.

(2) ***En ce sens, F. Mollo***, Les notions de données directement nominatives et indirectement nominatives, in Les sciences sociales et leurs données, Rapport au Ministre de l'Education Nationale, R. Silberman, juin 1999, Annexes juridiques, pp. 180-182. Disponible sur: http://education.gouv.fr/rapport/silberman/table.htm

(3) ***V. Julien LE CLAINCHE***, Le traitement des données à caractère personnel dans le cadre d'un site web, p. 6. Étude Disponible sur: http://www.droit-tic.com/pdf/dp.pdf

(4) ***Ibrahim COULIBALY***, Th. préc., p. 19.

من المعلومات مثل رقم الهاتف أو رقم البطاقة المدنية أو رقم الضمان الاجتماعي أو غيرها من الأرقام التي ترتبط بأنشـــطة الشـــخص وحياته اليومية، كذلك العنوان الجغرافي، ولوحة الترخيص، وبصمات الأصابع، وعنوان البريد الإلكتروني.... الخ.

وعليه يمكن تقسـيم بيانات التعرف غير المباشـر إلي الأرقام الشـخصـية، الاختبارات التقنية والنفسية، البيانات الإحصائية، البصمات، هندسة كف اليد. وهو ما يمكن تفصيله كالآتي:

أولاً: الأرقام الشخصية:

تحيط بالفرد مجموعة من الأرقام الخاصـــة به وهذه الأرقام تســـمح بتميزه وتحديد هويته بشـكل غير مباشـر، لذا تعتبر من البيانات التعريفية للشـخص، وهذه الأرقام هي: رقم بطاقة الهوية، رقم الهاتف، رقم السـيارة، رقم الحسـاب البنكي، رقم الضمان الاجتماعي. وهو ما سنفصله كالآتي:

أ- رقم بطاقة الهوية:

رقم بطاقة الهوية أو تحقيق الشـخصـية هو رقم خاص بكل شـخص طبيعي يحمل جنسـية الدولة، ويعرف في مصـر وفرنسـا بالرقم القومي، ويمكن من خلاله تحديد هوية الشخص[1]، نظرًا لارتباطه بقاعدة بيانات الرقم القومي والتي تشتمل على الاسم الكامل لصاحب البطاقة، صورة فوتوغرافية للوجه، تاريخ الميلاد، العنوان، رقم تعريف مميز، المهنة أو الرتبة. كما تدرج بعض الدول خانة الديانة أو الطائفة أو التصـنيف إثني أو عرقي، والحالة الاجتماعية لبطاقة الهوية[2]. كما تسـمح التقنيات الحديثة بجعل بطاقات الهوية تحمل بيانات قياس حيوية، مثل الصـورة، أبعاد الوجه، أبعاد اليد، بصمة العين أو بصمة الأصابع [3].

---

(1) ***Nathalie MELLET-POUJOL***, Op. cit., n° 65. p. 22.

(2) كمصر وإسرائيل والسلطة الوطنية الفلسطينية.

(3) وتســـتخـدم بطـاقـات الهويـة الإلكترونيـة في بعض الـدول مثـل: هونـغ كونغ، ماليزيا، إستونيا، فنلندا، بلجيكا،غواتيمالا، البرتغال، المغرب وإسبانيا، انظر:

ب- رقم الهاتف:

يعتبر رقم الهاتف الخاص بشخص معين من البيانات الشخصية[1] والذي من خلاله يتم تحديد هوية صاحبه سواء كان الهاتف منزليًا أو جوالًا علي اعتبار أن أرقام الهاتف لا تتكرر[2]، وانما تختلف من عميل لآخر.

ج- رقم لوحة السيارة:

يعتبر رقم السيارة المملوكة لشخص معين بيانًا شخصيًا[3] يتعلق بهذا الشخص، إذ يمكن من خلال هذا الرقم تحديد هوية الشخص المعني بها – مالكها- بشكل غير مباشر[4]، علي اعتبار أن لكل سيارة رقمًا خاصًا لا يتكرر مع غيرها.

د- رقم رخصة القيادة:

يعتبر رقم رخصة القيادة Le numéro du permis de conduire من الأرقام المتفردة ، بحيث يكون لكل فرد رقم خاص به، لا يتكرر مع غيره، ومن ثم يعد من البيانات الشخصية التي تحدد هوية الشخص[5].

ذ- رقم الحساب البنكي:

---

https://ar.wikipedia.org/wiki/

(1) ***Nathalie MELLET-POUJOL***, Op. cit., n° 65. p. 22.

وقد قضي بأن رقم تليفون منزل الشخص من البيانات الشخصية التي تقع جريمة إفشاء البيانات المعالجة آليا بإفشائه إلي الغير.

Trib. Corr. GBriey, 15 sept. 1992, D. 1994. Somm. 289. Obs. Mails.

(2) ***Marie LAURE-LAFFAIRE***, Protection des données à caractère personnel, Éditions d'Organisation, 2005, p. 42. . Étude Disponible sur: http://www.eyrolles.com/Chapitres/9782708132351/chap2_Laffaire.pdf

(3) ***Ibrahim COULIBALY***, Th. préc., p. 19.

(4) ***Pierre PEREZ et Jean DUCHAINE***, Données à caractère personnel, École supérieure de l'éducation nationale, de l'enseignement supérieur et de la recherche (ESENESR), 2013. p. 1. Disponible sur: http://www.esen.education.fr/fileadmin/user_upload/Modules/Ressources/Themes/management_numerique/internet_responsable/textes_juridiques/5-04-2_donnees_personnelles.pdf

(5) ***Marie LAURE-LAFFAIRE***, Op.cit., p. 42.

مما لاشـك فيه أن رقم الحسـاب البنكي Le numéro de compte bancaire يعتبر بيان شـخصـي للعميل يمكن من خلاله تحديد هوية صـاحبه، طالما أنه رقم متفرد غير قابل للتكرار[1]. وهذا الرقم يحصـل عليه العميل كنتيجة طبيعية لفتح حساب لدي البنك ايًا كان نوعه[2]. كما تعتبر أرقام كروت الائتمان وبيانات القروض وتقارير الحسـابات البنكية وكل ما يتعلق بحياة الشـخص المالية أو تعاملاته بيانات شخصية[3].

ثانياً: العناوين الشخصية:

منذ وقت قريب لم يكن يعرف للإنسـان سـوي عنوان السـكن أو العمل إلي جانب المحل المختار، أما في الوقت الحاضـر، فقد تطور مفهوم العنوان، ليأخذ أشـكالا أخري، مثل: عنوان البريد الالكتروني، وعنوان بروتكول الانترنت، وهو ما سنفصله تباعًا كالآتي:

أ- العنوان الجغرافي:

يعتبر العنوان الجغرافي للإنسـان – سـواء أكان عنوان منزله الذي يقيم فيه بشـكل دائم أو عنوان عمله أو المكان المخصـص لقضـاء عطلاته الصـيفية– من البيانات الشخصية[4].

ب-عنوان البريد الإلكتروني:

---

(1) **Idem.**

(2) د/ أيمن مصطفي أحمد، الحماية القانونية للبيانات الشخصية في إطار أنشطة البحث العلمي، مجلة الدراسات القانونية، تصدرها كلية حقوق أسيوط، العدد 37 الجزء الأول، ص 611.

(3) د/ مروة زين العابدين صالح، المرجع السابق، ص 87.

(4) ***V. Ibrahim COULIBALY***, Th. préc., p. 19 ***et V. aussi. Julien LE CLAINCHE***, Op.cit., p. 5.

يعتبر عنوان البريد الإلكتروني L'adresse e-mail من البيانات الشخصية غير غير المباشـرة، لأنه يمكن من خلاله تحديد هوية الشـخص الطبيعي[1]. ولا يهم ما إذا كان لا يحتوي علي اســـم الشـــخص المعني؛ لأن العنوان الإلكتروني عنوان متفرد لايتكرر ولا يختلط بغيره، وعلى هذا النحو، يخضـــع تجميع عنـاوين البريد الإلكتروني للإطار العام للقانون الفرنسي رقم 78-17 بشأن المعلوماتية والحريات[2].

وفي ذات الســياق اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنســا أن عنوان البريد الإلكتروني ذي الطابع المهني بيانًا شـخصـيًا، إذ يمكن من خلاله تحديد هوية صـاحبه؛ نظرًا لأنه يتضـمن الاسم واللقب واسم الشركة أو المنظمة التي يعمل لديها[3]. وعليه فإن قائمة الرســـائل الإلكترونية التي تحتوي على هذا النوع من المعلومات هي معالجة للبيانات الشخصية.

ج- عنوان بروتوكول الإنترنت (L'adresse IP):

عنوان بروتكول الانترنت هو رقم التعريف المخصـص لجهاز الحاسـب الآلي أثناء التصـفح علي شـبكة الإنترنت والذي يعد بمثابة العنوان الخاص بكل مسـتخدم علي الشـبكة[4]. ويسـتطيع مقدم خدمة الإنترنت تحديد موقع جهاز معين من خلال

---

(1) فبمجرد كتابة عنوان البريد الإلكتروني للشـــخص معين علي محرك البحث جوجل يمكن تحديد موقع الشـخص المعني فضـلا عن الحصـول علي كافة المعلومات المتاحة عنه نظرًا لارتباطه بشبكات التواصل الاجتماعي. انظر:

QU'est ce qu'une donnée à caractère personnel? données personnelle. Disponible sur: https://se-developper-sur-internet.com/donnee-a-caractere-personnel/

(2) ***Blandine POIDEVIN,*** La CNIL et les fichiers e-mails. Disponible sur site suivente: https://www.jurisexpert.net/la_cnil_et_les_fichiers_e_mails/

(3) Accueil du site → L'informatique et les technologies de l'information → Un e-mail est-il une donnée personnelle? Disponible sur: www. Cil.cnrs.fr/CIL/spip.php?article1574

(4) يتكون عنوان بروتوكول الإنترنت من أربعة أرقام علي الأقل كل واحد منها يشـير إلي عنوان البلد، والتالي يشـير إلي عنوان الشـركة الموزعة، والثالث إلي مؤسـس الخدمة المُسـتخدمة، والرابع هو المستخدم. وتبدو أهميته في تعقب مرتكبي الجريمة المعلوماتية عبر شبكة الإنترنت.

د/ محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية 2016، ص 42.

هذا الرقم، ومن ثم التواصل معه، ويعتبر من البيانات الشخصية[1] إذا ارتبط بشخص معرف أو قابل للتعريف. كما يمكن أن يكون عنوانًا شخصيًا لأكثر من شخص إذا كان العنوان يستخدم بواسطة أكثر من شخص[1].

---

(1) ***V. Grégoire (G)***, Le statut de l'adresse IP: conséquences sur les mécanismes de constat, d'avertissement et de sanction du peer to peer envisagées par les accords de l'Elysée et le projet de loi « Création et Internet », in Les nouvelles frontières de la vie privée. Droits de la personnalité – Protection des données personnelles, LEGICOM, n° 43 – 2009/2, p. 103.

وتجدر الإشارة إلي أن الساحة القضائية والفقهية الفرنسية قد شهدت في السنوات الماضية جدل حول مدي اعتبار عنوان برتكول الإنترنت بيانًا شخصيًا أم لا؟ حيث ذهبت بعض المحاكم إلي عدم اعتباره بيانًا شخصيا تأسيسًا علي عنوان برتكول الانترنت قد استخدم لتحديد آلة وكمبيوتر وليس لتحديد شخص، ومن ثم يستبعد عنوان بروتوكول الإنترنت من نطاق تطبيق قواعد حماية البيانات الشخصية.

CA de Paris, arrêt du 27 avril 2007, 13ème chambre, Section B, Anthony G. /SCPP.; CA de Paris, arrêt du 15 mai 2007, 13ème chambre, Section A, Henri S. / HCPP; Cass. crim., 13 janvier 2009, Juris-Data n° 2009-046824.

بينما ذهبت بعض المحاكم واللجنة الوطنية للمعلوماتية والحريات إلي اعتبار بروتوكول الإنترنت بيانًا شخصيا إذا يمكن أن يسمح بتحديد الشخص بطريقة غير مباشرة.

Voir par Example. TGI Saint-Brieuc, 6 sept. 2007, Ministère public, SCPP.; CA de Rennes, 3è chambre, 23 juin 2008, M. T. L. c/ Ministère Public. ***Et voir aussi. CNIL***, 28 ème Rapport d'activité 2007, Doc. fr. Paris, 2008. p. 56.

كما انتهت محكمة العدل بالاتحاد الأوربي في حكم لها بتاريخ 24 نوفمبر 2011 إلي أن عناوين بروتوكول الإنترنت للمستخدمين المسئولين عن إرسال المحتوي غير القانوني علي الشبكة، هي بيانات شخصية محمية؛ لأنها تسمح بتحديد دقيق للمستخدمين المذكورين.

CJUE, 24 novembr 2011, 3e chamber, affaire C-70/10, Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). 2011 Disponible sur site suivent: http://curia.europa.eu/juris/

وفي حكم آخر لها اعتبرت أن بروتوكول الإنترنت حتي لو كان ديناميكيا، هو بيانات شخصية بالمعني المقصود وفقا لقواعد الجماعة الأوربية، شريطة أن يكون من الممكن تحديد الشخص المعني بوسائل معقولة، وهذا هو الحال عندما ينص النظام القانوني علي إمكانية الحصول علي المعلومات اللازمة لربط عنوان IP بالشخص، علي سبيل المثال المعلومات التي يمكن أن يحتفظ بها مقدم خدمة الإنترنت لديه.

CJUE, 19 octobre 2016, 2e chamber, affaire C-582/14, Breyer c. Bundesrespublik Deutschland. 2016. Disponible sur site suivent: http://curia.europa.eu/juris/

ثالثاً:- الخصائص البيوميترية للإنسان:

تعتمد الخصائص البيومترية بصفة اساسية علي مواصفات الشخص الفسيولوجية مثل بصمة الاصبع أو بصمة كف اليد أو بصمة العين أو بصمة الصوت، وبالرغم من أن تلك الخصائص لا تضع توصيفًا محددًا للشخص فإنها تستخدم للتأكد من هويته هذا الشخص والتعرف عليه خلال تلك الخصائص حيث أنها لا تتشابه من شخص لأخر وتدخل البصمة الوراثية أيضا ضمن قائمة الخصائص البيومترية[2].

وقد عرفت اللجنة الوطنية للمعلوماتية والحريات بفرنسا الخصائص البيوميترية للإنسان بأنها:« جميع العمليات التي من شأنها التعرف علي الفرد اعتمادًا علي قياس واحد أو أكثر من خصائصه الفيزيولوجية أو السلوكية أو المادية. وتضيف اللجنة قائلة أن الخصائص الحيوية هي: ... التطبيقات التي تتيح التعرف التلقائي علي الشخص والوقوف علي مدي أهليته للحصول علي الحقوق وخدمات معينة علي أساس الخصائص الفيزيائية (بصمات الأصابع، بصمة العين، بصمة

كما أكدت محكمة النقض الفرنسية في حكم حديث لها بأن البيانات الشخصية بموجب القانون هي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده، بصورة مباشرة أو غير مباشرة، وذلك بالرجوع إلي رقم الهوية أو عنصر واحد أو اكثر من العناصر الخاصة به، وهو ما ينطبق علي بروتكول الإنترنت.

Cour de cassation, 1ère ch. civ., arrêt du 3 novembre 2016 Disponible sur site suivents: https://www.legalis.net/jurisprudences/cour-de-cassation-1ere-ch-civ-arret-du-3-novembre-2016/
http://www.juricaf.org/arret/FRANCE-COURDECASSATION-20161103-1522595

يبدو لنا أنه من الصعب القول بأنه بروتوكول الإنترنت لا يسمح بتحديد هوية الأشخاص الذين تتصل بهم بصورة غير مباشرة، ومن ثم، ينبغي أن يقر اقتراح بتعديل قانون المعلوماتية والحريات بما يسمح باعتبار عنوان بروتوكول الإنترنت من ضمن البيانات الشخصية.

V. Proust (OLIVIER), Etats des lieux sur la proposition de loi du Sénat visant à modifier la loi « Informatique et libertés », Rev. LDI, n° 55, décembre 2009, p. 39.

(1) د/ مروة زين العابدين صالح، المرجع السابق، ص 87.

(2) المرجع السابق، ص 98.

الصـوت، هندسـة اليد الحيوية، الحمض النووي،) أو العناصـر السـلوكية (بصـمة التوقيع ...)»[1]. وعليه سوف نلقي الضوء علي هذه الخصائص كالآتي:

أ- بصمة الأصابع:

البصـمة هي أثر الختم بالإصـبع، وهي لا تتشـابه من شـخص لآخر، حتي لدي التوائم المتماثلة، فهي لا تقبل التكرار، وغالبا ما كانت تسـتخدم في مجالات الاشـتباه الجنائي والإجراءات القضـائية، بوصـفها وسـيلة دقيقة لتحديد هوية الأشخاص[2]. إلا أن مجالات استخدامها قد اتسعت مع تطور استخدام الآلة ودخول عصـر الإلكترونيات، حيث أصـبح يكشـف تطابق بصـمات الأصـابع عن طريق وضعها فوق ماسح إلكتروني حساس للحرارة، فيقرأ التوقيع الحراري للإصبع، ثم يقوم الماسـح بصـنع نموذج للبصـمة ومضـاهتها بالبصـمات المخزنة[3]. كما أن الخيارات الأمنية لجهاز iphone 5S توفر الخيار للمسـتهلك لتكون قادرة على فتح هاتفه باسـتخدام بصـمات الأصـابع فيما يعرف بمُعرف اللمس أو جهاز الاسـتشـعار البيوميتري[4].

---

(1) ***CNIL***, « La biométrie », Mai 2005, Disponible sur: http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI- biometrie/LA_ BIOMETRIEmai2005.pdf

(2) د/ أحمد هندي، طرق الإثبات المعاصرة فقه العدالة في الإسلام، "دراسة في البصمة الوراثية وبصمات الأصابع والعين والصوت والدم والرائحة والإثبات الإلكتروني وموقف الفقه الإسلامي منها، ورقة عمل مقدمة لندوة " فقه العصـر– مناهج التجديد الدينى والفقهى" الذى تنظمه وزارة الأوقاف والشئون الدينية بسلطنة عمان– الندوة الرابعة عشرة – (تطور العلوم الفقهية 5 – 8 ابريل 2015)، ص 15.

(3) د/ عباس أحمد الباز، الندوة العلمية للجوانب الشـرعية والقانونية لاسـتخدام الوسـائل العلمية الحديثة فى التحقيق الجنائى "البصـمة البصـرية والصـوتية ودورها فى الإثبات الجنائى شـرعا وقانونا" ، جامعة نايف للعلوم الأمنية، 2007 ، ص 3.

(4) ***V. Julie M-GAUTHIER***, Cadre juridique de l'utilisation de la biométrie au Québec: sécurité et vie privée, Mémoire présenté à la Faculté de Droit en vue de l'obtention du grade de Maîtrise (L.L.M.), Droit des technologies de l'information, Université de Montréal, 2014, p 21.

وتستخدم بصمات الأصابع علي نطاق واسع داخل دول الاتحاد الأوربي للتحقق مما إذا كان تم بالفعل تقديم طلب اللجوء في بلد آخر من دول الاتحاد، حيث تم وضع قاعدة للبيانات المركزية Eurodac علي الإنترنت لمقارنة بصمات طالبي اللجوء[1].

ب- بصمة كف اليد:

تستخدم هندسة كف اليد للتعرف على الهوية البشرية، وتعتمد علي إدخال اليد فى جهاز يقيس أصابع الشخص وكف وراحة يديه بدقة، وذلك لأن أصابع وكف كل شخص لها سماتها الخاصة التي لا تتكرر، ويتم تمييزها أكثر بالتعرف على الأوردة التى تقع خلف راحة اليد [2].

واتساقا مع ذلك، اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنسا أن بصمة اليد بيان شخصيا أيا كانت صورة هذه البصمة سواء كانت بصمة الأصابع أو بصمة كف اليد[3]. وذلك بمناسبة تناولها للأنظمة الأمنية لبعض الجهات التي تعتمد علي بصمات الأصابع وهندسة اليد للأشخاص.

ج- بصمة العين:

يعتمد قياس بصمة العين على جزئين أساسيين هما: بصمة الشبكية، وبصمة القزحية . فأما بصمة القزحية L'iris فهي ذلك الجزء الملون داخل العين، والذي يتحكم في كمية الضوء النافذ من خلال البؤبؤ، وقد تم تطوير تقنية للتعرف على الهوية البيومترية عبر قزحية العين في العديد من مطارات العالم مثل كندا

---

(1) ***ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE***, « Technologies fondées sur la biométrie », Éditions OCDE, No. 77, 2005, p. 25.

(2) ***V. Julie M-GAUTHIER***, Th. préc, p. 21.
See also, Charles A. SHONIREGUN & Stephen CROSIER, « Securing Biometrics Applications », Éditions Springer, University of East London, United Kingdom, 2008, n° 20. p. 37.

(3) ***CNIL***, Délibération n°00-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par le collège Jean Rostand de Nice, destiné à gérer à la cantine scolaire par la connaissance des empreintes digitales (demande d'avis n° 636-783).

وهولندا واليابان، كما تستخدم في تأمين خزائن البنوك حيث تعتبر من أكثر التقنيات مصداقية فى العالم؛ نظرًا لاستحالة استنساخها، فلكل فرد قزحية مختلفة عن سواه[1]، أما بصمة الشبكية La rétine فهي توزيع الأوردة الدموية علي شبكة العين، وهي تختلف من شخص لآخر في شكلها ومكانها وفي تفرعاتها، وحتي من عين الشخص اليمني إلي عينه اليسري[2].

د- بصمة الصوت:

تعتمد بصمة الصوت علي كيفية التحكم في نبرات وطبقات الصوت، والتي لا يمكن تقليدها؛ لأنها تعتمد علي الأحبال الصوتية وتجويف الأنف والفم، وهي تستخدم في مجالات عدة، كفتح الأبواب آليآ، أو استخدام أجهزة المحمول، التي لا تستجيب لنبرة صوت سوي صاحبها[3].

ذ- بصمة الحمض النووي DNA:

بصمة الحمض النووي هي تلك الصفات الوراثية الخاصة بكل إنسان بعينه والتي تحملها الجينات أو الجينوم البشري وتعرف أيضا بالشفرة الوراثية، وتحمل في

---

(1) ***Julie M-GAUTHIER***, Th. pérc, pp. 22-23.

(2) د/ عباس أحمد الباز، المرجع السابق، ص 7.

(3) المرجع السابق، ص 10.

وبالرغم من ذلك فإن تكنولوجيا بصمة العين تعد مكلفة جدا لذا يصعب تعميمها، كما تتغير شبكة الأوعية الدموية للعين قليلا بسبب ارتفاع تركيز الكحول في الدم أو لمرض السكر، بالإضافة إلي مخاطر الضرر الحراري – الماسح الضوئي- علي العين بسبب ضوء الأشعة تحت الحمراء والذي ينطبق بالتساوي علي تقنيات التعرف علي الشبكية والقزحية. لمزيد من التفصيلات حول محاذير استخدام تقنية بصمة العين.

See. Nikolaos KOURKOUMELIS & Margaret TZAPHLIDOU, « Eye Safety Related toNear Infrared Radiation Exposure to Biometric Devices », in The Scientific World Journal, Department of Medical Physics, Medical School, University of Ioannina, Ioannina, Greece, March 1st, 2011.n° 115. ***See also Charles A. SHONIREGUN & Stephen CROSIER***, « Securing Biometrics Applications », Éditions Springer, University of East London, United Kingdom, 2008, p.17. n° 70. p. 55.

تكوينها الخصائص الجينية لذلك الشخص، والتي يتفرد بها عن غيره من الأشخاص؛ وذلك لأنها لا تقبل التكرار.

ط- بصمة التوقيع:

بصمة التوقيع لا يتم التعرف عليها من خلال الشكل الظاهر لها فقط، وإنما هناك أجهزة تتعرف على (فورمة التوقيع) وشكله وطريقته ووقت ونقاط الكتابة وزاوية الميل والضغط علي القلم وسرعته وهي من الجوانب التي يتم قياسها[1]، كما يمكن تحليل هذه البيانات باستخدام قرص الكتروني أو قلم قارئ[2]، وحتى الكتابة على الآلة الكاتبة أو لوحة مفاتيح الحاسب الآلى يمكن الوصول إلى الأصابع التى لامستها بالاستعمال وذلك بواسطة قياس طريقة وقوة الضغط على كل مفتاح[3]. ومن ثم تسمح بتحديد هوية صاحبها.

نخلص مما سبق إلي أن الخصائص البيومترية تعد من قبيل البيانات الشخصية؛ نظرا لأنها غير قابلة للتكرار، إذ تسمح بتفريد الشخص، وبالتالي إمكانية تحديد هويته وتمييزه عن غيره من الأشخاص، وإن كان ذلك بطريقة غير مباشرة[4].

الفرع الثالث

البيانات الحساسة

أثرت غالبية التشريعات المقارنة [5] عدم وضع تعريف للبيانات الحساسة تاركة الأمر للفقه، فقانون المعلوماتية والحريات الفرنسي مثلاً لم يعط تعريفا لها وإنما

---

(1) انظر: د/ عباس احمد الباز، المرجع السابق، ص 3.

See also. BIOMETRICS INSTITUTE, « Types of biometrics », UK, online: http://www.biometricsinstitute.org/pages/types-of-biometrics.html

(2) ***Julie M-GAUTHIER***, Th. pérc, p. 27.

(3) انظر: د/ عباس احمد الباز، المرجع السابق، ص 3.

(4) ***GUERRIER (Claudine)***, Protection des données personnelles et application biométriques en Europe, C.C.E., juillet 2003, n° 7-8, chron., p. 19.

(5) بخلاف التشريع المغربي الذي عرفها بأنها: معطيات ذات طابع شخصي تبين الأصل العرقي أو الإثني أو الآراء السياسية أو القناعات الدينية أو الفلسفية أو الانتماء النقابي للشخص

خلق فئة من البيانات – المباشرة وغير المباشرة – المحمية بشكل خاص التي تكشف الأصول العرقية أو الآراء السياسية والفلسفية أو الانتماء الديني أو الانتماء النقابي أو أخلاق الأشـــخاص[1]. كذلك قانون حماية البيانات البلجيكي الذي حددها في المادة السادسة منه بأنها البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني، أو الآراء السـياسـية، أو المعتقدات الدينية أو الفلسـفية، أو النقابية فضـلا عن البيانات الخاصـة بالحياة الجنسـية للشـخص[2]. بالإضـافة إلي البيانات الشـخصـية المتعلقة بالصحة (المادة 7 من قانون حماية البيانات البلجيكي) [3].

كما يصـــف قانون المملكة المتحدة لحماية البيانات لعام 1998 المعلومات بأنها حساسة إذا كانت متعلقة بالأصل العرقي لصاحب البيانات، أو آرائه السياسية، أو الدينية أو ما شابه ذلك من معتقدات، أو الانتماء إلي النقابات العمالية، أو صحته الجسـدية أو العقلية أو جريمة مرتكبة أو أي جريمة متهم بها، أو أي محاكمات علي أي جريمة مرتكبة أو متهم بارتكابها.

وفي ذات الاتجاه عددت المادة 1/8 من التوجيه الأوربي رقم 95–46 تلك البيانات بأنها الكاشـفة للأصـل العرقي، أو الآراء السـياسـية، والمعتقدات الدينية أو الفلســفية، والعضــوية في النقابات العمالية، ومعالجة البيانات المتعلقة بالصــحة أو الحياة الجنسية[4].

المعني أو تكون متعلقة بصـحته بما في ذلك المعطيات الجينية (المادة 1 بند 3 من قانون رقم 08–09 الخاص بحماية المعطيات ذات الطابع الشخصي).

(1) ***Danièle BOURCIER***, donnée sensible et risqué informatique de l'intimité menace à l'identité virtueue**,** CURAPP - Questions sensibles, PUF, 1998. p. 41.

(2) ***LÉONARD (Th) et POULLET (Y)***, « La protection des données à caractère personnel en pleine révolution : la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », J.T., 1999, p. 386.

(3) ***Cécile DE TERWANGNE***, La nouvelle loi belge des données à caractère personnel, chapitre 4, p. 110. Étude Disponible sur: https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr4.pdf

(4) L'article 8.I de la Directive 95/46/CE dispose que les États membres « interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle».

ولعل عدم وضع التشريعات المقارنة تعريفًا للبيانات الحساسة، ووضعها عناصر فقط يرجع إلي رغبتها في ترك الباب مفتوحًا أمام ما يستجد مستقبلًا من عناصر أخري، يمكن اعتبارها من البيانات الحساسة، خاصة في ظل التطور العلمي الذي تمر به المجتمعات، وما يعيشه العالم من ثورة، في مجال الاتصالات وتكنولوجيا المعلومات، والتقنيات الحيوية[1]. ولعل ذلك ما دفع البعض للقول بأن جميع البيانات تصبح حساسة: " بقدر طبيعتها، والمخاطر المترتبة عن الإفصاح عنها والغرض استخدامها بما في ذلك تلك البيانات التي تبدو لأول وهلة عدم وجود أضرار من تداولها أو معرفتها "[2].

ويصنف غالبية الفقه الفرنسي البيانات الحساسة لثلاثة أنواع، وهي الآراء السياسية والنقابية والمعتقدات الدينية، الحالة الصحية والحياة الجنسية، الجنسية الأصول العرقية[3]. وهو ما يمكن تفصيله كالآتي:

---

(1) نتيجة لذلك يميل القضاة إلى توسيع نطاق البيانات الحساسة توسعًيا ملفت للنظر، فليس غريبًا – والحال كذلك – أن نري قرارات مثل قرار محكمة العدل الأوروبية: يفسر إصابة الشخص في قدمه – هو في أجازة مرضية – علي أنه يشكل بيانات شخصية تتعلق بالصحة بالمعنى المقصود في المادة 8 (1) من التوجيه الأوربي رقم 46/95 .

Voir par Example, CJCE, 6 nov. 2003, Rev. DTI., n° 19/2004, n° 15. p. 68, Obs Cécile de Terwangne. ***et Voir aussi. Thiébaut DEVERGRANNE***, Donnée sensible CNIL: quelle règlementation? disponiaple sur:
https://www.donneespersonnelles.fr/donnee-sensible-cnil

(2) ***André Lucas, Jean Devèze, et Jean FRAYSSINET,*** Droit de l'informatique et de l'Internet. P.U.F, 2001, p. 137.

(3) ***Idem; Rosario DUASO CALÉS***, La protection des données personnelles contenues dans les documents publics accessibles sur Internet: le cas des données judiciaires, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître en droit (LL.M.), Université de Montréal - Faculté des études supérieures, Décembre, 2002.pp 23-24.

في حين اقام البعض تصنيفًا للبيانات الحساسة وفقًا لدرجة الحساسية والسرية degré de sensibilité et de confidentialité حيث قسم هذا الجانب البيانات الحساسة إلي ثلاث فئات: أولها، "البيانات الحساسة جدًا"، وهي المعلومات التي تكشف عن المخاطر أو الحميمية أو التمييز بالنظر إلي أن سوء استخدام هذه البيانات قد يؤدي إلى إلحاق أضرار جسيمة بالأشخاص المعنيين. وثانيها، "البيانات الحساسة" فقط وهي المعلومات التي قد تكون معروفة عن الشخص أو من

أولاً: الآراء السياسية والنقابية والمعتقدات الدينية:

لقد أكد المشرع الفرنسي صراحة، أن البيانات المتعلقة بالآراء السياسية والفلسفية أو النقابية، وكذلك المعلومات المتعلقة بالمعتقدات الدينية للإنسان، تعتبر بيانات شخصية (المادة 8 من القانون رقم 78-17 الخاص بالمعلوماتية والحريات).

كما اعتبرت اللجنة الوطنية للمعلوماتية والحريات أن البيانات المتعلقة بالآراء السياسية والفلسفية أو النقابية، كذلك المعتقدات الدينية، هي من قبيل البيانات الشخصية، وبالتالي يتعين الحصول علي موافقة خطية من الأشخاص المعنيين، لإمكان القيام بتجميعها[1].

ثانياً: الحالة الصحية والحياة الجنسية:

يقصد بالحالة الصحية للشخص، أي معلومة عن التاريخ الصحي للشخص والتي يمكن أن تستخدم لتعريف شخص بعينه، والتي استخدمت من قبل لتقديم خدمة طبية مثل التشخيص أو العلاج، بالإضافة إلي بيانات الحمض النووي وغيرها من التحاليل والفحوصات الطبية الخاصة بالشخص[2]. كما تشمل الصحة أيضا الحياة الجنسية للشخص وهي تعد من البيانات الشخصية الماسة بحرمة الحياة الخاصة،

الممكن أن النفاذ إليها والتي يؤدي إفشائها أو استغلالها أو إلي عواقب على سمعة الشخص وما يتمتع به من هدوء وسكينة. أما الفئة الثالثة فيطلق عليها "البيانات المحايدة" وهي البيانات هي التي من شأنها الكشف عن الجانب الاجتماعي للشخص. وقد اعتبر هذا الرأي أن نشر هذه البيانات دون تجميعها هو الذي يلحق الأضرار بالأشخاص المعنيين.

V. Fatima EL ATMANI, « Données sensibles: la notion de consentement de la personne concernée », Lamy Droit de l'informatique. 1996. n° 83. 1996.1.

(1) ***V. CNIL***, Délibération n° 85-050 du 22 oct. 1985 portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 17 nov 1985.
Voir aussi. CNIL, 13 ème Rapport d'activité 1992, Doc. fr. Paris, 1993. p. 153; CNIL, 14 ème Rapport d'activité 1993, Doc. fr. Paris, 1994. p. 119.

(2) ***Narayanan. A, Shmatikov. V,***″ Myths and Fallacies of 'personally Identifiable Information". Communications of the ACM, Vo. 53, N°. 6, June 2010, pp. 24-26.

ومن ثم لا يجوز بأي حال انتهاك هذه البيانات أو إفشائها ولو من الطبيب المعالج[1].

وقد أكد المشرع الفرنسي صراحة، أن البيانات المتعلقة بالحالة الصحية أو الحياة الجنسية للإنسان، هي من قبيل البيانات الشخصية (المادة 8 من القانون رقم 78-17 الخاص بالمعلوماتية والحريات). وقد اعتبرت اللجنة الوطنية للمعلوماتية والحريات أن البيانات الطبية والحياة الجنسية المتعلقة بالإنسان، هي من قبيل البيانات الشخصية، وبالتالي يتعين الحصول علي موافقة خطية من الأشخاص المعنيين، لإمكان القيام بتجميعها[2].

ثالثاً: الجنسية والاصول العرقية:

يقصد بالجنسية حالة الشخص الطبيعي، من حيث انتسابه إلي دولة معينة وارتباطه بها برابطة التبعية والولاء، ويطلق عليها الحالة السياسية. وقد اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنسا، أن البيانات المتعلقة بجنسية الإنسان من قبيل البيانات الشخصية التي تخضع للحماية القانونية بمقتضي قانون حماية البيانات الشخصية[3].

في حين يقصد بالأصول العرقية للشخص، الانتساب إلي جماعة من الجماعات الإنسانية، وفق تصنيف يعتمد علي القوميات، أو السلالات المختلفة للبشر[4]. وقد نص المشرع الفرنسي علي أن البيانات المتعلقة بالأصول العرقية، هي

---

(1) د/ مصطفي أحمد عبد الجواد حجازي، المسئولية المدنية للصحفي عن انتهاك حرمة الحياة الخاصة، دار النهضة العربية، 2004، ص 87.

(2) ***V. CNIL***, Délibération n° 85-050 du 22 oct. 1985 portant recommandation relative aux modalités de collecte d'informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 17 nov 1985.

(3) ***CNIL***, Délibération n° 91-033 du 7 mai. 1991 portant avis relative à la création d'un traitement automatiséd d'informations nominatives concernant une application de gestion des dossiers des ressortissants étrangers en France, CNIL, 12 éme rapport d'activité 1991, La documentation francaise, Paris, 1992, p. 233.

(4) د/ أيمن مصطفي أحمد، المرجع السابق، ص 617.

من قبيل البيانات الشـــخصـــية، وذلك بمقتضـــي المادة 8 من قانون المعلوماتية والحريات[1].

المبحث الثاني
مفهوم معالجة البيانات الشخصية

يستلزم خضوع البيانات الشخصية لمقتضيات الحماية التي جاء بها القانون الفرنسي رقم 78-17 الخاص بالمعلوماتية والحريات، أن تكون محلًا للمعالجة. وهو ما يتعين علينا ان نبين تعريف معالجة البيانات الشـــخصـــية، وأي أنواع المعالجة تخضع للحماية القانونية.

وبناء عليه سوف نتناول الموضوع في مطلبين علي النحو التالي:

المطلب الأول: تعريف معالجة البيانات الشخصية.

المطلب الثاني: صور معالجة البيانات الشخصية.

المطلب الأول
تعريف معالجة البيانات الشخصية

معالجة البيانات الشخصية Le traitement de données personnelles هي ببســـاطة كافة العمليات التي تجري علي هذه البيانات، وقد عرفتها الفقرة (2) من المادة الثانية من القانون سالف الذكر علي أنها: كل عملية أو مجموعة من العمليات تنفذ علي هذه البيانات، أيًا كانت الآلية المستخدمة، بما في ذلك الجمع، التسجيل، التنظيم، التخزين، والتحوير أو التعديل، والاسترجاع، والاستعلام، والاتصال عن طريق الإرسال أو الإتاحة بأي شكلٍ من الأشكال، وكذلك التقريب والدمج ومنع الوصول، فضلًا عن المحو والتدمير[2].

---

(1) **Art. 8/1** Loi n° 78-17, précité.

(2) ***Article 2, alinéa 2*** de la loi Informatique et libertés modifiée du 6 août 2004.

ومن ثم يتضـــح من خلال هذا التعريف أن المشـــرع الفرنســـي قام بتكديس accumulation مجموعة من المصـطلحات الدالة علي عمليات المعالجة، وقد سـار المشـــرع البلجيكي[1] والتونســـي[2] والمغربي[3] في هذا الأطار علي نهج التوجيه الأوربي رقم 46/95 وباقي التشـريعات الأوربية، ولعل ذلك يجد تفسـيره في رغبة هذه التشـــريعات في منح معنيً واســـع جدًا لكلمة معالجة، مما يجعل مدلولها يختلف عن مدلولها في نطاق لغة البرمجيات[4].

ولتقريب الصـــورة إلي ذهن القارئ حول المقصـــود بمعالجة البيانات عمومًا، نضـرب مثالا بالشـخص الذي يكتب رسـالة علي جهاز الحاسـب الآلي، فالكتابة في حد ذاتها هي شكل من أشكال المعالجة، وبعد الكتابة من الطبيعي أن يأتي التنسيق، وهو شـــكل آخر للمعالجة، ثم التخزين، وقد يســـتتبعه الاســـترجاع، أو التعديل، أو المحو، أو غير ذلك من العمليات التي تتم علي الرسالة[5].

ويعد الحاسـب الآلي الوسـيلة الأسـاسـية لمعالجة البيانات الشـخصـية؛ حيث ينظر إليـه علي أنـه بمثـابـة مكنـة لإنتـاج معطيـات جـديـدة انطلاقًـا من المعلومـات

---

(1) ***Article 1 er***, § 1er nouveau de la loi belge du 8 décembre 1992.

(2) العمليات المنجزة سواء بطريقة آلية أو يدوية من شخص طبيعي أو معنوي والتي تهدف خاصة إلى جمع معطيات شـخصـية أو تسـجيلها أو حفظها أو تنظيمها أو تغييرها أو اسـتغلالها أو استعمالها أو إرسالها أو توزيعها أو نشرها أو إتلافها أو الاطلاع عليها وكذلك جميع العمليات المتعلقة باســتغلال قواعد البيانات أو الفهارس أو الســجلات أو البطاقات أو بالربط البيني. (الفصل السادس من القانون رقم 64 لسنة 2004 المتعلق بحماية المعطيات الشخصية).

(3) كل عملية أو مجموعة من العمليات تنجز بمسـاعدة طرق آلية أو بدونها وتطبق على معطيات ذات طابع شـخصـي، مثل التجميع أو التسـجيل أو التنظيم أو الحفظ أو الملاءمة أو التغيير أو الاستخراج أو الاطلاع أو الاستعمال أو الإيصـال عن طريق الإرسـال أو الإذاعة أو أي شكل آخر أو من أشـكال إتاحة المعلومات، أو التقريب أو الربط البيني وكذا الإغلاق أو المسـح أو الإتلاف. (المادة الثانية من القانون رقم 09-08 لســنة 2004 المتعلق بحماية الاشـــخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي).

(4) ***André Lucas, Jean Devèze et Jean FRAYSSINET***, Op.cit., 82.

(5) د/ محمد سامي عبد الصادق، المرجع السابق، ص 43-44.

المعالجة[1]، إلا أن تحقق المعالجة لا يتوقف علي التقنيات المستخدمة[2]، ولعل هذا ما حدا بالبعض للحديث عن مبدأ يسمي الحياد التكنولوجي La neutralité technologique، حيث تتحقق المعالجة بأي إجراء من الإجراءات المذكورة في المادة 2/2 من قانون المعلوماتية والحريات أو ما يماثلها، ولو لم يتم استعمال طريقة آلية[3].

وتجدر الإشارة إلي التعداد الذي جاء به المشرع الفرنسي في المادة 2/2 سالفة الذكر لعمليات المعالجة لا يعد حصريًا بل هو علي سبيل المثال فقط، ويظهر ذلك جليًا من استعمال المشرع لعبارة " بأي شكل آخر" مما يعني أن معالجة البيانات الشخصية يمكن أن تتم عن طريق عمليات أخري غير الواردة بهذه المادة، وبالتالي يدخل في عداد معالجة البيانات الشخصية أي إجراء يتم اتخاذه ويكون متعلقًا بهذه البيانات[4].

وبناء عليه يمكن أن تتم معالجة البيانات الشخصية من خلال مجموعة من العمليات كتجميع البيانات وتنظيمها، كما يمكن أن تقتصر علي عملية واحدة من المنصوص عليها في المادة 2/2 سالفة الذكر كتعديل هذه البيانات أو استرجاعها

---

(1) ***Pierre KAYSER,*** La protection de la vie privée par le droit, Economica/Presses universitaires d'Aix-Marseille, 3è éd., 1995, p. 437.

(2) حيث تقضي الحيثية 27 من التوجيه الأوربي بأن: " حماية الأشخاص يجب أن تنطبق علي المعالجة الألية للبيانات، بالإضافة إلي المعالجة اليدوية، كما أن نطاق الحماية يجب ألا يتوقف علي التقنيات المستخدمة ...".

Directive 95/46/CE, précité, considérant 27 et article 3.

(3) ***André Lucas, Jean Devèze, et Jean FRAYSSINET,*** Op.cit., p. 82.

(4) ***Benoit TABAKA et Yann TESAR***, Loi informatique: un nouveau cadre juridique pour le traitement des données à caractère personnel, Dossier, 2004, p. 8. Disponible sur: www.foruminternet.org

أو نقلها[1]. **وفي هذا الصدد ثار التساؤل الآتي: هل يشترط حصول تغيير أو تحويل في المعلومة محل المعالجة حتي يمكن القول بوجود معالجة للبيانات الشخصية ؟**

الإجابة تكون بالنفي، فليس من الضـــروري أن يترتب علي المعالجة تحويل أو تغيير في شـــكل المعلومة التي خضـــعت لذلك، فالمعالجة تعتبر متحققة ولو احتفظت المعلومة التي خضعت للمعالجة بشكلها الأصلي، ويتضح ذلك من خلال اعتبار مجرد التجميع أو الحفظ من العمليات التي تتم بها معالجة البيانات الشـخصـية. وإزاء هذا التوسـع في مفهوم معالجة البيانات، نجد أنفسـنا أمام نتيجة ضـمنية ألا وهي أن كل عملية تجري علي البيانات ذات الطابع الشـخصـي يمكن بسبب مبدأ الغاية المحددة لها أن تحمل اعتداء علي حقوق وحريات الأشخاص، وهو ما يقتضي اعتبارها معالجة للبيانات الشخصية[2].

بالمقابل يلاحظ تردد موقف القضاء الفرنسي تجاه التوسع في مفهوم معالجة البيانات الشـــخصـــية، ففي الوقت الذي اعتبرت فيه محكمة Nantes الابتدائية بأن المعالجة تتحقق بمجرد تسـجيل البيانات الاسـمية للأشـخاص عبر نظام إلكتروني لتحديد الملفات والرد تلقائيا علي أي طلب بناء علي رقم الملف[3]. نجد أن قضـــاء النقض الفرنسي أكثر تضيقا لمفهوم معالجة البيانات الشخصية[4].

---

(1) حيث قضـــت محكمة باريس الابتدائية في حكمين لها بأن عملية واحدة كافية للقول بوجود معالجة للبيانات الشخصية، والقول بعكس ذلك من شأنه تفريغ النص من محتواه وتشويه، ولا يهم بعد ذلك ما إذا كانت المعالجة تحضيرية أو تجريبية لإنشاء المعالجة.

TGI Paris 7 mai 1991 et 5 décembre 1991, TGI Paris, 5 décembre 1991. Cité par CNIL, 12ème Rapport d'activité 1991, Doc. fr. Paris, 1992. p.30.

(2) ***André Lucas, Jean Devèze et Jean FRAYSSINET***, Op.cit., p. 85.

(3) TGI Nantes, 3ème chambre, 16 décembre 1985 Cité par. CNIL, 6 ème Rapport d'activité 1985, Doc. fr. Paris, 1986. p. 275.

(4) حيث قضي بأن استعمال الحاسوب الصغير لا يشكل في حد ذاته معالجة للبيانات الشخصية، وذلك بمناسبة قضية عرضت عليه، وتتمثل في طباعة الحواسيب الصغيرة لقائمة المرضي بأحد المستشفيات عبر إدخال المعلومات المدونة في الملفات الورقية دون حفظها علي دعامة ممغنطة من أجل معالجة لاحقة، إذ اعتبر هذه المســـألة أكثر بســـاطة من أن يطلق عليها

ومما لا شـك فيه أن اتسـاع التعريف التشـريعي لمفهوم المعالجة قد ألقي بظلاله علي القضـاء الفرنسـي وذلك من خلال مجموع القضـايا التي طرحت والتي سـتطرح عليه، فهو مطالب بتحديد ماهية معالجة البيانات الشـخصـية مع الأخذ في الاعتبار ضـرورة حماية المواطن من الاستعمال التعسفي لبياناته لشخصية. ومن ثم يثور التساؤل الآتي: **هل كل المعالجات التي تجري علي بيانات ذات طابع شخصي تمثل خطورة علي حقوق وحريات الأشخاص؟**

بالرجوع إلي نصـوص القانون الفرنسـي رقم 78-17 يمكن لنا القول بأن أغلب هذه المعالجات تمس حقوق وحريات الأفراد، ما عدا الحالة التي نصـت عليها المادة 1/22 من هذا القانون والتي أعفي فيها المشـرع المسـئول عن المعالجة من الأخطار المسـبق، والتي تتعلق بالمعالجات التي يكون الغرض منه مسـك سـجل الغرض من إعلام الكافة، ويكون متاح للفحص من قبل أي شـخص له مصـلحة مشروعة في ذلك.

وفي هذا الصـدد يمكن أن تلعب اللجنة الوطنية للمعلوماتية والحريات دورًا محوريًا في تحديد هذا النوع من المعالجة، ففي اجتهاد للجنة الوطنية ضـمن مداولة لها تحت رقم 80-34 بتاريخ 21 أكتوبر 1980 متعلقة بالمعالجة الآلية للمحاسـبات العامة، اعتبرت اللجنة أن الغرض الوحيد من هذه المعالجة تمثل الذمة المالية لجهاز المحاسـبات والوقوف علي مركزه المالي، وبذلك تعفي من شـرط التصـريح المسـبق، علي الرغم من إدراجها المعلومات الاسـمية للأشـخاص في نظم المحاسـبة العامة الآلية، إلا أن هذه المعلومات لا تؤثر بشـكل مباشـر أو غير مباشـر علي الهوية البشرية أو حقوق الإنسان أو الحريات الفردية، أو العامة[1].

معالجة؛ وذلك لكونها تنطوي – فقط – علي اسـتخدام أحد أوجه الحاسـوب كأداة في الكتابة والطباعة.

Crim., 6 juillet 1994; CNIL, 15 ème Rapport d'activité 1994, Doc. fr. Paris, 1995, pp. 36 et 468.

(1) ***CNIL***, Délibération n° 80-34 du 21 octobre 1980 relative au traitement automatisé de la comptabilité Générale. Disponible sur le site suivant: https://www.legifrance.gouv.fr/

كما أخرجت اللجنة الوطنية للمعلوماتية والحريات من المفهوم التشـــريعي للمعالجة الآلية للبيانات الشخصية، نتائج كاميرات المراقبة التي يتم وضعها بالأماكن العامة لمراقبة حركة السـير، فوضـع هذه الكاميرات لا يعد معالجة للبيانات الاسـمية متي كانت الصـــور المســـتقبلة غير رقمية وغير مســـجلة، مما يجعل اللجنة غير مختصة بإعطاء ترخيص بشأن ذلك[1].

معالجة البيانات علي شبكة الإنترنت:

إذا كانت المعالجات التي تتم علي شـــبكة الإنترنت تتشـــابه مع المعالجات التي تتم خارج هذا الفضاء في مجموعة من النقاط، فإنها تنفرد بخصوصيات معينة، وفي هذا الأطار إذ يعد كل تجميع للبيانات الشخصية انطلاقا من موقع إلكتروني أو أي خدمة علي شـــبكة الإنترنت خاضـــعًا للقانون رقم 78-18 بشـــأن المعلوماتية والحريات منذ لحظة التجميع. والذي يوجب إعلام الشـــخص المعني، ويســـري نفس الأمر بالنسبة لعمليات المعالجة الأخري علي الشبكة كعملية الاطلاع.

اتســـاقًا مع ذلك، قضـــت محكمة العدل الأوربية في حكمها الصـــادر في 6 نوفمبر عام 2003 بأن عملية وضع البيانات الشخصية علي صفحة الإنترنت تعتبر معالجة آلية، حيث فسرت ذلك بأن استخدام الإنترنت في حد ذاته ينطوي علي تنفيذ إجراءات يجب اعتبارها آلية[2]. وفي ذات الاتجاه اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنســـا بأن جعل المعلومات تظهر علي شـــبكة الإنترنت يعني وفقًا لإجراءات التقنية والحوســـبة المطبقة حاليا- من تحميل الصـــفحة علي الخادم، والعمليات الأخري اللازمة لجعل الصفحة في متناول المتصلين بالشبكة – أنها نفذت ولو بطريقة آلية[3].

---

(1) ***V. CNIL***, Deliberation n°2006-048 du 23 février 2006 portant autorisation de la mise en oeuvre par la société ALIS d'un traitement automatisé de données à caractère personnel au suivi des clients en infraction. Disponible sur le site suivant: https://www.legifrance.gouv.fr/ ***Voir aussi. Pierre KAYSER,*** Op.cit., p.438.

(2) ***CJCE***, 6 novembre 2003, aff. 101/01 Göta Hovrätt c/Bodil Lindqvist.

(3) ***CNIL***, 24 ème Rapport d'activité 2003, Doc.fr. Paris, 2004, pp. 507-523.

والمسئول عن معالجة البيانات هو – بحسب الأصل– الشخص أو السلطة العامة أو الوكالة أو الهيئة التي تحدد كيفية وغاية معالجة البيانات، وذلك حسبما نص التوجيه الأوربي وقانون المعلوماتية والحريات الفرنسي[1]؛ وبالتالي فإن معالجة البيانات الشخصية عبر شبكة الإنترنت عموما أو شبكات التواصل الاجتماعي يُسأَل عنها مقدم خدمة التواصل، وهو قد يعهد بها للآخر الذي يتولي المعالجة لصالحه أو يقوم بها بواسطة العاملين لديه؛ بحيث يتولي جمع البيانات وتخزينها وتصنيفها والتوفيق بينها وصولًا إلي نتائج معينة تفيده في مجالات الدعاية والتسويق[2].

المطلب الثاني
صور معالجة البيانات الشخصية

حدد المشرع الفرنسي ثلاث صور لمعالجة البيانات الشخصية وهي المعالجة الآلية، والمعالجة غير الآلية (اليدوية)، والمعالجة لغرض نشاط شخصي محض،

---

(1) ***Art 3/1, Loi n° 78-17*:** «Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ».

(2) هذا الصدد يقول: الأستاذ الدكتور/ محمد سامي صادق موضحًا دور معالجة البيانات الشخصية عبر شبكات التواصل الاجتماعي في الدعاية والتسويق، حيث يفترض سيادته أن من بين المستخدمين للموقع الإلكتروني رجلاً متوسطَ العمر تُظهر بياناته الشخصية عضويته بأحد الأندية الرياضية، وممارسته علي سبيل الهواية لنشاط رياضي معين، مع حرصه علي إبراز لقطات تجمعه مع عدد من مشاهير الرياضة علي صفحته الخاصة علي الموقع، فمن الممكن بمعالجة هذه البيانات الوصول إلي اهتمام هذا المستخدم بالمنتجات الرياضية، وفي الوقت ذاته تساعد بياناته الشخصية التي سبق أن دوَّنها عند تسجيله للانضمام إلي موقع التواصل علي مخاطبته من جانب المعلنين برسائل نصية، سواء عبر بريده الإلكتروني أو رقم هاتفه الجوال، بشأن عروض الشراء علي الملابس والأحذية والحقائب والأدوات الرياضية؛ وبذلك تكون معالجة البيانات الشخصية قد أثمرت في مجال الدعاية والتجارة. راجع مؤلف سيادته، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، المرجع السابق، ص 44.

Crim., 6 juillet 1994; CNIL, 15 ème Rapport d'activité 1994, Doc. fr. Paris, 1995, pp. 36 et 468.

حيث ذكر في المادة 1/2 من القانون رقم 78-17 المعدل لسنة 2004 الخاص بالمعلوماتية والحريات أنه: " ينطبق على المعالجة الآلية للبيانات الشخصية، فضلا عن المعالجة غير الآلية للبيانات الشخصية الواردة أو المراد إدراجها في الملفات، باستثناء عمليات المعالجة المنفذة للأغراض الشخصية الخاصة حصرًا، حيث يستوفي الشخص فيها الشروط المنصوص عليها في المادة 5"[1].

وسوف نتناول المعالجة الآلية للبيانات الشخصية (أولا)، نعقبها ببيان المعالجة اليدوية للبيانات الشخصية (ثانيا)، ثم معالجة البيانات لأغراض شخصية محضة (ثالثا).

أولاً: المعالجة الآلية للبيانات الشخصية:

ويقصد بالمعالجة الآلية للبيانات الشخصية[2]، المعالجة التي تتم بواسطة استخدام الحاسب الآلي أو أحد تطبيقاته المختلفة؛ فأي إجراء خاص بالبيانات الشخصية يتم عبر استخدام الكمبيوتر من تنظيم أو تعديل أو تصنيف للمعلومات الشخصية في قواعد البيانات يعد معالجة آلية للبيانات الشخصية[3]. ولا يهم بعد ذلك نوع أجهزة الكمبيوتر المستخدمة، فيمكن أن يكون جهاز كمبيوتر كبير أو أحد الحواسيب الصغيرة، أو معدات المكاتب[4]. كما لا يهم أيضا نوع الوسيلة المستخدمة

---

(1) ***Article 2/I, loi n° 78-17***: « La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

(2) ***V. Claudine GUERRIER***, Op.cit., p. 133; ***Julien LE CLAINCHE,*** Op.cit., p. 7.

(3) بل يكفي أن تنطوي في جزء منها فقط، على استخدام الوسائل الآلية، علي سبيل المثال تخزين المعلومات في البداية على وسط محوسب ومن ثم طباعتها أو نقلها باستخدام العمليات الآلية، حتى لو كانت على الورق (الفاكس). انظر:

Cécile DE TERWANGNE, Op.cit., p. 102.

(4) ***V. Ibrahim COULIBALY***, Th. préc., p. 97.

إذ تشمل الوسائل الآلية: جميع تكنولوجيا المعلومات، تكنولوجيا الاتصال عن بعد، وشبكات الاتصالات السلكية واللاسلكية[1].

وتجدر الإشارة إلي أن المعالجة الآلية قد تتجاوز المعالجة البسيطة التي تتم بواسطة الحاسوب لتشمل أي نوع من وسائل إدارة البيانات مثل المعالجات الدقيقة بواسطة شرائح (البطاقات المصرفية، بطاقات Sim للهاتف المحمول) مينيتل أو خادم Wib[2]، كما تشمل أيضًا كل تكنولوجيا الإعلام المعلوماتية télématique، وشبكات الاتصال عن بعد كالإنترنت[3]. فالعبرة ليست في الآلة في حد ذاتها وإنما بما تمكنه من معالجة آلية للبيانات الشخصية، ومن ثم فإن القانون الفرنسي رقم 87-17 المعدل لسنة 2004 يشمل مجال تطبيقه للمعالجة الآلية الموجودة حاليا[4]، وتلك التي من الممكن أن تظهر مستقبلًا إذ كانت تمكن من المعالجة الآلية للبيانات. شأن نظيره البلجيكي الصادر في 8 ديسمبر 1992 والمعدل لسنة 1998 والذي قدم مفهومًا واسع جدًا للمعالجة الآلية بغض النظر عن التكنولوجيات المتطورة المستخدمة في المعالجات[5].

ثانياً: المعالجة اليدوية للبيانات الشخصية:

يقصد بالمعالجة اليدوية للبيانات الشخصية وضع هذه البيانات في ملفات يدوية تقليدية؛ أي وضع البيانات في أوراق وجمعها في ملفات، وتتخذ هذه الملفات

---

(1) ***V. Cécile DE TERWANGNE***, Op.cit., p. 102.

(2) ***Julien LE CLAINCHE***, Op.cit., p. 7.

(3) ***V.*** La commission de la protection de la vie privée, la protection des données à caractère personnel en Belgique, vie privée- principes de base. Disponible sur le site suivant: http://www.privacycommission.be/

(4) ***André Lucas, Jean Devèze et Jean FRAYSSINET***, Op.cit., p. 83.

(5) ***Leonard (T) et Poullet (Y)***, « La protection des données à caractère personnel en pleine révolution. La loi du 11 décembre 1998 transposant la directive95/46/CE du 24 octobre 1995 », J.T., 1999, p. 379.

وحول تفصيلات المعالجة الآلية في القانون البلجيكي، راجع:

MARC (VAN- OVERSTRAETEN) et Sébastien (DEPRÉ), Le traitement des données à caractère personnel et le droit au respect de la vie privée en Belgique, Rev. trim. dr. h., n° 3- 2003, n° 10. pp 678-679.

تصـــنيفا وهيكلة وفق لمعيار هجائي، أو رمزي، أو كرونولوجي ... إلخ، حيث يتم معالجة البيانات دون الاستعانة ببرامج الحاسب الآلي[1].

والجدير بالذكر أن القانون الفرنســـي رقم 78-17 الخاص بالمعلوماتية والحريات قبل تعديله لسنة 2004 كان يقصر نطاق معالجة البيانات الشخصية علي المعالجات الآلية مع إمكانية التطبيق علي المعالجات غير الآلية المتعلقة بالبحوث الطبية[2]، وهو ما كان محل انتقاد واســـع من الفقه نظرا لأن الملفات اليدوية ترتبط حتما بالمعالجة الالية حيث لم يضـــع القانون في الاعتبار "الروابط الوظيفية التي غالبا ما تربط الأوارق والملفات الآلية [3]. وهو تداركه المشـرع الفرنســي والبلجيكي[4] عقب التوجيه الأوروبي رقم 46/95 الصـادر لسـنة 1995 بشـأن حماية الاشـخاص الطبيعين بالنظر إلي معالجة البيانات ذات الطابع الشخصي [5].

ثالثاً: معالجة لأغراض شخصية:

يقصـد بالمعالجة لغرض شـخصـي محض أن يقوم الشـخص بتجميع بيانات لأفراد يعرفهم شخصيًا، وعقب ذلك يقوم بتصنيف هذه البيانات بهدف ممارسة أنشطة شـخصـية أو منزلية، أو أن يقوم شـخص ما بتجميع أرقام التليفونات الخاصـة بزملائه وأصدقائه وأقاربه، أو عمل ملف للزملاء والأقارب والأصدقاء يحتوي علي كل الأرقام الخاصـــة بهم وعناوينهم الشـــخصـــية والبريدية والإلكترونية[6]. لذلك لا تمثل هذه

---

(1) ***Baffard WILLIAM***, Op. cit., p. 16.

(2) ***V. Isabelle (DE LABERTERIE), Henri (JAQUES- LUCAS)***, Informatique libertés et recherche médicale, Edition CNRS, 2001, n° 54. p. 29.

(3) ***V. Frayssinet (J), Pédrot (P),*** La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé, JCP 1994, éd. G., I, 3810. p. 562; ***Alain BENSOUSSAN***, Informatique et libertés, Editions Francis Lefebvre, 2008, n° 73. p.23.

(4) ***V. Boulanger (M-H), De Terwangne (C) et Leonard (T)***, « vie privée à la protection de ha l'égard des traitements de données à caractère personnel. La loi du 8 décembre 1992», J.T., 1993, p. 372; ***Leonard (T) et Poullet (Y),*** « La protection des données à caractère personnel en pleine révolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995», J.T., 1999, p. 379.

(5) ***Directive 95/46/CE***, précité, considérant 27 et article 3.

(6) ***Benoit TABAKA et Yann TESAR,*** **O**p.cit., p. 9.

المعالجة أي تهديد للحياة الخاصة للأفراد، ومن ثم استبعدها المشرع الفرنسي من نطاق تطبيق القانون رقم 78-17 الخاص بالمعلوماتية والحريات[1].

نخلص مما سبق أن القانون الفرنسي رقم 78-17 الصادر لسنة 1978 والمعدل لسنة 2004 سالف الذكر يسري نطاق تطبيقه ومن ثم حمايته للبيانات الشخصية الخاضعة للمعالجة علي نوعين من المعالجات هما: المعالجة الآلية للبيانات الشخصية، والمعالجة اليدوية للبيانات الشخصية، بينما لا ينطبق علي المعالجات لغرض شخصي محض.

المبحث الثالث

المخاطر المتصلة بمعالجة البيانات الشخصية

تمهيد:

إذا كان التقدم العلمي والتطور التكنولوجي قد فتح آفاقًا ضخمة أمام تقدم الإنسانية وتحقيق مستوي أفضل ومتقدم للحياة، إلا أنه ألقي بظلاله علي الحقوق والحريات الشخصية؛ حيث أدت هذه التطورات إلي ظهور أجهزة ومعدات حديثة سهلت انتهاك خصوصية الفرد وتسللت داخله واستحال الإنسان معها إلي مجموعة من البيانات مسجلة في بنوك المعلومات[2].

ونظرًا للكم الهائل من المعلومات التي يتم تجميعها وتخزينها حول الأشخاص داخل بنوك المعلومات[3] والذي قد يجري معالجتها آليا في غيبة الضمانات المقررة.

---

(1) ***Baffard WILLIAM,*** Op.cit., p. 18.

(2) فمن خلال بنوك المعلومات وأجهزة الكمبيوتر، أصبح من اليسير جمع كافة المعلومات المسجلة عن شخص معين مثل عمره وحالته الاجتماعية الصحية ومركزه المالي وأرائه السياسية والنقابية إن وجدت، وتقييم رب العمل له والتوصيات المقررة بشأنه وغير ذلك من البيانات، واستخدامها لأغراض مختلفة عما سجلت به، وأولها بقصد رقابة هذا الشخص والاعتداء علي حياته الخاصة. د/ محمود سلامة جبر، المرجع السابق، ص 87.

(3) ويقصد ببنوك المعلومات: تكوين قواعد بيانات تفيد موضوعا معينا وتهدف لخدمة غرض معين، ومعالجتها بواسطة أجهزة الحاسبات الالكترونية لإرجاعها في صورة معلومات تفيد

فقد نما الشـــعور بالخطر وتطور بفعل الحالات الواقعية للاســـتخدام غير القانوني للبيانات الشـخصـية، واتسـاع دائرة الاعتداء علي حق الأفراد في الحياة الخاصـة مما اسـتدعي بالضـرورة إيجاد مبادئ وقواعد من شـأن مراعاتها حماية الحق في الحياة الخاصـــة، وتحقيق التوازن بين حاجات المجتمع لجمع وتخزين ومعالجة البيانات الشـخصـية، وكفالة حماية لهذه البيانات من مخاطر الاسـتخدام غير القانوني لتقنيات معالجتها[1].

وفي هذا الصدد أشارت المحكمة الدستورية في كارلسروه بألمانيا الإتحادية إلي مخاطر معالجة البيانات الشـخصـية بقولها: أن التقنيات الجديدة لجمع البيانات الشـخصـية والاحتفاظ بها واسـتخدامها من المرجح أن تقوض الحق العام في احترام الحق في الحياة الخاصـة، وذلك من خلال التخزين غير محدود للبيانات واسـتخدامها في أي وقت، لأغراض مختلفة عن تلك التي بررت جمعها، وبدون أن يكون الشخص قادرا على السيطرة على استخدام هذه البيانات [2].

مســـتخدمين مختلفين في أغراض معينة ومتعددة. وتتجه جميع دول العالم بمختلف هيئاتها ومؤسـساتها إلي إنشـاء هذه البنوك لتنظيم أعمالها، وقد تكون مقصـورة علي بيانات ومعلومات تتصـــل بقطاع بعينه، مثل بنوك المعلومات القانونية وبنوك معلومات الشـــركات المالية والمصارف، وقد تكون شاملة لمختلف الشئون والقطاعات، كما قد تكون مهيأة للاستخدام علي المستوي الوطني أو الإقليمي أو الدولي. انظر:

د/ محمد حسام محمود لطفي، بنوك المعلومات وحقوق المؤلف، بدون دار نشر، 1999، ص 5 وما بعدها؛ د/ اســـامة عبد الله قايد، الحماية الجنائية للحياة الخاصـــة وبنوك المعلومات، المرجع سابق، دار النهضة العربية، 1994، ص 49.

(1) د/ يسري عبد الله عبد الباري، الحماية المدنية للخصـوصـية المعلوماتية دراسـة مقارنة، رسـالة دكتوراة – حقوق عين شمس، 2016، ص 145.

(2) ***Cour constitutionnelle de Karlsruhe***, 15 décembre 1983. Pour un commentaire de cette décision, M. Fromont, République fédérale d'Allemagne, la jurisprudence constitutionnelle en 1982 et 1983, Revue du droit public et de la science politique, 1984, pp. 1562-1568.

وعلي ضـــوء هذا القرار يمكن لنا تفهم المخاطر الكامنة في معالجة البيانات الشـــخصـــية، وهي تتعلق بمجمل عملية معالجة البيانات، بدءا من جمع البيانات، وصولًا إلى معالجتها واستغلالها. وتعتبر حوسبة البيانات في المرحلتين خطرا محددا.

وبناء عليه سوف نتناول هذا الموضوع في ثلاثة مطالب علي النحو التالي:

المطلب الأول: المخاطر المتعلقة بتجميع البيانات الشخصية.

المطلب الثاني: المخاطر المتعلقة باستخدام البيانات الشخصية.

المطلب الثالث: المخاطر المتعلقة بحوسبة البيانات الشخصية.

المطلب الأول

المخاطر المتعلقة بتجميع البيانات الشخصية

يقصد بتجميع البيانات الشخصية Le collecte des données personnelles ، كل عمل من أعمال الجمع والترتيب recueillir et de rassembler لعناصر البيانات الشخصية لأحد الأشخاص، وإدراجها علي بطاقة معلومات لذات الشخص، سواء كانت هذه البطاقة ورقية أو إلكترونية[1].

وإذا كانت تجميع البيانات الشـخصـية وترتيبها بهذه الكيفية، أمرًا لازمًا لتنفيذ معالجة البيانات، فإن معالجة البيانات لا تخلو في كثير من الأحيان من بعض المخاطر، المتمثلة في خطر التعدي على الحقوق والحريات الفردية للأشـــخاص المعنيين بهذه البيانات، أو انتهاك حرمة حياتهم الخاصـة[2]، علي ضـوء قيام الكثير

---

(1) ***Cynthia (CHASSIGNEUX)***, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas (Paris II) , 2003. nº 278, p. 154.

(2) ***Raoul (DEPOUTOT) et Gérard (LANG),*** Le secret statistique concernant les entreprises: Situation 2000 et perspectives d'évolution, janvier 2002, CNIS, Division environnement juridique de la Statistique, janvier 2002, p. 17. Étude disponible sur: https://www.cnis.fr/wp-content/uploads/2017/10/RAP_2002_71_secret_statistique_entrprises.pdf

من المؤسسات الحكومية[1] والشركات الخاصة[2] بتجميع بيانات عديدة ومفصلة عن المتعاملين معها كتلك التي تتعلق بالوضـــع المادي والصـــحي والتعليمي والعائلي والاتجاهات الاجتماعية وغيرها، مما يفتح الباب علي مصراعيه لإساءة استخدامها أو توجيهها توجيهًا منحرفًا أو خاطئًا أو لمراقبة الأفراد والحكم عليهم حكمًا خفيًا من واقع سجلات البيانات الشخصية المخزنة[3].

أضف إلي أن ربط الأجهزة الإلكترونية بعضها البعض بواسطة جهاز مركزي أو عبر شـبكات عامة للاتصـال يؤدي إلي تبادل المعلومات والبيانات الشـخصـية للأفراد فيما بين الأنظمة المعلوماتية، ومن ثم التوصـل إلي بيانات ومعلومات جديدة عن الأشخاص[4]. كما يمكن في وقتنا الحاضر تجميع البيانات الشخصية دون علم الأشـخاص المعنيين بها، وذلك بفضـل الوسـائل التكنولوجيا الحديثة ولا سـيما الانترنت[5]، والتي يمكن من خلالها تجميع البيانات الشخصية للمستخدمين وتخزينها، عن طريق رسائل الكوكيز[6]، أو تقنية تحديد الهوية باستخدام موجات الراديو RFID

---

(1) كمؤسـسـات وزارة الصـحة ومصـلحة الأحوال المدنية، ووزارة القوي العاملة، ووزارة التضـامن الاجتمـاعي، ووزارة التـأمينـات والشـــئون الاجتمـاعيـة، ووزارة التعليم العـالي، ووزارة التجـارة والصناعة.

(2) كقطاع البنوك وقطاع التأمين شـركات البريد الخاصـة ونقل الأموال وشـركات الاتصـالات الخاصة.

(3) د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات ، مكتبة الآلات الحديثة، 1992، ص 179 وما بعدها.

(4) د/ محمود عبد الرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية، العدد التاسـع السـنة الثالث، مارس 2015، ص 109؛ د/ هشام محمد فريد رستم، المرجع السابق، ص 179 وما بعدها.

(5) ***En ce qui concerne l'Internet, voir, CNIL***, 21ème Rapport d'activité 2000, Doc. fr. Paris, 2001. p. 138.

(6) الكوكيز عبارة عن ملفات نصية تضعها معظم مواقع الويب علي القرص الصلب في الخاص بالمتصـفح (الزائر)، عند زيارته لهذه المواقع، بغرض جمع بعض المعلومات عن المسـتخدم، تتيح للموقع الذي أودعها أن يسترجعها عند الحاجة إليها، ومكمن الخطورة في هذه الملفات أنه

[1] أو برامج التتبع بحيث يتم جمع هذه المعلومات ومعالجتها بسرعة فائقة[2]. بالإضافة إلي ما تقوم به مواقع التجارة الإلكترونية علي شبكة الإنترنت، حيث تطلب الشركات من المستخدمين تعبئة نماذج خاصة تحتوي في جنباتها الاستفسار عن بعض المعلومات علي سبيل المثال: اسم المستخدم، وعنوان عمله ومنزله ورقم هاتفه وبريده الإلكتروني ومكان اقامته ودخله الشهري أو السنوي ... إلخ، أما الموقع الذي يتم فيه دفع ثمن المبيعات فإنه يطلب رقم بطاقة ائتمان المشتري ونوعها وتاريخ انتهائها[3].

بالإضافة إلي 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 علي حساب خاص به، ووفقًا للسياسات الخصوصية

من الممكن استغلالها في انتهاك خصوصية المستخدمين وجمع معلومات عنهم خلال تصفحهم لمواقع الويب المختلفة. انظر:

Joan E. Rigdon, Internet Users Say They'd Rather Not Share Their "Cookies", Wall Street Journal, (Feb.14,1996), p.25.

[1] تقوم هذه التقنية بتحديد الهوية بشكل تلقائي بالاعتماد على جهاز يسمي "RFID Tags " وهو عباره عن كائن صغير يمكن إدراجه بالمنتجات أو الحيوانات أو الإنسان. يحتوي هذا الجهاز على شريحة مصنوعة من السيلكون وهوائي (انتينا) لكي يستطيع استقبال وإرسال البيانات والاستعلامات من خلال موجات الراديو.

G. Avoine, Sécurité de la RFID: comprendre la technique sans être technicien, in La sécurité de l'individu numérisé, Réflexions prospectives et internationales, sous la direction de S. Lacour, L'Harmattan, 2008, pp. 17-27.

[2] وهي وسيلة تتبع لجمع أكبر قدر من المعلومات السرية والخاصة عن طريق ما يعرف بانظمة جمع المعلومات (تشممها).

[3] وقد ورد عنشركة (كونسيومز انترناشيونال) استنادًا إلي استنتاجات تحقيق شمل 751 موقعًا أوربيًا وأمريكيًا علي شبكة الإنترنت أن: « كثير من الشركات جمعت كما وافرا من المعلومات الشخصية جدًا وغير الضرورية بخصوص المستهلكين»، وذكرت أن ثلثي المواقع الأمريكية التي شملتها الدراسة مازالت تطلب من مستخدمي الشبكة تزويدها بمعلومات شخصية بحتة.
د/ محمود عبد الرحمن، المرجع السابق، ص 108.

التي لا يقرأها عادة المستخدم قد يكون هناك تنازل صريح للفرد عن بياناته، فضلًا عما يقوم به الشخص بشكل يومي من إفصاح عن حياته الشخصية، وحالته المزاجية، آرائه السياسية وغيرها مما يعد معلومات لا يجوز للغير الاطلاع عليها إلا بموافقة صاحب هذه البيانات وعدم قراءة سياسات الخصوصية ينجم عنه استغلال البيانات الشخصية لمستخدمي هذه الشبكات[1].

وفيما يتعلق بمجال البحث العلمي، يمكن أن يمثل تجميع البيانات الشخصية شكل آخر لإساءة استخدامها، وبيان لذلك عند إجراء المرء للاختبارات عموما والاختبارات الجينية عبر الإنترنت علي وجه خاص، تقوم المعامل بتجميع العديد من البيانات الشخصية، التي يمكن استخدامها لبحوث خاصة أو في أغراض غير التي جمعت لها أو نقلها لجهات بحثية أخري، كما أن الأشخاص المعنيين لن يستطيعوا معارضة استخدام بياناتهم التي أدلوا بها بمجرد الحصول علي النتائج المطلوبة، وحتي لو مارس هؤلاء الأشخاص حقهم في الاعتراض علي معالجة بياناتهم في أغراض البحث العلمي فلن يكون اعتراضهم محل اعتبار يذكر في ظل عدم خضوع البحوث العلمية لأي تقييم أخلاقي[2].

المطلب الثاني

المخاطر المتعلقة باستخدام البيانات الشخصية

يقصد باستخدام البيانات الشخصية L'utilisation des données personnelles، أن يقتصر توظيف البيانات المجمعة علي غايات المعالجة، بحيث لا يتجاوز استخدام البيانات الشخصية حدود الأهداف المعلنة[3].

---

(1) ***Lori Andrews***, I Know Who You Are and I Saw What You Did: Social networks and the Death of privacy, NY: free press, 2012, p. 121-137.

(2) ***Elsa SUPIOT,*** Le consommateur de tests génétiques, un patient avisé ou berné ?, Rev. D.C., Octobre 2009, pp. 1582-1584.

(3) ***En ce sens. Cynthia CHASSIGNEUX***, Th. préc., nº 292, p. 160.

وعلى غرار المخاطر المرتبطة بجمع البيانات الشـــخصـــية، هناك أيضـــا مخاطر كثيرة ومتنوعة تحيط باســـتخدام هذه البيانات[1]، بعض منها يرجع إلي نتائج معالجة البيانات ذاتها، والبعض الآخر يرتبط بأهداف المعالجة، والبعض الثالث ينشأ من جراء تدفقها عبر شـبكة الإنترنت، وأخير قد تنتج عن تسـويق هذه البيانات. وهو ما سنتناوله في أربعة أفرع علي النحو التالي:

الفرع الأول: المخاطر المتعلقة بنتائج معالجة البيانات.

الفرع الثاني: المخاطر المرتبطة بالهدف من معالجة البيانات.

الفرع الثالث: المخاطر الناجمة عن تدفق البيانات عبر الإنترنت.

الفرع الرابع: المخاطر الناشئة عن تسويق البيانات.

الفرع الأول
المخاطر المتعلقة بنتائج معالجة البيانات

قد تكون معرفة نتائج معالجة البيانات الشـخصـية شـاقة في بعض الحالات المرتبطة بالبحث العلمي عموما والبحوث الوراثية خاصـــة أو أن معرفة نتائجها من شـــأنه أن يعرض الأشـــخاص المعنيين بها لقدر أكبر من المخاطر[2]. لذلك اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنســـا الأبحاث المتعلقة بالوراثة، ولا ســـيما المرتبطة بالهوس الذهني أو الفصام، هي علي قدر كبير من الحساسية، وبالتالي فإن معالجة البيانات الشـــخصـــية في إطار البحوث الجينية قد تعرض الشـــخص المعني بالبيانات وأقاربه أيضًا لأخطار جسيمة، وذلك برفض المجتمع لهم، إذا ما تم الكشف عن هذه البيانات، وبما تحمله من نتائج، تشـير إلي مرض وراثي لدي أصـحابها[3].

---

(1) ***Ibrahim COULIBALY***, Th. préc., p. 72.

(2) ***V. CNIL***, 8 ème Rapport d'activité 1987, Doc.fr. Paris, 1988. pp. 107-108 et 9 ème Rapport d'activité 1988, Doc. fr. Paris, 1989. pp. 156-157 (sur une recherche de l'INED sur les maladies génétiques rares).

(3) ***Idem.***

ولذلك يجب استخدام الاختبارات الجينية التي تسمح باكتشاف المعلومات الجينية في ظل ظروف دقيقة جدا[1].

وقد تكون نتائج الأبحاث الجينية في نهاية المطاف مؤسفة للشخص المعني بالبيانات أو سبب في حرمانه من آفاق العلاج، إذا ما تم العثور علي ملف معلوماته الجينية[2]، ويرجع ذلك إلي أن علم الصيدلة pharmacogénomique يٌمكن من خلاله التعرف علي مدي استجابة جسد المريض للتأثير الدوائي بالنظر إلي استعداده البيولوجي والوراثي، وبالتالي يمكن تصنيف الأفراد وفقا لاستعدادهم الجيني مثلاً علي القضاء على المخدرات في الدم بسرعات عالية أو تراكم الدواء في الجسم من دون القضاء عليها، ومن ثم تفهم أسباب رفض المريض للعلاج أو عدم استجابته للتأثير الدوائي[3].

أيضًا فإن الاستخدام الفعلي لنتائج البحوث الإحصائية التي شملت مجموعات من المراهقين من ذوي الأصول الإجرامية[4]، تفسر الرابط بين جنوح هؤلاء الأحداث وسلوكهم المعادي للمجتمع في مرحلة المراهقة[5]، حيث دعا البعض إلي الكشف المبكر عن الأطفال المعرضين لخطر الإنحراف، في حين رفض البعض الآخر خضوعهم لمثل هذا الفحص بحجة عدم الملائمة، وتدخل عوامل البيئة في

---

(1) ***Trudo LEMMENS et Lisa AUSTIN,*** « Les défis posés par la réglementation de l'utilisation de l'information génétique », www.isuma.net, Automne 2001, vol. 2, no 3, p. 31.

(2) ***V. Louise BERNIER***, Le développement de la pharmacogénomique. Quelques questions éthiques et légales, in Les pratiques de la recherche biomédicale visitées par la bioéthique, sous la direction de C. Hervé, B. M. Knoppers, P. A. Molinari, Dalloz, Collection pharmacogénomique. Quelques questions éthiques et légales, in Les pratiques de la recherche biomédicale Thèmes et commentaires, 2003, p. 98.
Voir également. ***Thiercelin (J-F)***, Place de la bioéthique dans la recherche et le développement d'un nouveau médicament, RGDM, numéro spécial « Dix ans des lois de bioéthique en France », Les Etudes Hospitalières, 2006, pp. 135-141.

(3) ***CCNE*** : Avis n° 25 du 24 juin 1991 sur l'application des tests génétiques aux études individuelles, études familiales et études de population. « Problèmes des banques d'ADN, des banques de cellules et de l'informatisation des données ». Disponible sur: https://www.ccne-ethique.fr/sites/default/files/publications/avis025.pdf

(4) ***Ehrenberg (A)***, Malaise dans l'évaluation de la santé mentale, Esprit, mai 2006, p. 89 et s.

(5) ***Pour une analyse des résultats cette recherche sur le plan statistique: Voir. Gauvrit (NICOLAS),*** Statistiques. Méfiez-vous!, Ellipses, 2007, pp. 186-190.

السلوك الإجرامي، أضف إلي أن الكشف المبكر عن الأطفال المعرضين للإنحراف، من شأنه انتهاك حرمة الحياة الخاصة لهؤلاء ولعائلاتهم[1].

الفرع الثاني

المخاطر المرتبطة بالهدف من معالجة البيانات

وبخصوص المخاطر المرتبطة بالهدف من معالجة البيانات الشخصية، فهي لا تتعرض لمشروعية الغرض من معالجة البيانات الشخصية – كما سيأتي لاحقا – وإنما لاحتمالات إساءة استخدام البيانات في غير الهدف المشروع[2]، والذي علي أساسه تم جمعها، أو إعادة استخدام هذه البيانات[3]. فاليوم هناك اتجاه قوي نحو عدم تحديد أهداف معالجة البيانات الشخصية بدقة وبصورة مسبقة، ولا سيما في المجالات الطبية، وغالبا ما يكون الهدف إنشاء نظام معلوماتي علي درجات عالية من التأمين، وفيما بعد يتم تحديد الأهداف، وهو ما يمثل الخطر الأساسي من

---

(1) ***Goldberg (M), et Padieu (R),*** Quelles règles déontologiques pour les enquêtes à visée de recherche ou de surveillance ? A propos de l'enquête sur la santé physique et mentale des écoles primaires parisiennes, p. 3. Disponible sur: http://hal.archives-ouvertes.fr/docs/00/22/21/18/PDF/Goldberg_MEdito-RESP-Final.pdf

(2) ***André Lucas, Jean Devèze, et Jean FRAYSSINET***, Op.cit., n° 11. p. 9.

(3) ولتوضيح خطورة إعادة استخدام البيانات يقول الأستاذ Yves Poullet أن بعض نظم الحجز الآلي للرحلات لدي شركات الطيران لديها رموز استخدامها قد يكشف عن بعض خصائص المسافرين، علي سبيل المثال، أهمية المسافر، كونه بالغًا أم قاصرًا، برفقة ولي الأمر أم لا، مدخن أم غير مدخن، مريض بالسكر أم لا، نوع الوجبة ، نوع الوجبة المقدمة لمسلم أم غير مسلم ..... إلخ، وتتجلي خطورة هذه البيانات فيما إذا تم إرسالها إلي وكالات السفر عموما، أو المنظمات والشركات العاملة معهم. ولنا أن نتخيل حجم الأضرار التي قد تصيب الأشخاص إذا ما تم نقل هذه البيانات إلي شركات التأمين.

Yves POULLET, Protection des données à cractere personnel et obligation de securite, p. 6. Étude Disponible sur: http://www.crid.be/pdf/public/4674.pdf

معالجة البيانات الشـخصـية؛ نظرًا لانتفاء الهدف من المعالجة وعدم تحديده بصـورة واضحة لا لبس فيها، الأمر الذي يضفي علي هذه المعالجة صفة عدم المشروعية[1].

كذلك أيضًـــا فإن غموض أهداف المعالجة أو وســعها من جانب المســئول عنها، والذي يلتزم بإعلانها – كما ســـيأتي لاحقًا – إلي اللجنة الوطنية للمعلوماتية والحريات، يعطيه مساحة كبيرة للمناورة[2]، كما أن ربط المعالجة بالعديد من الأهداف يصـــبح معها من المســـتحيل الحكم علي مشـــروعية هذه المعالجة، مما لا يعطي الأشخاص المعنيين ضمانة حقيقة علي بياناتهم محل المعالجة[3].

الفرع الثالث

المخاطر الناجمة من جراء تدفق البيانات عبر الإنترنت

لقد أتاحت تكنولوجيا الاتصـــالات عبر الحدود، للأفراد أن يعطوا بياناتهم ومعلوماتهم لجهات داخلية وخارجية وربما جهات ليس لها مكان معروف، وهو ما يثير مخاطر إســاءة اســتخدام هذه البيانات خاصـــة في الدول التي لا تتوافر فيها مســتويات الحماية القانونية للبيانات الشــخصــية. وقد لا تخدم القوانين الوطنية هذا الفرض، كما أن تضمينها نصوصا بشأن السيطرة علي نقل البيانات قد لا يكون فعالا في ظل غياب التنســـيق وضـــمان أن يكون نقل البيانات محكوما باتفاقات تكفل حمايتها أو تضمن توفير حماية مماثلة في الدول المنقول لها البيانات.

وتتســع المخاطر مع نشــوء ملاجي آمنة لا تقيد عمليات المعالجة بأي قيد ولا تتوافر عندها أي قيود علي جمع ومعالجة البيانات، ومن ثم تهرب إليها مؤسسات

---

(1) ***Jean HERVEG,*** " La gestion des risques spécifiques aux traitements de données médicales en droit européen", in Systèmes de santé et circulation de l'information. Encadrement éthique et juridique, Paris, Dalloz, 2006, p. 92.

(2) ***Marot (Pierre-Yves)***, Th. préc, p. 176.

(3) إذا أن تعدد أغراض المعالجة يؤدي للامحدودية البيانات لدي المسئول عن المعالجة، انظر في مخاطر هذا الموضوع:

Frayssinet (J), Loi « Informatique et libertés » et durée de conservation des données personnelles, note sous, CA Douai, 29 déc. 2006, M. Olivier Q., n° 060A 00107 (2), Rev. LDI, n° 28, juin 2007, pp. 27-29.

الأعمال في بيئة الإنترنت للإفلات من القيود القانونية علي معالجة البيانات الشخصية[1].

الفرع الرابع

المخاطر الناشئة عن تسويق البيانات الشخصية

لاشك أن المخاطر الناجمة من تجارة البيانات الشخصية هي الأكثر خطورة في وقتنا الحاضر بعد أن أصبحت المعلومات والبيانات الشخصية المسجلة لدي العديد من الجهات مثل شركات الهاتف والمصارف تجارة رائجة تتداولها شركات التسويق المحترفة في السوق المصري[2]، فسهولة جمع البيانات الشخصية وانخفاض تكاليفها في أغلب المجالات أغري الكثير علي التخصص في جمع ومعالجة وبيع هذه البيانات إلي الجهات التي تريدها[3]. مما يشكل خطرًا كبيرًا علي الأشخاص المعنيين بهذه البيانات حيث تصبح بيانات هؤلاء الأشخاص وخصوصياتهم سلعة تباع وتشتري لمن يملك الثمن وبغض النظر علي موافقتهم أو رفضهم[4].

كما يرتبط هذا الجانب – أيضًا – بشيوع استخدام الأفراد لخدمات مجتمع المعلومات مثل: محركات البحث أو مواقع التجارة الإلكترونية أو الشبكات

---

(1) د/ مروة زين العابدين صالح، المرجع السابق، ص 323.

(2) محمود عبد العظيم، بزنس البيانات الشخصية يغزو السوق المصرية، جريدة الاتحاد الإماراتية، تاريخ النشر: الأحد 08 يناير 2006، علي الرابط التالي:
http://www.alittihad.ae/details.php?id=44592&y=2006

(3) ***V. Cédric CREPIN***, Le correspondant informatique et libertés: un nouvel outil de régulation pour la protection des données à caractère personnel, mémoire de master professionnel mention droit de cyberspace, Université de Lille II, Année universitaire 2004-2005, p. 16. Disponiable sur:
http://www.droit-tic.com/pdf/correspondant_donnees_personnelles_crepin.pdf

(4) ***V. Cynthia CHASSIGNEUX***, Th. préc., pp. 64-65.
S'agissant de données de santé, voir, Liliane DUSSERRE, La commercialisation des informations médicales est-elle 'déontologiquement correcte'? Rapport adopté par le Conseil de l'Ordre des médecins lors de la Session des 29 et 30 juin 2000. Disponible sur:
https://www.conseil-national.medecin.fr/sites/default/files/commercialisation.pdf

الاجتماعية[1]، فالخدمات التي تقدمها هذه المواقع أو الشبكات والتي يبدو أنها مجانية لها في الواقع بعد اقتصادي، إلا وهو تسييل البيانات الشخصية لمستخدميها مقابل منحهم حق الولوج المجاني[2].

المطلب الثالث

المخاطر المتعلقة بحوسبة البيانات الشخصية

يقصد بحوسبة البيانات عمومًا، تحويل المعلومات والبيانات الشخصية إلي بيانات إلكترونية بواسطة تسجيلها علي دعامات ممغنطة، في صورة نبضات كهربائية، عن طريق استخدام الحاسوب، بحيث لا تقرأ إلا من خلاله[3]، 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 [4].

---

(1) إذ تعرض موقع التواصل الاجتماعي Facebook للعديد من الانتقادات بسبب سياسات الخصوصية والتي تسمح له بانتهاك خصوصية البيانات الشخصية لمستخدميه واستغلالها في الترويج للإعلانات عن طريق بيعها لشركات الإعلان، كذلك تطبيق Wathsapp الذي تعرض بدوره للعديد من الانتقادات علي أثر قيام عدد من المنظمات المهتمة بحماية البيانات والخصوصية بالكشف عن تقرير يُفيد قيامه بالنفاذ إلي كل الأرقام المسجلة علي هاتف المستخدم دون سؤاله. انظر:

http://almohakmoonalarab.ahlamontada.com/t96

Dutch and Canadian DPAs challenge What App's compliance with their privacy laws. at: https://www.privacylaws.com/Publications/enews/

(2) ***Murielle CAHEN***, Utilisation des données personnelles. Disponible sur: http://www.murielle-cahen.com/publications/donnees.asp

(3) ***En ce sens. Delphine (ROIGT)***, Appel à une méthode proportionnelle d'évaluation éthique et une réelle réflexion éthique dans le recherche ayant recours à des données et du matériel biologique, in systèmes de santé et circulation de l'information Encadrement juridique et éthique, sous la direction de la HERVE (C), KNOPPERS (B-M), MOLINARI (P-A) et GRIMAUD (M-A), Dalloz, 2007, p. 5.

(4) ***Yannis ZOUGHAILECH***, L'Informatisation des données de santé Considérations éthiques : Cas de l'AMP Vigilance, Master 2 Éthique médicale et bioéthique, Universite Paris Descartes, Faculté de Médecine, Année universitaire 2013-2014, pp.8-9. disponiable sur: http://www.ethique.sorbonne-paris-cite.fr/sites/default/files/memoire%20zoughailech.pdf

ونلفت الانتباه إلي أن الإنسـان قد عرف جمع ومعالجة البيانات الشـخصـية 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 حوسـبة البيانات الشـخصـية، فإن اسـتخدام الحواسـيب في معالجة هذه البيانات، ترتب عليه زيادة في حجم المخاطر، التي يتعرض لها الأشـــخاص المعنيون بهذه البيانـات[1]، بـالنظر إلي إمكـانيـات الحواسـيب الهائلة في جمع البيانات وقدرتها علي أعدادها وتجهيزها، بالإضـافة إلي سهولة نقلها عبر الشبكات المركزية أو من خلال شبكة الإنترنت[2].

كذلك يصـاحب عملية نقل البيانات الشـخصـية عبر هذه الشـبكات بعض المخاطر، والتي تتعلق بعدم قدرة شبكات الاتصـال علي توفير الأمان المطلق لسرية ما ينقل عبرها من بيانات، وإمكانية استخدامها عن بعد في الحصول علي المعلومات بصـورة غير مشـروعة، حيث لم تُحد وسـائل الأمان التقني من هذه المخاطر علي الرغم من تطورها[3].

---

(1) ***Isabelle (FALQUE-PIERROTIN)***, Production et diffusion des données à caractère personnel sur Internet : enjeux nouveaux et questions éthiques, in « Les données personnelles, entre fichiers nominatifs et jungle Internet. Actes de la journée d'études de l'Association des archivistes français, 17 mars 2009 », Gazette des archives, 2009/3, n° 215, journée d'études de l'Association des archivistes français, 17 mars 2009 », Gazette des archives, 2009/3, n° 215, pp. 175-178.

ولمزيد من التفاصيل حول مخاطر حوسبة البيانات الشخصية، انظر:

Yves POULLET, « La loi des données à caractère personnel: un enjeu fondamental pour nos sociétés et démocraties? », in La régulation des données personnelles, LEGICOM, n° 42 –2009/1, pp. 47-69; « La protection des données: un nouveau droit constitutionnel? Pour génération de réglementations de protection des données », Jurisletter, n° 3, octobre 2005, pp. 1-48. ***Voir également. Stéphanie LACOUR*** (dir.), La sécurité de l'individu numérisé. Réflexions prospectives et internationales, L'Harmattan, 2008.

(2) د/ مني تركي الموسـوي، الخصـوصـية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة، مجلة كلية بغداد للعلوم الاقتصادية، 2013، ص 10-11.

(3) د/ مروة زين العابدين صالح، المرجع السابق، ص 323.

أضـف إلي هذا أن مسـألة تأمين النظام المعلوماتي ليسـت بمنأي عن كل خطر، بالنظر إلي سهولة التسلل إلي هذه الأنظمة، أو تعرضـها لهجمات تهدف إلي تقويضـها من أجل الوصـول إلي البيانات، وهي من الأخطار القائمة، والتي تهدد النظام المعلوماتي بأكملة[1].

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 يسـمح للفاعل بالاطلاع علي البيانات التي يحويها النظام أو إدخال تعديلات عليها أو حذفها أو نسـخها لحسـابه الشـخصـي ومعالجتها مرة أخري، أو بيعها أواسـتخدامها لأهداف غير مشـروعة. وتتضـح الخطورة وبشـكل مضـاعف إذا ما كان النظام المعلوماتي يحوي بيانات لا يجوز جمعها أو معالجتها بداية إلا برضاء الشخص المعني بالبيانات كالبيانات الحساسة.

---

[1] الإشارة السابقة.

الفصل الثاني

الضوابط المقررة لحماية البيانات الشخصية

تمهيد وتقسيم:

اقتضت الحماية الجنائية للبيانات الشخصية وضع مجموعة من الضوابط لحماية الأشخاص المعنيين بمعالجة بياناتهم الشخصية، وتتمثل هذه الضوابط التي هي بمثابة ضمانات قررها المشرع الفرنسي لهؤلاء في نوعين من الضمانات: **أولهما**، إلزام المسئول عن المعالجة الآلية للبيانات ببعض الالتزامات التي تهدف إلي خضوع المعالجة إلي رقابة اللجنة الوطنية للمعلوماتية والحريات أو حصول المسئول عنها علي الترخيص من جهة المختصة بحسب الأحوال من الجهة، بالإضافة إلي المحافظة علي أمن البيانات الشخصية وسريتها من جهة أخري.

وثانيهما، منح الأشخاص المعنيين بمعالجة بياناتهم الشخصية مجموعة الحقوق في مواجهة المسئول عن المعالجة لضمان أن تتم معالجة البيانات الشخصية في أطار من الشفافية والنزاهة، بالإضافة لاصلاح كل ضرر يمكن أن يلحق بهذه البيانات من جراء التعدي عليها من قبل الغير.

ولا شك أن إقرار هذه الضمانات من شأنه أن يخلق نوع من التوازن بين حقوق الأشخاص المعنيين بمعالجة بياناتهم الشخصية من جهة، وبين الالتزامات الملقاة علي عاتق المسئولين عن هذه المعالجة من جهة أخري.

وعليه سوف نتناول في هذا الفصل مجموعة الالتزامات التي يتعين علي المسئول عن معالجة البيانات الشخصية مراعاتها واحترامها، وتلك الحقوق المقررة للأشخاص المعنيين بمعالجة بياناتهم الشخصية، وذلك في مبحثين علي النحو التالي:

المبحث الأول: التزامات المسئول عن معالجة البيانات الشخصية.

المطلب الثاني: الحقوق المقررة للأشخاص المعنيين بمعالجة بياناتهم.

المبحث الأول

التزامات المسئول عن معالجة البيانات الشخصية

ضمانا لاحترام حقوق وحريات الأشخاص وضعت القوانين الخاصة بحماية البيانات الشخصية مجموعة من المبادئ يتعين احترامها من قبل المسئول عن معالجة البيانات الشخصية وذلك خلال المراحل المختلفة لجمعها ومعالجتها، سواء تعلق الأمر بمعالجة آلية أو يدوية، كما يجب ألا تخضع البيانات الشخصية أو تكون محلًا لأي إجراء من إجراءات المعالجة إلا في إطار احترام هذه الإجراءات للمبادئ الأساسية لمعالجة البيانات الشخصية.

وعليه سوف نتناول مجموعة الالتزامات التي تقع علي عاتق المسئول عن معالجة البيانات الشخصية في مطلبين علي النحو التالي:

المطلب الأول: الالتزام بالإجراءات القانونية لمعالجة البيانات الشخصية.

المطلب الثاني: الالتزام بالمبادئ الأساسية لمعالجة البيانات الشخصية.

المطلب الأول

الالتزام بالإجراءات القانونية لمعالجة البيانات الشخصية

لكي تكتمل منظومة حماية البيانات الشخصية ألقت قوانين حماية هذه البيانات علي عاتق المسئول عن معالجة البيانات الشخصية بالكثير من الالتزامات، ويمكن تقسيم هذه الالتزامات إلي نوعين: **الأول،** التزامات سابقة علي إنشاء نظام معالجة البيانات. **والثاني،** التزامات لاحقة علي معالجة البيانات الشخصية.

وسوف نتناول هذه الالتزامات في فرعين مستقلين علي النحو التالي:

الفرع الأول: الالتزامات السابقة علي معالجة البيانات الشخصية.

الفرع الثاني: الالتزامات اللاحقة علي معالجة البيانات الشخصية

الفرع الأول

الالتزامات السابقة علي معالجة البيانات الشخصية

الالتزامات السابقة علي معالجة البيانات الشخصية، عبارة عن الإجراءات التي يتعين علي معالج البيانات اتخاذها قبل القيام بإنشاء نظام لمعالجة البيانات، وتتمثل هذه الالتزامات في وجوب أخطار اللجنة الوطنية للمعلوماتية والحريات بنظام معالجة البيانات المزمع إنشاؤه حتى يتسنى له معالجة البيانات، كما تخضع بعض صور المعالجة لشرط الحصول علي الترخيص. وهو ما سنتناوله كالآتي:

أولاً: أخطار اللجنة الوطنية للمعلوماتية والحريات:

نصت المادة 1/22 من القانون الفرنسي رقم 78-17 بشأن المعلوماتية والحريات، علي أنه: .... تخضع المعالجة الآلية للبيانات الشخصية للأخطار، بواسطة اللجنة الوطنية للمعلوماتية والحريات.

وطبقًا لهذا النص يتعين علي كل مسئول أن يتقدم بإخطار إلي اللجنة الوطنية سالفة الذكر، وذلك قبل القيام بمعالجة أي بيانات شخصية، وهو حكم عام يسري علي جميع المعالجات سواء كان القائم بها من أشخاص القانون العام أو من أشخاص القانون الخاص، طالما أنها تتم بصورة آلية[1].

والحكمة من هذا الإجراء أنه يمكن اللجنة الوطنية للمعلوماتية والحريات من ممارسة عدة أدوار: **أولها**، تستطيع بمقتضاه ممارسة دورها الإعلامي وكذلك الاستشاري للتوعية بأخطار هذه المعالجات علي الحريات والحقوق الأساسية للأفراد وكيفية تجنبها، **وثانيها**، تمكنها من ممارسة دورها الرقابي علي كافة المعالجة للآلية للبيانات الشخصية والتأكد من التزامها بالقانون[2]. **وثالثها**، يتعلق بما يحققه الإخطار

---

(1) ***Christiane FÉRAL- SCHUHL***, Cyber droit: le droit à l'épreuve de l'Internet , Dalloz, 2 ème éd, 2000. p. 59.

(2) ***V. Cynthia CHASSIGNEUX***, Th. préc. nº 495, pp 263-264.

من شـــفافية la transparence لمن يتم معالجة بياناتهم، من ثم تُشـــيع لديهم الطمأنينة من أن نظام المعالجة هذا سوف يحترم حقوقهم الأساسية وحرياتهم[1].

وتكريسًـا لمبدأ الإخطار المسـبق أكدت اللجنة الوطنية للمعلوماتية والحريات علي ضـــرورة قيام المســـئول عن المعالجة بهذا الإجراء، وذلك بمناســـبة قيام إحدي الجمعيات بإنشـاء موقع علي شـبكة الإنترنت يتضـمن تجميع للبيانات الشـخصـية للأعضاء بالجمعية بغرض إرسال نشرات دورية مشددة علي أنه كان يجب إخطار اللجنة الوطنية قبل إنشاء هذا الموقع[2].

وفي هذا الصدد ثار التساؤل حول كيفية توجيه الإخطار من قبل المسئول عن معالجة البيانات الشخصية إلي اللجنة القومية للمعلوماتية والحريات؟

الحقيقة أن المشرع الفرنسي لم يشترط وسيلة بعينها يتعين إتباعها للقيام بهذا الالتزام حيث يجوز ذلك بموجب خطاب موجه للجنة القومية للمعلوماتية (م 1/23 من قانون المعلوماتية والحريات)، بل إن المشـرع – وتسـهيلًا علي المسـئول– نص علي إمكانية توجيه هذا الإخطار بواســـطة رســـالة إلكترونية par voie

---

(1) ***Grévin ANTHONY***, les rapports entre les secret professionnel et le droit de la protection des des données personnelles, Mémoire de D.E.A informatique et droit, Université Montpellier I, Année Universitaire 2001/ 2002. p. 62. Disponible sur: http://www.droit-ntic.com/pdf/secretpro.pdf

(2) ***CNIL.*** Délibération 99-026 du 22 avril 1999. Deliberation portant modification de la norme simplifee nº 23 concernant les traitements automatises d'information nominatives relatives à la gestion des members des associations a but non lucrative régies par la loi du 1er juillet 1991, et Disponible sur: www.legifrance.gouv.fr/

كما اعتبرت اللجنة أن الاستبيان الاختياري الذي يقوم به الشخص عند الدخول للموقع أو الاستمرار عليه والذي يتطلب بعض البيانات الشخصية من قبيل المعالجة الآلية للبيانات الشخصية، كذلك عمليات تتبع الأثر الذي يقوم بها مورد الخدمة والذي يتمكن من خلالها من التعرف علي المواقع التي زارها المستخدم ووقت وتاريخ الزيارة وصفح تلك المواقع ويقوم بتخزين هذه البيانات والتي يتمكن من خلالها من تحديد شخصية المستخدم. وقد ألزمت اللجنة القومية للمعلوماتية والحريات تلك الجهات بإخطار العملاء بقيام الجهة باستخدام برامج Cookies حتي يتسني لها الاعتراض علي ذلك. راجع:

Christiane FÉRAL-SCHUHL, Op.cit., p. 58.

électronique موجهة للجنة تتضـــمن الإخطار بإنشـــاء نظام معالجة البيانات الشخصية[1].

وفور استلام الخطاب أو تلقي الرسالة يتعين علي اللجنة أن ترسل للمسئول إيصالًا، وأتاح للأخيرة عند الضرورة أن ترسل هذا الإيصال بوسيلة إلكترونية، ويجوز للمســئول عند اســتلامه لهذا الإيصــال القيام بإجراءات المعالجة التي أخطر عنها اللجنة، وإن كان القيام بواجب الإخطار لا يعفيه من مسئولياته[2].

كما ثار تساؤل آخر بشأن فحوي هذا الإخطار مفاده هو هل هناك عناصر أو بيانات يتعين علي المسئول معالجة البيانات التقيد بها عند تحرير هذا الإخطار المقدم لهذه اللجنة؟

الإجابة تكون بالإيجاب إذ لم يشــأ المشــرع الفرنســي أن يترك الأمر لحرية المسئول عن المعالجة في تحرير محتوي الإخطار، بل ضمن نص الفقرة الثانية من المادة 23 من قانون المعلوماتية والحريات عناصـر البيانات التي يجب أن يتضـمنها الإخطار، والتي يتعين علي المســئول التقيد بها عند تحرير هذا الإخطار، وهي كالتالي:

1- هوية وعنوان المسئول عن المعالجة أو ممثله القانوني، .... .

2- الغرض من المعالجة أو أغراض هذه المعالجة طبقا للمواد 25،26، 27 ، ووصف عام لمهامها.

---

(1) لذا إنشــئت اللجنة الوطنية للمعلوماتية والحريات موقعًا لها علي شــبكة الإنترنت لاســتقبال الإخطارات المتعلقة بإنشاء نظم معالجة البيانات الشخصية، عبر الرابط التالي:

www.cnil.fr

(2) ***Art. 23-I*** Modifié par Loi n°2004-801 du 6 août 2004: « La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi. Elle peut être adressée à la Commission nationale de l'informatique et des libertés par voie électronique. La commission délivre sans délai un récépissé, le cas échéant par voie électronique. Le demandeur peut mettre en oeuvre le traitement dès réception de ce récépissé; il n'est exonéré d'aucune de ses responsabilités».

3- إذا اقتضـــي الأمر، الترابط وعمليات الدمج أو أي شـــكل أخر من أشـــكال الاتصال مع المعالجات الأخري.

4- فئات البيانات الشـخصـية محل المعالجة وأصـلها، وكذلك فئات الأشـخاص المعنيين بهذه المعالجة.

5- مدة حفظ المعلومات المعالجة.

6- الإدارة ، أو الإدارات المسـئولة عن تنفيذ المعالجة، وكذلك فئات الأشـخاص الذين – بســـبب آدائهم لوجباتهم أو متطلبات وظائفهم- يحق لهم الولوج المباشر للبيانات المسجلة.

7- المستلمون أو فئات المتلقين المسموح لهم الإطلاع علي البيانات المسجلة.

8- الشـــخص أو القســـم الذي عن طريقه يمارس حق الولوج إلي البيانات المنصـــوص عليها في المادة 39، وكذلك الإجراءات المتعلقة بممارســـة هذا الحق.

9- الخطوات المتخذة لضمان تأمين المعالجات والبيانات، وكذلك ضمان سريتها المكفولة بنص القانون، وعند الاقتضاء الإشارة إلي مساعد القائم بالمعالجة.

10- إذا لزم الأمر نقل البيانات الشخصية لدولة ليست عضوًا في الاتحاد الأوروبي، تحت أي شـكل كان، باسـتثناء المعالجات التي لا يتم اسـتخدامها إلا لأغراض العبور علي الأراضـي الفرنسـية، أو أراضـي دولة أخري عضـو في الاتحاد الأوربي[1].

---

(1) ***Art. 30-I*** Modifié par Loi n°2006-64 du 23 janvier 2006: « Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent :

1- L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre Etat membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande;

2- La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions;

3- Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements;

4- Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement;

الاستثناءات علي وجوب الإخطار:

بعد أن أقر المشـــرع الفرنســـي – القاعدة العامة – وجوب قيام المســـئول بإخطار اللجنة القومية للحريات والمعلوماتية بالمعالجة، استثني المشرع بعض صور معالجة البيانات الشخصية من شرط الإخطار المسبق، وهي:

1- المعالجات التي تهدف إلي إنشـــاء ســـجل أو دفتر بموجب قواعد قانونية، ويكون الهدف من هذا الدفتر أو السجل إعلام الكافة، أو أي شخص له الحق في الحصـول علي المعلومة منه مادامت له مصـلحة مشـروعة في ذلك[1]. كالســـجل الذي يتم إنشـــاؤه لكي يقيد به المزارعين وفقا للقانون الزراعي، أو الســـجل التجاري الذي يتم إنشـــاؤها للتجار بحيث تتضـــمن بيانات عن كل تاجر[2].

2- المعالجات التي تتم بواســـطة الجمعيات أو الهيئات الأخرى، والتي لا تهدف إلي تحقيق الربح، وتتعلق بالمعتقدات الدينية والآراء الفلسـفية والسـياسـية أو

5- La durée de conservation des informations traitées;
6- Le ou les services chargés de mettre en oeuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées;
7- Les destinataires ou catégories de destinataires habilités à recevoir communication des données;
8- La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à l'article 39, ainsi que les mesures relatives à l'exercice de ce droit;
9- Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant;
10- Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5».

(1) ***Art. 22-II*** Modifié par Loi n°2016-1321 du 7 octobre 2016: «Toutefois, ne sont soumis à aucune des formalités préalables prévues au présent chapitre :
1- Les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime; »

(2) ***Benoit TABAKA et Yann TESAR***, Op. cit., p. 45.

الانتماء النقابي لأعضـــائها، بحيث تقتصـــر هذه المعالجات علي أعضـــاء الجمعية أو الهيئة، وعند الاقتضـــاء يمكن أن تشـــمل بيانات الأشـــخاص المتعاملين معها بشكل منتظم، وفي إطار ممارستها لنشاطها[1][2].مثل إنشاء ملف خاص داخلي بأعضـــاء كل حزب ســـياســـي، إذ يجوز للحزب تناول الأصـــول العرقية والآراء الســـياســـية والمعتقدات الدينية للأعضـــاء ومعالجة بياناتهم دون الحاجة للإخطار سالف الذكر[3].

3- المعالجات التي في إطار التعبير الأدبي أو الفني، أو في إطار ممارســـة مهنة الصحافة بشرط احترام القواعد المهنية لهذه المهنة[4].

ثانياً: الحصول علي الترخيص:

إذا كان المشرع الفرنسي ألزم المسئول عن معالجة البيانات بضرورة إخطار اللجنة القومية للمعلوماتية والحريات بنظام المعالجة المزمع إنشـــاؤه، إلا أنه وجد أن هناك معالجات للبيانات الشخصية – تتسم بالخطورة- لا يكفي فيها مجرد الإخطار حيث ألزم معالج البيانات ضرورة الحصول علي ترخيص قبل القيام بهذه المعالجة.

---

(1) ***Art. 8-II*** Modifié par Loi n°2016-1321 du 7 octobre 2016: «…
3- Les traitements mis en oeuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical:
- pour les seules données mentionnées au I correspondant à l'objet de ladite association ou dudit organisme
- sous réserve qu'ils ne concernent que les membres de cette association ou de cet organisme et, le cas échéant, les personnes qui entretiennent avec celui-ci des contacts réguliers dans le cadre de son activité; ».

(2) ***Voir par Example. CNIL***, Délibération n° 2010-229 du 10 juin 2010 dispensant de déclaration les traitements automatisés de données à caractère personnel mis en œuvre par des organismes à but non lucratif abrogeant et remplaçant la délibération n° 2006-130 du 9 mai 2006 (décision de dispense de déclaration n° 8). Disponible sur: https://www.legifrance.gouv.fr/

(3) ***Benoit TABAKA et Yann TESAR***, Op.cit., p. 46.

(4) ***Art. 67-II*** Modifié par Loi n°2016-1321 du 7 octobre 2016: « Le 5° de l'article 6, les articles 8, 9, 22, les 1° et 3° du I de l'article 25, les articles 32, et 39, le I de l'article 40 et les articles 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en oeuvre aux seules fins :
1° D'expression littéraire et artistique;
2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession».

وقد تعمد المشـرع الفرنســي إلا يضــع نظاما واحدًا للترخيص وإنما صــنف الترخيص علي درجات ثلاثة بحسب خطورة البيانات الشخصية التي سوف تخضع للمعالجة: أولها، ترخيص يمكن الحصـــول عليه من اللجنة القومية للمعلوماتية والحريات، وثانيها، ترخيص لا يمكن الحصول عليه إلا بمرسوم، وثالثها، لا يصدر إلا من مجلس الدولة. وهو ما سنتناوله كالآتي:

أ- الترخيص الصادر من اللجنة القومية للمعلوماتية والحريات:

حدد المشرع الحالات تتطلب معالجة البيانات الشخصية فيها إلي ترخيص من اللجنة القومية للمعلوماتية والحريات، وهي كالآتي:

1- المعالجات الإحصـــائية الآلية أو غير الآلية التي يقوم بها المعهد الوطني للإحصاء والدراسات الاقتصادية، أو أي جهة إحصائية وزارية، وذلك طبقا للقانون رقم 51-711 الصـــادر في 7 يونيه 1951، والمتعلق بالالتزام والتنسيق والسرية في مجال الإحصاءات[1].

2- المعالجة الآلية أو غير الآلية التي تظهر بطريق مباشـــر أو غير مباشـــر الأصول العرقية أو الآراء السياسية أو الدينية أو الانتماء النقابي للشخص المعني، أو تلك البيانات المتعلقة بحالته الصحية أو حياته الجنسية[2].

3- المعالجة الآلية للبيانات الجينية، باستثناء ما يكون ضروريا لأغراض الطب الوقائي أو التشخيص الطبي أو رعاية المرضي[3].

4- المعالجات الآلية أو غير الآلية التي تتعلق بالجرائم أو أحكام الادانة أو الإجراءات الأمنية باستثناء ما يتم منها بمعرفة معاوني القضاء وذلك بمناسبة قيامهم بمهام الدفاع عن الأشخاص الذين تتم معالجة بياناتهم[4].

---

(1) ***Art. 25-I. n°1 de la Loi n° 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(2) ***Art. 25-I. n°1 de la Loi n° 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(3) ***Art. 25-I. n°2 de la Loi n° 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(4) ***Art. 25-I. n°3 de la Loi n° 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

5- المعالجات الآلية التي يمكن أن تؤدي إلي حرمان بعض الأشـــخاص من الانتفاع بحق، أو الحصـــول علي قرض، أو إبرام عقد، وذلك بالنظر إلي طبيعة البيانات والهدف من المعالجة[1].

6- المعالجة الآلية المتعلقة :

- الربط بين الملفات الخاصـــة بواحد أو أكثر من الأشـــخاص الاعتبارية، التي تدير خدمة عامة، والتي تتوافق أهدافها مع المصالح العامة المختلفة.
- الربط بين الملفات الخاصة بأشخاص اعتباريين آخرين، والتي تختلف أهدافهم الرئيسية[2].

7- المعالجات التي تجري علي بيانات الرقم القومي للأشخاص الطبيعين[3].

8- المعالجات الآلية للبيانات التي تتضـــمن تقييمًا اجتماعيًا للصـــعوبات التي يواجهها الأفراد[4].

9- المعالجات الآلية التي تجري علي بيانات بيومترية لازمة للتحقق من هوية الأشخاص[5].

10- معالجة البيانات الشخصية بهدف إجراء بحوث علمية طبية[6].

11- معالجة البيانات الصـحية ذات الطابع الشـخصـي، والتي تهدف إلي تقييم ممارسات الرعاية والوقاية[7].

---

(1) ***Art. 25-I. nº4 de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(2) ***Art. 25-I. nº5 de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(3) ***Art. 25-I. nº6 de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(4) ***Art. 25-I. nº7 de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(5) **Art. 25-I. nº8 de la Loi nº 78-17** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(6) ***Art. 54-I. de la Loi nº 78-17*** Modifié par Loi n°2016-41 du 26 janvier 2016.

(7) ***Art. 62. de la Loi nº 78-17*** Modifié par Loi n°2016-41 du 26 janvier 2016.

12- نقل البيانات الشخصية لدولة ليست عضوًا بالاتحاد الأوروبي، ولا تقدم مستوي كاف لحماية الخصوصية والحريات الأساسية للأفراد المعنيين بهذه البيانات[1].

وفي هذا الصدد ثار التساؤل حول كيفية حصول المسئول عن معالجة البيانات الشخصية علي الترخيص من اللجنة القومية للمعلوماتية والحريات؟

يتم الحصـــول علي الترخيص من اللجنة القومية للمعلوماتية والحريات، وذلك بناء علي طلب يقدم إلي هذه اللجنة، والتي أعطاها المشرع الفرنسي مهلة شهرين للرد علي الطلب من تاريخ استلامه- يجوز تجديدها لمرة واحدة بقرار مسبب من رئيسها- وإذا لم يتلق الطالب ردًا من اللجنة بالإيجاب أو الرفض خلال هذه المدة، عُد الطلب مرفوضًا[2].

ونلفت الانتباه إلي أن المشرع الفرنسي لم يتطلب شروطًا خاصة في الطلب المقدم للحصول علي الترخيص، ومن ثم يجب أن يتضمن ذات البيانات المنصوص عليها في المادة 1/30 من قانون المعلوماتية والســـابق الحديث عنها في شـــأن الإخطار.

ب-الترخيص الصادر بمرسوم:

أورد المشرع الفرنسي في حالتين تتم فيها المعالجة لحساب الدولة، هاتين الحالتين يتعين الحصول فيها علي ترخيص يصدر بمرسوم وزاري طبقا للمادة 1/26 من قانون المعلوماتية والحريات، وهاتان الحالتان، هما:

- إذا كانت البيانات تتعلق بأمن الدولة أو بالدفاع عنها أو بالأمن العام[3].
- لمنع حدوث الجرائم الجنائية أو الاستدلال عن جريمة أو أو إثباتها أو ملاحقة مرتكبيها أو لتنفيذ العقوبات الجنائية أو التدابير الأمنية[4].

---

(1) ***Art. 62. de la Loi nº 78-17*** Modifié par Loi n°2016-41 du 26 janvier 2016.

(2) ***Art. 25-III. de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

(3) ***Art. 26-I. nº1 de la Loi nº 78-17*** Modifié par Loi n°2004-801 du 6 août 2004.

(4) ***Art. 26-I. nº2 de la Loi nº 78-17*** Modifié par Loi n°2004-801 du 6 août 2004.

ج- الترخيص الصادر من مجلس الدولة:

حدد المشرع الفرنسي في قانون المعلوماتية والحريات بعض صور معالجة البيانات التي يجب فيها الحصول علي هذا الترخيص من مجلس الدولة وهذه الحالات تضمنتها المواد 26،27،69 من القانون سالف الذكر، وهذه الحالات تتعلق أيضا بالمعالجات التي تتم لحساب الدولة، وبيانها كالآتي:

1- إذا كان الهدف منها المحافظة علي أمن الدولة أو الدفاع عنها أو الحفاظ علي الأمن العام، ويمكن أن تؤدي – بطريقة مباشرة أو غير مباشرة – إلي إظهار الأصول العرقية أو الآراء السياسية أو الدينية أو الانتماء النقابي أو تتعلق بالحالة الصحية أو الحياة الجنسية للشخص المعني[1].

2- إذا كان الهدف منها منع حدوث الجرائم الجنائية أو الاستدلال عليها أو إثباتها أو ملاحقة مرتكبيها أو تنفيذ العقوبات الجنائية أو التدابير الأمنية ويمكن أن تؤدي – بطريقة مباشرة أو غير مباشرة – إلي إظهار الأصول العرقية أو الآراء السياسية أو الدينية أو الانتماء النقابي أو تتعلق بالحالة الصحية أو الحياة الجنسية للشخص المعني[2].

3- إذا كانت المعالجة تتم لحساب الدولة، أو لحساب شخص معنوي عام، أو لحساب شخص معنوي خاص يقدم خدمة عامة، وتتضمن بيانات شخصية، من ضمنها الرقم القومي للشخص المعني[3].

4- إذا كانت المعالجة تتم لحساب الدولة، وتتضمن بيانات بيومترية ضرورية لتحديد هوية الشخص المعني[4].

5- إذا كانت المعالجة تتم لحساب الدولة، ويكون الهدف منها الحفاظ علي أمن الدولة أو الدفاع عنها أو الحفاظ علي الأمن العام، وتتضمن نقل البيانات

---

(1) ***Art. 26-II. de la Loi nº 78-17*** Modifié par Loi n°2004-801 du 6 août 2004.

(2) ***Art. 26-II. de la Loi nº 78-17*** Modifié par Loi n°2004-801 du 6 août 2004.

(3) ***Art. 27-I. nº1 de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 6 octobre 2016.

(4) ***Art. 27-I. nº2 de la Loi nº 78-17*** Modifié par Loi n°2016-1321 du 6 octobre 2016.

الشـخصـية لدولة ليسـت عضـوًا في الاتحاد الأوربي، ولا تقدم مسـتوي كافيًا لحماية الحريات والحقوق الأســـاســـية للأفراد في مواجهة معالجة البيانات الشخصية[1].

6- إذا كانت المعالجة تتم لحساب الدولة، ويكون الهدف منها منع حدوث الجرائم الجنائية أو الاسـتدلال عليها أو إثباتها أو ملاحقة مرتكبيها أو تنفيذ العقوبات الجنائية أو التدابير الأمنية، وكانت تتضمن نقل بيانات شخصية لدولة ليست عضــوًا في الاتحاد الأوربي ولا تقدم مســتوي كاف لحماية الحريات والحقوق الأساسية للأفراد في مواجهة معالجة البيانات الشخصية[2].

الفرع الثاني
الالتزامات اللاحقة علي معالجة البيانات الشخصية

لم تكتف قوانين حماية البيانات المقارنة بإلزام معالج البيانات اتخاذ إجراءات معينة قبل إنشاء نظام معالجة البيانات الشخصية، بل ألقت علي كاهله عدة التزامات لاحقة لحماية البيانات التي يقوم بمعالجتها؛ فمجرد قيامه بالإجراءات الســـابقة علي المعالجة لا يجعله حرًا في معالجة البيانات، وإنما هناك التزامات أخري تقيده أثناء القيام بهذه المعالجة.

وتتمثل هذه الالتزامات – الضــمانات اللاحقة علي إجراءات المعالجة – في توفير مستوي ملائم لتأمين البيانات الشخصية وحفظها، ومحدودية مدة حفظ البيانات الشخصية المعالجة، وهو وما سنتناوله كالآتي:

---

(1) ***Art.69. AL.2 de la Loi n° 78-17*** Modifié par Loi n°2004-801 du 6 août 2004.

(2) ***Art.69. AL.2 de la Loi n° 78-17*** Modifié par Loi n°2004-801 du 6 août 2004.

أولاً: تأمين البيانات الشخصية وسريتها:

يقصد بتأمين البيانات الشخصية وسريتها حفظها في بيئة مؤمنة تنأي بها عن الأخطار التي تتعرض لها البيانات[1] من حيث إمكانية إطلاع أي شخص عليها أو إفشائها أو التعديل فيها، الأمر الذي من شأنه أن يلحق الضرر بالأشخاص المعنيين بها[2].

وقد أقر المشرع الفرنسي هذا المبدأ في المادة 34 من قانون رقم 78-17 بشأن المعلوماتية والحريات، والتي نصت علي أنه : « يتعين علي المسئول عن معالجة البيانات الشخصية اتخاذ الاحتياطيات اللازمة، بالنظر إلي طبيعة البيانات، والمخاطر المتحصلة من المعالجة، وذلك للحفاظ علي أمن هذه البيانات، والحيلولة دون تشويهها، أو إتلافها، أو الولوج إليها من أشخاص غير المصرح لهم بذلك»[3].

يعد هذا الالتزام أحد المحاور الرئيسية لحماية البيانات الشخصية؛ لأن عدم وجود هذا الالتزام سيؤدي إلي زيادة المخاطر التي تتعرض لها هذه البيانات من حيث إمكانية اطلاع أي شخص عليها، أو إفشاء هذه البيانات أو التعديل فيها[4]. أو

---

(1) بالنظر إلي أن استخدام التقنيات الرقمية في حفظ البيانات الشخصية في صورة قواعد بيانات وارتباط قواعد البيانات بشبكة الإنترنت أدي لتعاظم خطر الدخول علي هذه البيانات من أشخاص غير مصرح لهم بالدخول إليها أو الاطلاع عليها.

(2) **V. En ce sens, Cynthia CHASSIGNEUX**, Th. préc. p. 164.

(3) **Art. 34 Loi nº 78-17** Modifié par Loi n° 2004-801 du 6 août 2004: « Le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.».

(4) د/ سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية– دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، العدد 9 السنة الثالثة، مارس 2015، ص 418.

وحول الدور الذي تقوم به CNIL لضمان أمن البيانات وسريتها، راجع:

CNIL, 36 ème Rapport d'activité 2015, Doc.fr. Paris, 2016. pp 28-29.

بمعني آخر أن هذا الالتزام يلقي علي عاتق المسئول عن معالجة البيانات اتخاذ ما يلزم من الإجراءات التي من شأنها الحفاظ علي أمن البيانات المستخدمة وذلك بالنظر إلي طبيعة هذه البيانات، وذلك للحيلولة دون الاعتداء عليها بالتشويه أو التدمير أو الاطلاع علي مضمونها من أشخاص غير مصرح لهم بذلك[1].

وقد تستلزم إجراءات الحماية – وفقًا للمفهوم السابق– نظم تقنية متعددة تختلف باختلاف الخطر الذي يتهددها؛ لذا يجب أن يكون معالج البيانات الشخصية مزودًا بتقنيات حماية ذات مستوي متقدم[2]، وأن يكون لديه فريق تقني عالي المستوي قادر علي اتخاذ الإجراءات المناسبة حال حدوث أي مشكلات يمكن أن تصيب البيانات.

كما يمكن اللجوء إلي تقنية تشفير La cryptographie البيانات وخاصة حال نقلها عبر شبكة الإنترنت أو عبر الشبكات المركزية وذلك لتوفير الحماية القصوي للبيانات الشخصية ضد أي محاولة لاعتراضها أو معرفة مضمونها[3]. كما يمكن أيضا اللجوء إلي إجراءات إخفاء الهوية أو تجهيل اسم الشخص المعني بالبيانات[4].

---

(1) ***N'Da Brigitte Etien-Gnoan***, L'encadrement juridique de la gestion électronique des données médicales, Thèse, Université Lille II, 2014, p. 90.

(2) كبرامج الحماية من الفيروسات، وبرامج الجدران النارية التي تحمي البيانات من الاختراق غير المشروع للنظام المعلوماتي ككل، بالإضافة إلي استخدام Password التي لا تسمح بالدخول للنظام المعلوماتي إلا للمصرح لهم بذلك.

Voir par Exemple, CNIL, Les guides de la cnil, la sécurité des données personnelles, 2010, p. 15, Disponible sur: http://www.cnil.fr

(3) ***Cynthia CHASSIGNEUX***, Th. préc., nº 309, p. 166.

ولمزيد من التفاصيل حول هذا الموضوع، راجع:

Serge GUINCHARD, Michèle HARICHAUX et Renaud DE-TOURDONNET, Internet pour le droit, Paris, Montchrétien, 1999, p. 165 ets; ***Pierre KAYSER,*** La protection de la vie privée par le droit, Economica, Presses universitaires d'Aix-Marseille, 3è éd., 1995. p. 21.

(4) ***V. Claude BOURGEOS***, L'anonymat et les nouvelles technologies de l'information, Universite Paris V, Thèse, 2003, p. 11; ***Cynthia CHASSIGNEUX***, La protection des données personnelles en France, Lex Electronica, vol. 6, n°2, hiver 2001, nº 59. p. 17.

وفي ذات السياق نود أن نشير إلي أن فضيحة أدورد سنودن كانت سببًا رئيسيًا في تطوير تقنيات التشفير Le chiffrement حيث بدأت الشركات في تنفيذ المزيد من آليات التشفير علي تدفق بيانات عملائها وقواعد البيانات، حتي أصبح HTTPS هو معيار ترتيب النتائج علي بعض محركات البحث. وبالمثل فإن الخدمات المقدمة للجمهور في مجال الاتصالات السلكية واللاسلكية سواء خدمة الرسائل أو صناعة الهواتف الذكية أصبحت تقنيات التشفير جزءًا من مكوناتها. كما أصبح من الشائع استخدام الرسائل الآمنة – المشفرة – بين الناس عامة والمراهقين خاصة، والتي تحول دون الوصول إليها من قبل مزود الخدمة علي سبيل المثال (الواتس أب، التليجرام .... الخ). كذلك أنظمة التشغيل الرئيسية للهواتف الذكية جوجل وأبل أصبحت تسمح لمستخدمها بتشفير البيانات المخزنة علي الهواتف الذكية والتي ليس للغير الوصول إليها وهو ما يسمي التشفير في يد المستخدم « à la main de l'utilisateur» والذي يحتاج إلي تنشيط هذه التقنية[1].

وقد أكدت محكمة النقض الفرنسية علي التزام المسئول عن معالجة البيانات بتأمينها بالوسائل المناسبة التي من شأنها منع نفاذ الأشخاص غير المصرح لهم بالاطلاع عليها[2]. كما رفضت اللجنة الوطنية للمعلوماتية والحريات السماح بإنشاء

---

(1) ***V. CNIL,*** 37 ème Rapports d'activité 2016, Doc.fr. Paris, 2017. p. 46.

لذلك أصبح التشفير Le chiffrement مقياسًا أساسيًا لحماية خصوصية وأمن البيانات، فالقواعد العامة لحماية الخصوصية وأمن البيانات تشير صراحة إلي التشفير باعتباره واحدًا من التدابير التقنية التي من شأن الأخذ بها إلي الوصول لمستوي عال من الأمن في معالجة البيانات الشخصية والذي من شأنه أن يحد من مخاطر اختراق البيانات. وبالمثل قانون المعلوماتية والحريات المعدل بالقانون الصادر في 7 أكتوبر 2016 بشأن الجمهورية الرقمية خص التشفير باعتباره واحدًا من تكنولوجيات حماية الحياة الخاصة Technologies protectrices de la vie privée والذي خولت اللجنة الوطنية للمعلوماتية والحريات بموجبه مهمة جديدة للارتقاء بأمن تكنولوجيا المعلومات.

CNIL, 37 ème Rapports d'activité 2016, précité. pp. 46-47.

(2) Crim. 30 octobre 2001, 99-82.136, Inédit. Disponible sur: https://www.legifrance.gouv.fr

أنظمة لمراقبة حضور وانصراف العاملين لعدة شركات تقوم علي أساس بصمة اليد نظرًا لغياب التأمين الكافي لهذه الأنظمة علي البيانات[1].

وتجدر الإشارة إلي أن هذا الالتزام– تأمين البيانات – يقع علي عاتق معالج البيانات منذ قيامه بجمعها إلي أن يقوم بتخزينها في أي شـــكل بمعني أن يظل هذا الالتزام مســـتمر وملازم لأي إجراء من إجراءات المعالجة[2]. كما لا يقتصـــر هذا الالتزام علي تأمين البيانات من دخول الغير للاطلاع عليها، وإنما يمتد ليشـــمل تأمينها من أي خطر قد يهدد وجودها، كتدميرها نتيجة لحادث تقني أو عمل تخريبي أو العبث بها أو تغييرها[3].

ثانياً: محدودية مدة حفظ البيانات الشخصية:

يقصـــد بمبدأ محدودية مدة حفظ البيانات الشـــخصـــية Principe de durée limitée de conservation de données personnelles، بالا يحتفظ معالج البيانات بها مدي الحياة أو لفترة زمنية مطلقة، إذ ينبغي أن تتحدد مدة الحفظ بشـــكل مؤقت علي ضوء الغايات المرتبطة بالهدف من المعالجة الآلية للبيانات[4]. حيث يرتبط هذا المبدأ بأحد الحقوق الأساسية للأشخاص ألا وهو الحق في الدخول في طي النسيان Le droit à l'oubli [5]، والذي يهدف إلي حماية هؤلاء الأشـــخاص من مضـــايقتهم

---

(1) ***Pierre PIAZZA et Ayse CEYAN,*** L' Identification biométrique: Champs, acteurs, enjeux et controversies, Éditions de la Maison des sciences de l´homme, 2014. p. 270.
poour plus de precisions, cf: CNIL, Communication de la CNIL relative à la mise en oeuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données. 28 December 2007. pp 7-8. Disponible sur: https://www.cnil.fr/sites/default/files/typo/document/Communication-biometrie.pdf

(2) ***Cynthia CHASSIGNEUX***, Th. préc., nº 308. pp 165-166.

(3) ***Benjamin EGERT,*** Les problemes juridiques des logicielsindiscrets, mémoire de D.E.A informatique et droit, faculté de droit, Univesité Montpellier I, 2002, p.81. Disponible sur: http://www.juristic.net

(4) ***Marie-Laure LAFFAIRE***, Op. cit., p. 204.

(5) ***Raymond LINDON***, Dictionnaire juridique: les droits de la personnalité, Dalloz. Paris, 2003, p. 271.

ولمزيد من التفاصيل بخصوص الحق في الدخول في طي النسيان، انظر:

طوال حياتهم، من خلال بياناتهم، التي تحويها الملفات الخاصة بهم بحيث تخرج من هذه الدائرة المغلقة لتسقط في دائرة النسيان[1].

وقد نصت المادة 5/6 من قانون المعلوماتية والحريات الفرنسي لسنة 1978 المعدل بالقانون رقم 801 لسنة 2004 الصادر في 6 اغسطس 2004 علي أن يتم الاحتفاظ بالبيانات الشخصية بشكل يسمح بتحديد هوية الأشخاص المعنيين، خلال فترة لا تتجاوز المدة اللازمة لتحقيق الغاية التي من أجلها تم جمع هذه البيانات ومعالجتها[2].

وبذلك لم يترك المشرع الفرنسي تحديد مدة حفظ البيانات الشخصية لمحض إرادة المسئول عن معالجة هذه البيانات، وإنما وضع ضابطًا لتحديد هذه المدة علي كل معالج الالتزام به مؤداه تحديد مدة الاحتفاظ بالبيانات الشخصية بالفترة الضرورية لتحقيق الغايات التي تم جمعها من أجلها ومعالجتها فيما بعد.

وحرصاً من المشرع الفرنسي في ألا تستخدم الغاية من تحقيق الهدف من المعالجة – كضابط في تحديد فترة الاحتفاظ بالبيانات– مبررا لمدّ مدة الاحتفاظ بالبيانات دون مبرر، ألزم المشرع الفرنسي المسئول عن معالجة البيانات، بضرورة

Charlotte HEYLLIARD, Le droit à l'oubli sur Internet, Mémoire de Master 2 recherch, Mention DNP, l'Université Paris-Sud, Faculté Jean Monnet-Droit, Économie, Gestion, Année Universitaire 2011-2012; ***Alain BENSOUSSAN***, Le driot à l'oubli sur Internet, 6 février 2010 Gaz. pal. nº 37, p.3; ***Christian CHARRIERE- BOURNAZEL***, Propos autour d'Internet: l'histoire et l'oubli, Gaz. pal, 21 avril 2011, nº 111, p.6; ***Guillaume DESGENS-PASANAU***, Le driot à l'oubli existe-t-il sur Internet?, Expertise nº 343, janvier 2010; ***Agathe LEPAGE***, Le driot à l'oubli: une Jurisprudence tâtonnante, Recueil Dalloz 2001, p. 2079; ***Roseline LETTERON***, « Le droit à l'oubli », Revue de Droit Public et de la Science Politique. 1996. vol. 112, nos 1-3. 393 et ***Nathalie MELLET-POUJOL,*** Op.cit., nº 157. p.44.

(1) ***V. André Lucas, Jean Devèze et Jean FRAYSSINET,*** Droit de l'informatique et de l'Internet. P.U.F, 2001, p. 128; ***Théo HASSLER***, Droit de la personnalité: rediffusion et droit à l'oubli, Recuiel Dalloz, 2007, p. 2829.

(2) ***Article 6 Loi nº 78-17*** Modifié par Loi n°2016-41 du 26 janvier 2016**:**
« Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes ….
5°- Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées».

تضـمين الإخطار أو طلب الترخيص – بحسـب الأحوال– المُقدم إلي اللجنة الوطنية للمعلوماتية والحريات بندا، يحدد فيه علي مدة حفظ البيانات وذلك لكي تخضع لرقابة هذه اللجنة[1].

المطلب الثاني

الالتزام بالمبادئ المتعلقة بمعالجة البيانات الشخصية

تخضـع معالجة البيانات الشـخصـية لمجموعة من المبادئ تتعلق في جانب منها بالشخص المعني بالبيانات، إذ تقتضـي ضـرورة الحصـول علي موافقة الشـخص المعني بالبيانـات علي إجراء المعالجـة، والجـانب الآخر يتعلق بـالمعالجـة ذاتها من ضـرورة التزامها بمبادي المعالجة كالمشروعية والتناسب والغاية والنزاهة والشفافية ... إلخ.

وعليه سـوف نتناول المبادئ المتعلقة بمعالجة البيانات الشـخصـية في فرعين علي النحو التالي:

الفرع الأول: موافقة الشخص المعني بالبيانات علي إجراء المعالجة.

الفرع الثاني: احترام المبادئ الأساسية الخاصة بمعالجة البيانات.

الفرع الأول

موافقة الشخص المعني بالبيانات علي إجراء المعالجة

مبدأ الموافقة المسبقة للشخص المعني بالبيانات علي إجراء المعالجة تقتضـي منا التعرض لمضـمون هذه الموافقة، وطبيعتها، وشـروطها، والاسـتثناءات التي ترد عليها، وذلك علي التفصيل التالي:

---

(1) ***Nathalie MELLET-POUJOL***, Op. cit., nº 158. p. 44.

أولاً: مضمون موافقة الشخص المعني بالبيانات:

يخضع تنفيذ معالجة البيانات الشخصية لشرط وجوبي وهو ضرورة الحصول علي موافقة الشـــخص المعني– وهو حكم عام يســـري علي جميع المعالجات – ؛ بالنظر لما تضـفيه هذه الموافقة من شـرعية علي معالجة البيانات Le lègitimité du traitement de data minig[1].

وقد نص المشرع الفرنسي في المادة السابعة من القانون رقم 78–17 بشأن المعلوماتية والحريات علي أن: « معالجة البيانات الشخصية تستوجب الحصول علي موافقة مسبقة من الشخص المعني بها، أو تلبي هذه المعالجة أحد الشروط التالية:

1– الامتثال لالتزام قانوني مفروض علي المسئول عن المعالجة.
2– الحفاظ علي حياة الشخص المعني بهذه البيانات.
3– تنفيذ مهمة لخدمة عامة يتولاها المسئول أو متلقي المعالجة.
4– تنفيذ عقد يكون الشخص المعني بالبيانات طرفًا فيه، أو تنفيذ إجراءات سابقة علي التعاقد بناء علي طلب الأخير.
5– تحقيق مصـــلحة مشـــروعة يســـعي إليها المســـئول عن المعالجة أو متلقي البيانات، شـــريطة عدم تجاهل المصـــالح أو الحقوق والحريات الأســـاســـية للشخص المعني بالبيانات.

وبناءً عليه يتعين علي من يقوم بمعالجة البيانات الشخصية أن يحصل علي موافقة **Le Consentement** الشـخص المعني بالبيانات قبل القيام بالمعالجة، وهو ما يسـتدعي أن يخبره بكل إجراءات المعالجة التي سـوف يقوم بها والغرض منها[2]، أن

---

(1) ***Sulliman OMRAJEE***, Le data mining : Aspects juridiques de l'intelligence artificielle auregard de la protection des données personnelles. Mémoire, Faculté de Droit Université Montpellier I, Année Universitaire 2001-2002, p. 26. Disponible sur: www.droit-ntic.com/pdf/Data_mining.pdf.

(2) ***V. Ibid***, p. 27. *et* ***Nathalie MALLET- POUJOL***, Op. cit., p. 37.

يخيره بعد ذلك بين قبوله القيام بهذه المعالجة أو رفضـــها[1]. وهو ما أكدته اللجنة الوطنية للمعلوماتية الحريات بصـدد رفضـها التصـريح للمجلس الممثل للمؤسـسـات اليهودية في فرنسا، بإجراء استبيان حول رأي اليهود هناك[2].

لكن المشرع الفرنسي لم يضـع تعريفًا لهذه الموافقة، كما لم يحدد شكلا معينًا لها، إلا أن التوجيه الأوربي رقم 95-46 بشأن حماية البيانات الشخصية قد تعرض لهذا الأمر، حينما عرف الموافقة في المادة الثانية منه بقوله بأنها: « كل مظهر للتعبير عن إرادة حرة ومحددة ومستنيرة، والتي عن طريقها يقبل الشخص المعني بها خضوعه لإجراءات معالجة البيانات الشخصية»[3].

ثانياً: طبيعة الموافقة وشروطها:

لم يحدد المشـرع الفرنسـي[4] في نص المادة السـابعة – سـالفة الذكر – نوع الموافقة المتطلبة من الشـــخص المعني بالبيانات، **لذا ثار التســـاؤل حول الطبيعة القانونية للموافقة، وكيفية التعبير عنها من الشخص المعني بالبيانات ؟**

بالنسـبة للشـق الأول من السـؤال فقد اختلف الفقهاء حول الطبيعة القانونية للموافقة المتطلبة من الشـــخص المعني بالبيانات حيث ذهب البعض إلي القول أنه

---

(1) ***Thierry LEONARD***, E-Marketing et protection des données à caractère personel, p. 16, Étude Disponible sur: https://www.droit-technologie.org/wp-content/uploads/.../17-1.pdf

(2) ***CNIL***, Délibération n° 2006-078 du 21 mars 2006 portant refus d'autorisation de mise en œuvre par le conseil représentatif des institutions juives de France d'un traitement automatisé de données à caractère personnel destiné à constituer un échantillon de sondage à partir d'un tri sur le nom des intéressés. Disponible sur: le site suivant: https://www.legifrance.gouv.fr/

(3) ***Art. 2/h Directive nº 95/46/CE*** le consentement de la personne concernée comme: « tout manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

(4) بالمقابل كان المشـرع التونسـي أكثر وضـوحًا حيث اشـترط الموافقة الصـريحة والكتابية من الشخص المعني بالبيانات، إذ نص الفصل 27 من القانون رقم 63 لسنة 2004 الصادر في 27 يوليه 2004 الخاص بحماية المعطيات الشـــخصـــية علي أنه: « ....، لا يمكن معالجة البيانات الشخصية إلا بالموافقة الصريحة والكتابية للمعني بالأمر، .... ».

يكفي مجرد الرضـا البسـيط بإجراء المعالجة حتي تتصـف المعالجة بالمشـروعية، إلا أنه اسـتدرك ذلك بأن إلقي عبء إثبات حدوث الرضـا عند حدوث النزاع علي عاتق المسئول عن المعالجة[1].

في حين لم يعول البعض علي شـكل التعبير عن الرضـا؛ إذا يجوز أن يتم التعبير عنه شـفاهة أو كتابة كما أنه يمكن أن يكون رضـاءً صـريحًا أو ضـمنياً، إلا أنه في جميع هذه الحالات سيقع علي عاتق المسئول عن المعالجة إثبات رضاء من قام بمعالجة بياناته الشخصية[2].

لكن الرأي الغالب يذهب إلي القول بضرورة توافر الرضا الصريح خاصة أن الرضـا البسيط لا يكفي لإمكان معالجة بعض فئات من البيانات الشـخصـية، كالتالي تضمنتها المادة الثامنة من قانون المعلوماتية والحريات – سالفة الذكر – حيث اشترط المشرع ضـرورة الحصـول علي الرضـا المسبق للشـخص المعني قبل القيام بإجراءات المعالجة[3]. فمجرد الموافقة الضـــمنية أو غيابها من باب أولي يؤدي إلي تطبيق العقوبة المنصـــوص عليها في المادة 226/ 19 عقوبات فرنســـي[4]. لذلك اعتبرت اللجنة الوطنية للمعلوماتية والحريات أن الرضـا الصـريح للشـخص المعني بالبيانات، هو ما يتم التعبير عنه كتابة[5].

---

(1) د/ أيمن مصطفي أحمد، المرجع السابق، ص 678.

(2) ***Thierry LEONARD***, Op.cit., p. 16.

(3) ***V. Art. 8-II*** Modifié par Loi n°2016-1321 du 7 octobre 2016.

انظر أيضا: د/ أسماء حسن سيد محمد رويعي، الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراة – حقوق القاهرة، 2013، ص 291.

(4) ***Jean PRADEL et Michel DANTI-JUAN,*** Droit pénal, droit pénal spécial, T. III Edition Cujas, 1995, p. 212.

(5) ***CINL***, 7 ème Rapport 1986, Doc. fr. Paris, 1987, p. 79.

وقد أوضـــحت CNIL أهمية الحصـــول علي موافقة الشـــخص كتابة وخصـــوصًـــا في حالة جمع البيانات التي تكشف بشكل مباشر أو غير مباشر أخلاق الأفراد وذلك بمعرض المداولة الخاصـة بإجراءات تسجيل البيانات في جهاز DMI2 والمتعلقة بطريقة انتقال فيروس نقص المناعة SAID

أما بالنسبة للشق الثاني من السؤال المتعلق بشروط هذه الموافقة أو كيفية التعبير عنها، فهي كالآتي:

1- يجب أن تكون هذه الموافقة صادرة عن إرادة حرة libre، وهو ما يقتضي أمرين: **أولهما**، خلو هذه الإرادة من أي ضغط أو إكراه. يمكن أن يشوبها[1]. **وثانيهما**، أن تؤسس علي دراية تامة بموضوع المعالجة الذي تنصب عليه الموافقة[2].

2- يجب أن تؤسس الموافقة علي دراية واعية ومستنيرة informé[3]: فالشخص المعني بالبيانات يجب أن يكون علي علم تام بجميع المعلومات التي تمكنه من التعبير عن موافقته[4]، وهو ما يعني التزام المسئول بإحاطة الشخص

لما تكشفه من السلوك الجنسي للاشخاص المعنيين. لذا يتعين الحصول علي موافقة خطية من المريض قبل معالجة بياناته.

CNIL, Délibération n° 96-055 du 18 juin 1996 cité par CNIL, 17 ème Rapport d´activité 1996, Dco. fr. Paris, 1997. P. 312.

(1) ***Sulliman OMRAJEE***, Op.cit., p. 27.

(2) وعليه إذا ما تمت معالجة البيانات الشخصية لشخص عديم الأهلية أو ناقصها، فلا يعفي المسئول عن المعالجة من شرط الحصول علي الموافقة المسبقة من الشخص المعني، حيث يتعين في هذه الحالة الحصول علي موافقة الممثل القانوني لهذا الشخص.

Voir par Exemle. ***CINL***, 19 ème Rapport d´activité, 1986, Doc. fr. Paris, 1998, p. 150.

وقد أكدت اللجنة القومية للمعلوماتية والحريات ضرورة الحصول علي موافقة الممثل القانوني لأي شخص غير قادر علي التعبير عن إرادته في كل حالة يتم فيها معالجة البيانات الشخصية له.

Voir par Exemle. CINL, délibération 98-061 du 16 juin 1998, Délibération portant avis sur la mise en oeuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives à l'occasion de l'enquête "Handicaps-Incapacités-Dépendance" menée auprès des personnes séjournant en institutions. Disponible sur: https://www.cnil.fr/

(3) ***Thierry LEONARD***, Op.cit., p. 17.

(4) ***Rosa JULIA-BARCEL, Étienne MONTERO et Anne SALAUN***, La proposition de directive européenne sur le commerce électronique: questions choisies , in Commerce électronique: le temps des certitudes, Cahiers du CRID., Numéro 17 Bruxelles: Académia Bruylant, 2001, p.1 et s.

المعني بهذه المعلومات، وإلا كانت الموافقة غير صـــحيحة؛ لأنها – أي الموافقة – قائمة علي غياب المعلومات أو المعلومات غير الصحيحة[1].

لذلك يشـــكل أي إعتداء علي الحريات من جانب المســـئول عن معالجة البيانات عموما والمتعلق بموافقة الشـخص المعني خصـوصًـا – وفقا للشـكل سـالف الذكر – ما يجعل الموافقة لاغية، هو ما يثير مسئولية القائم بالمعالجة[2].

3- يجب أن تكون الموافقة محددة spécifique بمعني أن تقتصـــر علي عملية معالجة واحدة، فإذا تم معالجة البيانات لهدف آخر غير الذي تم الحصـــول علي رضـا صـاحب البيانات عليه، انتفي الرضـا عن المعالجة الأخري؛ لأنها تمت دون رضا صاحب البيانات[3].

ثالثا: الاستثناءات التي ترد علي المبدأ:

إذا كان المشرع الفرنسي اشترط الحصول علي موافقة من يتم معالجة بياناته في (م 7 من قانون المعلوماتية والحريات) إلا أنه أقر خمس حالات في ذات المادة يجوز فيها للمســـئول عن معالجة البيانات الشـــخصـــية، تنفيذ هذه المعالجة دون الحصول علي موافقة الشخص المعني بها، وذلك في الحالات الآتية:

1- إذا كان هناك التزام قانوني يقع علي عاتق المســـئول عن المعالجة: فالقيام بمعالجة البيانات تنفيذًا لالتزام قانوني – سـواء كان مصـدر هذا الالتزام نصًـا تشريعيًا أم لائحيًا – يؤدي إلي إعفاء معالج البيانات من الحصول علي رضا

---

(1) ***Sulliman OMRAJEE***, Op.cit., p. 27.

(2) ***Art. 23/h Directive nº 95/46/CE***: Responsabilité comme: « Les Etats membres prévoient que toute personne ayant subi un dommage du fait d'un traitement illicite, o u de tout action incompatible avec les dispositions nationals prises en vertu de la présente directive a le droit d'obtenir du responsible du traitement reparation du prejudice subi».

(3) ***Sulliman OMRAJEE***, Op.cit., p. 27.

من يتم معالجة بياناته[1]. وهو نفس الحكم الذي تضـــمنته المادة 7 من التوجيه الأوروبي رقم 94-46 بشأن حماية البيانات الشخصية[2].

2- المحافظة علي حياة الشـــخص الذي يتم معالجة بياناته: كما لو تعلق الأمر بمعالجة بيانات شـخصـية تخص ضـحايا الحمي الناتجة عن نقل دم ملوث بغرض تحديدهم[3].

3- تنفيذ مهمة لخدمة عامة يتولاها القائم بالمعالجة: فمتي كانت المعالجة ضـرورية لتنفيذ إحدي المهام التي تدخل في إطار الصـالح العام أو ضـمن ممارسـة السـلطة العامة لنشـاطها فلا حاجة للحصـول علي رضـا الشـخص المطلوب معالجة بياناته. كما لو تعلق الأمر بالضـــرائب أو الجمارك أو ارتبطت تلك المعالجات بالأنشـــطة العامة للمؤســـســـات الخدمية، كمرفق الإسكان أوالتعليم أو الكهرباء أو المياه أو الغاز .... إلخ.

4- تنفيذ عقد يكون من تم معالجة بياناته طرفًا فيه: حيث يتعلق هذا الاســـتثناء بالعقود التي يكون فيها الشـخص الذي تمت معالجة بياناته الشـخصـية طرفًا فيهـا، والطرف الأخر هو القائم بمعالجـة هذه البيانـات ويلجأ الأخير لهذه المعالجة لتنفيذ العقد. كأن تقوم شـــركة بمعالجة بيانات عميل لديها متعاقد

---

(1) ***V. Marie-Claire PONTHOREAU,*** La directive 46-95 du 24 octobre 1995 relative à la protection à caractère personnes physiques à l'égard du traitement des données à caractère personel et à la libre circulation des ces données, Rev. F.D.adm., janv-fév. 1997, p. 144 et s.

(2) ***Art. 7/h Directive nº 95/46/CE***: « Les État members prévoient que le traitement des données à caractère personel ne peut être effectué qui si:

a- la personne concernée indubitablement donné son consentement, ou …….

c- il est nécessaire au respect d'une obligation légale à laquelle le responsible du traitement est soumis…».

(3) ***André Lucas, Jean Devèze et Jean FRAYSSINET,*** Op.cit., p. 133.

وتجدر الإشـارة إلي أن عبارة " المحافظة علي حياة الشـخص المعني" الواردة في النص الفرنسـي سـالف الذكر تعد أكثر دقة مما جاء بالمادة السـابعة بند 3 من التوجيه الأوربي رقم 46-95 بشـأن حماية البيانات الشـــحصـــية، حيث جاء الاســـتثناء فيها بعبارة " الحفاظ علي المصـــالح الحيوية للشـخص المعني ، وهي عبارة غير دقيقة توسـع من نطاق الاسـتثناء أكثر مما ينبغي، بالإضـافة لكونها لا تتماشي مع حالة الضرورة.

معها بهدف تقديم الخدمة له، أو توصـــيل ســـلعة إلي منزله تعاقد عليها معها[1]. كذلك العقود الشراء أو البيع التي تبرم عبر شبكة الإنترنت، وكانت معالجة البيانات ضرورة يقتضيها تنفيذ الالتزام بالتسليم أو القيام بالأداء محل العقد[2].

5- إذا كان من يقوم بالمعالجة يسعي لتحقيق مصلحة مشروعة: فإذا كان من يقوم بمعالجة البيانات الشخصية يسعي لتحقيق لهذه الغاية، فإن له معالجة هذه البيانات دون الحصول علي رضا الشخص المعني شريطة عدم تجاهل المصالح أو الحقوق والحريات الأساسية لهذا الشخص.

ونظرًا لغموض الاســتثناء الأخير، وعدم وضــع المشــرع لمعيار يمكن من خلاله تحديد المصـــلحة المشـــروعة للمســـئول عن المعالجة، ومتى تتعارض تلك المصلحة مع حقوق وحريات الشخص المعني؛ وجهت سهام النقد لهذا الاستثناء، حيث رأي البعض[3] أن الصياغة الواسعة لهذا الاستثناء فتحت الباب علي مصراعيه لهدم شرط الرضا الذي يتطلبه المشرع كشرط أساسي للقيام بعمليات معالجة البيانات الشخصية.

ولعل ذلك ما دفع التوجيه الأوربي رقم 46-95 بشـــان حماية البيانات الشـــخصـــية إلي تعداد بعض الأمثلة في الحيثية رقم 30 منه والتي تدخل في نطاق

---

(1) ***Benoit TABAKA et Yann TESAR***, Op.cit., p. 34.

(2) ***V. Thibault VERBIEST et Etienne WÉRY***, Le droit de l'Internet et de la société de l'information, Droits européen, belge et français, Bruxelles, Larcier, 2001. p. 34.

ويسري هذا الاستثناء علي كافة أنواع وأشكال العقود، كما ينطبق ايضًا علي الإجراءات السابقة علي تنفيذ العقود طالما ارتبطت معالجتها بهذه الإجراءات، وهو ما ينطبق علي المعاملات التي تبرم عبر شبكة الإنترنت، ومنها الإجرات الخاصة بتسجيل الطلبات أو الاشتراكات المقدمة من العملاء.

V. Christiane FÉRAL- SCHUHL, Cyber droit: le droit à l'épreuve de l'Internet, Dalloz, 2 ème éd, 2000, p. 100 et s.

(3) ***Benoit TABAKA et Yann TESAR***, Op.cit., p. 34.

المصلحة المشروعة، والتي تبرر إعمال هذا الاستثناء، إلا أنه لم يضع – هو أيضًا – ضابطًا أو معيار يمكن من خلاله تحديد هذه المصالح المشروعة[1].

الفرع الثاني
احترام المبادئ الأساسية لمعالجة البيانات الشخصية

لم تكتف تشـــريعات حماية البيانات المقارنة بإلزام المســـئول عن معالجة البيانات بالحصـــول علي موافقة الشـــخص المعني علي إجراء المعالجة باعتبارها ضـــمانة ســـابقة علي تجميع هذه البيانات؛ بل ذهبت أبعد من ذلك حيث ألزمت المسـئول عن المعالجة بمجموعة من المبادئ يتعين عليه اتباعها عند جمع ومعالجة وتخزين هذه البيانات. كما نصت أيضا علي عدد من الحقوق لأولئك الذين يتم جمع بياناتهم الشخصية.

وتتعلق مبادئ حماية البيانات الشخصية بعامل المشروعية، والغائية، والنزاهة والشـفافية، والضـرورة والتناسـب، ودقة البيانات وجودتها... إلخ. وهو ما سـنتناوله كالآتي:

أولاً: مبدأ المشروعية:

يعد مبدأ المشروعية Le principe de légitimité من أهم المبادئ المقررة لحماية البيانات الشـخصـية ويفترض أمرين: أولهما، ضـرورة أن يكون تجميع هذه البيانات قد تم بطريقة مشـــروعة خالية من الغش والاحتيال. وثانيهما، أن يقتصـــر استخدام البيانات التي تم تجميعها علي الأغراض المشروعة [2].

---

(1) ***En ce sens. Marie-Claire PONTHOREAU,*** Art. préc, p. 141.

(2) ***V. Julien LE CLAINCHE***, La protection des données personnelles nominatives dans le cadre de la recherché dans le domaine de la santé. Comparaison du droit français et américain, Mémoire de D.E.A. Faculté de droit des sciences économiques et de gestion, Université Montpellier I, 2001, p. 46.

انظر ايضًا: د/ أشرف محمد إسماعيل، التقنيات المعلوماتية الحديثة وانعكاساتها علي حق العامل في الخصـــوصـــية، بحث مقدم لمؤتمر القانون والتكنولوجيا الذي نظمته كلية الحقوق بجامعة عين شمس في الفترة من 9–11 ديسمبر 2017، مجموعة أعمال المؤتمر – الجزء الثاني، ص 1354.

لذلك لا نستطيع إضفاء المشروعية علي أي عملية للحصول علي البيانات الشخصية إلا إذ تم إخبار صاحبها عن وجود تجميع لهذه البيانات وعن طريقة التجميع والغاية منها وأنواع البيانات التي تم تجميعها. إذ أن مشروعية تجميع البيانات مرتبط بإخبار من يتم جمع بياناته بهذا التجميع، فإن لم يتم إخباره بذلك قبل التنفيذ كان أي جمع للبيانات غير مشروع[1].

ونلفت الإنتباه إلي أن مبدأ المشروعية يرتبط بشكل عام بمبدأ أساسي آخر في ألا وهو مبدأ الشفافية والذي يستلزم في كل معالجة أن تكون بحسن نية وبعلم الشخص المعني، وأن تستند علي مبررات كافية ومشروعة، وهو ما يقتضي الحصول علي موافقة الشخص المعني، أو تكون لازمة لحماية مصلحة مشروعة لهذا الأخير أو للمسئول عن المعالجة[2].

والجدير بالذكر أن المشروعية دائما ما تكون متوافرة في المعالجات التي تتم من قبل السلطة العامة في الدولة، كلما كان إجراؤها ضروريًا لتنفيذ أحد مهامها، في حين تتطلب المعالجات الخاصة إلي موافقة الأشخاص المعنيين بهذه البيانات قبل إجراء المعالجة، أو يكون لدي المسئول عنها مصلحة مشروعة شريطة ألا تطغي علي مصالح هؤلاء الأشخاص[3].

نخلص مما سبق إلي أن أي تجميع للبيانات الشخصية دون علم أصحابها– باستثناء المعالجات التي تقوم بها السلطة العامة لتنفيذ أحد مهامها– يعتبر فعلا غير مشروع، ولذلك اعتبرت اللجنة القومية للمعلوماتية والحريات أن تجميع عناوين البريد

---

(1) ***V. Suliman OMARJEE***, Op. cit., p. 29.

(2) أبا خليل، الحماية الجنائية للمعطيات ذات الطابع الشخصي علي ضوء القانون المغربي والقانون المقارن، رسالة دكتوراة، كلية الحقوق – جامعة السلطان حسن الأول، 2010. متاح علي الرابط التالي: http://www.droitetentreprise.com

(3) ***CINL***, 11 ème Rapport d´activité 1990, Doc.fr. Paris, 1990, p. 27.

الالكتروني لمســتخدمي الإنترنت دون علم صــاحب البريد الألكتروني يعتبر تجميعًا غير مشروع للبيانات الشخصية[1].

ثانياً: مبدأ الغائية:

يقتضـــي مبدأ الغائية Le Principe de Finalité أن يكون تجميع البيانات الشخصية ومعالجتها وتخزينها أو نقلها لأطراف ثالثة قد تم لغايات محددة déterminé ومعلنة وشـــرعية، وأن تكون كل معالجة لاحقة متوافقة Compatibles مع هذه الغايات[2].

وبناء علي ذلك فإن مبدأ الغائية يستلزم أمرين: أولهما، ضرورة استناد جمع البيانات الشخصية علي غايات محددة، ومعلنة ومشروعة. ثانيهما، أن تحترم الغايات المجمعة علي أساسها البيانات الشخصية في كل معالجة لاحقة.

ترتيبا علي ما سبق لا يجوز تجميع البيانات الشخصية سواء كان الجمع لمجرد تجميع البيانات أو أن القائم به لا يعلم الهدف من وراء هذا التجميع؛ لأن تجميع البيانات الشخصية يجب أن يحدد بدقة وعلي أساس غايات محددة وبشكل واضح، حيث يلزم في كل تجميع لهذه البيانات أن يكون ضروريًا من أجل الوصول إلي الأهداف المقررة والمعلن عنها مسبقًا من قبل الجهة التي تقوم بجمعها، شريطة ألا تخرج هذه الأهداف المحددة والمعلنة عن المشروعية. الأمر الذي يقتضـي معه أن تتم المعالجة وفق الغايات التي علي أساسها تم تجميع هذه البيانات وعدم الخروج

---

(1) ***V. Suliman OMARJEE***, Op. cit., p. 31.

تأكيدًا لذلك قضـت محكمة النقض الفرنسـية بأن تجميع شـركة Fabrice X عناوين البريد الإلكتروني للأفراد دون علمهم يعتبر تجميع غير مشـروع للبيانات الشـخصـية ويسـتحق فاعله العقاب.

Crim., 14 mars 2006, Bull. Crim., 2006, nº 69, p. 267.

(2) ***En ce sens, Thiébaut DEVERGRANNE***, Le principe de finalité. disponiable sur: https://www.donneespersonnelles.fr/le-principe-de-finalite

عليها، وإلا تعرض المســـئول عن المعالجة للعقوبة المنصـــوص عليها في المادة 226-21 عقوبات فرنسي.

اتســـاقًا مع ذلك اعتبرت اللجنة الوطنية للمعلوماتية والحريات أن الاختبار الذي أجري علي عينة من دم المريض والذي يهدف إلي تقييم مدي فاعلية المنتج الدوائي بالنســبة لجينات هذا المريض، لا يســوغ اســتخدامه لاحقًا لتحديد البصــمة الوراثية للشخص أثناء بحث رابطة الأبوة[1].

ونلفت الانتباه إلي أن البيانات ذات الطابع الشــخصـــي ليســت خطرًا في ذاتها، ولكن الخطورة تكمن في اســـتخدامها والهدف من وراء معالجتها، فمثلاً إذا تم تجميع بيانات طبية بهدف إجراء بحوث علمي طبي فالغاية تعد مشـروعة، أما إذا تم تجميع البيانات لغرض تجاري أو للدعاية السياسية فتعتبر الغاية غير مشروعة[2].

تطبيقًا لذلك اعتبرت اللجنة الوطنية للمعلوماتية والحريات بفرنســا أن تحويل الملف الخاص بإدارة شـئون الموظفين EDF-GDF إلي الصـندوق المركزي للأنشـطة الاجتماعية لذات الهيئة بغرض إدارة الأعمال الاجتماعية غاية مشـــروعة، بالمقابل اعتبرت نقل ذات الملف إلى حزب ســياســـي انتهاك لمبدأ الغائية[3]. بالإضـــافة لما يشكله فعل الكشف غير المصرح به من انتهاك لموجبات السرية المهنية[4].

---

(1) ***V. CNIL***, 24 ème Rapport d'activité 2003, Doc.fr. Paris, 2004, p. 210.

(2) ***Julien LE CLAINCHE***, Th. préc., p. 46 et s.

(3) ***CNIL***, Délibération. 20 novembre 1984. Cité par. ***Frayssinet (J)***, Atteinte aux droits des personnes résultant des fichiers ou des traitements informatiques, J-Cl. Code pén, mai 2006. fasc. 10.

(4) ***Grévin ANTHONY***, Op.cit., p. 72.

أتساقا مع ذلك قضت محكمة استئناف باريس في حكمها الصادر في 31 مايو 1995 بعدم مشروعية استعمال ملفات العمال وعناوينهم الإلكترونية لغايات الدعاية السياسية، كما قضت- في الحكم ذاته – بأن المعلومات المسجلة علي برنامج الحاسب الآلي من أجل حجز تذاكر النقل لا يمكن استعمالها من طرف أرباب العمل لمراقبة أنشطة العمال.

C.A. Paris, 31 mai 1995, cité par, CNIL, Guide pour les employeurs et les salaries, 2008, p.3. Disponible sur le site suivent: http//www.cnil.fr

والجدير بالذكر أن المشرع الفرنسي علي غرار التوجيه الأوربي قد اعتبر أن المعالجات اللاحقة لغايات إحصائية أو لغايات البحث العلمي أو التاريخي تعد بمثابة غايات مطابقة للغايات الأصلية التي جُمعت علي أساسها البيانات، وذلك مع احترام المقتضيات القانونية المنصوص عليها في القانون.

ثالثاً: مبدأ النزاهة والشفافية:

يفترض مبدأ النزاهة والشفافية Le principe de loyauté et de transparence أن يكون تجميع البيانات الشخصية محل المعالجة الآلية قد تم عبر الوسائل القانونية العادلة والمشروعة[1]، الأمر الذي يقتضي أخبار الشخص المعني قبل الشروع في جمع البيانات بما سوف يتم لبياناته الشخصية من إجراءات معالجة[2].

فشفافية إجراءات المعالجة ونزاهتها تقتضي أخبار الشخص بوجود معالجة لبياناته الشخصية، وأساليب هذه المعالجة وإجراءاتها، والغرض منها، وهل هي وجوبية أم اختيارية؟ ومن هم المستفيدين من هذه البيانات، وأخبار الشخص بذلك يجب أن يتم قبل القيام بأي إجراء من إجراءات المعالجة، بمعني أخر يجب أن تكون المعلومات التي يحصل عليها الشخص المعني – فيما يتعلق ببياناته– دقيقة إلي أكبر قدر ممكن وشاملة لكل التساؤلات حتي يستطيع أن يمارس حقوقه التي نص عليها القانون، وعدم القيام بذلك يشكل جريمة [3].

وبناء علي ذلك فإن إغفال اطلاع الشخص علي هذه المعلومات يشكل ذات الجريمة، وهو ما ينطبق من باب أولي إذا كان تجميع البيانات الشخصية تم عبر

---

(1) ***Dans le mêm sens, N'Da Brigitte Etien-Gnoan***, Th. préc., p.84. et ***Thiébaut DEVERGRANNE***, Le principe de loyauté et de licéitè de la collecte données. disponiable sur: http://www.donneespersonnelles.fr/le-principe-de-loyaute-et-de-liceite-de-la-collecte-des-donnees

(2) ***N'Da Brigitte Etien-Gnoan***, Th. préc., p.84.

(3) ***Art. 226-18*** du code pénal : « Le fait de collecter des données à caractère personnel frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d 'amende. Les articles 226-18 à 226-2 traitent tous d'infractions connexes .

الوسائل غير المشروعة أو الاحتيالية، وهو ما ينطبق أيضًا بخصوص القيام بإجراء المعالجة الآلية للبيانات الشخصية رغم معارضة الشخص المعني [1].

كما تعتبر الممارسات غير المرغوب فيها كتجميع عناوين البريد الإلكتروني للأشخاص من خلال مقاهي الإنترنت، وغرف الدردشة، والقوائم البريدية، والمواقع المختلفة، دون علم أصحابها مخالفة لمبدأ المشروعية والشفافية والنزاهة في جمع ومعالجة البيانات، ويستحق فاعله العقاب[2].

رابعاً: مبدأ الضرورة والتناسب:

يقتضي مبدأ الضرورة والتناسب Les principes de nécessité et de Proportionnalité أن تكون البيانات الشخصية محل المعالجة متوافقة ومتناسبة مع الغاية التي من أجلها تم جمع هذه البيانات ومعالجتها، وبحيث لا تكون هذه البيانات متجاوزة لهذه الغاية[3]، بمعني آخر أنه لا يجوز تجميع بيانات غير متناسبة مع الغاية من تجميعها أو تكون هذه البيانات أكثر من اللازم بحيث لا يكون هناك حاجة لكل البيانات التي تم جمعها في ضوء الغاية من هذا التجميع[4].

وبناء علي ذلك يستوجب مبدأ الملاءمة والتناسب في كل معالجة للبيانات الشخصية أن تبني علي معطيات تجمعها علاقة مباشرة مع الغايات التي تم علي

---

(1) Crim., 28 septembre 2004: Condamnation pour délit de traitement pour délit de traitement de données nominatives malgré opposition en vertu de l'article 226-18 du Code Pénal. Des personnes ayant fait opposition par l'intermédiaire de la CNIL, de leur droit d'opposition à être maintenues les fichiers l'ASESIF (église de scientologie) ont néanmoins continué à recevoir des couriers postérieurement.

(2) ***V. Marie-Charlotte Roques-Bonnet***, Le droit peut-il ignorer la révolution numérique? Michalon, 2010. p. 223.

(3) ***Cynthia CHASSIGNEUX***, Th. préc., nº 286-287. p. 158.

(4) د/ سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – القسم الأول، مجلة الحقوق الكويتية، العدد 3 س 35، سبتمبر 2011، ص 422.

أساسها تجميع هذه البيانات ومعالجتها، دون أي إفراط أو تجاوز بحيث تقتصر علي البيانات الشخصية الضرورية فقط، التي تحقق الغرض من جمعها ومعالجتها[1].

وتظهر أهمية مبدأ الضـــرورة والتناســـب في تقييد نطاق جمع البيانات الشـــخصـــية علي الضـــروري منها ومعالجتها وربطها بالهدف الذي تم جمعها في الأساس من أجله، بحيث ينسجم أسلوب المعالجة في النهاية مع الغاية من جمع هذه البيانات، وبالتالي يظل الهدف من جمع البيانات حاكمًا ومقيدًا لكل إجراء من إجراءات المعالجة الشخصية بعد ذلك، بالإضافة إلي أنه يؤدي إلي عدم استخدام البيانات الشخصية بعد جمعها استخداما غير مبرر، أي غير متوافق مع الغاية مع جمعها[2].

وقد أكدت CNIL هذا المعني، بمناسبة رفضها إنشاء قاعدة بيانات بيومترية قائمة علي قراءة التقنيات الحيوية للأشخاص والمتمثلة في بصمة الأصابع، وذلك بغرض تأمين النفاذ الآمن والســـريع للعاملين بمبني المدينة الجامعية بأكاديمية ليل، حيث اعتبرت اللجنة، أن الهدف من تأمين ســـيولة النفاذ للأكاديمية لا يبدو في عموميته مبررا لمشـــروعية إنشـــاء قاعدة بيانات البصـــمات لجميع موظفي المدينة الجامعية[3].

---

(1) ***Nathalie MALLET-POUJOL***, Op. cit., p. 42.

(2) ***Benoit TABAKA et Yann TESAR***, Op.cit., p. 33.

(3) ***CNIL***, 21ème Rapport d'activité 2000, Doc. fr. Paris, 2001, p. 116.

بالمقابل لم تر CNIL غضاضة في الموافقة علي إنشاء نظام المراقبة البيومترية بهدف تأمين نظام طباعة الامتحانات والدخول لغرف الأرشيف في إطار الحاجة إلى المحافظة على سرية الامتحانات والمسابقات. إذا بات واضحًا قصر اللجنة استخدام التقنيات الحيوية على ما هو ضروريًا حيث تخضع كل حالة لتقييم مدي تناسب الوسائل المستخدمة مع الخطر المحتمل علي الحقوق والحريات الأساسية للأفراد، في ضوء الغرض من المعالجة. لمزيد من التفاصيل حول هذا الموضوع، راجع:
P. Leclercq, « La CNIL, garante de la finalité, de la loyauté et de la sécurité des données p ersonnelles », in Les libertés individuelles à l'épreuve des NTIC, Etudes réunies sous la direction de M.-C. Piatti, Presses Universitaires de Lyon, 2001, p. 122.

وفي ذات المعني أكدت المادة 1121-1 من قانون العمل الفرنسي علي أنه لا يمكن بأي حال تقييد حقوق الأفراد أو الحقوق الفردية أو الجماعية بقيود لا تبررها طبيعة المهمة، ولا تتناسب مع الغرض المنشود[1].

وبناءً عليه فقد رأت CNIL أن تركيب أنظمة لمراقبة أجهزة العاملين لا يجب أن يؤدي إلي أي مساس بحقوق وحريات الأشخاص أو تقييد لها، وألا تكون متناسبة مع الهدف الذي وضعت من أجله والمبرر بالمصلحة المشروعة، وهكذا فإن وضع كاميرات المراقبة الدائمة لمكان العمل لا يجب اللجوء إليه إلا في أحوال الخطر الخاص ولتأمين العاملين المعنيين، وهو ما ينطبق – أيضا – علي تثبيت أجهزة قراءة البصمات الشخصية، للتحكم في النفاذ لأماكن بعينها، حيث لا يمكن تبرير وجودها إلا لمواجهة ضرورة أمنية، في ظل غياب بدائل أقل تطفلا علي الخصوصية [2].

كذلك فإن قيام شركات التوظيف بتجميع بيانات شخصية عن المتقدمين لشغل الوظائف كالحالة الصحية ورقم الضمان الاجتماعي غير ضروري حيث إن تجميع هذه البيانات يتجاوز الهدف من المعالجة بعكس التسجيل الدقيق لعنوان أسرة المتقدم الذي يمكن تبريره بالمصلحة التي تعود عليه هو وأسرته[3].

نخلص مما سبق إلي وجود التزام علي عاتق المسئول عن معالجة البيانات الشخصية وفقًا لمبدأ الضرورة والتناسب، مفاده أن تكون البيانات الشخصية التي تم تجميعها ملائمة ومتناسبة وضرورية – غير متجاوزة– بحيث تنسجم هذه البيانات في النهاية مع الهدف الذي تم من أجله جمعها ومعالجتها.

---

(1) ***Art. L 1121-1***, ***Code du travail Français***: « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».

(2) ***CNIL***, Guid pour les employeurs et les salaries, 2010, pp 3-4. Disponible sur: https://www.cnil.fr/sites/default/files/typo/document/Guide_employeurs_salaries.pdf.pdf

(3) ***Ibid***. p.3.

خامساً: مبدأ دقة وجودة البيانات:

يقصـــد بمبدأ دقة وجودة البيانات Les principes de exactitude et de qualité des données أن تكون البيانات الشـخصـية محل المعالجة دقيقة وكاملة، ومحدثة mises à jour ، علي ضـوء كل تغيير أو تعديل يطرأ علي حالة الشـخص المعني بها[1].

وبناء علي ذلك يقع علي عاتق المسـئول عن المعالجة ليس فقط الالتزام بضـمان دقة البيانات طوال فترة المعالجة، بل تحديثها كلما تطلب الأمر ذلك، وإلا عد ذلك إضـرارًا بحقوق الشـخص المعني بالبيانات وحرياته؛ وذلك نتيجة تشـويه وتغيير معالم شخصيته ووصفها علي غير حقيقتها[2].

ونلفت الانتباه إلي أن دقة البيانات وجودتها قد تتوقف في بعض الأحيان علي الشـخص المعني حين يمارس الأخير الحق في الاعتراض أو التصـحيح، وهو ما يقتضي من المسئول عن معالجة البيانات السماح للشخص المعني بالتدخل عندما تكون هذه البيانات غير دقيقة أو ناقصـة أو مضـللة أو عفا عليها الزمن وذلك لتصـحيحها أو تعديلها، أو محو الخاطئ منها حتي تتطابق مع الواقع[3]، وتكون متوافقة مع الهدف من جمعها ومعالجتها.

وتطبيقًا لهذه الشـروط أبدت CNIL بعض الملاحظات علي اسـتخدام أنظمة المراقبة الألية للطرق بهدف مراقبة التصـرفات الاجرامية المحتملة لبعض العملاء، حيث اعتبرت اللجنة أن الأنظمة الآلية التي تسـتخدمها شـركة ALIS ليسـت من

---

(1) ***Dans le même sens. Thiébaut DEVERGRANNE***, L'exactitude et la qualité des données, Disponible sur: http://www.donneespersonnelles.fr/exactitude-et-la-qualite-des-donnees

(2) ***V. André Lucas, Jean Devèz et Jean FRAYSSINET,*** Op.cit., p. 127.
Voir aussi. CNIL, Deliberation nº 2006-103 du 27 avril 2006 portant autorisation unique de mise en oeuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire. Disponible sur: https://www.cnil.fr/fr/declaration/au-009-biometrie-acces-aux-cantines-scolaires

(3) ***Cynthia CHASSIGNEUX***, Th. préc., nº 317. p. 171.

معدات التحكم الآلي المشـــار إليها في المادة 9-130 من القانون رقم 2003-495 الصـــادر في 12 يونيو 2003 الخاص بالمرور، حيث رأت اللجنة أن أجهزة التحكم الآلي هي التي توفر على الأرجح ضـــمان دقة وســـلامة البيانات التي تمت معالجتها[1].

نخلص مما سبق إلي وجود التزام علي عاتق المسئول عن معالجة البيانات الشـخصـية وفقًا لمبدأ دقة البيانات وجودتها، مفاده التزام هذا المسـئول باتخاذ كافة التدابير المناسـبة التي من شـأنها تصـحيح البيانات الخاطئة أو إكمالها في حالة نقصـــها أو محوها إذا كانت غير مطابقة للحقيقة أو عفا عليها الزمن، وذلك كله بالنظر إلي الهدف الذي من أجله تم جمع هذه البيانات ومعالجتها.

المبحث الثاني
الحقوق المقررة للأشخاص المعنيين بالمعالجة

تمتد الحماية الجنائية إلي مرحلة ما بعد تجميع أو تخزين البيانات الشخصية داخل الحاســب الآلي، فلا تنتهي بإتمام التخزين. وباســتقراء قوانين حماية البيانات المقارنة يتضـــح لنا تقريرها مجموعة من الحقوق لمن تخصـــه البيانات يســـتطيع ممارسـتها في مواجهة المسـئول عن المعالجة، وهي عبارة عن طائفتين من الحقوق: **أولهما**، الحقوق المتعلقة بالإعلام والاطلاع. **وثانيهما**، الحقوق المتعلقة بالاعتراض والتصحيح.

وبصـفة عامة يمكننا القول أن هذه الحقوق تعبر عن شـكل جديد من حقوق الإنسان المعاصر، كالحق في الإعلام والحق في الشفافية والنزاهة[2] من ناحية، كما

---

(1) ***CNIL***, Deliberation n°2006-048 du 23 février 2006 portant autorisation de la mise en oeuvre par la société ALIS d'un traitement automatisé de données à caractère personnel au suivi des clients en infraction. Disponible sur le site suivant: https://www.legifrance.gouv.fr/

(2) ***André Lucas, Jean Devèze et Jean FRAYSSINET,*** Op. cit., p. 99.

أنها تجسد علي الجانب الآخر ضمانًا لحماية هوية هذا الإنسان، ولإصلاح كل ضرر يمكن أن يلحق بها من جراء التعدي عليها من قبل الغير[1].

وبناء عليه سوف نتناول الحقوق المقررة للأشخاص المعنيين بالمعالجة في مطلبين علي النحو التالي:

المطلب الأول: الحقوق المتعلقة بالإعلام والاطلاع.

المطلب الثاني: الحقوق المتعلقة بالاعتراض والتصحيح.

المطلب الأول
الحقوق المتعلقة بالإعلام والاطلاع

تتسق المبادئ الأساسية المتعلقة بحماية البيانات الشخصية بشكل عام مع القواعد القانونية المقررة لحماية الحق في الحياة الخاصة التي تكفل للفرد قدرًا من الاطمئنان علي صحة ما يتم معالجته من معلومات وبيانات شخصية.

من أجل ذلك نجد أن القانون الفرنسي رقم 87-17 بشأن المعلوماتية والحريات، قد منح الأشخاص المعنيين بمعالجة بياناتهم الحق في الإطلاع علي ما يتم تسجيله عنهم من بيانات، ذلك الحق الذي يعد امتدادًا طبيعيًا للالتزام بالإعلام الواقع علي عاتق معالج البيانات، واللذان يهدفان إلي مراقبة مدي احترام قواعد المعالجة التي نص عليها القانون، بالإضافة إلي تجنب الاعتداء علي هذه الحقوق وضمان سرية البيانات الشخصية للأفراد[2].

وعليه سوف نتناول كل من حق الإعلام والحق الاطلاع كل في فرع مستقل علي النحو التالي:

الفرع الأول: الحق في الإعلام.

---

(1) ***Pierre KAYSER,*** La protection de la vie privée par le droit, Op. cit., p. 491.

(2) ***En ce sens, Claudine GUERRIER et Merie- Christine MONGET***, droit de Sécurité des telecommunications, Collection technique et scientifique des télécommunications, Paris, édition springer, 2000, p. 245.

الفرع الثاني: الحق في الاطلاع.

الفرع الأول

الحق في الإعلام

أولاً: مضمون الحق في الإعلام:

يعد الحق في الإعلام Le droit d'informer أحد محاور الحماية الجنائية للبيانات الشخصية وهو يلقي علي عاتق من يقوم بمعالجة البيانات الأتزام بالشفافية؛ وذلك بأن يكشف عن كل ما يقوم به من إجراءات تتعلق بالبيانات الشخصية منذ تجميعها[1].

وقد اشترط المشرع الفرنسي في قانون المعلوماتية والحريات، ضرورة إعلام الشخص المعني بالبيانات، ببعض المعلومات عن الإجراءات الخاصة بالمعالجة، والتي من شأنها أن تعطي هذا الشخص فكرة واضحة ومسبقة عنها، تمكنه من اتخاذ القرار بقبول أو رفض إجراء هذه المعالجة. إذ نصت المادة 1/32 من القانون الفرنسي 78-17 بشأن المعلوماتية والحريات المعدلة بالقانون 1321 الصادر في 7 اكتوبر 2016، علي أن الشخص الذي يتم جمع بيانات شخصية متعلقة به يجب إعلامه، إلا إذا تم من قبل بواسطة المسئول عن المعالجة أو من يمثله:

1- بهوية المسئول عن المعالجة وعند الاقتضاء وهوية من يمثله.
2- بالغاية المتصلة بهذه المعالجة المخصصة لها تلك البيانات.
3- بالطابع الإلزامي أو الاختياري للإجابات.
4- بالعواقب المحتملة للخطأ في الرد.
5- بالمرسل إليهم أو الفئات المرسل إليها هذه البيانات.
6- بالحقوق المقررة به طبقا لأحكام القسم الثاني من هذا الفصل بما في ذلك تحديد المبادئ التوجيهية لمصير البيانات الشخصية بعد الوفاة.

---

(1) د/ سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية – القسم الثاني، مجلة الحقوق الكويتية ، العدد 4 س 36، ديسمبر 2011، ص 236.

7- عند الاقتضـــاء، الإجراءات المقترحة لنقل البيانات الشـــخصـــية لدولة غير عضو في الاتحاد الأوربي.

8- بالعمر الافتراضـــي لفئات البيانات التي ســـيتم معالجتها، وإن لم يكن ذلك ممكنا، المعايير المســـتخدمة لتحديد هذه المدة عندما يتم جمع هذه البيانات عن طريق الاستبيانات والتي يجب أن تنص علي الشروط الواردة في المواد 6-1،2،3 [1].

وبناءً عليه يقع علي عاتق المسئول عن إجراء المعالجة أو من يمثله الالتزام بإعلام الأشخاص المعنيين بالبيانات، ببعض المعلومات حول هذه المعالجة، وهو ما يشكل نوع من الحماية المسبقة للبيانات الشخصية التي حرص المشرع الفرنسي علي تقريرها[2]. والحكمة من تقرير هذا الالتزام علي عاتق المســـئول عن المعالجة، هي ضمان تأسيس موافقة الأشخاص المعنيين بهذه البيانات علي رضا مستنير، بشأن إجراءات جمع هذه البيانات ومعالجتها[3].

ويظل هذا الالتزام قائما أيضـــا علي عاتق المســئول عن معالجة البيانات أو ممثله في حالة تجميع المعلومات عن طريق شـــبكة الإنترنت، إلا إذا كان علي علم مســبق بأن البيانات الشـــخصـــية المتعلقة به يمكن أن تكون محل للتداول علي هذه

---

(1) La personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou son représentant: Art. 32.I :
1- De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant.
2- De la finalité poursuivie par le traitement auquel les données sont destinées.
3- Du caractère obligatoire ou facultatif des réponses.
4- Des conséquences éventuelles, à son égard, d'un défaut de réponse.
5- Des destinataires ou catégories de destinataires des données.
6- Des droits qu'elle tient des dispositions de la section 2 du présent chapitre dont celui de définir des directives relatives au sort de ses données à caractère personnel après sa mort.
7- Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.
8- De la durée de conservation des catégories de données traitées ou, en cas d'impossibilité, des critères utilisés permettant de déterminer cette durée.
Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6° ».

(2) ***Cynthia CHASSIGNEUX***, Th. préc., p. 183.

(3) ***Julien LE CLAINCHE***, Th. préc., p. 23.

الشـبكة دون مراعاة ضـمانات الحماية، أو إمكانية الوصـول إليها أو اسـتخدامها من قبل أشخاص غير مرخص لهم بذلك.

ثانياً: الاستثناءات علي الحق في الإعلام:

بالرغم من أن المشرع الفرنسي فرض التزام علي عاتق المسئول عن إجراءات المعالجة، بإعلام الأشـخاص المعنيين بهذه الإجراءات، إلا أنه استثني من نطاق هذا الالتزام مجموعة من الحالات:

أولها، معالجة البيانات الشـــخصـــية لأغراض البحث العلمي في مجال الصـحة، إذ نصـت المادة 1/53 من القانون الفرنسـي رقم 78-17 بشـأن المعلوماتية والحريات والمعدلة بالقانون رقم 41-2016 الصـادر في 26 يناير 2016، علي أن: معالجة البيانات الشـخصـية المخصـصـة لغرض البحث في مجال الصـحة تخضـع لأحكام هذا القانون، باستثناء المواد من 23 إلي 26 والمواد38،32 [1].

ثانيها، إذا كانت البيانات الشـخصـية التي يتم تجميعها ومعالجتها ضـرورية للدفاع الوطني وأمن الدولة والســـلامة العامة أو لغرض تنفيذ الأحكام الجنائية أو الإجراءات الأمنية.

ثالثها، معالجة البيانات الشـــخصـــية لغرض الوقاية من الجريمة أو التحقيق والتحري أو الملاحقة القضائية للجرائم الجنائية(م 6/32).

---

(1) ***Art. 53.I*:** « Les traitement automatisés de données à caractère personnel ayant pour finalité la recherche ou les études dans le domaine de la santé ainsi que l'évaluation ou l'analyse des pratiques ou des activités de soins ou de prévention sont soumis à la présente loi, à l'exception des articles 23 et 24, du I de l'article 25 et des articles 26,32 et 38».

وعليه لا يلتزم الباحث بإعلام الأشـخاص المعنيين بالبيانات بإجراءات المعالجة، طالما تعلق الأمر بالبحث في المجال الطبي؛ وذلك لأن المشـرع اسـتثني هذا المجال من الخضـوع لأحكام المادة 32 سـالفة الذكر والتي نظمت أحكام الالتزام بالإعلام المفروض علي عاتق المسـئول بالمعالجة أو من يمثله.

N'Da Brigitte Etien-Gnoan, Th. préc., p. 93.

ورابعها، فتتعلق بتعذر إعلام الشخص المعني، وخاصة عند معالجة بياناته وحفظها لأغراض إحصائية أو تاريخية أو علمية (م 3/32).

الفرع الثاني
الحق في الاطلاع علي البيانات

يعد الحق في الاطلاع **Le droit d'accès** علي البيانات الامتداد الطبيعي للالتزام بالإعلام الذي يقع علي عاتق معالج البيانات، حيث يخوِّل الحق في الاطلاع لمن تخصه البيانات مراقبة مدي احترام معالج البيانات للقواعد التي نص عليها القانون[1]. لذا يشكل هذا الحق نوعًا من الرقابة اللاحقة يمارسها الشخص المعني بنفسه علي معالج البيانات الشخصية[2].

وقد أعطي المشرع الفرنسي للشخص المعني الحق في الاطلاع علي بياناته الشخصية التي خضعت لإجراءات المعالجة وذلك لفحصها والتأكد من مطابقتها للواقع، ومدي اتساقها مع الأهداف التي من أجلها تمت معالجة البيانات الشخصية للفرد[3]. وبذلك يكمل هذا الحق منظومة الشفافية التي وضعها المشرع الفرنسي التي تسمح للشخص المعني بالتعرف علي كل ما يحدث للبيانات الشخصية[4].

وقد أورد المشرع الفرنسي تنظيمًا لحق الاطلاع وذلك في المادة 39 من قانون المعلوماتية والحريات، وسوف نتناول مضمون هذا الحق، ثم نبين إجراءات ممارسته، ثم نعقبه ببيان الاستثناءات التي ترد عليه.

أولاً: مضمون الحق في الاطلاع:

---

(1) ***Grévin ANTHONY***, Op.cit., p.75.

(2) د/ أيمن مصطفي أحمد، المرجع السابق، ص 717.

(3) ***Jean MORANGE,*** Manuel des droits de l'homme et libertés publiques, Paris, PUF, 2007, p. 171.

(4) د/ سامح عبد الواحد التهامي، ضوابط معالجة البيانات الشخصية، المرجع السابق، ص 75.

نص المشرع الفرنسي في المادة 1/39 من قانون المعلوماتية والحريات علي أن: كل شـــخص طبيعي أبرز هويته له الحق في أن يوجه تســـاؤلات للقائم بمعالجة البيانات بهدف الحصول علي المعلومات الآتية:

1- التأكد مما إذا كانت البيانات الشخصية المتعلقة به تخضع للمعالجة أم لا.

2- معلومات حول أغراض المعالجة، فئات البيانات الشـــخصـــية محل المعالجة والمستفيدين منها، أو فئات المستفيدين الذين سيطلعون علي هذه البيانات.

3- وعند الاقتضـــاء، المعلومات المتعلقة بالنقل المقترح للبيانات الشـــخصـــية لدولة ليست عضوا في الاتحاد الأوروبي.

4- إذا ما كان هناك اتصـــال متاح لدي معالج البيانات وبيانات خاصـــة به لدي معالج بيانات آخر وما مصدر تلك البيانات الآخري.

5- المعلومات التي تسمح بمعرفة دوافع المعالجة الآلية للبيانات، .... .

ترتيبـا علي ذلـك النص يحق للشـــخص المعني الاطلاع علي بيـانـاتـه الشخصية التي خضعت للمعالجة من قبل المسئول عن المعالجة، كما يحق له توجيه الاستفسارات اللازمة لهذا الأخير، والتي من شأنها أن تمكنه من تكوين فكرة واضحة عن مصير تلك البيانات ومدي اتساقها مع الواقع الخاص لهذا الشخص.

وقد أكدت اللجنة الوطنية الفرنســية للمعلوماتية والحريات CNIL أهمية الحق في الاطلاع، وذلك كان بمناسبة إنشاء نظام لمعالجة البيانات البيومترية التي تهدف لتنظيم دخول الطلاب لمطعم المدرســة، حيث أشـارت اللجنة إلي حق كل طالب في الاطلاع علي بياناته التي يتم معالجتها، فضـــلا عن تضـــمين هذا الحق ضـــمن الاستمارة الخاصة بالاشتراك في هذا النظام[1].

ثانياً: إجراءات ممارسة الحق في الاطلاع:

---

[1] ***CNIL,*** Délibération n° 2006-103 du 27 avril 2006, portant autorisation unique de mise en oeuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire, Disponible sur le site suivant: https://www.cnil.fr

لقد خوَّل المشـــرع الفرنســـي بموجب المادة 1،2/39 من قانون المعلوماتية والحريات لمن تخصـه البيانات الاطلاع علي بياناته الشـخصـية وذلك بموجب طلب يقدم إلي معالج البيانات يطلب فيه الاطلاع علي بياناته الشـخصـية، ولا يتقيد الطلب بشـروط خاصـة سـوي دلالته عن هوية مقدم الطلب من أن البيانات تخصـه، كما أنه ليس هناك شكل خاص – نموذج– للطلب[1].

ونلفت الانتباه إلي أن الاطلاع علي البيانات وإن كان حق مقرر لصـــالح الشـــخص المعني بها، إلا أنه في ذات الوقت التزام مقرر علي عاتق المســئول عن المعالجة يتعين أداؤه بصـــورة واضـــحة وبلغة مفهومة تتحقق معها الغاية من تقرير الحق في الاطلاع[2]، كما لا يقتصـــر تنفيذ هذا الحق علي الاطلاع أصـــل البيانات الشخصية التي خضعت للمعالجة بل يتجاوز ذلك إلي النتائج المتحصلة عنها[3].

وإذا مارس المسـئول عن المعالجة إخفاء للبيانات الشـخصـية المعالجة، أو كان هناك اختفاء لهذه البيانات، فالقاضـــي المختص، بما في ذلك قاضـــي الأمور المستعجلة، اتخاذ جميع التدابير لتجنب ذلك[4].

وداخل ممارســـة الحق في الاطلاع يمكن التمييز بين نوعين: أولهما، عن طريق طلب كتابي: حيث أتاح المشـرع الفرنسـي إمكانية حصـول الشـخص المعني علي نسـخة من بياناته الشـخصـية التي خضـعت للمعالجة متي طلبها وذلك نظير رسوم الحصول علي هذه النسخة والتي يشترط ألا تتجاوز تكلفة إعدادها[5].

---

(1) ***Benoit TABAKA et Yann TESAR***, Op.cit., p. 28.

(2) ***MADEF***, Op. cit., p. 24.

(3) ***CE***, 7 juin 1995, caisse régionale de crédit mutuel agricole de dordogne, caisse nationale de crédit agricole, AJDA, 1996, p.162.

(4) ***Jean Frayssinet***, Refus de la CNIL de supprimer les informations figurant dans un fichier des renseignements généraaux, AJDA 1995. p. 567.

(5) ***Art. 39-I/2, Loi n° 78-17*** Modifié par Loi n° 2004-801 du 6 août 2004: « Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction».

وثانيهما، الاطلاع بعين المكان الذي تمت فيه إجراء المعالجة، وبدون أن يطلب الشخص المعني نسخة من بياناته التي خضعت للمعالجة، وهنا يتعين إتاحة الوقت الكافي للأخير في فحص هذه البيانات وبما يسمح له بأخذ ملاحظات كاملة علي هذه المعالجة[1].

وسواء قدم الطلب كتابة أو بعين المكان، فإنه يجب أن يتضمن: الاسم الشخصي والعائلي وتاريخ الطلب، ونسخة من بطاقة الهوية كما يمكن تضمينه كذلك معلومات أخري إذا كان مقدم الطلب علي علم بها، فضلا عن ذلك يلزم أن يكون الطلب موقعا ومؤرخا[2].

ثالثاً: الاستثناءات علي حق الاطلاع:

بعد أن أعطي المشرع الفرنسي لمن يتم معالجة بياناته الحق في الاطلاع علي البيانات الشخصية، أورد ذات المشرع عدة استثناءات علي هذا الحق، وتتمثل هذه الاستثناءات في حالات ثلاث وهي:

الحالة الأولي: حفظ البيانات بغرض البحث العلمي أو التاريخي أو الإحصاء:

وفقا للمادة 2/39 من قانون المعلوماتية والحريات استثني المشرع من الخضوع للحق في الاطلاع والفحص المقرر للشخص المعني علي بياناته التي تتم في اطار البحث العلمي أو التاريخي أو الإحصائي بشرط أن تكون البيانات الشخصية المعالجة محفوظة بطريقة تخلو من شبهة الاعتداء خصوصية الأفراد المعنيين بها وألا تتجازو مدة حفظ هذه البيانات القدر الضروري اللازم لهذه المعالجة[3].

---

(1) ***Julien LE CLAINCHE***, Th. préc., p. 34.

(2) أبا خليل، الحماية الجنائية للمعطيات ذات الطابع الشخصي، المرجع السابق.

(3) ***Voir par exemple, Thiébaut DEVERGRANNE***, Droit d'accès et droit de communication des données, nº 5. Disponible sur: https://www.donneespersonnelles.fr/droit-acces-et-de-communication-des-donnees-personnelles

الحالة الثانية: الممارسة التعسفية لحق الاطلاع:

استثني المشرع الفرنسي من الخضوع للحق في الاطلاع، حالة الممارسة التعسفية لحق الاطلاع من قبل الشخص المعني، حيث أعطي المشرع للمسئول عن المعالجة الحق في الاعتراض علي بعض الطلبات التي يبدو عليها التعسف في استعمال الحق في الاطلاع ، كما لو تمثل الأمر في تكرار طلب الاطلاع بشكل منهجي دون مبرر[1]. وعند النزاع يقع علي عاتق المسئول عبء إثبات عدم معقولية الطلبات وتكرارها تقع علي المسئول عن المعالجة، وهي تخضع في النهاية لتقدير قاضي الموضوع[2].

الحالة الثالثة: المعالجات الخاصة بمهنة الصحافة أو التعبير الفني أو الأدبي:

وفقا للمادة 1/67 من قانون المعلوماتية والحريات المعدلة بالقانون رقم 1321-2016 الصادر في 7 أكتوبر 2016 استثني المشرع الفرنسي من الخضوع لحق الاطلاع علي معالجة البيانات الشخصية كل من الأعمال التي تتم في إطار الأعمال الأدبية و الفنية أو في إطار ممارسة مهنة الصحافة بشرط احترام القواعد المهنية للصحافة[3].

المطلب الثاني
الحقوق المتعلقة بالاعتراض والتصحيح

---

(1) ***Jean Frayssinet***, Conditions du droit daccès et de communication aux données figurant dans les fichiers des services des Renseignements généraux, AJDA 1994. P. 145; Francois Bossuroy. L´accès aux fichiers des Renseignements généraux, AJDA 2000. p. 446

(2) ***MADEF***. Op.cit., p. 25.

(3) ***Article 67-I, Loi n° 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016: « Le 5° de l'article 6, les articles 8, 9, 22, les 1° et 3° du I de l'article 25, les articles 32, et 39, le I de l'article 40 et les articles 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en oeuvre aux seules fins :
1° D'expression littéraire et artistique;
2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession».

لعل من أهم الضـمانات اللاحقة علي معالجة البيانات الشـخصـية، إقرار قوانين حماية البيانات الشخصية للشخص المعني الحق في الاعترض علي معالجة بياناته الشـخصـية، سـواء كان ذلك قبل جمع البيانات ومعالجتها، أو بعد إجراء المعالجة. بالإضـافة إلي حقه في تصـحيح هذه البيانات بما يجعلها مطابقة للواقع أو محوها وإلغاؤها.

وهذه الحقوق التي أقرتها تشـريعات حماية البيانات تمثل نوعًا من الرقابة علي معالج البيانات الشخصية يمارسها الشخص المعني بنفسه؛ لذا ينظر الفقه إلي أن ممارسـة هذه الحقوق بالشـكل الصـحيح من شـأنه أن يضـمن جودة البيانات الشـخصـية بشكل عام وضـمان دقة هذه البيانات بشكل خاص وبما يجعلها مطابقة ومتسقة مع الواقع الفعلي للبيانات[1].

وسوف نتناول كل من الحق في الاعتراض والحق في التصحيح كل في فرع مستقل علي النحو التالي:

الفرع الأول: الحق في الاعتراض.

الفرع الثاني: الحق في التصحيح.

الفرع الأول
الحق في الاعتراض

يعد الحق في الاعتراض **Le droit d'opposition** علي معالجة البيانات الشـخصـية تطبيقًا لحق الشـخص في احترام حرياته الأسـاسـية فيما يتعلق بمعالجة بياناته، ففي مواجهة التطور الهائل في وسـائل وطرق معالجة البيانات الشـخصـية، يعتبر الاعتراض وسـيلة يسـتطيع من خلالها الشـخص أن يعلن رفضـه لأي إجراء يتعلق ببياناته الشـخصـية[2]، لأنه يعلم حين يفصـح عن بياناته الشـخصـية أنه في

---

(1) د/ أيمن مصطفي أحمد، المرجع السابق، ص 713.

(2) **Sulliman OMRAJEE**, Op.cit., p. 33.

المستقبل يستطيع أن يعترض على أي إجراء يمس هذه البيانات ؛ لذا ينظر الفقه إليه علي أنه بمثابة حق الفيتو Veto للفرد ضد معالجة البيانات الشخصية [1].

وقد وضع المشرع الفرنسي تنظيمًا لحق الاعتراض في المادة 38 من قانون المعلوماتية والحريات، وسوف نتناول مضمون هذا الحق (أولا)، ثم نعقبه ببيان الاستثناءات التي ترد عليه (ثانيا).

أولاً:- مضمون حق الاعتراض:

نصت المادة 38 من قانون المعلوماتية والحريات علي حق الأفراد في الاعتراض علي معالجة بياناتهم الشخصية، بقولها: « كل شخص طبيعي له الحق في الاعتراض علي معالجة بياناته الشخصية، وذلك إذا كان هناك مبرر مشروع لهذا الاعتراض»[2].

وبناءً علي ذلك يمكن ممارسة الحق في الاعتراض في أي وقت، فيمكن أن يتم الاعتراض في أي مرحلة من مراحل المعالجة، سواء تم ذلك في مرحلة جمع البيانات برفضه الإفصاح عنها، أو تم في مرحلة لاحقة كأن يرفض مثلا نقلها لجهة أخري غير من قامت بجمعها[3].

تطبيقا لذلك قضت محكمة النقض الفرنسية علي أن معالجة البيانات الشخصية علي الرغم من الاعتراض علي ذلك هو أمر غير مشروع، فقد اعتبرت المحكمة أن تجميع عناوين البريد الالكتروني للأفراد علي الرغم من اعتراضهم يعتبر

---

(1) ***Idem; André Lucas, Jean Devèze et Jean FRAYSSINET,*** Op. cit., p. 114.

(2) ويجري نص المادة 1/38 من قانون الفرنسي رقم 17-78 للمعلوماتية والحريات والمعدل بالقانون 801-2004 الصادر في 6 أغسطس 2004 علي النحو التالي:

***Article 38-I*:** «Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement».

(3) ***Voir*, *Julien LE CLAINCHE***, Th. préc., p. 38; ***MADEF***, Op. cit., p. 27.

أمرًا غير مشـــروع[1]. كما أيدت الحكم بالغرامة علي إحدي مســـتشـــفيات الأمراض العقلية لمعالجتهم البيانات الصحية لبعض المرضي علي الرغم من اعتراضهم[2].

ولكن التسـاؤل الذي يفرض نفسـه في هذا المقام: هو : **هل يجوز للشـخص الذي عبر عن قبوله- المســبق- بمعالجة بياناته الشـــخصـــية بممارســـة حق الاعتراض علي هذا الإجراء بعد ذلك؟ وهل فرض المشـــرع الفرنســـي شـــكلاً معينا لممارسة الحق في الاعتراض ؟!**

الإجابة علي هذا الشـق الأول من السـؤال تكون بالإيجاب؛ وذلك لأن نص المادة 38 سـالفة الذكر من السـعة بحيث يشـمل حالة اعتراض المعني علي معالجة بياناته بعد أن وافق من قبل علي هذه المعالجة[3]. وهو ما يتفق مع المادة 14 من التوجيه الأوروبي رقم 95-46 بشـأن حماية البيانات الشـخصـية والتي تخول للفرد الحق في ممارسة حق الاعتراض في أي وقت[4].

أما الشـق الثاني من السـؤال فالإجابة تكون بالنفي، إذ لم يشـترط المشـرع شكل معين للممارسة الحق في الاعتراض؛ فيجوز أن يتخذ أي شكل من الأشكال[5]، ولكن المهم أن يكون هناك تصـرف ايجابي حتي يعتبر حق الاعتراض قد تم التعبير عنه، فمجرد السكوت لا يفيد الاعتراض علي معالجة البيانات[6].

إلا أن المشرع الفرنسي لم يرد ترك الموضوع لحرية للإفراد المطلقة وإنما قيد حق ممارسة الاعتراض علي معالجة البيانات الشخصية بضرورة وجود مبرر مشروع

---

(1) Cass. Crim., 14 mars 2006, Bull. Crim., 2006, nº 69, p. 267.

(2) Cass. Crim., 28 sept 2004, Bull. Crim., 2004, nº 224, p. 801.

(3) ***Frédérique LESAULNIER***, Th. préc., p. 160.

(4) Directive nº 95/46 CE Art. 14: Droit d'opposition de la personne concernée Les États membres reconnaissent à la personne concernée le droit:
a- au moins dans les cas visés à l'article 7 points e) et f), de s'opposer à tout moment, pour des raisons prépondérantes et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement.

(5) ***Grévin ANTHONY***, Op. cit., p. 66.

(6) ***Sabine LIPOVESTSKT et Audry YANON- DAUVET***, Le devnir de la protection des données personnelles sur internet, Gaz. Pal. 12.13 septembre 2001. nº 255-256. p. 8.

لهذا الاعتراض، وعند النزاع يخضع هذا السبب من حيث وجوده ومشروعيته لتقدير قاضي الموضوع[1].

ثانياً:- الاستثناءات علي حق الاعتراض:

بعد أن أقر المشرع الفرنسي القاعدة العامة بحق الشخص المعني في الاعتراض علي معالجة بياناته، أورد ذات المشرع استثناءين علي هذه القاعدة، إذا نصت المادة 3/38 من قانون المعلوماتية والحريات علي أن : لا تسري أحكام الفقرة الأولي إذا كانت المعالجة تتم تنفيذا لالتزام قانوني، أو إذا كان تطبيق هذه الأحكام مستبعد بنص صريح في العقد الذي نظم معالجة البيانات بين الشخص والجهة التي ستقوم بمعالجة البيانات[2].

وعليه لا يجوز للشخص المعني ممارسة حق الاعتراض علي إجراءات معالجة بياناته الشخصية في حالتين: أولهما، إذا كانت المعالجة تتم تنفيذًا لالتزام قانوني يقع علي عاتق المسئول عن المعالجة أو حتي علي الشخص المعني بالبيانات. كما في حالة معالجة البيانات الشخصية لأغراض التسجيل في قاعدة بيانات الرقم القومي، أو معالجة البيانات الخاصة بممولي الضرائب، أو معالجة البيانات الشخصية للمجرم من قبل الجهات القضائية والأمنية في الدولة[3].

---

(1) Cass. Crim., 25 oct 1995, Bull. Crim., 1995, nº 320, p. 890.

وبالرغم من ذلك أورد المشرع الفرنسي حالتين لا يشترط فيهما إبداء أي تبرير لممارسة حق الاعتراض: **أولها،** إذا كانت هذه البيانات تستخدم لأغراض الدعاية – ولاسيما التجارية منها (م 2/38 من قانون المعلوماتية والحريات)، **وثانيها،** إذا كانت تلك البيانات تتعلق بالبحوث الطبية (م 1/56 من قانون المعلوماتية والحريات).

(2) ويجري نص المادة 3/38 من قانون الفرنسي رقم 17-78 للمعلوماتية والحريات والمعدل بالقانون 801-2004 الصادر في 6 أغسطس 2004 علي النحو التالي:

***Art. 38-III*:** « Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement».

(3) ***Grévin ANTHONY***, Op.cit., p.66.

وثانيهما، إذا ما تنازل هذا الشـــخص عن حقه في الاعتراض علي معالجة بياناته مقدمًا، فهذا التنازل يكون صـحيحًا بشـرط أن يرد في شـرط صـريح في العقد الذي ينظم معالجة البيانات. فمثلا إذا تعاقد شـخص مع شـركة الهاتف الجوال، فإن العقد قد يرد فيه تنظيم لمعالجة البيانات، كأن يحق للشـركة أن ترسـل رسـائل للعميل تعلمه بوجود خدمة معينة أو عطل في الشـبكة بمنطقة معينة، فإذا تضـمن هذا العقد شرطا صريحا للتنازل عن حق الاعتراض، فإن هذا الشرط يكون صحيحا[1].

ويشـترط لكي ينطبق هذا الاسـتثناء أن يكون هذا التنازل صـريحًا، بمعني أن يصدر عن إرادة حرة لا يشوبها أي عيب من عيوب الإرادة، وواعية لحقيقة ما تسعي إليه، بالإضـــافة لكونها مســـتنيرة بفضـــل الالتزام الملقي علي عاتق المســـئول عن المعالجة تجاه الشخص المعني بهذه البيانات[2].

الفرع الثاني
الحق في التصحيح والحذف

يعد الحق في التصـــحيح والحذف **le droit de réctification et de radiation** التتمة الضـرورية والملازمة للحق في الاطلاع علي البيانات وفحصـها[3]، وقد تقرر هذا الحق ليس فقط لحماية الحريات الفردية فقط وإنما أيضـــا للســـيطرة علي الآثار الخاطئة للمعالجة التي قد يقوم بها معالجون مبتدئون[4]، فكيف يمكن الســـماح

---

(1) د/ سـامح عبد الواحد التهامي، الحماية القانونية للبيانات الشـخصـية– القسـم الثاني، المرجع السابق، ص 253.

(2) د/ أيمن مصطفي أحمد، المرجع السابق، ص 717.

(3) ***V. Julien LE CLAINCHE***, Le traitement des données à caractère personnel dans le cadre d'un site web, Op. cit., p. 33.

(4) ***N'Da Brigitte Etien-Gnoan***, Th. préc., p.100.

للشخص بمراجعة وفحص بياناته الشخصية محل المعالجة، ولا يستطيع– في الوقت نفسه– تحديثها إذا كانت متقادمة، أو تصويبها حال كونها غير دقيقة، أو استكمال ما بها من نقص، أو حذفها إذا كان محظور جمعها، أو استخدامها، أو تخزينها؟!

أولاً: مضمون الحق في التصحيح والحذف:

نصت المادة 1/40 من القانون الفرنسي رقم 78–17 بشأن المعلوماتية والحريات علي حق الأفراد في التصحيح، بقولها: « لكل شخص طبيعي يدلل علي هويته، أن يطلب من المسئول عن معالجة البيانات بحسب الأحوال، تصحيح أو استكمال، أو تحديث، أو غلق، أو محو البيانات الشخصية المتعلقة به، والتي تكون غير دقيقة، أو ناقصة، أو غامضة، أو متقادمة، أو البيانات المحظور جمعها، أو استخدامها، أو تخزينها »[1].

ووفقا لنص المادة 40 سالفة الذكر لا يثبت هذا الحق للشخص إلا إذا كانت البيانات التي جري معالجتها من قبل المعالج غير دقيقة أو ناقصة، أو غامضة أو تم تجميعها أو استخدامها أو حفظها بطريقة محظورة. بالإضافة إلي أنه يجب علي الشخص المعني أن يدلل علي هويته حتي يجيبه معالج البيانات علي طلبه بتصحيح البيانات أو محوها علي حسب الأحوال[2].

وحرصًا من المشرع الفرنسي علي تكريس هذا الحق وضمانًا لفاعليته، أعطي المشرع لمن يطلب تصحيح البيانات أو محوها من معالج البيانات تقديم الدليل علي قيامه بالتصحيح أو المحو، فيكون من حق الشخص المعني الاطلاع علي البيانات بعد تصحيحها أو محوها للتأكد والاطمئنان علي صحة التعديل[3].

---

(1) ***Art. 40-I, Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016: « Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite».

(2) ***N'Da Brigitte Etien-Gnoan***, Th. préc., p.96.

(3) ***Benjamin EGERT,*** Op. cit., p.76.

وفي أغلب الأعم من الأحوال يقوم معالج البيانات بإعطاء نسخة من البيانات المعدلة لمن تخصـــه البيانات، وذلك للاطلاع عليها والاطمئنان علي صـــحة التعديل[1].

ونلفت الانتباه إلي أن الحق في تقديم طلب التصـــحيح أو المحوه لا يتقيد بحدود زمنية معينة إذا يمكن ممارســـته في أي وقت طالما توافرت حالة من حالاته التي نص عليها القانون[2]، لذا ذهب البعض للقول بأن: « معالج البيانات يقع عليه التزام بتصحيح البيانات وتحديثها دائما»[3].

والجدير بالذكر أيضا أن المشرع الفرنسي لم يحدد مدة معينة لمعالج البيانات ليُجِيب علي طلب من تخصـه البيانات بالتصـحيح أو المحو، إلا أنه يمكن القول إنه يجب أن يقوم بذلك دون تأخير والمعيار هنا هو المدة المعقولة[4]. وقد حددها المشرع التونسي بشهر من تاريخ تقديم الطلب[5].

ثانياً: الاستثناءات علي الحق في التصحيح:

بعد أن أعطي المشـــرع الفرنســـي للفرد الحق في الاطلاع علي بياناته الشـخصـية التي خضـعت لإجراءات المعالجة وتصـحيحها حال كونها غير دقيقة أو غير مكتملة أو غامضـــة أو محوها كلية إذا كان محظورًا جمعها أو اســـتخدامها أو تخزينها، أورد ذات المشرع استثناءً وحيدًا علي هذا الحق في المادة 1/67 من قانون المعلوماتية والحريات، ويتمثل فيما إذا كان المســـئول عن المعالجة يقوم بذلك في

---

(1) **Idem.**

(2) ***Grévin ANTHONY***, Op.cit., p.77.

(3) ***Benjamin EGERT,*** Op.cit., p. 67.

(4) ***Julien LE CLAINCHE***, Le traitement des données à caractère personnel …, Op.cit., p. 33.

(5) الفقرة الرابعة من الفصل 60 من القانون التونسي رقم 63 لسنة 2004 الصادر في 27 يوليه المتعلق بحماية المعطيات الشخصية. متاح علي الرابط التالي:
http://www.e-justice.tn/fileadmin/fichiers_site_arabe/ministere/L_2004_63.pdf

إطار ممارسة مهنة الصحافة وبشرط احترامه للقواعد المهنية للصحافة، أو بغرض القيام بعمل فني أو أدبي[1].

الفصل الثالث

حماية البيانات الشخصية في التشريعات المقارنة

تمهيد وتقسيم:

لقد أظهرت الدراسات الجنائية عدم كفاية النصوص التجريمية التقليدية في مواجهة مخاطر تقنية المعلومات واتساع دائرة الاعتداء علي الحقوق الشخصية للأفراد بفعل الاستخدام غير القانوني للبيانات الشخصية؛ لذلك كان لهذه الدراسات

---

(1) ***Art. 67-I, Loi nº 78-17*** Modifié par Loi n°2016-1321 du 7 octobre 2016:« Le 5° de l'article 6, les articles 8, 9, 22, les 1° et 3° du I de l'article 25, les articles 32, et 39, le I de l'article 40 et les articles 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en oeuvre aux seules fins :
1° D'expression littéraire et artistique ;
2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession».

أثر في إصـــدار أو اقتراح قوانين جديدة في العديد من الدول لكفالة ســـرية البيانات الشخصية وحمايتها من مخاطر الاستخدام غير القانوني لتقنيات معالجتها.

وقد اختلفت ردود أفعال الدول المختلفة في كيفية التحرك التشـــريعي لحماية البيانات الشـــخصـــية المعالجة آليا ومواجهة الاعتداء عليها، فنجد دولة مثل فرنســـا، والولايات المتحدة الأمريكية، وانجلترا قد قامت بإصـــدار قوانين خاصـــة، فضـــلًا عن تعديل قانون العقوبات لمواجهة الجرائم المعلوماتية، ودول أخري قامت بمعالجة هذه الجرائم عن طريق التطبيق علي جرائم أخري موجودة ســـلفًا ومنصـــوص عليها في القوانين العقابية العامة أو قوانين خاصة كما هو الحال في القانون المصري.

وبناء عليه ســوف نتناول صــور الحماية الجنائية للبيانات الشــخصــية في التشريعات المقارنة في مبحثين علي النحو التالي:

المبحث الأول: حماية البيانات الشخصية في التشريعات الأجنبية.

المبحث الثاني: حماية البيانات الشخصية في التشريعات العربية.

المبحث الأول
حماية البيانات الشخصية في التشريعات الأجنبية

يختلف نظام حماية البيانات الشـــخصـــية في كل من فرنســـا وانجلترا عن الولايات المتحدة الأمريكية؛ ويرجع الســـبب في ذلك إلي وجود مرجعية عليا ملزمة لدول الاتحاد الأوروبي متمثلة في التوجيه رقم 95-46 بشـــأن حماية البيانات الشـــخصـــية حيث يتعين علي الدول الأعضـــاء في هذا الاتحاد تعديل تشـــريعاتها الداخلية لتتواءم وأحكام هذا التوجيه.

وعليه سوف نتناول حماية البيانات الشخصية في التشريعات الأجنبية علي النحو التالي.

المطلب الأول: حماية البيانات الشخصية في التشريع الفرنسي.

المطلب الثاني: حماية البيانات الشخصية في التشريع الإنجليزي

المطلب الثالث: حماية البيانات الشخصية في التشريع الأمريكي.

المطلب الأول

حماية البيانات الشخصية في التشريع الفرنسي

تعتبر فرنسا من أوائل الدول الغربية التي سارعت إلي إصدار تشريعات خاصة لحماية البيانات المعالجة آليا[1]. إذ نص القانون الفرنسي الصادر في 6 يناير 1978 والمعدل بالقانون رقم 801-2004، الخاص بحماية البيانات الشخصية للمواطنين في مواجهة نظم المعالجة الألية للمعلومات، علي عدة جرائم لحماية البيانات الشخصية لتعلقها بالحياة الخاصة للأفراد. حيث استند المشرع بموجب نصوص هذا القانون إلي أن المعالجة الآلية للبيانات يجب ألا تحمل تعديًا علي حصانة الفرد وحياته الخاصة[2].

ولم يحاول المشرع الفرنسي عند قيامه بوضع القانون الجنائي الحديث أن يغير روح قانون 1978 أو يقلص سلطات اللجنة الوطنية للمعلوماتية والحريات، وقد تضمن القانون الجنائي الفرنسي الحديث المواد 41-44 من قانون 1978 في الفصل الخاص بحماية الشخصية، وتناول الجرائم الخاصة بحماية البيانات الشخصية والأحكام الخاصة بالعقاب في المواد 16/226 إلي المادة 24/226 من قانون العقوبات الحديث مع إجرائه لبعض التعديلات في هذه الجرائم[3]، والأفعال التي تناولها قانون العقوبات الفرنسي الحديث والمتعلقة بالبيانات الشخصية.

ترتيبا علي ذلك سوف نلقي الضوء علي الجرائم المتعلقة بالاعتداء علي البيانات الشخصية في القانون العقوبات الفرنسي، وذلك علي النحو التالي:

---

(1) د/ حسين بن سعيد الغافري، السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، 2009، ص 427.

(2) انظر: د/ أسامه عبد الله قايد، المرجع السابق، ص 133.

(3) انظر: د/ أيمن عبد الله فكري، جرائم نظم المعلومات- دراسة مقارنة، رسالة دكتوراه -حقوق المنصورة، 2005، ص 526-527.

الفرع الأول: عدم مراعاة الإجراءات الشكلية لمعالجة البيانات.

الفرع الثاني: عدم اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية.

الفرع الثالث: المعالجة غير المشروعة للبيانات الشخصية.

الفرع الرابع: حفظ البيانات الشخصية خارج الوقت المصرح به.

الفرع الخامس: الانحراف عن الغاية من معالجة البيانات الشخصية.

الفرع السادس: الإفشاء غير المشروع للبيانات الشخصية.

الفرع الأول

جريمة عدم مراعاة الإجراءات الشكلية لمعالجة البيانات

أولاً: النص القانوني:

نصـــت المادة 226-16 من قانون العقوبات الفرنســـي الجديد علي جريمة عدم مراعاة الإجراءات الشـــكلية لمعالجة البيانات بقولها: يعاقب كل من يقوم ولو بإهمال بمعالجة الكترونية للبيانات الشخصية دون مراعاة الإجراءات الشكلية اللازمة بموجب القانون، وذلك بالحبس 5 سنوات وبغرامة 300 ألف يورو.

ثانياً: أركان الجريمة:

يجب لقيام جريمة عدم مراعاة الإجراءات الشـــكلية لمعالجة البيانات توافر ركنين مادي، ومعنوي[1].

أ- الركن المادي:

يتحقق الركن المادي للجريمة بتوافر عنصـــرين: أولهما، الســـلوك الإجرامي والذي يتمثل في المعالجة الإلكترونية للبيانات الشـخصـية، سـواء كان ذلك في شـكل

---

[1] د/ عمر فاروق الحســيني، المشــكلات الهامة في الجرائم المتصــلة بالحاســب الآلي وأبعادها الدولية، بدون دار نشر، 1995، ص 57.

إدخال للبيانات أو تصـــنيفها أو توزيعها، أو دمجها مع بيانات أخري أو تحليلها كي تعطي معلومة ذات دلالة خاصة أو استرجاع المعلومات الشخصية[1].

وثانيهما، إجراء هذه المعالجة دون الحصـــول علي موافقة اللجنة الوطنية للمعلوماتية والحريات اســـتنادا لما ورد في المادتين 16،15 من القانون رقم 78-17 لسنة 1978 الخاص بالمعلوماتية والحريات[2].

ب- الركن المعنوي:

تعد هذه الجريمة من الجرائم غير العمدية[3]، ويتحقق الركن المعنوي فيها بالإهمال وهو مســـتفاد من نص المادة 16/226 عقوبات، والتي تعاقب علي القيام بتنفيذ المعالجات الالكترونية للبيانات الشخصية دون مراعاة الإجراءات الشكلية ولو تمت عن طريق الإهمال[4]. وبالتالي لا تتطلب الجريمة قصدًا جنائيًا، وتقع الشكليات علي عاتق كافة الأشخاص التي يمكن أن تقرر إنشاء بطاقات معلوماتية[5].

ثالثاً: العقوبة:

عاقب المشرع الفرنسي علي هذه الجريمة بموجب المادة 16/226 عقوبات بالحبس خمس سنوات وغرامة 300 ألف يورو بعد أن كانت في قانون 1978 الحبس لمدة 3 سنوات والغرامة 45 ألف يورو. كما يتعرض المذنب أيضًا للعقوبات التكميلية

---

(1) ***Patrice GATTEGNO***, Droit pénal spécial, Dalloz, 1995, p. 156.

(2) راجع: د/ أيمن عبد الله فكري، المرجع السابق، ص 527-528.

(3) ***Michel VÉRON,*** Droit pènal spécial, Armand Colin, 6è éd 1996. p.149.

(4) تطبيقًا لذلك اعتبرت محكمة النقض الفرنســـية الجريمة المنصـــوص عليها في المادة 41 من قانون 1978 – المقابلة للمادة 226-16 من قانون العقوبات الفرنســـي- من الجرائم المادية التي يفترض توافر القصد الجنائي فيها بمجرد ارتكاب الفعل.

Crim 3 nov. 1987, Bull. Crim. n° 382, Rev. Sc. crim. 1988. 295, ***Obs. Delmas Saint Hilaire*** et JCP 1988, I.3323, chron. ***Frayssinet (J).***

(5) ***Jean LARGUIER et Marie ANNE-LARGUIER***, Droit pènal spécial, Dalloz, 10è éd, 1998. p. 114.

المشار إليها في المادة 31/226 ولا سيما تجريم ممارسة النشاط المهني والاجتماعي، والذي من خلال ممارسته أو بمناسبته وقعت الجريمة[1].

الفرع الثاني

جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات الشخصية

أولاً: النص القانوني:

نصـــت المادة 226-17 من قانون العقوبات الفرنســـي الجديد علي جريمة عدم اتخاذ الاحتياطات اللازمة لحماية البيانات الشـــخصـــية بقولها: يعاقب كل من يقوم أو يعمل علي إجراء معالجة آلية للبيانات الشـــخصـــية دون الالتزام بالتدابير المنصـــوص عليها في المادة 34 من القانون رقم 17-78 الصـــادر في 6 يناير 1978.

ثانياً: أركان الجريمة:

يجب لقيام جريمة عدم اتخاذ الاحتياطات أو التدابير الوقائية لحماية البيانات الشخصية توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

يقوم الركن المادي لجريمة عدم اتخاذ إجراءات حماية البيانات الشـــخصـــية بتحقق العنصرين التاليين: **أولهما**، السلوك الإجرامي والذي يتمثل في القيام أو العمل علي القيام بمعالجة آلية للبيانات الشخصية، سواء كان ذلك في شكل تسجيل للبيانات أو تصـنيفها أو توزيعها، أو دمجها مع بيانات أخري أو تغييرها أو الاطلاع عليها أو اسـتعمالها أو ايصـالها عن طريق الإرسـال أو الاذاعة أو أي شـكل أخر من أشـكال إتاحتها[2]. **وثانيهما**، العمل أو ممارسـة العمل علي المعالجة دون اتخاذ الاحتياطات

---

(1) ***Michel VÉRON,*** Droit pènal spécial, Op. cit., p. 149.

(2) وقد ذهبت محكمة النقض الفرنســـية إلي أبعد من ذلك عندما اعتبرت أن الحماية المقررة بمقتضـي قانون رقم 17-78 الصـادر في 6 يناير 1978، لا تقتصـر علي الأشـخاص الذين

أو التدابير التي يتطلبها القانون، والتي تقوم علي شـــروط خاصـــة للدخول في المعالجة، والتي تقتصر علي الحائزين علي المفاتيح والتقنيات[1].

ب- الركن المعنوي:

تعد هذه الجريمة من الجرائم غير العمدية، ويتحقق الركن المعنوي فيها بالإهمال علي الرغم من أن المادة 17/226 عقوبات لم تتحدث عن الإهمال بشكل صريح؛ وذلك لأن غياب الاحتياطات تستند إلي الإهمال أو الامتناع[2].

ثالثاً: العقوبة:

عاقب المشرع الفرنسي علي جريمة القيام أو العمل علي إجراء معالجة آلية للبيانات الشخصية دون اتخاذ التدابير المنصوص عليها في المادة 34 من قانون رقم 17-78 الصـــادر في 6 يناير 1978 بالحبس خمس ســـنوات وغرامة 300 آلف

تكون معلوماتهم الشخصية محل معالجة، بل تشمل أيضًا كل الأشخاص المعنيين بشكل مباشر أو غير مباشر باستغلال هذه المعالجة.

Crim. 19 déc. 1995, Bull. Crim., n° 387; Rev. Sc.crim. 1996, 676, Obs. ***Francillon***; Dr. penal 1996, somm. 126, ***Obs Véron***; Gaz. Pal. 1996. II. Somm. 418, note ***Mole***.

(1) ***V. Fabrice MATTATIA***, CNIL et tribunaux: concurrence ou complémentarité dans la repression des infractions à la loi informatique et libertés?. Rev. Sc.crim. 2009. p. 323.

(2) تطبيقا لذلك أيدت محكمة النقض حكم محكمة الاستئناف الذي قضي بتوافر جميع العناصر المكونة لجريمة عدم اتخاذ تدابير الحماية والتي نصـــت عليها المادة 17/226 عقوبات بعدما أثبت أن المتهمين استعملوا نظام للمعالجة الآلية للبيانات الشخصية دون اتخاذ التدابير الوقائية التي من شأنها منع الاطلاع علي المعلومات الطبية بالنسبة للموظفين الإداريين غير المرخص لهم بذلك.

Crim. 30 oct. 2001, Gaz. Pal. 2002. II, 1476, note ***Mole et Lebon***.

وفي ذات الصدد قضت محكمة Rennes بتاريخ 13 يناير 1992 بتوافر عناصر غياب تدابير الأمن المعلوماتي إلي جانب جرائم أخري في حق مدير مؤسسة الائتمان الذي قام بتبليغ بعض التجار لائحة معلوماتية لأشخاص من بين عملاء المؤسسة مما يفترض معه أنه يشكل خطورة علي القروض المحتملة.

Rennes, 13 janv. 1992, Dalloz. 1993. Somm. 54, ***Obs***. ***Michel VASSEUR***; Idem. 1994. Somm. 287, Obs. Maisl.

يورو، كما يتعرض المذنب أيضًا للعقوبات التكميلية المشار إليها في المادة 25/226. ويمكن تقرير المسئولية الجنائية للأشخاص المعنوية بنفس الأوضاع السابق الإشارة إليها [1].

الفرع الثالث

جريمة المعالجة غير المشروعة للبيانات الشخصية

أولاً: النص القانوني:

نصت المادة 226-18 من قانون العقوبات الفرنسي الجديد علي جريمة المعالجة غير المشروعة للبيانات الشخصية بقولها: يعاقب علي جمع البيانات الشخصية بطريق العنف أو الاحتيال أو بطريق غير مشروع .

ثانياً: أركان الجريمة:

يجب لقيام جريمة المعالجة غير المشروعة للبيانات الشخصية توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

يتحقق الركن المادي لجريمة المعالجة غير المشروعة للبيانات بتحقق أحد العنصرين التاليين: **أولهما**، كل جمع للبيانات الشخصية بطريق التدليس أو الغش أو أي طريق غير مشروع، مثل التنصت علي التليفون أو التسجيل منه دون إذن قضائي[2]، أو جمع البيانات التي تقتضي طبيعتها عدم جمعها كالبيانات الحساسة[3].

---

(1) ***Michel VÉRON***, Droit pènal spécial, Op. cit., p.150.

(2) ***Michel MASSE***, Le droit pénal spécial né de l'informatique (Introduction et première partie d'un rapport fait avec M.SARGOS, Conseiller référendaire à la Cour de cassation) in Informatique et Droit pénal, Travaux de l'Institut des sciences criminelles de Poitiers, t. 4, Éditions Cujas 1982, p. 36.

(3) انظر: أسماء حسن سيد محمد رويعي، المرجع السابق، ص 517.

والجدير بالذكر أن القضاء الفرنسي لم يوضح طبيعة الوسائل الاحتيالية أو غير النزيهة أو غير المشروعة، لكن يمكن تصور أنها تتعلق بكافة وسائل التجميع المعلوماتي للبيانات الذي يتم بغير علم من صاحب الشأن[1].

تطبيقًا لذلك حكم في عام 2004 علي شركة "Impact Net" نظرًا لإجرائها استطلاعًا سريًا علي شبكة الانترنت ، وقد نشر علي أنه استطلاع مجهول، حيث طالب المشتركين في الاستطلاع بتاريخ الميلاد والوضع المهني والاجتماعي والثقافي فضلا عن المرشح المختار . وقد رأت المحكمة أن هذه المعلومات تسمح بتحديد هوية الشخص، وأن الاستطلاع كان اسميًا، وأنه أجري بطريقة غير مشروعة(المادة 226-18)، كذلك قضي بتوافر الأركان المنشئة للجريمة المعاقب عليها بمقتضي المادة 226-19 عقوبات المتعلقة بالطابع السياسي للمعلومات التي تم تجميعها.

T. corr., Nanterre, Jugement du 1 juin 2001. Cité par ***Fabrice MATTATIA***, CNIL et tribunaux: Op.cit., p. 323. note (18).

كما أدانت المحاكم الفرنسية قديما الوسيلة التي لجأ إليها مدير المنشأة في تسجيلة لمعلومات تتعلق بالعمال، والتي ترد علي الانتماءات السياسية لهم، أو النقابية، وبالنسبة لحياتهم الخاصة، نظرًا لأن هذه المعلومات تم تجميعها دون الحصول علي موافقة الأشخاص المعنيين.

T. corr., Creteil, 10 Juillet 1987, D., 319. note ***Frayssinet***.

كما قضت محكمة النقض الفرنسية بأن عناصر الجريمة تعد متوافرة بالقيام بدون موافقة صريحة للشخص المعني، بالتخزين الآلي للبيانات الشخصية التي تظهر علي وجه الخصوص الآراء السياسية، أو الفلسفية، أو الدينية.

Voir par Example. Crim 4 mars. 1997, Bull. Crim., n° 83; Dr. pénal 1997. 75, Obs. ***Véron***; Gaz. Pal. 1997. I. 320, note J. P. D; Rev. Se. crim 1997. 669, Obs**. *Dintilhac*.**

(1) ***Jean PRADEL et Mechil DANTI JUAN***, Droit penal: Droit pènal spécial, Edition Cujas, 1995. p.210.

تطبيقًا لذلك اعتبرت محكمة النقض الجمع غير النزيه للبيانات الشخصية متحققا في: 1- أي اطلاع علي العناوين الالكترونية واستعمالها، ولو دون تسجيلها في ملف، من أجل إرسال رسائل إلكترونية لأصحاب هذه العناوين. 2- أي تجميع للعناوين الإلكترونية للأشخاص الطبيعيين دون علمهم من خلال الفضاء العام للإنترنت باعتبار أن هذه الطريقة تشكل عائقا أمام ممارسة الحق في الاعتراض.

Crim. 14 mars 2006. Bull. Crim. n° 69; D. 2007. Pan. 404, ***Obs. Garé***.

ثانيهما، إجراء معالجة للبيانات الشخصية رغم معارضة هذا الشخص، متي كانت المعارضة تقوم علي أسباب مشروعة[1].

ب- الركن المعنوي:

تعد جريمة المعالجة غير المشـــروعة للبيانات من الجرائم العمدية التي لا يتصور وقوعها عن طريق الإهمال أو السهو وهو واضح من الوسائل الاحتيالية أو غير النزيهة أو غير المشروعة والتي تدخل في الأركان المنشئة للجريمة المشار إليها في المادة 18/226 من قانون العقوبات [2]، ويقتضـي المشـرع لقيامها توافر القصـد الجنائي العام، ولا عبرة للبواعث الدافعة لارتكابها، وينبني علي ذلك عدم ارتكاب الجريمة عن طريق الإهمال أو السهو، بمعني أنه لا يتصور وقوعها في صورة غير عمدية[3].

أما بالنسبة لجريمة معالجة البيانات الحساسة بدون رضا الشخص المعني جريمة عمدية لا تقوم إلا بتوافر القصـد الجنائي بعنصـريه، أي العلم والإرادة، حيث يلزم أن يعلم الجاني بأن الأفعال التي يقوم بها تشـكل معالجة للبيانات الشـخصـية، وأن البيانات التي يعمل علي معالجتها تشكل معطيات حساسة، وأنه يجري المعالجة دون الحصول علي موافقة صريحة من الشخص المعني.

ثالثاً: العقوبة:

---

(1) تطبيقًا لذلك قضـت محكمة اسـتئناف باريس بأن تجميع عناوين متنزهات علي شـبكة الإنترنت لإرسالها للدعاية دون طلب ذلك من الشركة التي قامت بذلك يعد تجميع غير مشروع للبيانات الشخصية ومعالجة لهذه البيانات دون رضاء الأشخاص المعنيين.

CA Paris, 11e chamber, section B, 18 mai 2005.

وقد أكدت محكمة النقض حكم الإدانة والغرامة 300 آلف يورو في القضية السابقة، وهكذا اعتبرت محكمة الاستئناف أن حق الاعتراض لا يتصور دون إعلام سابق، ودون الحصول علي الرضا، مما يعني تماثل الاعتراض وغياب الرضا.

Fabrice MATTATIA, Art. préc., p. 322.

(2) ***Jean PRADEL et Mechil DANTI JUAN***, Op.cit., p. 210.

(3) د/ أسامة عبد الله قايد، المرجع السابق، رقم 66 ص 143.

عاقب المشرع الفرنسي على جمع البيانات الشخصية بالوسائل الاحتيالية أو غير النزيهة أو غير المشروعة بالسجن لمدة خمس سنوات وبغرامة قدرها 000 300 يورو.

ويعاقب من يجري معالجة لبيانات شخصية متعلقة بشخص طبيعي بالرغم من معارضة ذلك الشخص، وذلك عندما تستهدف هذه المعالجة غرضا تجاريا بصفة خاصة، أو عندما يستند هذا الاعتراض علي أسباب مشروعة بالسجن لمدة خمس سنوات وغرامة قدرها 300 ألف يورو.

وبالنسبة لمعالجة البيانات الحساسة تعاقب المادة 19/226 علي عدم المحافظة علي هذه البيانات، والتي تتعلق بالجرائم والإدانات، أو المتعلقة بالتدابير الاحترازية، أو الكشف عن البيانات الشخصية التي تكشف، بصورة مباشرة أو غير مباشرة، عن أصول عرقية أو إثنية، وآراء سياسية أو فلسفية أو دينية، أو عضوية النقابات العمالية للأشخاص، أو المتعلقة بصحتهم أو ميولهم الجنسية أو هويتهم الجنسية، وذلك خارج الحالات المنصوص عليها قانونا[1]، بالسجن لمدة خمس سنوات وبغرامة 300 ألف يورو[2].

الفرع الرابع

جريمة حفظ البيانات الشخصية خارج الوقت المصرح به

أولاً: النص القانوني:

نصت المادة 226-20 من قانون العقوبات الفرنسي علي جريمة حفظ البيانات الشخصية خارج الوقت المصرح به وفقا للطلب أو الإعلان بقولها: يعاقب كل من يقوم بالاحتفاظ بالبيانات الشخصية لمدة أكثر من المدة المنصوص عليها في

---

(1) ***Jean PRADEL et Mechil DANTI JUAN***, Op.cit., p. 211.

(2) ***Fabrice MATTATIA***, Art. préc., p. 323.

القانون أو اللائحة، بناء علي الترخيص، أو الإشـــعار أو الاخطار المســـبق الموجه للجنـة الوطنيـة للمعلومـاتيـة والحريـات، مـا لم يتم حفظهـا لأغراض تـاريخيـة، أو إحصـــــائية، أو علمية علي النحو المنصـــــوص عليه في القانون، وذلك بالحبس 5 سنوات وغرامة 300 ألف يورو.

ويعاقب بذات العقوبة كل من يقوم بالمعالجة للبيانات الشـــخصـــية لأغراض تاريخية، أو إحصـــائية بعد انقضـــاء الفترة المذكورة في الفقرة الأولي، بخلاف ما هو منصوص عليه في القانون.

ثانياً: أركان الجريمة:

يجب لقيام جريمة حفظ البيانات الشـخصـية خارج الوقت المصـرح به توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

نص المشـــرع علي فعل واحد تقوم بـه الجريمـة، وهو الاحتفاظ بـالبيـانـات الشـخصـية لمدة تزيد عن المدة المنصـوص عليها في النصـوص التشـريعية المعمول بها أو المنصـوص عليها في الترخيص أو الإذن ويكون ذلك عندما يحتفظ الشـخص بمعطيات شـــخصـــية لمدة تتجاوز المدة المحددة في النصـــوص التشـــريعية أو المنصوص عليها في التصريح أو الإذن.

وبناءً عليه تقع الجريمة إذا كانت عملية المعالجة والحفظ قد تمت وفق أحكام القانون ولكن تم حفظ البيانات لمدة تجاوز المدة المطلوبة للحفظ، وبهذا يؤكد المشـرع أن البيانات الشـخصـية لا يمكن أن تحفظ لمدة غير محددة إلا في حالات اسـتثنائية يفترض فيها قانونا وصـراحة، وخصـوصـا أن حفظ البيانات آليا في ذاكرة الحاسـوب صـار أمرًا في غاية السـهولة علي الرغم من أن المعلومات المحفوظة قد تتعلق بأمور بسيطة إلا أنها قد تمس الشخص في سمعته واعتباره[1].

---

[1] د/ أسامة عبد الله قايد، المرجع السابق، رقم 65 ص 143.

ب-الركن المعنوي:

هذه الجريمة عمدية، يقتضـــي المشـــرع لقيامها توافر القصـــد الجنائي العام بعنصريه العلم والإرادة، إذا يجب أن يعلم الجاني بأن الفعل الذي يأتيه يشكل احتفاظًا ببيانات شخصية لمدة تتجاوز المدة اللازمة لإنجاز الغايات التي تم جمعها ومعالجتها لاحقا من أجلها، أو معالجة للبيانات الشـخصـية لأغراض غير تاريخية أو إحصـائية أو علمية تم الاحتفاظ بها بعد المدة القانونية من أجل أغراض تاريخية او احصـــائية او علمية.

كما يلزم أن تتجه إرادة الجاني إلي القيام بهذه الأفعال بذاتها، وإلا انتفي القصـــــد الجنائي، ومن ثم الركن المعنوي للجريمة. ونلفت الانتباه إلي أن الركن المعنوي لهذه الجريمة يقوم بمجرد تحقق القصد الجنائي العام دون حاجة إلي القصد الخاص.

ثالثاً: العقوبة:

شدد المشرع العقوبة في هذه الجريمة بموجب التعديل التشريعي الصادر في 6 أغســـطس 2004 بالقانون رقم 801-2004 في المادة 226-19، 20 من قانون العقوبات الفرنســي حيث جعل العقوبة الحبس لمدة خمس سـنوات والغرامة 300000 يورو.

الفرع الخامس

جريمة الانحراف عن الغاية من معالجة البيانات الشخصية

أولاً: النص القانوني:

نصـــت المادة 226-21 من قانون العقوبات الفرنســـي الجديد علي جريمة الانحراف الغاية من معالجة البيانات الشـخصـية بقولها: يعاقب كل من حاز بيانات شـخصـية بمناسـبة قيامه بتسـجيلها، أو تصـنيفها، أو نقلها، أو في أي صـورة أخري للمعالجة إذا غير من الوجهة النهائية المقررة لهذه البيانات، وفقا للقانون أو القرار

الصـادر في شـأنها، أو في الإخطار المسـبق علي القيام بالمعالجة، وذلك بالحبس 5 سنوات وبغرامة 300 ألف يورو.

ثانياً: أركان الجريمة:

يجب لقيام جريمة عدم مراعاة الإجراءات الشـــكلية لمعالجة البيانات توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

يتوافر هذا الركن إذا ما انحرف الجاني عن الغاية أو الهدف من المعالجة الآلية للبيانات الشخصية، ويستوي لدي القانون أن يكون الشخص حائزا لهذه البيانات بغرض تصـنيفها، او نقلها، أو علاجها تحت أي شـكل[1]. ويتحقق هذا الركن بمجرد الانحراف عن الهدف من معالجة البيانات الشـخصـية. والغاية هي موضـوع المعالجة الآلية، أي الغرض المتوخي من علاج البيانات الشـــخصـــية، وهي المبرر الوحيد لمعالجة البيانات الشـخصـية آليا[2].وقد نص المشـرع علي ضـرورة تحديد الغاية أو الغرض من المعالجة الآلية للبيانات الشـخصـية في الطلب المقدم إلي اللجنة القومية (المـادة 15 ومـا يليهـا من قـانون 1978)، إذ هو المنوط بـه تحـديـد الانحراف، أو الخروج عن الغـايـة، أو الغرض الـذي من أجلـه تمـت المعـالجـة الآليـة للبيـانـات الشخصية[3].

ب- الركن المعنوي:

---

(1) د/ أسماء حسن سيد محمد رويعي، المرجع السابق، ص 528.

(2) ***Michel MASSE***, Op. cit, p. 42.

(3) د/ أسامة عبد الله قايد، المرجع السابق، رقم 76 ص 155.

يتخذ الركن المعنوي في هذه الجريمة صورة القصد الجنائي العام، أي يجب أن يعلم الجاني أن ما يأتيه من أفعال يؤدي إلي الانحراف عن الهدف أو الغرض من معالجة البيانات، كما يجب أن تتجه إرادته إلي الوصول إلي ذلك الهدف[1].

فإذا استغل شخص البيانات الخاصة بآخر في الكشف عن مصادر ثروته، أو تهربه من الضرائب، أو معرفة مركزه المالي، أو الاستدلال عليه، يتحقق الركن المعنوي لهذه الجريمة[2].

ثالثاً: العقوبة:

عاقب المشرع الفرنسي كل من حاز بيانات شخصية بمناسبة قيامه بتسجيلها أو تصنيفها أو نقلها أو في أي صورة أخري للمعالجة إذا غير من الوجهة النهائية المقررة لهذه البيانات، وفقا للقانون أو القرار الصادر في شأنها، أو في الإخطار المسبق علي القيام بالمعالجة بالحبس لمدة خمس سنوات وبغرامة 300 ألف يورو[3].

الفرع السادس

جريمة الإفشاء غير المشروع للبيانات الشخصية

أولاً: النص القانوني:

---

(1) المستشار/ عادل الشهاوي، والمستشار/ محمد الشهاوي، الاعتداء علي الحياة الخاصة بواسطة القنوات الفضائية ووسائل الإعلام والاتصال، دار النهضة العربية، 2015، رقم 89، ص 78.

(2) د/ أسامة عبد الله قايد، المرجع السابق، رقم 77 ص 156.

(3) تطبيقًا لذلك النص قضت محكمة استئناف Aix-en-Provence عام 2005 بإدانة رجلي شرطة لقيامهم بصورة غير مشروعة بالاطلاع علي بطاقة نظام المعالجة للجرائم الثابتة للشرطة الوطنية – التي تضم المتهمين والشهود والمجني عليهم – وقيامهم بنشر المعلومات الموجودة في البطاقة للمسئول المحلي لهذه الطائفة، والذ يعد هو أيضا متهم؛ وذلك لمخالفتهم واجب الحفاظ علي الاسرار المهنية (المادة 13/226 عقوبات)، والتعسف في استعمال البطاقات الشخصية والانحراف بها عن غايتها (المادة 21/226 عقوبات).

Fabrice MATTATIA, Art. préc., p. 320.

نصـــت المادة 226-22 من قانون العقوبات الفرنســـي الجديد علي جريمة الإفشـاء غير المشـروع للبيانات الشـخصـية بقولها: يعاقب كل من يقوم بالكشـف عن بيانات شـخصـية بمناسـبة قيامه بتسـجيلها، أو تصـنيفها، أو نقلها، أو في أي صـورة أخري للمعالجة، والتي يترتب علي كشـفها الاعتداء علي اعتبار صـاحب الشـأن أو حرمة حياته الخاصة، وذلك بدون التصريح من صاحب الشأن للغير التي لا توجد له صفة في تلقي هذه المعلومات، وذلك بالحبس 5 سنوات وبغرامة 300 ألف يورو.

ثانياً: أركان الجريمة:

يجب لقيام جريمة الإفشـاء غير المشـروع للبيانات الشـخصـية توافر ركنين مادي، ومعنوي.

أ- الركن المادي:

نص المشـرع علي فعلين تقوم بهما الجريمة: أولهما، فعل الحيازة، ويسـتوي لدي القانون أن تكون حيازة البيانات الشـخصـية بقصـد تصـنيفها، أو نقلها، أو أي شـكل آخر من أشـكال معالجتها، وبالتالي يجب لتحقق هذا الفعل ثبوت واقعة الحيازة لهذه البيانات للقيام بأي إجراء من الإجراءات السابقة[1].

أما الفعل الثاني فيتمثل في إفشـــاء هذه البيانات للغير، والذي لا يكون من حقه الاطلاع عليها، ومن عناصـر الركن المادي أن تتحقق نتيجة إجرامية، وهي أن يترتب علي فعل الإفشاء إضرار للشخص، أو اعتداء علي حرمة حياته الخاصة، أو شـرفه، أو اعتباره، وأن ترتبط هذه النتيجة بالفعل بعلاقة السـببية. ويعني ذلك إذا لم يترتب علي الإفشاء اعتداء علي كرامة الشخص، أو اعتباره أو حرمة حياته الخاصة لا تتوافر عناصـــر الركن المادي، ومن ثم ينتفي الركن المادي ولا تقوم الجريمة في حق المفشي[2].

---

[1] د/ أسامة عبد الله قايد، المرجع السابق، رقم 70 ص 146.

[2] د/ أسماء حسن سيد محمد رويعي، المرجع السابق، ص 532.

ب-الركن المعنوي:

يتخذ الركن المعنوي لهذه الجريمة إحدي صورتين العمد أو الخطأ. أما العمد فيقوم بتوافر القصد الجنائي العام بعنصريه العلم والإرادة. فيجب أن يعلم مرتكب الجريمة أنه يقوم بالإفشاء غير المشروع للبيانات الشخصية للمجني عليه، وأن تتجه إرادته إلي ذلك وأنها تشكل اعتداء علي الشرف أو الاعتبار أو الحياة الخاصة. والاعتداء يفترض توافر القصد الجنائي لدي المعتدي. أما الخطأ فيتضح مما أورده المشرع من العقاب علي الجريمة إذا وقعت نتيجة الإهمال أو الرعونة أو ترك للبيانات الشخصية[1].

وعليه ينبغي إثبات الغاية أو الغرض من فعل الإفشاء إذا كان الفعل إراديا عن وعي وإدراك، أو أن هذا الفعل كان نتيجة خطأ أو أهمال.

ثالثاً: العقوبة:

فرق المشرع في العقاب علي الجريمة علي أساس الركن المعنوي، فنص علي عقوبة مشددة في حالة الافشاء العمدي، عن حالة الافشاء غير العمدية. حيث عاقب الجاني بعقوبة الحبس 5 سنوات وغرامة 300 ألف يورو إذا كان الإفشاء عمديًا إذ. بينما عاقب بعقوبة الحبس 3 سنوات وغرامة 100 ألف يورو إذا كانت الجريمة نتيجة رعونة، أو أهمال ترتب عليه إفشاء البيانات[2].

المطلب الثاني
حماية البيانات الشخصية في التشريع الإنجليزي

---

(1) د/ آدم عبد البديع آدم، المرجع السابق، ص 581.

(2) تطبيقًا لذلك النص أدانت محكمة استئناف باريس عام 2004 وكيلًا عقاريًا باع لوكلاء عقاريين دون إذن من الأشخاص المعنيين، بطاقات تتضمن أسماء، وعناوين، وأرقام التليفونات الخاصة ببائعي الوحدات العقارية وذلك للإفشاء العمدي دون إذن من أصحاب البطاقات، الأمر الذي يشكل اعتداء علي حرمة الحياة الخاصة.

CA. Paris, chambre correctonnelle, Bull. n° 17. p. 2004.

يعد قانون حماية البيانات لسنة 1998 التشريعي الرئيسي الذي ينظم حماية البيانات الشخصية في المملكة المتحدة، وقد حل هذا القانون محل قانون حماية البيانات لسنة 1984 سعيًا إلي تنفيذ التوجيه الأوربي الخاص بحماية البيانات الصادر لسنة 1995. وقد بدأ سريان قانون حماية البيانات لسنة 1998 في الأول من مارس سنة 2000 حيث معظم أحكامه قد وضعت موضع التنفيذ اعتبارًا من 24 أكتوبر 2001.

ويكمن الهدف الأساسي من قانون حماية البيانات في حماية حقوق وخصوصية الأفراد والتأكد من أن البيانات التي تخص الأفراد لا يتم معالجتها دون معرفتهم وأنه قد تم معالجتها بموافقتهم متي كان ذلك ممكنا.

ويسري قانون حماية البيانات علي البيانات الشخصية المرتبطة بالأفراد الأحياء ويقوم بتعريف البيانات الشخصية الحساسة والتي تخضع لمزيد من الشروط الصارمة في معالجتها مقارنة بما هو مقرر مع سائر البيانات الشخصية [1].

ويعرف القانون البيانات الشخصية بأنها: البيانات المتعلقة بفرد حي يمكن تحديده من تلك البيانات، أو من غيرها من المعلومات التي في حوزة مراقب البيانات أو يحتمل أن تكون في حوزته وتتضمن أي تعبير عن الرأي بشأن الفرد وأي مؤشر علي نوايا مراقب البيانات أو أي شخص آخر فيما يتعلق بالفرد[2].

---

(1) Report, Review of the Implementation of the Human Rights Act, Department of the constitutional Affaires, Justice rights and democracy, July 2006. p. 8.Available at: https://webarchive.nationalarchives.gov.uk/+/http:/www.dca.gov.uk/peoples-rights/human-rights/pdf/full_review.pdf

(2) «personal data» : means data which relate to a living individual who can be identified:
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
https://www.legislation.gov.uk/ukpga/1998/29/section/1

أما البيانات الشخصية الحساسة فتتعلق بالأصول العرقية لصاحب البيانات أو أرائه السياسية، أو الدينية أو ما شابه ذلك من معتقدات، أو الانتماء إلي النقابات العمالية، أو صحته الجسدية أو العقلية أو الحياة الجنسية أو السجل الجنائي [1].

ويسري قانون حماية البيانات سالف الذكر علي البيانات التي يتم الاحتفاظ بها في نماذج إلكترونية كما ينطبق أيضًا علي البيانات اليدوية التي يتم الاحتفاظ بها فيما يطلق عليه القانون بنظام حفظ الملفات المعنية.

وينشئ قانون حماية البيانات حقوقًا لهؤلاء الذين يتم تخزين بياناتهم بالمقابل يلقي مسئوليات علي عاتق من يقومون بتجميع أو تخزين أو بث تلك البيانات. وتتمثل حقوق هؤلاء الذين تتم معالجة بياناتهم في الآتي:

- الحق في الاطلاع علي البيانات التي تحتفظ بها هيئة من الهيئات، بناء علي طلب يقدم من الشخص المعني مقابل رسم رمزي.
- الحق في تصحيح المعلومات الخاطئة، فإذا ما تجاهلت الشركة الطلب، يمكن للمحكمة أن تأمر بتصحيح أو تدمير البيانات وفي بعض الحالات يمكن الحكم بالتعويض.
- الحق في المطالبة بعدم استخدام البيانات بأي شكل من الأشكال والتي من الممكن أن تتسبب في ضرر للشخص المعني.
- الحق في المطالبة بعدم استخدام بيانات الشخص في عمليات التسويق المباشر.

وتعد اللجنة الفرعية الاستشارية لعمليات الأنظمة Operations Advisory Subcommittee System (SOAS) مراقب للبيانات فيما يخص البيانات التي تخضع لمسئوليتها. ومن ثم تعد اللجنة الفرعية مسئولة وفقا لقانون حماية البيانات عن القرارات المتعلقة بمعالجة البيانات الشخصية بما في ذلك قرارات

---

(1) ***Duke***, Privacy: The Development of a Law and the Legal Theory, UK BOOKS, 2011. p. 163.

وأفعال معالج البيانات الخارجيين والذين يعملون نيابة عن اللجنة الفرعية الاستشارية لعمليات الأنظمة. ويطالب قانون حماية البيانات بضرورة أن يتم تنفيذ المعالجة وفقا لمبادئ حماية البيانات[1] وهي ذات المبادئ التي نص عليها قانون المعلوماتية والحريات الفرنسي السابق دراستها.

المطلب الثالث

حماية البيانات الشخصية في التشريع الأمريكي

الواقع أنه ليس هناك قانون شامل ينظم الحصول علي البيانات الشخصية وتخزينها واستخدامها في الولايات المتحدة. وبشكل عام، أي شخص يبذل جهدًا في الحصول علي البيانات يكون له حق تخزينها واستخدامها حتي إذا ما تم جمع البيانات دون تصريح.

فعلي سبيل المثال، نجد أن إخضاع التأمين الصحي لقابلية النقل والمحاسبة لسنة 1996، وقانون حماية خصوصية الأطفال علي الإنترنت لسنة 1998، وقانون المعاملات الائتمانية العادلة والدقيقة لسنة 2003 كلها أمثلة للقوانين الأمريكية الفيدرالية التي تحوي نصوصًا تميل إلي تشجيع كفاءات تدفق المعلومات.

وبالرغم من ذلك نجد عددا قليلا للغاية من الولايات التي تقر بأحقية الفرد في الخصوصية باستثناء ولاية كاليفورنيا. فهناك حق للخصوصية غير قابل للتصرف فيه (المادة 1 من القسم الأول من دستور كاليفورنيا)، كما قام المجلس التشريعي بسن عدد من التشريعات التي استهدفت حماية هذا الحق.

---

(1) حول مبادئ حماية البيانات في قانون حماية البيانات الشخصية في المملكة المتحدة، أنظر:

Jonathan Morgan, Privacy, Confidence and Horizontal Effect: "Hello" Trouuble, Cambridge Law Journal, Vol. 62. N°. 2, 2003, pp. 444-473.

H.M Fenwick & G. Phillipson, 'Privacy and Confidence: A Re-Examination'. Cambridge Law Journal, Vol.55, N°. 3, 1996, pp. 447-455.

R. Singh & J. Strachan, Privacy Postponed, European Human Rights Law Review, 2003. pp. 12-15.

وبذلك تجنبت الولايات المتحدة الأمريكية سـن تشـريع عام شـامل لحماية الخصـوصـية، وفضـلت إصـدار قوانين معينة تحكم قطاعات بعينها في مسـألة الخصوصية. بالإضافة إلي التشريعات العادية التي تحمي الخصوصية

ترتيبًا علي ما تقدم نجد لزامًا علينا أن نسـتعرض التشـريعات القطاعية والتشـريعات العادية في الولايات المتحدة لحماية الخصـوصـية المعلوماتية، وذلك في فرعين علي النحو التالي:

الفرع الأول: التشريعات القطاعية المخصصة.

الفرع الثاني: التشريعات العادية لحماية الخصوصية.

الفرع الأول
التشريعات القطاعية المخصصة

اعتمدت الولايات المتحدة الأمريكية علي فكرة القوانين القطاعية والتي تحكم قطاع معين في مسألة الخصوصية، ويتجلي ذلك في قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة، وقانون الإبلاغ عن الائتمان العادل، علي التفصيل الأتي:

أولاً: قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة (HIPAA)

تكمن الفكرة الرئيسـية لقانون إخضـاع التأمين الصـحي لقابلية النقل والمحاسبة Health Insuranve Portability & Accountability Act الصادر 1996 والذي وضـع موضـع التنفيذ في 21 أغسطس 1996، في أنه يجب علي الفرد الذي يخضـع لعملية التعرف الفردية علي المعلومات الصـحيحة أن تتوافر لديه إجراءات معمول بها لممارسـة حقوق خصـوصـية المعلومات الصـحيحة الفردية، وأن يكون الإفصاح عن المعلومات الصحيحة الفردية مصرح به[1].

(1) ***Wolf M, Bennett C.,*** ″Local perspective of the impact of the HIPAA privacy rule on research″. Cancer, 2006. p. 146-150.

وتكمن الصعوبات التي تواجه قانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة في ضرورة وجود آلية لاعتماد حق المريض في النفاذ إلي بياناته إذا طلب ذلك؛ لذلك بدأت المرافق الطبية في السؤال عن رقم الضمان الاجتماعي من المرضي، وبذلك يمكن القول بأنه تم الحد من الخصوصية بواسطة تبسيط إجراء ربط السجلات الطبية بالسجلات الأخري.

وتمثل قضية الحصول علي الموافقة مشكلة وفقا لقانون إخضاع التأمين الصحي لقابلية النقل والمحاسبة وذلك لأن مقدمي الخدمات الطبية يجعلون الرعاية مشروطة بالموافقة علي معايير الخصوصية المعمول بها[1].

ثانياً: قانون الإبلاغ عن الائتمان العادل (FCRA):

ينظم قانون الإبلاغ عن الائتمان العادل Fair Credit Reporting Act جمع ونشر واستخدام المعلومات الخاصة بالمستهلكين بما في ذلك المعلومات المتعلقة بالحاسبات الائتمانية للمستهلكين، ويطبق في ذلك مبادئ الممارسة العادلة للمعلومات لوكالات الإبلاغ عن عمليات الائتمان[2].

ووفقا لقانون المعاملات الائتمانية العادلة والدقيقة، فأنه يمكن لكل شخص الحصول علي تقرير سنوي مجاني عن وضعه الائتماني. كما يزود المستهلكين بالقدرة علي مراجعة وتصحيح ومعارضة والحد من استخدام تقارير الائتمان. كذلك يعمل علي حماية وكالة الائتمان من تهمة النشر بطريقة مهملة في حالة ما إذا ادعي الطالب تحريف البيانات.

كما تغطي القوانين الإضافية النوعيات المختلفة من المعلومات الخاصة. فعلي سبيل المثال، يطالب قانون الحقوق التعليمية والخصوصية العائلية Family

---

(1) ***Atchinson & Daniel M. Fox,*** The Politics of The Health Insurance Portability and Accountability Act". Health Affairs 1997. p. 146-150.

(2) ***Cooper, Marion B, Drinker Biddle & Reath LLP.,*** "January 1, 2013: New Fair Credit Reporting Act"FCRĂ From Required by New Enforcement Agency". TNL Review, 2013. p. 93.

Educational Right & Privacy Act والذي تم سنه عام 1974 الوالدين أو الطالب الراشد بالموافقة علي الدخول علي سجلات الطلاب لمعظم الأغراض[1].

ولدي العديد من الوكالات الفيدرالية الأمريكية قوانين خصوصية تغطي عملية جمع المعلومات الخاصة واستخدامها. مثل مكتب الإحصاء الرسمي للسكان، ووكالة خدمة العائدات الداخلية والمركز القومي لإحصائيات التعليم. بالإضافة إلي ذلك، يحمي قانون حماية المعلومات السرية والكفاءة الاحصائية Confidential Information Protection & Statistical Efficiency Act سرية البيانات التي يتم تجميعها من وكالات الإحصاء الفيدرالية[2].

الفرع الثاني

القوانين العادية التي تحمي الخصوصية

أولاً: قانون شرف شفافية البلاغ لعام 1970:

يشتمل هذا القانون علي حقوق المستهلك من حيث المحافظة علي خصوصية المعلومات حول المستهلك، والذي يتضمن أحقية المستهلك في معرفة من يطلع علي حقائق استهلاكه، ومن ثم يلزم موافقته المسبقة علي ذلك.

ثانياً: قانون الخصوصية لعام 1974 (The Privacy):

تم إصدار القانون الخاص بالخصوصية في 31 ديسمبر 1974 والمعدل بالقانون رقم 94-393 في سبتمبر 1976، 95-38 في أول يونيو 1977.

ويطبق هذا القانون علي البيانات الشخصية التي تخزن تحت أي شكل، وتُكشف للسلطات الفيدرالية، وإن كان البعض يرجع السبب في إصداره إلي فضيحة

---

(1) ***Mendelsohn, Stephen A.,*** ″ U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures″. The National Law Review. 2012. p. 59.

(2) CIPSEA Report on confidentiality and data sharing from the U.S. Energy Information Administration retrieved from www.eia.gov 2013.

وتورجيت[1]. ويشتمل هذا القانون علي عدة أسس لحماية البيانات الشخصية وهي كالتالي:

1- متطلبات الإشعار العام: غالبا ما يشير قانون الخصوصية إلي نظام السجلات[2]، ولكي يمنع وجود قواعد بيانات سرية إلزم الوكالات بنشر بنشر كافة أنظمة سجلاتها في السجل الفيدرالي، وبيان الاستخدامات المرجوة من النظام، وسمح للأفراد المعنيين بتقديم بيانات مكتوبة أو وجهات نظرهم أو منازعاتهم إلي الوكالة[3].

2- النفاذ للسجلات: ألزم قانون الخصوصية أي وكالة تحتفظ بنظام للسجلات أن تمكن الفرد من الدخول علي أي سجلات تتعلق به والسماح له بمراجعته والحصول علي نسخة منه، فإذا ما وجد السجل غير كامل أو به خطأ يحق للفرد أن يطلب تصحيح هذا السجل، وعلي الوكالة أن تستجيب للطلب خلال عشرة أيام سواء بإجراء التعديلات المطلوبة أو إبلاغ الفرد بسبب رفض تغيير السجل، وفي الحالة الأخيرة علي الوكالة أن تخبر الفرد إذا ما أراد مراجعة الرفض من المسئول الأعلي درجة الذي يتعين مخاطبته.

---

(1) ***Jean FRAYSSINET***, L´informatique et le secret des fichiers, Rev. adm. 1977. p. 183.

(2) ويعرف نظام السجلات بأنه: مجموعة من السجلات يتم من خلالها استدعاء المعلومات باسم الفرد أو مفتاح تعريف، أما قواعد البيانات ومجموعات السجلات التي لا تسمح باستدعاء معلومات حول فرد بعينه فهي غير مشمولة بالحماية.

(3) ***Scott, Craiag R, HIPA***., Privacy Complaint Turns into Federal Criminal Prosecution for frist Time. Compliance Corner (University of Missouri Healthcare. 2012.

وضمانًا لحقوق الأفراد وحفاظًا علي بياناتهم قيد المشرع الوكالات عند إنشائها نظام للسجلات أو رغبتها في إجراء تغيير بارز في هذا النظام، بضرورة إخطارها المسبق لكل من اللجنة المعنية بالعمليات الحكومية بمجلسي النواب والشيوخ، ومكتب الإدارة والميزانية؛ وذلك لتقييم التأثير المحتمل علي حقوق الأفراد.

3- متطلبات كشف الحكومة للمعلومات: يقيد القسم الفرعي (ب) من قانون الخصوصية قدرة الوكالة الحكومية علي كشف المعلومات القائمة في نظام سجلاتها. ويجوز للوكالة ان تكشف فقط عن المعلومات إذا ما رخص الفرد للوكالة ذلك.

4- طرق التدقيق: ينص القسم الفرعي (ج) علي ضرورة أن تحتفظ أي وكالة بحسابات دقيقة تبين متي ولمن تم الكشف علي السجلات الشخصية وتشمل معلومات الاتصال الخاص بالشخص أو الوكالة التي طلب السجلات الشخصية.

5- متطلبات تقنين البيانات: علي أي وكالة تحتفظ بأدني قدر من المعلومات " المعنية والضرورية" لتحقيق أغراضها، إذا ما كان لها أثر علي تقليص حقوق الفرد أو مصالحه أو امتيازاته . أن تخطر الفرد ماهية القانون أو الأمر التنفيذي الذي يخول للوكالة جمع المعلومات، والاستخدامات الروتينية التي قد تفيد فيها البيانات والآثار التي التي من المحتمل أن تنجم نتيجة امتناع الفرد عن تزويد المعلومات المطلوبة[1].

6- عقوبات انتهاك الخصوصية: عاقب المشرع الأمريكي كل مسئول أو موظف في وكالة حكومية كشف عن عمد معلومات تعريف شخصية بعقوبة الجنحة والغرامة بمبلغ أقصاه خمسة آلاف دولار. وبالمثل عاقب كل موظف أو مسئول حكومي يحتفظ عن عمد بنظام سجلات دون الكشف عن وجوده والتفصيلات المعنية به بمبلغ أقصاه خمسة آلاف دولار. كما يمكن أن تطبق عقوبة الجنحة نفسها والغرامة القصوي البالغة

(1) ***Harry A Hammitt et al.,*** Litigation under the federal open government laws: covering the Freedom of Information Act, the Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act, Washington, D.C., 2002, p.71.

خمسة آلاف دولار علي أي شخص يطلب عن عمد سجل أحد الأفراد من إحدي الوكالات بادعاء مزيف[1].

ثالثاً: قانون خصوصية الاتصالات الإلكترونية لسنة 1986:

الهدف من هذا القانون هو السعي إلي مد الاختصاص القضائي الفيدرالي إلي نطاق الاتصالات الإلكترونية، وذلك من ناحية تجريم المراقبة غير المصرح بها للاتصالات الإلكترونية المخزنة أو المتبادلة. حيث حظر القانون المذكور مراقبة وبث مضمون الاتصالات الالكترونية المخزنة. ومن جهة أخري يحظر هذا القانون الدخول غير المصرح به إلي المراسلات والبيانات التي لها صلة بذاكرة الحاسوب[2].

رابعاً: قانون حماية خصوصية المستهلك لعام 1997:

ينظم قانون حماية خصوصية المستهلك الصادر لسنة 1997 استخدامات تقديم شركات خدمات البرامج التفاعلية – مقدمي خدمات الإنترنت – مدخلات المستخدمين لبياناتهم الشخصية[3]. إذ يحظر القانون سالف الذكر علي هذه الشركات الكشف عن أي معلومات تعريفية شخصية قدمها المشترك دون موافقتة الكتابية. كما خوله القانون سحب هذه الموافقة في أي وقت ومطالبة شركة تقديم الخدمة بالتوقف عن كشف مثل هذه المعلومات[4]. كما يحظر عليها أن تكشف عمدًا إلي طرف ثالث أي معلومات تعريفية شخصية يقدمها المشترك.

وإعمالا لمبدأ حق الشخص في الاطلاع علي المعلومات الشخصية وتدقيقها وتصحيحها إذا ما شابها خطأ، خول القانون للمشترك مجموعة من الحقوق: **أولها،**

---

(1) ***Geal RF***, Federal Trade Commission, Fair Information Practice Principles, (FIPs) review 2009. p. 30.

(2) د/ أسماء حسن سيد محمد الرويعي، المرجع السابق، ص 497.

(3) ***Angela Choy, Marcia S.Smith and Jane Bortnick Griffith***, Protecting privacy on the internet: a summary of legislative proposal, CRS Report for Congress, Congressional Reasearch Service, The liberary of Congrsess, 1997. p. 135.

(4) ***Lanier & Saini***, Understanding Consumer Privacy: A Review and Future Directions, Academy of Marketing Science, 2008. p. 24.

أن يطلب من شـــركة تقديم الخدمة تزويده بمعلوماته التعريفية التي تحتفظ بها، **وثانيها**، السـماح بالتحقق من المعلومات التعريفية وتصـحيحها اذا شـابها خطأ، **وثالثها**، إعلام الشخص بما إذا كان هناك طرف ثالث تلقي هذه المعلومات أم لا.

وحرصًـا من المشـرع علي تسـيير ممارسـة الشـخص لهذه الحقوق وتفعيلها حظر علي شركات تقديم الخدمة فرض رسوم تثقل كاهل المشترك نظير إتاحة مثل هذه المعلومات[1].

خامساً: قانون حماية خصوصية الضمان الاجتماعي علي الخط لسنة 1997:

تكمن العلة في إصـدار قانون حماية خصـوصـية الضـمان الاجتماعي في رغبة المشـرع الأمريكي في تنظيم اسـتخدام شـركات تقديم خدمات البرامج التفاعلية لأرقام الضـمان الاجتماعي ومعلومات التعريف الشـخصـية، حيث حظر هذا القانون نشر رقم حساب الضمان الاجتماعي أو معلومات التعريف الشخصية المرتبطة به دون الحصول علي موافقة الشخص المعني.

وحرصًـا علي سرية بيانات الضـمان الاجتماعي وعدم تداولها بين الشركات حظر المشـرع الأمريكي علي شـركات تقديم خدمات البرامج التفاعلية الكشـف لطرف ثالث عن رقم حسـاب الضـمان الاجتماعي للفرد، أو معلومات التعريف الشـخصـية التي يحويها هذا الحســـاب دون الحصـــول علي موافقة الفرد المســـبقة مقررًا جزاء الايقاف للشركة لمخالفتها هذا الحظر[2].

---

(1) وقد منح المشرع مفوضية التجارة الفيدرالية السلطة للتحري عما إذا كانت شركة تقديم الخدمة متورطة أو مشـــاركة في أي عمل أو ممارســـة يحظرها هذا القانون، وإذا كان الأمر كذلك، تصـــدر مفوضـــية التجارة الفيدرالية أمر بإيقاف الشـــركة التي تقدم الخدمة، كما لو كانت تنتهك أحكامًا محددة من قانون مفوضـية التجارة الفيدرالية. لمزيد من التفاصـيل، راجع: د/ مروة زين العابدين صالح، المرجع السابق، ص 239 وما بعدها.

(2) PRIVACY IN AMERICA: SOCIAL SECURITY NUMBERS, https://www.aclu.org/other/privacy-america-social-security-numbers

سادساً: قانون الخصوصية الشخصية علي الإنترنت لسنة 2001-2002[1]:

يحظر قانون الخصـــوصـــية الشـــخصـــية علي الإنترنت علي مقدم خدمة الإنترنت أو مشغل المواقع التجارية من جمع أو كشف المعلومات التعريفية الشخصية للمستخدم دون إشعار واضح وصريح للمستخدم.

وقد ألزم المشـــرع مقدم خدمة الإنترنت بمجموعة من الالتزامات: **أولها**، ضرورة الحصول علي موافقة كتابية أو إلكترونية لجمع وكشف المعلومات التعريفية الشـخصـية. **وثانيها**، أن يقدم إشـعار واضـح وجلي بفرصـة التقيد بجمع أو كشـف معلومات التعريف الشخصية للمستخدمين. **وثالثها**، ضرورة إخطار المستخدمين بأي تغيير في السياسة المعنية بجمع أو استخدام أو كشف معلومات المستخدم التعريفية الشـخصـية[2]. **رابعها**، أن يحافظ علي سرية وتكامل معلومات التعريف الشـخصـية وكفالتة لنظام تقني لحمايتها فضـــلا عن إتاحة الدخول علي المعلومات التي يتم جمعها والاحتفاظ بها من قبل المستخدم.

سابعاً: قانون تحديث الخصوصية لمواكبة عصر المعلومات لسنة 2011[3]:

مواكبة لعصـــر المعلومات والتوســع في اســتخدامات التكنولوجيا وانتشـــار معلومات التعريف الشـــخصـــية في أيدي الوكالات الحكومية جاء قانون تحديث الخصـوصـية، معززا العقوبات الجنائية والمدنية للإفصـاح غير الملائم عن معلومات

وقد خول المشـرع مفوضـية التجارة الفيدرالية سـلطة التفتيش علي شـركات تقديم خدمات البرامج التفاعلية والتحري عنها لتحديد ما إذا كانت متورطة أو مشـــاركة في أي عمل يحظره هذا القانون. فإذا ثبت ذلك كان لها أن تصـدر أمر بايقافها فضـلا عن تعرضـها للعقوبات المدنية المنصـوص عليها في القسم الخامس من هذا القانون.

Angela Choey, Protecting Privacy on the Internet, Alegislative Proposal, 1997. p. 7.

(1) Online Personal Privacy Act Available at https://www.congress.gov/bill/107th-congress/senate-bill/2201 .

(2) ***Andru E. Wall,*** Prying Eyes, The legal conseqences of Reading Your Spouses Electronic Mail, 30 FAM. L.Q. 2003. p. 56.

(3) The Privacy Act Modernization for the Information Age Act of 2011 Available at https://www.govtrack.us/congress/bills/112/s1732/text

التعريف الشخصية، مستحدثًا في ذات الوقت وظيفة كبير مسئولي الخصوصية الفيدرالي بمكتب الإدارة والميزانية.

كما توسع قانون تحديث الخصوصية لأجل مواكبة عصر المعلومات في سلطة التحري الممنوحة حاليا لإدارة كبار مسئولي الخصوصية بأمن البلاد لتمنح لمسئولي الخصوصية بالوكالات الأخري[1].

المبحث الثاني

حماية البيانات الشخصية في التشريعات العربية

بصفة عامة يمكن القول أن التشريعات العربية لم تتصد بنصوص جنائية عامة تدرج في قوانينها العقابية لمواجهة الاعتداءات الواقعة علي البيانات الشخصية المعالجة آليا كالتشريع الفرنسي، وإنما اكتفت بمحاولة تطويع النصوص العقابية القائمة للتطبيق علي الأنماط المختلفة للجريمة المعلوماتية، وتعد مصر نموذجًا بارزًا لهذا النمط من التشريعات.

في حين هجرت بعض من الدول العربية هذا النمط لكي تواجه الاعتداءات علي البيانات الشخصية المعالجة آليا عبر قوانين مكافحة جرائم التقنية.

وبالرغم من ذلك نجد هناك اتجاهًا تبنته نفر من الدول العربية اعتمد علي مواجهة الاعتداءات الواقعة علي البيانات الشخصية عبر القوانين الشاملة لحماية البيانات الشخصية.

وعليه سوف نتناول حماية البيانات الشخصية في التشريعات العربية في ثلاثة مطالب علي النحو التالي:

المطلب الأول: حماية البيانات الشخصية في التشريع المصري.

المطلب الثاني: حماية البيانات الشخصية عبر قوانين مكافحة جرائم التقنية.

---

(1) Annual Report on the Administration of the Privacy Act 2011-2012 Available at http://www.esdc.gc.ca/eng/transparency/ati/reports/annual_privacy/2011_2012/index.shtml retrived 162013/5/

المطلب الثالث: حماية البيانات الشخصية عبر التشريعات الشاملة لحماية البيانات.

المطلب الأول
حماية البيانات الشخصية في التشريع المصري

لم يصدر المشرع المصري قانونا خاصا لحماية البيانات الشخصية المعالجة آليا، بل لجأ عند إعداده لبعض التشـــريعات العامة والخاصـــة لإضـــافة مواد هدفها حماية هذا النوع من البيانات. حيث تقتصـر حماية البيانات الشـخصـية علي بعض الطوائف من البيانات الواردة في القوانين المختلفة. وســـوف نتناول حماية البيانات الشخصية في التشريع المصري في فرعين علي النحو التالي:

الفرع الأول: حماية البيانات الشخصية في التشريعات العامة.

الفرع الثاني: حماية البيانات الشخصية في التشريعات الخاصة.

الفرع الأول
حماية البيانات الشخصية في التشريعات العامة

تتمثل حماية التشـــريعات العامة للبيانات الشـــخصـــية في قانون العقوبات، وقانون الإجراءات الجنائية، وقانون الإثبات في المواد المدنية والتجارية.

أولاً: قانون العقوبات:

نصـت المادة 310 من قانون العقوبات علي جريمة إفشـاء الأسـرار، فأقرت بعقاب أي من الأطباء، أو الجراحين، أو الصـيادلة، أو القوابل، أو غيرهم إذا أفشـوا أســـرارًا أودعت إليهم بمقتضـــي وظيفتهم في غير الأحوال التي يلزمهم القانون فيها بتبليغ ذلك.

ويري جانب من الفقه أنه لا يمكن إعمال نص المادة 310 ســـالفة الذكر لتجريم إساءة استعمال البيانات المعالجة آليا؛ نظرًا لأن العبارات المستخدمة لا تحمل

إمكانية تطبيقها علي إفشـــاء المعلومات المخزنة علي قواعد البيانات، حيث يحظر القياس في تفسير النصوص الجنائية[1].

بينما يري جانب آخر أن البيانات الشـخصـية قد تشـمل في جزء منها علي بيانات تتعلق بأســـرار الناس، وأن يأتي العلم بها نتيجة مباشـــرة أعمال الوظيفة أو المهنة[2]، مثال ذلك الأطباء أو المختبرات أو المســـتشـــفيات الذين يقومون بحفظ المعلومات الخاصـة بمرضـاهم ولاسيما المتعلقة بالبيانات الحساسـة الخاصـة بالحالة الصـحية والحياة الجنسـية لهؤلاء، أو بيانات الحمض النووي والتحاليل والفحوصـات الطبية علي قواعد بيانات الحاسب الآلي الخاص بهم، كذلك المحامين الذي يحفظون معلومات تتعلق بموكليهه وقضـــاياهم[3]. لذلك إذا أفشـــي هؤلاء البيانات المثبتة علي قواعد البيانات الموجودة لديهم ارتكبوا الجريمة المنصـــوص عليها في المادة 310 عقوبات. ويســـتوي في ذلك أن تكون البيانات محفوظة علي قواعد للبيانات أو علي ملف لموقع من الإنترنت، كما يستوي لدي المشرع وسيلة الإفشاء أو كيفيته، سواء تم ذلك بالقول أو الفعل أو الكتابة، بما في ذلك استخدام الوسائل الإلكترونية[4].

---

(1) د/ أسامه عبد الله قايد، المرجع السابق، ص 133.

(2) د/ علاء محمود يسن حراز، المرجع السابق، ص 854.

(3) فقد أصبح من المعتاد الأن أن يقوم المحامون بإبداء الاستشارات القانونية عبر الإنترنت مقابل الأتعاب التي يقوم بســـدادها بطريق بطـاقـات الائتمـان أو بطريق التحويلات البنكيـة عبر الإنترنت، كذلك يقوم بعض الأطباء أو الصـــيادلة بتقديم خدماتهم عبر الإنترنت، وبالتأكيد يؤتمن كل من هؤلاء علي المعلومات التي أطلعهم عليها العملاء لإبداء الرأي أو الاسـتشـارة أو تقديم التشـخيص أو العلاج المناسـب، وبالتاكيد يقوم هؤلاء بحفظ هذه المعلومة الشـخصـية والخاصة علي قواعد للبيانات.

(4) د/ مدحت عبد الحليم رمضـــان، الحماية الجنائية للتجارة الإلكترونية – دراســـة مقارنة، دار النهضة العربية، 2001، ص 115–117.

ثانياً: قانون الإجراءات الجنائية:

أقرت المادة 57 من قانون الإجراءات الجنائية اعتبار إجراءات التحقيق والنتائج التي تسفر عنها من الأسرار، وأوجبت علي قضاة التحقيق، وأعضاء النيابة العامة، ومساعديهم من كتاب، وخبراء، وغيرهم ممن يتصلون بالتحقيق، أو يحضرونه بسبب وظيفتهم أو مهنتهم عدم إفشائها.

كما عاقبت المادة 58 من القانون نفسه كل من يكون قد وصل إلي علمه بسبب التفتيش عن معلومات الأشياء والأوراق المضبوطة، وأفضي بها إلي شخص ذي صفة، أو انتفع بها بأية طريقة كانت.

ثالثاً: قانون رقم 25 لسنة 1968 بشأن الأثبات في المواد المدنية والتجارية:

أوجبت المادة 65 من القانون رقم 25 لسنة 1968 بشأن الإثبات في المواد المدنية والتجارية علي الموظفين المكلفين بخدمة عامة ألا يشهدوا ولو بعد تركهم العمل عما يكون قد وصل إلي علمهم أثناء قيامهم به من معلومات لم تنشر بالطريق القانوني، ولم تأذن السلطة المختصة في إذاعتها، وسمحت لهذه السلطة أن تأذن لهم في الشهادة بناء علي طلب المحكمة أو أحد الخصوم.

كما حظرت المادة 66 من القانون نفسه علي من علم من المحامين، أو الوكلاء، أو الأطباء، أو غيرهم عن طريق مهنتهم أو صنعتهم بواقعة أو بمعلومات أن يفشوها ولو بعد انتهاء خدمتهم أو زوال صفتهم ما لم يكن ذكرها لهم مقصودًا به ارتكاب جناية أو جنحة، كما أوجبت علي الأشخاص المذكورين أن يؤدوا الشهادة علي تلك الواقعة أو المعلومات متي طلب ذلك من أسرها إليهم علي ألا يخل ذلك بأحكام القوانين الخاصة بهم.

وتجدر الإشارة إلي أن القانون رقم 25 لسنة 1968 سالف الذكر لا يحمي سوي البيانات التي تعد من قبيل الأسرار المهنية، شأنه في ذلك شأن المادة 310 من قانون العقوبات.

الفرع الثاني
حماية البيانات الشخصية في التشريعات الخاصة

تقتصر حماية البيانات الشخصية في القانون الجنائي المصري علي طوائف مختلفة من البيانات تناولتها بعض القوانين الجنائية الخاصة، وهي كالآتي:

أولاً: قانون الإحصاء والتعداد الصادر بقرار رئيس الجمهورية رقم 35 لسنة 1960 المعدل بالقانون رقم 28 لسنة 1982:

أصدر المشرع المصري القانون المشار إليه لينظم عملية الإحصاء والتعداد لبيانات المواطنين، وقد تضـــمن هذا القانون بعض المواد التي تهدف إلي حماية البيانات الشخصية التي تم إحصاؤها[1]، وتتمثل هذه المواد في الآتي:

المادة الثالثة: أكدت هذه المادة ســـرية البيانات الفردية التي تجمع لأغراض التعداد والإحصـــاءات الســـكانية، فحظرت إطلاع أي فرد أو هيئة عامة أو خاصـــة عليها أو إبلاغ شـيء منها، كما أوجبت عدم اسـتخدامها لغير الأغراض الإحصـائية أو نشـر ما يتعلق منها بالأفراد إلا بمقتضـي إذن مكتوب من ذوي الشـأن. وحظرت كذلك اسـتغلال أي بيان إحصـائي كأسـاس لربط ضـريبة أو لترتيب أي عبء مالي آخر، أو اتخاذه دليلا في جريمة، أو أساسًا لأي عمل قانوني.

المادة الرابعة: عاقبت بالحبس مدة لا تقل عن شهر ولا تزيد عن ستة أشهر وغرامة لا تقل عن مائة جنيه ولا تتجاوز خمســـمائة جنيه أو بإحدي هاتين العقوبتين لـ:.

1- كل من أخل بسـرية البيانات الإحصـائية، أو أفشـي بيانًا من البيانات الفردية أو سرًا من أسرار الصـناعة أو التجارة، أو غير ذلك من أساليب العمل التي يكون اطلع عليها بمناسبة عمله في الإحصاء أو التعداد.

---

[1] د/ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصـــنفات الفنية، دراســـة مقارنة، منشأة المعارف بالإسكندرية، 2000، ص 288.

2- كل من حصـــل بطريق الغش أو التهديد أو الإيهام بأية وســـيلة أخري علي بيانات أو معلومات سرية بشأن الإحصاءات أو التعدادات أو شرع في ذلك.

نخلص مما ســـبق أن هذا القرار بقانون يحمي هذا النوع من البيانات والمعلومات الفردية عن المواطنين أيًا كانت الوســـيلة التي يحتفظ بها بما في ذلك حفظها وتخزينها في نظم المعلومات ويشـــمل كافة أنواع الأنشـــطة التي تؤدي إلي الاطلاع عليها أو تمكن من الحصـــول عليها، وجعل المحافظة علي ســـريتها واقعة علي عاتق من له صلة بتلك البيانات بحكم طبيعة عمله.

ثانياً: قانون الأحوال المدنية رقم 143 لسنة 1994:

نظرًا لقيام قطاع الأحوال المدنية بوزارة الداخلية باستخدام سجلات إلكترونية في حفظ البيانات الشخصية للمواطنين، فقد أصدر المشرع قانون الأحوال المدنية الجديد رقم 143 لسنة 1994 الذي ألغي قانون الأحوال المدنية القديم رقم 260 لسنة 1960. وقد أقر قانون الأحوال المدنية الجديد حماية البيانات الشـــخصـــية المعالجة آليا[1]، وذلك من خلال المواد التالية:

المادة الثالثة عشرة: أكدت علي سرية البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين والتي تشـتمل عليها السـجلات أو الدفاتر أو الحاسـبات الآلية أو وسـائط التخزين الملحقة، ولم تسـمح هذه المادة بالإطلاع عليها أو الحصـول علي بياناتها، إلا في الأحوال التي نصـت عليها هذه المادة[2]. بل أن المشـرع المصـري اعتبر أن المعلومات أو البيانات أو الإحصـــائيات المجمعة التي تشـــتمل عليها الســـجلات والدفاتر الإلكترونية ســـرًا قوميًا لا يجوز الإطلاع عليها أو نشـــرها إلا لمصـــلحة قومية أو علمية وبإذن كتابي من مدير مصـــلحة الأحوال المدنية أو من ينيبه وفقًا للأوضاع والشروط التي يحددها القانون واللائحة التنفيذية (المادة 2/13).

---

(1) د/ عمر أبو الفتوح عبد العظيم الحمامي، الحماية الجنائية للمعلومات المســـجلة إلكترونيًا ، دراسة مقارنة، دار النهضة العربية، 2010، ص 356 وما بعدها.

(2) د/ محمد هشام فريد رستم، المرجع السابق، ص 370.

كما حظرت الفقرة الثالثة من ذات المادة نقل السجلات سالفة الذكر في غير أغراض العمل الرسمية. وأوجبت علي النيابة العامة إذا أصدرت قرارًا بالاطلاع أو فحص هذه السجلات، أن ينتقل القاضي المنتدب أو المحقق للاطلاع والفحص في الجهة المحفوظ بها السجلات، أو أن يطلب صورة من الواقعة أو البيانات المسجلة، أو صورة طبق الأصل من المستند المدخلة بياناته بالسجلات، إلا إذا كان هذا المستند محلا لتحقيق في جريمة تزوير (المادة 4/13).

المادة الخامسة والستون: أوجبت هذه المادة علي مصلحة الأحوال المدنية اتخاذ كافة التدابير اللازمة لتأمين البيانات الشخصية والمجمعة والمخزنة بالحاسبات الآلية أو بوسائط التخزين الملحقة بها ضد أي اختراق، أو عبث، أو اطلاع، او إفشاء، او تدمير ، أو مساس بها بأية صورة كانت.

المادة الرابعة والسبعون: عاقبت هذه المادة بالحبس والغرامة أو بإحدهما كل من اطلع، أو شرع في الاطلاع أو الحصول علي البيانات أو المعلومات التي تحويها السجلات، أو الحاسبات الآلية، أو وسائط التخزين الملحقة بها، أو قام بتغييرها بالإضافة و بالحذف أو بالإلغاء أو بالتبديد، أو المساس بها بأي صورة من الصور أو إذاعتها أو إفشائها، في غير الأحوال التي نص عليها القانون. أما إذا وقعت الجريمة علي البيانات أو المعلومات أو الإحصاءات المجمعة تكون العقوبة السجن.

المادة السادسة والسبعون: عاقبت هذه المادة بالسجن المشدد كل من اخترق أو حاول اختراق سرية البيانات أو المعلومات أو الإحصاءات المجمعة بأي صورة من الصور [1].

---

[1] بذلك ساوي المشرع المصري بين الاختراق الفعلي لسرية البيانات و محاولة الاختراق في العقوبة المقررة إمعانًا منه في تقرير الحماية اللازمة لهذه البيانات، بجعل عقوبة الشروع هي نفس عقوبة الجريمة التامة بالاختراق الفعلي، ولعله في ذلك تأثر بقانون الغش المعلوماتي الفرنسي رقم 19 لسنة 1999 الذي ساوي بين الجريمة التامة والشروع في العقوبة.

وهذه الجريمة عمدية يكفي فيها القصد الجنائي العام بعنصريه العلم والإرادة، فيكتفي بأن يكون الفاعل عالمًا بأنه يخترق أو يحاول اختراق سرية البيانات أو المعلومات الخاصة بمصلحة الأحوال المدنية، وأن تتجه إرادته إلي الاختراق أو محاولة اختراق هذه السرية، ولا يشترط قصد جنائي خاص مثل نية الإضرار بالغير [1].

ثالثاً: قانون البنك المركزي والجهاز المصرفي والنقد رقم 88 لسنة 2003:

سبق لنا القول بأن البيانات المالية للفرد تُعد من قبيل البيانات الشخصية، وقد أصدر المشرع المصري قانون البنك المركزي والجهاز المصرفي والنقد رغبة منه في حماية هذا النوع من البيانات. وقد أقرت المواد (97 ، 98، 100) من الباب الرابع من هذا القانون الحفاظ علي سرية حسابات العملاء[2]، وذلك علي النحو التالي:

المادة السابعة والتسعون: أكدت علي سرية حسابات العملاء، وودائعهم، وأماناتهم، وخزائنهم في البنوك، وكذلك المعاملات المتعلقة بها، وحظرت الاطلاع عليها وإعطاء بيانات عن طريق مباشر أو غير مباشر إلا بإذن كتابي من صاحب الحساب، أو الوديعة، أو الأمانة، أو الخزينة، أو من أحد ورثته، أو من أحد الموصي لهم بكل أو بعض هذه الأموال، أو النائب القانوني، أو الوكيل المفوض في ذلك، أو بناء علي حكم قضائي، أو حكم من المحكمين.

المادة الثامنة والتسعون: سمحت هذه المادة للنائب العام، أو لمن يفوضه من المحامين العامين الأول علي الأقل من تلقاء نفسه، أو بناء علي طلب جهة رسمية، أو أحد من ذوي الشأن أن يطلب من محكمة استئناف القاهرة الأمر بالاطلاع أو

---

[1] د/ عمر أبو الفتوح عبد العظيم الحمامي، المرجع السابق، ص 363.

[2] د/ شمس الدين إبراهيم أحمد، وسائل مواجهة الاعتداءات علي الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، دراسة مقارنة، دار النهضة العربية، الطبعة الأولي 2005، ص 198 وما بعدها.

الحصـول علي أية بيانات أو معلومات تتعلق بالحسـابات، أو الودائع، أو الأمانات، أو الخزائن المنصـــوص عليها في المادة الســـابقة، أو المعاملات المتعلقة بها إذا اقتضي ذلك كشف الحقيقة في جناية أو جنحة قامت الدلائل الجدية علي وقوعها.

المادة المائة: حظرت هذه المادة علي رؤســـاء، أو أعضـــاء مجالس إدارة البنوك ومديريها، أو العاملين بها إعطاء أو كشف أية معلومات أو بيانات عن عملاء البنوك، أو حســـاباتهم، أو ودائعهم، أو الأمانات، أو الخزائن الخاصـــة بهم، أو معاملاتهم في شأنها، أو تمكين الغير من الاطلاع عليها في غير الحالات المرخص بها بمقتضي أحكام هذا القانون.

رابعاً: قانون الضريبة علي الدخل رقم 91 لسنة 2005:

رغبة من المشـرع في الحفاظ علي بيانات الملف الضـريبي للممول، فقد أقر المشـرع في قانون الضـريبة علي الدخل رقم 91 لسـنة 2005 حماية هذا النوع من البيانات، وذلك بموجب المادة 101 التي تقع ضـــمن الباب الرابع المعنون باســـم الفحص والتحريات من القانون المشار إليه.

وقد أوجبت هذه المادة علي كل شـــخص يكون لـه بحكم وظيفتـه، أو اختصاصـه، أو عمله شأن في ربط أو تحصيل الضرائب المنصوص عليها في هذا القانون، أو الفصل فيما يتعلق بها من منازعات بمراعاة سرية المهنة.

كما حظرت الفقرة الثانية من ذات المادة علي أي من العاملين بالمصـــلحة ممن لا يتصل عملهم بربط أو تحصيل الضريبة إعطاء أي بيانات، أو إطلاع الغير علي أية ورقة، أو بيان، أو ملف، أو غيره إلا في الأحوال المصرح بها قانونًا.

كما حظرت الفقرة الثالثة من ذات المادة إعطاء بيانات من الملفات الضريبية إلا بناءً علي طلب كتابي من الممول، أو بناءً علي نص في أي قانون آخر.

وتجدر الإشارة إلي عدم تضمن القانون رقم 91 لسنة 2005 سالف الذكر عقوبة لمخالفة الالتزام بمراعاة سرية هذه البيانات، ومن ثم لا مناص من الرجوع إلي نص المادة 310 من قانون العقوبات.

خامساً: قانون الكسب غير المشروع رقم 62 لسنة 1975:

المادة السابعة عشرة: أقرت هذه المادة سرية الإقرارات المنصوص عليها في هذا القانون والشكاوي التي تقدم عن كسب غير مشروع وما يجري في أنها من فحص وتحقيق، كما أوجبت علي كل من له شأن في تنفيذ هذا القانون عدم إفشائها.

المادة الثامنة عشرة: حظرت هذه المادة علي الجهات والهيئات المنوط بها تلقي الإقرارات وحفظها، أو تداولها، أو فحصها، أو إجراء التحقيق، أو التصرف فيها، أن تفشي ما بها من بيانات، واعتبرت هذه المادة الإقرارات والشكاوي التي تقدم عن كسب غير مشروع من الأسرار.

وتجدر الإشارة إلي أن هذا القانون يعد بمثابة تشريع خاص وضع لتقرير الحماية القانونية لنوع محدد من البيانات وهي الإقرارات والشكاوي التي تقدم عن كسب غير مشروع.

مما سبق يتضح لنا أن المشرع المصري لم يأت بحماية شاملة أو وافية لما يمكن أن يواجه البيانات الشخصية المعالجة آليا من اعتداءات، فلم يصدر قانونًا خاصًا لحماية هذه البيانات أسوة بنظيره الفرنسي، كما لم يصدر أيضا قانونًا لمكافحة جرائم التقنية، وإنما لجأ في هذا الشأن إلي التشريعات العامة والخاصة بإضافة مواد هدفها حماية هذا النوع من البيانات، ومن ثم جاءت حمايته للبيانات الشخصية عمومًا والبيانات الشخصية المعالجة آليا حماية معيبة وقاصرة.

المطلب الثاني
حماية البيانات الشخصية عبر قوانين
مكافحة جرائم التقنية

يمكن القول أن أغلبية دول الخليج العربي قد أصـــدرت تشـــريعات خاصـــة لمكافحة جرائم التقنية، وقد تضـمنت هذه التشـريعات مواد عدة تتعلق بحماية البيانات الشـخصـية المعالجة آليا. وسـوف نتناول حماية البيانات الشـخصـية عبر تشـريعات مكافحة جرائم التقنية في تلك الدول علي النحو التالي:

الفرع الأول: الإمارات العربية المتحدة.

الفرع الثاني: المملكة العربية السعودية.

الفرع الثالث: مملكة البحرين.

الفرع الرابع: سلطنة عمان.

الفرع الخامس: الكويت.

الفرع الأول
الإمارات العربية المتحدة

أصـدر المشـرع الإماراتي المرسـوم بقانون رقم 5 لسـنة 2012 بشـأن مكافحة جرائم تقنيـة المعلومـات. وقد جرم هذا القانون في بعض مواده الأفعـال التي تتعلق بالمساس بالبيانات الشخصية المعالجة آليا عبر المواد الأتية:

المادة السـابعة: عاقبت هذه المادة كل من حصـل، أو اسـتحوذ، أو عدَل، أو أتلف بغير تصـــريح بيانات أي مســـتند إلكتروني، أو معلومات الكترونية عن طريق الشـــبكة المعلوماتية، أو موقع إلكتروني، أو نظام المعلومات الإلكتروني، أو وســـيلة تقنيـة المعلومات وكانت هذه البيانـات أو المعلومات تتعلق بفحوصـــــات طبية، أو تشخيص طبي، أو علاج، أو رعاية طبية، أو سجلات طبية.

المادة الثانية عشرة: عاقبت هذه المادة كل من توصـل بغير حق، عن طريق اســـتخدام الشـــبكة المعلوماتية، أو نظام معلومات إلكتروني، أو إحدي وســـائل تقنية

المعلومات، إلي أرقام، أو بيانات بطاقة ائتمانية أو إلكترونية، أو أرقام أو حسابات مصرفية، أو أي وسيلة من وسائل الدفع الإلكتروني. كما تعاقب هذه المادة كل من نشر أو أعاد نشر هذه البيانات.

المادة الخامسة عشرة: تعاقب هذه المادة كل من التقط أو اعترض عمدًا وبدون تصريح أي اتصال عن طريق أي شبكة معلوماتية، كما تعاقب كل من أفشي المعلومات التي حصل عليها عن طريق استلام أو اعتراض الاتصالات بغير وجه حق.

المادة الحادية والعشرون: تعاقب هذه المادة كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدي وسائل تقنية المعلومات، في الاعتداء علي خصوصية شخص في غير الأحوال المصرح بها قانونًا بإحدي الطرق التالية:

1- استراق السمع، أو اعتراض، أو تسجيل، أو نقل، أو بث، أو إفشاء محادثات، أو اتصالات، أو مواد صوتية، أو مرئية.
2- التقاط صور الغير، أو إعداد صور إلكترونية، أو نقلها، أو كشفها، أو نسخها، أو الاحتفاظ بها.
3- نشر أخبار، أو صور إلكترونية، أو صور فتوغرافية، أو مشاهدة، أو تعليقات، أو بيانات، أو معلومات، ولو كانت صحيحة وحقيقية.

كما تعاقب هذه المادة كل من أجري تعديلًا أو معالجة علي تسجيل، أو صورة أو مشهد، بقصر التشهير أو الإساءة إلي شخص آخر، أو الاعتداء علي خصوصيته أو انتهاكها.

الفرع الثاني

المملكة العربية السعودية

أصدر المنظم السعودي قانون مكافحة الجرائم المعلوماتية لسنة 2007. وقد جرم هذا القانون في بعض مواده الأفعال التي تتعلق بالمساس بالبيانات الشخصية المعالجة آليا وهذه المواد هي:

المادة الثالثة: تعاقب هذه المادة كل من تنصت علي ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ قانوني صحيح – أو التقاطه، أو اعتراضه. كما تعاقب أيضا كل من انتهك حرمة الحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرات أو ما في حكمها.

المادة الرابعة: تعاقب هذه المادة كل من اطلع – دون مسوغ قانوني صحيح – علي أية بيانات بنكية أو ائتمانية، للحصول علي أموال، او ما تتيحه من خدمات.

المادة الخامسة: تعاقب هذه المادة علي الدخول غير المشروع لإلغاء بيانات خاصة، أو حذفها، أو تدميرها، أو تسريبها، أو إتلافها، أو تغييرها، أو إعادة نشرها. كما تعاقب علي إيقاف الشبكة المعلوماتية عن العمل، أو تعطيلها، أو تدمير أو مسح البرامج أو البيانات الموجودة أو المستخدمة فيها، أو حذفها، أو تسريبها، أو إتلافها، أو تعديلها، أو إعاقة الوصول إلي الخدمة، أو تشويهها، أو تعطيلها، بأي وسيلة.

المادة السادسة: تعاقب هذه المادة علي إنتاج ما من شأنه المساس بالنظام العام، أو القيم الدينية، أو الآداب العامة، أو حرمة الحياة الخاصة، أو إعداده، أو إرساله، أو تخزينه عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي.

وقد أعطت المادة رقم 14 من القانون سالف الإشارة إليه لهيئة الاتصالات وتقنية المعلومات وفقًا لاختصاصها تقديم الدعم والمساندة الفنية للجهات الأمنية المختصة خلال مراحل ضبط هذه الجرائم، والتحقيق فيها، وأثناء المحاكمة.

الفرع الثالث

مملكة البحرين

أصدر المشرع البحريني المرسوم بقانون رقم 60 لسنة 2014 بشأن مكافحة جرائم تقنية المعلومات. وقد تضـــمن هذا القانون مواد عدة تتعلق بحماية البيانات الشخصية المعالجة آليا وهذه المواد هي:

المادة الثالثة: تعاقب هذه المادة كل من أحدث تلفًا في بيانات وســـيلة تقنية المعلومات، وضـــاعفت العقوبة إذا ترتب علي ارتكاب الجريمة تغيير أو تعييب أو شطب فحوص طبية أو تشخيص طبي أو علاج إنسان.

المادة الرابعة: تعاقب هذه المادة كل من تنصـت، أو التقط، أو اعترض دون مسوغ قانوني مستخدمًا وسائل فنية، إرسالًا غير موجه للعموم لبيانات وسيلة تقنية المعلومات، ســـواء كانت البيانات مرســـلة من نظام تقنية المعلومات، أو إليه، أو ضمنه، ويشمل هذا الإرسال أي انبعاثات لموجات كهرومغناطيسية من نظام تقنية المعلومات تحمل معها هذه البيانات. وإذا نتج عن التنصـــت، أو الالتقاط، أو الاعتراض إفشاء للإرسال، أو جزء منه دون مسوغ قانوني عد ذلك ظرفا مشددًا.

الفرع الرابع

سلطنة عمان

أصدر المشرع العماني المرسوم بقانون رقم 12 لسنة 2011 بشأن مكافحة جرائم تقنية المعلومات. وقد جرم هذا القانون في بعض مواده الأفعال التي تتعلق بالمساس بالبيانات الشخصية المعالجة آليا وهذه المواد هي:

المادة الخامســـة: تعاقب هذه المادة كل من غير، أو عدل، أو أتلف عمدًا ودون وجه حق باســـتخدام وســـائل تقنية المعلومات بيانات، أو معلومات إلكترونية عبارة عن تقرير فحص، أو تشـــخيص، أو علاج، أو رعاية طبية مخزن في نظام معلوماتي، أو وسائل تقنية معلومات.

المادة الثامنة: تعاقب هذه المادة كل من اعترض عمدًا ودون وجه حق باستخدام وسائل تقنية المعلومات خط سير البيانات أو المعلومات الإلكترونية المرسلة عبر الشبكة المعلوماتية أو وسائل تقنية المعلومات أو قطع بثها أو استقبالها أو تنصت عليها.

المادة السادة عشر: تعاقب هذه المادة كل من استخدم الشبكة المعلوماتية، أو وسائل تقنية المعلومات كالهواتف النقالة المزودة بآلة تصوير في الاعتداء علي حرمة الحياة الخاصة، أو العائلية للأفراد وذلك بالتقاط صور، أو نشر أخبار، أو تسجيلات صوتية، أو مرئية تتصل بها ولو كانت صحيحة، أو في التعدي علي الغير بالسب، أو القذف.

الفرع الخامس

الكويت

أصدر المشرع الكويتي المرسوم بقانون رقم 63 لسنة 2015 بشأن مكافحة جرائم تقنية المعلومات. وقد جرم هذا القانون في بعض مواده الأفعال التي تتعلق بالمساس بالبيانات الشخصية المعالجة آليا وهذه المواد هي:

المادة الثالثة: تعاقب هذه المادة كل من غيّر، أو أتلف عمدًا مستندًا إلكترونيًا يتعلق بالفحوصات الطبية، أو التشخيص الطبي، أو العلاج الطبي، أو الرعاية الطبية، أو سهل للغير فعل ذلك، أو مكنه منه، وذلك باستعمال الشبكة المعلوماتية، أو باستخدام وسيلة من وسائل تقنية المعلومات.

المادة الرابعة: تعاقب هذه المادة كل من تنصت، أو التقط، أو اعترض عمدًا، دون وجه حق، ما هو مرسل عن طريق الشبكة المعلوماتية، أو وسيلة من وسائل تقنية المعلومات، وتشدد العقوبة إذا أفشي ما توصل إليه.

المادة الخامسة: تعاقب هذه المادة كل من استخدم الشبكة المعلوماتية، أو إحدي وسائل تقنية المعلومات للوصول دون وجه حق إلي أرقام، أو بيانات بطاقة ائتمانية، أو ما في حكمها من البطاقات الإلكترونية.

المطلب الثالث

حماية البيانات الشخصية عبر القوانين الشاملة لحماية البيانات

فرضت تشريعات حماية البيانات في الدول التي أخذت بمبدأ الحماية الشاملة للبيانات الشخصية [1]، حماية جنائية للمعطيات ذات الطابع الشخصي حيث جرمت مجموعة من الأفعال التي تشكل اعتداءً علي كل من القواعد الموضوعية والقواعد الإجرائية التي يلزم علي المسئول أو القائم بالمعالجة مراعاتها. وسوف نتناول كلا النوعين من الجرائم في فرعين مستقلين علي النحو التالي:

الفرع الأول: الجرائم الماسة بالقواعد الموضوعية لمعالجة البيانات.

الفرع الثاني: الجرائم الماسة بالقواعد الشكلية لمعالجة البيانات.

الفرع الأول

الجرائم الماسة بالقواعد الموضوعية لمعالجة البيانات

تتمثل الجرائم الماسة بالقوعد الموضوعية لمعالجة البيانات ذات الطابع الشخصي في طائفتين من الجرائم: أولهما، الجرائم المتعلقة بتسيير المعطيات الشخصية، وثانيهما، الجرائم المتعلقة بحقوق الشخص المعني، وذلك علي التفصيل التالي:

أولاً: الجرائم المتعلقة بتسيير معالجة البيانات الشخصية:

جرم المشرع في هذه التشريعات مجموعة من الأفعال التي تشكل خرقًا للقواعد الموضوعية التي يلزم علي المسئول عن معالجة البيانات ذات الطابع

---

[1] تمثل هذه التشريعات في التشريعات الأتية: التشريع التونسي رقم 24 لسنة 2004 الصادر في 27 يونيه 2004 المتعلق بحماية المعطيات الشخصية، والتشريع المغربي 09.08 الصادر في 18 فبراير 2009 والمتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، والتشريع القطري رقم 13 لسنة 2016 بشأن حماية خصوصية البيانات الشخصية.

الشـــخصـــي مراعاتها عند القيام بكل معالجة لهذه البيانات. وقد تتعلق هذه الأفعال بتسـيير المعطيات، كجريمة المعالجة غير المشـروعة أو الاسـتعمال غير المشـروع للبيانات.

أ- جريمة المعالجة غير المشروعة:

جرمت تشـــريعات حماية البيانات الســـابقة الإشـــارة إليها المعالجة غير المشـــروعة للبيانات الشـــخصـــية. ويتعين لقيام هذه الجريمة توافر ركنين مادي، ومعنوي.

ويتحقق الركن المادي لهذه الجريمة بتوافر أحد عنصـرين: **أولهما**، الجمع أو المعالجة غير المشروعة للمعطيات الشخصية[1]. وتشتمل علي الأفعال الآتية:

1- إنجاز معالجة لأغراض أخري غير المصرح بها أو المرخص لها.
2- إخضـــاع المعطيات الشـــخصـــية لمعالجة لاحقة متعارضـــة مع الأغراض المصرح بها أو المرخص لها.

ثانيهما، حفظ المعطيات الشخصية لمدة تزيد عن المدة القانونية المنصوص عليها في النصـوص التشـريعية المعمول بها أو المنصـوص عليها في التصـريح أو الإذن.

أما فيما يتعلق بالركن المعنوي، فيتخذ صـورة القصـد الجنائي العام بعنصـريه العلم والإرادة، إذ يجب أن يعلم الجاني بالطبيعة الشـــخصـــية للمعطيات ونشـــاط معالجتها وبعدم مشروعيتها كما لو مارس جمعًا للمعطيات الشخصية بطريقة تدليسية أو غير نزيهة أو غير مشـروعة أو إنجاز معالجة تتنافي مع الأغراض المصـرح بها أو المرخص لها أو إخضاعها لمعالجة لاحقة تتنافي مع هذه الأغراض.

---

(1) انظر: المادة 54 من التشريع المغربي 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشـخصـي المقابلة للمادة 94 من التشـريع التونسـي الخاص بحماية البيانات الشخصية، والمادة 10، 23 من التشريع القطري الخاص بحماية البيانات الشخصية.

كما تتحقق الجريمة بقيام المتهم بالاحتفاظ بالمعطيات ذات الطابع الشخصي لمدة تزيد عن المدة القانونية أو لاحتفاظه بهذه المعطيات لمدة تتجاوز المدة اللازمة لإنجاز الغايات التي تم جمعها ومعالجتها لاحقا من أجلها.

ويشـترط لتحقق الركن المعنوي لهذه الجريمة أن تتجه إرادة الجاني إلي القيام بهذه الأفعال بذاتها، وإلا انتفي القصد الجنائي ومن ثم الركن المعنوي لهذه الجريمة.

وقد عاقب المشـــرع المغربي عن الأفعال الســـابقة المكونة لجريمة المعالجة غير المشروعة بعقوبة الحبس من 3 أشـهر إلي سـنة وبغرامة من 20 ألف درهم إلي 200 ألف درهم أو بإحدهما[1][2]. في حين قصـــرها المشـــرع القطري علي عقوبة الغرامة فقط[3]. بينما عاقب عليها المشرع الفرنسي بعقوبة الحبس لمدة خمس سنوات وغرامة مقدارها 300 آلف يورو، حيث يلزم الحكم بهما معًا.

ب-جريمة الاستعمال غير المشروع للمعطيات:

جرم المشرع المغربي في المادة 61 من القانون رقم 09.08 المتعلق بحماية الأشـخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشـخصـي الاسـتعمال غير المشـروع للمعطيات الشـخصـية حيث ينبغي لقيام هذه الجريمة توافر ركنين مادي، ومعنوي.

ويتحقق الركن المادي لهذه الجريمة بتوافر العنصـــرين التاليين معا: أولهما، أن ترتكب هذه الجريمة من قبل أشخاص معينين (المسئول عن المعالجة، أو المعالج

---

(1) راجع المادة 54، 55 من التشـــريع المغربي رقم 09.08 المتعلق بحماية الأشـــخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

(2) بينما جعلها المشرع التونسـي السـجن ثلاثة أشـهر والغرامة التي مقدارها 3 ألف دينار(الفصـل 94) من القانون التونسي رقم 24 لسنة 2004 المتعلق بحماية المعطيات الشخصية.

(3) إذا نصـت المادة 23 من قانون حماية البيانات الشـخصـية القطري علي عقوبة الغرامة بمقدار مليون ريال؛ وذلك لمخالفة حكم المادة 10 الخاصة بالمعالجة غير المشروعة للبيانات.

من الباطن، أو الشـــخص المكلف بالمعالجة). وثانيهما، التســـبب في الاســـتعمال التعسفي أو التدليسي للمعطيات المعالجة أو المستلمة أو تسهيل ذلك بالأهمال.

أما فيما يتعلق بالركن المعنوي، فإنه يتطلب قصـدًا جنائيا يوحي بعلم الجاني بان الأفعال التي يقوم بها من شـأنها أن تسـبب أو تسـهل الاسـتعمال التعسـفي للمعطيات المعالجة أو المســتلمة، وإرادته إلي القيام بهذه الجريمة. كما يمكن أن ترتكب هذه الجريمة عن طريق الخطأ، ولا يلزم أن يكون الخطأ المرتكب في صـــورة إهمال فقط، بل يمكن أن يكون في أي صورة من صور الخطأ كعدم التبصر[1].

وهكذا سايرت المادة 61 من التشريع المغربي سالف الذكر المادة 22/226 عقوبات فرنســـي التي اعتبرت هذه الجريمة يمكن ان ترتكب عن طريق القصـــد أو الخطأ.

وقد عاقب المشـرع المغربي عن الأفعال السـابقة المكونة لجريمة الاسـتعمال غير المشـروع للمعطيات بعقوبة الحبس من 6 أشـهر إلي سـنة وبغرامة من 20 ألف درهم إلي 200 ألف درهم أو بإحدي هاتين العقوبتين فقط، بينما جعلها المشـــرع التونسي السجن ثلاثة أشهر والغرامة التي مقدارها ألف دينار (الفصل 94). في حين قصرها المشرع القطري علي عقوبة الغرامة فقط[2].

ثانياً: الجرائم المتعلقة بحقوق الشخص المعني بالبيانات:

كما جرم المشـرع مجموعة من الأفعال التي تشـكل خرقًا للقواعد الموضـوعية الواجب مراعاتها عند القيام بمعالجة للمعطيات ذات الطابع الشـخصـي. جرم أيضًـا مجموعة من الأفعال تشـكل اعتداءً علي حقوق الشـخص المعني أو انتقاصًـا منها

---

(1) راجع: ابا زيد، الحماية الجنائية للمعطيات ذات الطابع الشخصي، المرجع السابق.

(2) إذا نصت المادة 24 من قانون حماية البيانات الشخصية القطري علي عقوبة الغرامة بمقدار 5 مليون ريال؛ وذلك لمخالفة حكم المادة 13 الخاصة بالاستخدام غير المشروعة للبيانات.

كالمعالجة بدون رضـــاء هذا الشـــخص أو الاعتداء علي حقوقه المنصـــوص عليها قانونا.

أ- جريمة المعالجة بدون رضا الشخص المعني:

تتحقق هذه الجريمة من خلال القيام بمعالجة البيانات ذات الطابع الشخصي دون الحصول علي الموافقة المسبقة للشخص المعني. ولكي تقوم هذه الجريمة يتعين توافر الركنين المادي والمعنوي:

ويقوم الركن المادي لهذه الجريمة بتحقق العناصـــر التالية: أولها، إجراء معالجة للبيانات الشخصية، وثانيها، القيام بالمعالجة دون رضا الشخص المعني. وثالثها، ألا تتعلق المعالجة بالحالات المستثناة من شرط الموافقة المسبقة للشخص المعني.

أما فيما يخص الركن المعنوي فيتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة أي يجب أن يعلم الجاني بإنه يقوم بفعل يشـــكل معالجة للبيانات الشخصية، وأن هذه المعالجة يجريها دون رضا مسبق للشخص المعني، ودون أن تندرج معالجته ضمن الاستثناءات التي أوردها المشرع والتي لا يتطلب فيها الحصول علي الرضا المسبق لهذا الشخص. بالإضافة إلي اتجاه إرادة الجاني إلي القيام بهذه الأفعال وإلي تحقيق نتيجتها.

وقد عاقب المشـــرع المغربي عن الأفعال الســـابقة المكونة لجريمة المعالجة بدون رضا الشخص المعني بعقوبة الحبس من 3 أشهر إلي سنة وبغرامة من 20 ألف درهم إلي 200 ألف درهم أو بإحدي هاتين العقوبتين[1]، بينما عاقب عليها

[1] راجع المادة 56 من التشـــريع المغربي رقم 09.08 المتعلق بحماية الأشـــخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي.

المشـرع التونســي بعقوبة الســجن مدة سـنتين بالإضــافة إلي الغرامة عشـرة آلاف دينار[1]، في حين قصرها المشرع القطري علي عقوبة الغرامة فقط[2].

ب- جريمة الاعتداء علي حقوق الشخص المعني:

تتحقق هـذه الجريمـة من خلال الاعتـداء علي حقوق الشـــخص المعني بالبيانات والتي كفلها له القانون. ولكي تقوم هذه الجريمة يتعين توافر الركنين المادي والمعنوي.

ويقوم الركن المادي لهذه الجريمة بتحقق أحد العنصرين الآتيين:

1- رفض ممارســة الشــخص المعني بالبيانات لحق الولوج أو التصــحيح أو الاعتراض.

2- إجراء المعالجة رغم اعتراض الشـخص المعني شـريطة أن يكون الاعتراض مبنيًا علي أسباب مشروعة.

ونلفت الانتباه إلي أن جريمة الاعتداء علي حقوق الشـــخص المعني في صــورتيها هي جريمة شــكلية لا يتوقف قيامها علي تحقق نتيجة معينة كالإضــرار بالحياة الخاصــة للشــخص المعني مثلا، بل تتوافر بمجرد رفض المســئول عن المعالجة لحقوق الشــخص المعني، أو إجرائه المعالجة بالرغم من اعتراض الأخير علي ذلك.

أما فيما يتعلق بالركن المعنوي فيتخذ صـورة القصـد الجنائي العام بعنصـريه العلم والإرادة، أي يجب أن يعلم الجاني أنه يرتكب فعل يشكل رفضا للحق في الولوج أو الحق في التصــحيح أو الحق في الاعتراض، أو أنها تشــكل معالجة لمعطيات

---

[1] إذا نصـت المادة 23 من قانون حماية البيانات الشـخصـية القطري علي عقوبة الغرامة بمقدار مليون ريال؛ وذلك لمخالفة حكم المادة 4 الخاصــة بضــرورة الحصــول علي موافقة الشــخص المعني علي معالجة بياناته.

[2] راجع (الفصــل 87) من القانون التونســي رقم 24 لســنة 2004 المتعلق بحماية المعطيات الشخصية.

شخصية متعلقة بشخص طبيعي رغم اعتراضه المبني علي أسباب مشروعة، وأن تتجه إرادته للقيام بهذه الأفعال دون غيرها.

عاقب المشرع المغربي عن هذه الجريمة بعقوبتين مختلفتين، حيث عاقب في المادة 53 علي الفعل المكون لرفض حق الولوج أو التصحيح أو الاعتراض بعقوبة مخففة تتمثل في الغرامة فقط. في حين عاقب عنها المشرع التونسي بالسجن مدة ثمانية أشهر وبغرامة 3 آلاف دينار (الفصل 92). فيما عاقب المشرع الفرنسي عن هذا الفعل بالحبس سنة واحدة وغرامة تصل إلي 300 ألف يورو (المادة 19/226-1 عقوبات).

أما فيما يخص معالجة المعطيات الشخصية المتعلقة بشخص طبيعي رغم اعتراضه، فقد عاقب المشرع المغربي عنها بالحبس من 3 أشهر إلي سنة، وغرامة من 20 ألف إلي 200 ألف درهم، أو بإحدي هاتين العقوبتين (المادة 59)، في حين عاقب عنها المشرع التونسي بالسجن لمدة عام وبغرامة قدرها 5 آلاف دينار (الفصل 91). فيما عاقب المشرع الفرنسي عن هذا الفعل بالحبس خمس سنوات وغرامة 300 ألف يورو (المادة 18/226-1 عقوبات).

الفرع الثاني
الجرائم الماسة بالقواعد الشكلية لمعالجة البيانات

فرضت التشريعات سالفة الذكر ضرورة احترم مجموعة من القواعد الشكلية بهدف حماية الاشخاص الذاتيين في مواجهة معالجة هذه البيانات، حيث يلزم المسئول علي المعالجة قبل إجراءها استيفاء بعض الشكليات المسبقة التي تخوله معالجة المعطيات الشخصية، ومن ثم كل مخالفة لهذه الشكليات تشكل جريمة معاقب عليها (أولاً). وضمانًا لسلامة هذه المعطيات وحمايتها من مختلف المخاطر التي يمكن أن تتعرض لها ولاسيما انتهاك سريتها، فُرض علي المسئول عن المعالجة اتخاذ مجموعة من الإجراءات لضمان أمن هذه المعطيات، بالإضافة إلي الزامه

باحترام مقتضـيات التعاون مع اللجنة الوطنية وإلا اعتبر مرتكب لجرائم معاقب عليها (ثانيًا).

أولاً: الجرائم المتعلقة بالشكليات المسبقة:

يتعين قبل إجراء معالجة للمعطيات ذات الطابع الشـخصـي تقديم المسـئول عن المعالجة تصريح بذلك أو حصوله علي الإذن من قبل اللجنة الوطنية، لذا تشكل كل معالجة يجريها الأول في غياب التصـريح أو الإذن جريمة معاقب عليها، وفي نفس الوقت يلزم المسـئول عن المعالجة ضـرورة الحصـول علي الرضـا المسـبق للشخص المعني إذا ما تعلق الأمر بمعالجة لمعطياته الحساسة.

أ- جريمة المعالجة بدون التصريح أو الإذن المسبق.

تتحقق هذه الجريمة من خلال القيام بمعالجة البيانات ذات الطابع الشخصـي دون الحصول علي التصريح أو الإذن المسبق. ولكي تقوم هذه الجريمة يتعين توافر الركنين المادي والمعنوي:

ويقوم الركن المادي لهذه الجريمة بتحقق العناصر التالية: أولها، انجاز ملف معطيات ذات طابع شـخصـي. وثانيها، عدم توافر الأذن أو التصـريح المسـبق، أو مواصلة المعالجة بعد سحبهما.

أما فيما يخص الركن المعنوي فيتخذ صـورة القصـد الجنائي العام بعنصـريه العلم والإرادة أي يجب أن يعلم الجاني بأن الأفعال التي يأتيها تشـكل إنجازًا لملف معطيات ذات طابع شـخصـي، وأنه لا يتوافر لديه تصـريح لممارسـة نشـاط معالجة البيانات الشخصية بعدما سحب منه التصريح أو الإذن. بالإضافة إلي عنصر العلم يتعين أن تتجه إرادة الجاني إلي ارتكاب هذه الأفعال.

عاقب المشـرع المغربي عن الأفعال السـابقة المكونة لجريمة المعالجة بدون التصـريح أو الإذن المسـبق بعقوبة الغرامة فقط والتي تتراوح قيمتها بين 10 آلاف درهم و 100 ألف درهم. بينما عاقب المشـرع التونسـي بعقوبة السـجن مدة عام

وبغرامة قدرها 5 آلاف دينار لكل من يتعمد معالجة المعطيات الشخصية دون تقديم التصريح المنصوص عليه بالفصل 7 أو الحصول على الترخيص المنصوص عليه بالفصلين 15، 69 من هذا القانون بعد منع المعالجة أو سحب الترخيص (الفصل 90). أما المشرع الفرنسي فقد عاقب عليها بالحبس لمدة خمس سنوات وغرامة مقدارها 300 ألف يورو.

ب-جريمة معالجة البيانات الحساسة:

تتحقق هذه الجريمة من خلال القيام بمعالجة للبيانات ذات الطابع الشخصي الحساسة دون الحصول علي موافقة الشخص المعني. ولكي تقوم هذه الجريمة يتعين توافر الركنين المادي والمعنوي:

ويتحقق الركن المادي لهذه الجريمة بتوافر أحد عنصرين: **أولهما**، أن تجري معالجة للبيانات الحساسة التي تظهر الأصول العرقية أو الإثنية أو الآراء السياسية أو الانتماءات النقابية أو المتعلقة بالصحة دون موافقة الشخص المعني[1]. **وثانيهما**، معالجة المعطيات الشخصية المتعلقة بالمخالفات أو الإدانات أو التدابير الوقائية؛ لأن معالجة هذا النوع من المعطيات محظور علي القطاع الخاص[2].

---

[1] لم يحدد كل من المشرع المغربي في المادة 57 من القانون رقم 09.08 والمشرع القطري في المادة 4 من القانون رقم 13 لسنة 2016 شكلا للموافقة علي معالجة البيانات ولاسيما الحساسة منها، في حين اشترط الأخير لمعالجتها ضرورة الحصول علي إذن من الإدارة المختصة (المادة 16). بالمقابل كان المشرع التونسي أكثر وضوحًا حيث اشتراط الموافقة الصريحة والكتابية من الشخص المعني بالبيانات، وزيادة علي ذلك إذا تعلق الأمر بطفل تعين الحصول علي موافقة وليه وإذن قاضي الأسرة (الفصل 27-28) من القانون التونسي رقم 24 لسنة 2004 المتعلق بحماية المعطيات الشخصية.

[2] إذ يختص بمعالجة هذا النوع من المعطيات المحاكم والسلطات العامة والأشخاص المعنويين الذين يسيرون مصلحة عمومية، ومساعدو القضاء لغاية مزاولة المهام التي يختصون بها بشكل قانوني (المادة 49 من القانون المغربي)، السلطات العمومية والجماعات المحلية والمؤسسات العمومية ذات الصبغة الإدارية (الفصل 53 من القانون التونسي).

أما فيما يخص الركن المعنوي فيتخذ صورة القصد الجنائي العام بعنصريه العلم والإرادة أي يجب أن يعلم الجاني بأن الأفعال التي يقوم بها تشكل معالجة لمعطيات ذات طابع شخصي، وأن المعطيات التي يعمل علي معالجتها تشكل معطيات حساسة، وأنه يجري المعالجة المذكورة دون الحصول علي موافقة صريحة من الشخص المعني. أما بالنسبة للفعل الأخير فيلزم أن يعلم الجاني بأنه يقوم بمعالجة معطيات ذات طابع شخصي تتعلق بمخالفات أو إدانات أو تدابير وقائية، فضلا عن ذلك يستوجب القصد أن تكون للجاني إرادة للقيام بهذه الأفعال من أجل تحقيق نتيجتها.

عاقب المشرع المغربي علي جريمة معالجة معطيات حساسة بدون رضا الشخص المعني، بعقوبة تعد من أقصي العقوبات التي جاء بها القانون 09.08 حيث عاقب عليها بعقوبة الحبس من 6 أشهر إلي سنتين وبغرامة من 50 ألف درهم إلي 300 ألف درهم أو بإحدهما (المادة 75). بينما عاقب عليها المشرع التونسي بعقوبة السجن مدة عامين وبغرامة قدرها 10 آلاف دينار (الفصل 87). أما المشرع الفرنسي فقد عاقب عليها بالحبس لمدة خمس سنوات وغرامة مقدارها 300 ألف يورو.

ثانياً: الجرائم المتعلقة بشكليات الحماية والتعاون مع اللجنة الوطنية:

كما فرضت التشريعات سالفة الذكر علي عاتق المسئول عن معالجة المعطيات ذات الطابع الشخصي الإلتزام بإتخاذ مجموعة من الإجراءات والتدابير لحماية المعطيات محل المعالجة من المخاطر التي يمكن أن تلحق بها، وبالتالي فإن أي إغفال أو تقصير في اتخاذ هذه الإجراءات يشكل جريمة معاقب عليها. كذلك ألزم المسئول عن المعالجة أيضا بالتعاون مع اللجنة الوطنية، وإلا تعرض للمساءلة الجنائية.

أ- جريمة عدم اتخاذ إجراءات حماية البيانات:

تتحقق هذه الجريمة من خلال القيام بمعالجة معطيات ذات طابع شخصي دون اتخاذ الاحتياطات اللازمة لحماية أمن هذه المعطيات. ولكي تقوم هذه الجريمة يتعين توافر الركنين المادي والمعنوي:

ويقوم الركن المادي لهذه الجريمة بتحقق العنصرين التاليين: أولهما، القيام أو العمل علي القيام بمعالجة معطيات ذات طابع شخصي. وثانيهما، غياب الإجراءات التي تهدف إلي ضمان أمن المعطيات. مثل الاجراءات التقنية والتنظيمية المناسبة والتي من شانها توفير حماية لهذه المعطيات في مواجهة كافة المخاطر التي يمكن أن تهددها[1].

أما فيما يتعلق بالركن المعنوي، فإن جريمة عدم اتخاذ إجراءات حماية المعطيات يمكن أن تقوم عن طريق القصد، أي بعلم الجاني بأنة يعالج معطيات ذات طابع شخصي دون أن يكون قد أنجز تدابير حماية أمن المعطيات كما يلزمه بذلك القانون[2]، وإرادته القيام بهذا الفعل. كما يمكن أن ترتكب هذه الجريمة عن

---

[1] راجع: المادة 24 من القانون المغربي رقم 09.08 لسنة 2009، والمادة 8 من القانون القطري رقم 13 لسنة 2016 .

[2] وقد فصلت المادة 19 من القانون التونسي الخاص بحماية البيانات الشخصية هذه الاحتياطات بالآتي:

- عدم وضع المعدات والتجهيزات المستعملة في معالجة المعطيات الشخصية في ظروف أو أماكن تمكن من الوصول إليها من قبل أشخاص غير مأذون لهم بذلك.
- عدم إمكانية قراءة السندات أو نسخها أو تعديلها أو نقلها من قبل شخص غير مأذون له بذلك.
- عدم إمكانية إقحام أي معطيات في نظام المعلومات دون إذن في ذلك وعدم إمكانية الاطلاع على المعطيات المسجلة أو محوها أو التشطيب عليها.
- عدم إمكانية استعمال نظام معالجة المعلومات من قبل أشخاص غير مأذون لهم بذلك.
- إمكانية التثبت اللاحق من هوية الأشخاص الذين نفذوا إلى نظام المعلومات والمعطيات التي تم إقحامها وزمن ذلك والشخص الذي تولى ذلك.

طريق الخطأ، ويتمثل ذلك في إجراء معالجة للمعطيات دون اتخاذ كل الإجراءات اللازمة لحماية أمن البيانات، سواء بإهمال اتخاذ هذه الإجراءات أو عدم التبصر بشأنها.

عاقب المشرع المغربي علي جريمة عدم اتخاذ إجراءات حماية المعطيات، بعقوبة الحبس من 3 أشهر إلي سنة وبغرامة من 20 ألف درهم إلي 200 ألف درهم أو بإحدهما (المادة 58). كذلك المشرع التونسي عاقب عليها بالسجن مدة 3 أشهر وبغرامة قدرها ألف دينار (الفصل 94)، في حين قصرها المشرع القطري علي الغرامة [1]. أما المشرع الفرنسي فقد عاقب عليها بعقوبة جد مشددة تتمثل في الحبس خمس سنوات وغرامة مقدارها 300 آلف يورو (المادة 17/226 عقوبات).

ب- جريمة الامتناع عن التعاون مع اللجنة الوطنية:

تتحقق هذه الجريمة كلما تم عرقلة اللجنة الوطنية عن ممارسة مهامها أو رفض التعاون معها. ولكي تقوم هذه الجريمة يتعين توافر الركنين المادي والمعنوي.

ويقوم الركن المادي لهذه الجريمة بتحقق أحد العناصر التالية: أولها، عرقلة ممارسة اللجنة الوطنية لمهام المراقبة. وثانيها، رفض استقبال مراقبي اللجنة الوطنية وعدم السماح لهم بإنجاز تفويضهم. وثالثها، رفض إرسال الوثائق أو المعلومات المطلوبة. ورابعها، رفض نقل الوثائق المنصوص عليها قانونا (المادة 62)، أو رفض تطبيق قراراتها(المادة 63).

- عدم إمكانية قراءة المعطيات أو نسخها أو تعديلها أو محوها أو التشطيب عليها أثناء إحالتها أو نقل سندها.
- الحفاظ على المعطيات عبر إحداث نسخ منها احتياطية وآمنة.

[1] إذا نصت المادة 23 من قانون حماية البيانات الشخصية القطري علي عقوبة الغرامة بمقدار مليون ريال؛ وذلك لمخالفة حكم المادة 8 الخاصة بعدم اتخاذ إجراءات حماية أمن البيانات.

أما فيما يتعلق بالركن المعنوي، فإن جريمة الامتناع عن التعاون مع اللجنة الوطنية لا تتحقق إلا عن طريق القصـــد، ويظهر ذلك من طبيعة الأفعال المعاقب عليها، والتي لا يتصور ارتكابها عن طريق الخطأ.

عاقب المشـرع المغربي علي جريمة الامتناع عن التعاون مع اللجنة الوطنية بالحبس من 3 أشهر إلي 6 أشهر وبغرامة من 10 آلاف درهم إلي 50 ألف درهم أو بإحدي هاتين العقوبتين فقط. فيما عاقب بالحبس من 3 أشـهر إلي سـنة وبغرامة من 10 آلاف إلي 100 ألف درهم أو بـإحدي هاتين العقوبتين فقط، علي رفض تطبيق قرارات اللجنة الوطنية.

الخاتمة

وبعدُ ... بِنْتَهِي بِنَا المطافُ في شَـأْن دراسـتنَا لموضـوع الحماية القانونية للبيانات الشـخصـية المعالجة آليا ذلك الموضـوع الذي شـغل بال المهتمين بحقوق الإنسـان عموما والحق في الخصـوصـية تحديدًا. وقد أبرزت الدراسـة مفهوم البيانات الشـخصـية وعناصـرها، وماهية معالجة البيانات الشـخصـية وصـور معالجتها، وأنواع المخاطر المتصـلة بمعالجتها. بالإضـافة لبيان الضـوابط القانونية لمعالجة هذا النوع من البيانات، وأخيرا صـور الحماية الجنائية للبيانات الشـخصـية في التشـريعات الأجنبية أو العربية.

وقد خلصـنا في نهاية دراستنا لموضـوع الحماية القانونية للبيانات الشـخصـية المعالجة آليا إلي جملة من النتائج[1] والمقترحات نتناولها علي التفصيل التالي:

أولاً:- النتائج :

(01) كشـفت الدراسـة عن تبني المشـرع الفرنسـي للمفهوم الواسـع للبيانات الشخصية بمقتضي التعديل الصادر لسنة 2004 مدعوما في ذلك بآراء الفقه وأحكام القضـاء ومداولات اللجنة الوطنية للمعلوماتية والحريات في هذا الشـأن، ذلك التعريف مؤداه أن تحديد الأشخاص الطبيعين من خلال بياناتهم لا يقتصر علي فكرة التعريف المباشـر بهم، عن طريق الاسـم الشـخصـي أو اللقب، ولكن يمتد ليشـمل أي بيان خاص بهذا الشخص، يمكن من خلاله تحديد هويته ولو بطريقة غير مباشرة.

(02) ويمكن رد عناصـر البيانات الشـخصـية إلي ثلاثة طوائف: أولهما، بيانات التعريف المباشـر، وتشـمل البيانات الاسـمية والصـوت والصـورة. وثانيهما،

---

[1] غني عن الإيضاح أن خاتمة الدراسة لا تحتل سرد كافة النتائج التي انتهينا إليها في كل جزئية من جزئيات البحث؛ لذا سنكتفي بإبراز النتائج التي تمثل معالم رئيسية لموضوع الدراسة.

بيانات التعريف غير المباشر، وتشمل الأرقام الشخصية كرقم بطاقة الهوية، الهاتف، لوحة السيارة، رخصة القيادة، والحساب البنكي، والعناوين الشخصية كالعنوان الجغرافي، والبريد الإلكتروني، وبرتوكول الإنترنت، والخصائص البيوميترية كبصمة الإصبع، واليد، والعين، والصوت، والحمض النووي، والتوقيع. وثالثهما، البيانات الحساسة، وتشمل الآراء السياسية والنقابية والمعتقدات الدينية، والحالة الصحية والحياة الجنسية، والأصول العرقية للشخص.

(03) ولعل عدم وضع التشريعات المقارنة تعريفًا للبيانات الحساسة، ووضعها عناصر فقط يرجع إلي رغبة المشرع في هذه البلدان في ترك الباب مفتوحًا أمام ما يستجد مستقبلًا من عناصر أخري، يمكن اعتبارها من البيانات الحساسة، خاصة في ظل التطور العلمي الذي تمر به المجتمعات، وما يعيشه العالم من ثورة في مجال الاتصالات وتكنولوجيا المعلومات، والتقنيات الحيوية.

(04) وضع المشرع الفرنسي تعريفًا واسعًا لمصطلح معالجة البيانات الشخصية؛ حيث اعتبر أي إجراء يتعلق بالبيانات الشخصية هو معالجة لهذه البيانات. حيث جاء التعداد الذي أورده المشرع الفرنسي في المادة 2/2 من قانون المعلوماتية والحريات علي سبيل المثال وليس حصريًا، ويظهر ذلك جليًا من استعمال المشرع الفرنسي لعبارة " بأي شكل آخر"، الأمر الذي يعني أنه يمكن أن تتم المعالجة بأي طريق آخر غير الوارد بهذه المادة.

وفي ذات الصدد كشفت الدراسة عن توسيع المشرع الفرنسي لنطاق معالجة البيانات الشخصية وذلك بمقتضي التعديل الصادر لسنة 2004 –علي أثر الانتقادات التي وجهت إليه– ليشمل إلي جانب المعالجة الآلية للبيانات، المعالجة اليدوية أيضًا بعد أن كان يقصر ذلك علي المعالجة الآلية والمعالجة اليدوية المتعلقة بالأبحاث الطبية فقط.

(05) ويعتبر المسئول عن معالجة البيانات هو– بحسب الأصل– الشخص أو السلطة العامة أو الوكالة أو الهيئة التي تحدد كيفية وغاية معالجة البيانات، وذلك

حسـبما نص التوجيه الأوربي وقانون المعلوماتية والحريات الفرنسـي (المادة 1/3). وبالتالي فإن المسئول عن معالجة البيانات الشخصية عبر شبكة الإنترنت عموما أو شبكات التواصل الاجتماعي هو مقدم خدمة التواصل.

(06) كشـفت الدراسـة عن ارتباط معالجة البيانات الشـخصـية في بعض الأحيان بمخاطر التعدي علي الحقوق والحريات الفردية للأشـخاص المعنيين بهذه البيانات بفعل التوسـع في جمع البيانات الأمر الذي فتح الباب لإسـاءة اسـتخدامها، ويزداد الأمر خطورة نتيجة لاسـتخدام التقنيات الحديثة لجمع البيانات والاحتفاظ بها واسـتخدامها وتبادلها بين النظم المعلوماتية، فضـلا عما تقوم به شـبكات التواصـل الاجتماعي من تجميع لبيانات المستخدمين والتي من خلالها يتنازل المستخدم مقدمًا عن بياناته الشخصية في سبيل الحصول علي حساب خاص. بالإضافة إلي ما يقوم به المستخدم لهذه الشبكات من إفصاح عن بعض الأمور التي تتعلق بحياته العائلية أو ظروفه المهنية أو معاناته الصـحية أو وضـعه المالي أو غيرها من الأمور التي تدخل ضمن عناصر الحياة الخاصة التي لا يجوز للغير الاطلاع عليها إلا بموافقة صاحب هذه البيانات.

ومن ناحية أخري يتمسـك مقدمي خدمات التواصـل الاجتماعي بالاحتفاظ بالبيانات الشـخصـية لأطول فترة ممكنة حتي بعد حذف الشـخص لحسـابه؛ وذلك لدواعي الدعاية والإعلانات. ففي الوقت التي تحترم فيه هذه الشـبكات المُسـتخدمين داخل دول الاتحاد الأوربي فتعمل علي احترام الحد الأقصـي للمدة التي تحتفظ فيها بالبيانات بعد حذف الشـخص لحسـابه عليها؛ وذلك خشـية وقوعها تحت طائلة المسـئولية التي تفرضـها توجيهات الاتحاد الأوروبي، لا نجدها تحترم بذات القدر المسـتخدمين في الدول الإفريقية والعربية؛ إذ تتجرأ هذه الشـبكات علي البيانات الشخصية للمستخدمين وتحتفظ بها لمدد طويلة من الوقت، وخصوصًا في ظل غياب ما يردعها من التعدي علي الخصـوصـيات نتيجة غياب تشـريعات حماية البيانات الشخصية في غالبية هذه البلدان.

(07) كشفت الدراسة عن وضع المشرع الفرنسي مجموعة من الالتزامات علي عاتق المسئول عن المعالجة الآلية للبيانات الشخصية بهدف المحافظة علي أمن البيانات وسريتها، ففيما يتعلق بالالتزامات السابقة علي جمع البيانات ومعالجتها اشترط المشرع الفرنسي في قانون المعلوماتية والحريات، ضرورة قيام المسئول عن المعالجة، بإخطار اللجنة الوطنية بإجراء هذه المعالجة وهو التزام عام يسري علي جميع المعالجات. كما اختص بعضًا منها، بضرورة حصول المسئول عنها علي ترخيص من اللجنة الوطنية قبل القيام بإجرائها، وذلك بالنظر إلي طبيعة البيانات محل المعالجة أو الغاية من هذه المعالجة.

وعلي الجانب الآخر أقر المشرع الفرنسي في قانون المعلوماتية والحريات مجموعة من الالتزامات اللاحقة علي إجراء المعالجة وهي في حقيقتها ضمانات من شأنها الحماية للبيانات الشخصية محل المعالجة؛ وذلك من خلال توفير مستوي ملائم لتأمين البيانات الشخصية بتقنين إجراءات حفظها، والتقيد بمدة ملائمة لحفظ البيانات الشخصية، لتدخل بعدها في طي النسيان.

وحتي تكتمل منظومة الحماية القانونية للبيانات الشخصية ألزم المشرع الفرنسي في قانون المعلوماتية والحريات المسئول عن معالجة البيانات بمجموعة من المبادئ يتعين احترامها والتي تقتضي في جانب منها ضرورة الحصول علي موافقة الشخص المعني بالبيانات علي إجراء المعالجة، والجانب الآخر يتعلق بالمعالجة ذاتها من ضرورة التزامها بمبادئ المشروعية والغائية والنزاهة والشفافية والضرورة والتناسب ومبدأ دقة وجودة البيانات.

(08) كشفت الدراسة عن اتساق الحماية المقررة للأشخاص الذين تخضع بياناتهم الشخصية للمعالجة مع الحماية المقررة لحماية الحق في الحياة الخاصة. إذا منح المشرع الفرنسي الأشخاص الحق في أن يعلموا ببعض المعلومات الخاصة بالمعالجة والتي من شأنها أن تعطيهم فكرة واضحة ومسبقة عن المعالجة، ومن ثم تمكنهم من اتخاذ القرار بقبول أو رفض إجراء هذه المعالجة. كما أعطاهم الحق في

الاطلاع علي ما يتم تسـجيله عنهم من بيانات وذلك لفحصـها والتأكد من مطابقتها للواقع؛ لذا يشـكل الحق في الاطلاع نوعًا من الرقابة اللاحقة يمارسـها الشـخص المعني بنفسه علي معالج البيانات الشخصية.

لعل من أهم الضـمانات اللاحقة علي إجراءات معالجة البيانات الشـخصـية، ما خوله المشـرع الفرنسـي للشـخص المعني من الحق في الاعترض علي معالجة بياناته الشـخصـية، سـواء كان ذلك قبل جمع البيانات ومعالجتها كرفضـه الإفصـاح عنها، أو بعد إجراء المعالجة كأن يرفض مثلا نقلها لجهة أخري غير من قامت بجمعها. بالإضـافة إلي ما قرره للشـخص المعني من حق تصـحيح البيانات حال كونهـا غير دقيقـة أو غير مكتملـة أو محوهـا كليـة إذا كـان محظور جمعهـا أو استخدامها أو تخزينها.

ثانياً- التوصيات :

في ضـوء ما أسفرت عنه الدراسـة من نتائج نود أن نسـوق بعض التوصـيات التي ندعو المشرع للأخذ بها وذلك لتلافي الانتقاصـات التي تكشـفت خلال الدراسـة. ومن أهمها:

1- ضـرورة إصـدار تشـريع متكامل لحماية البيانات الشـخصـية علي غرار التشـريع الفرنسـي، وذلك بعد أن تفاقمت المخاطر التي تحيط بالبيانات الشـخصـية في ظل التطور التكنولوجي الهائل وتطور وسـائل وأسـاليب التسـويق والدعاية، بحيث يكون الهدف منه منع الممارسات غير المشروعة لاستخدام هذه البيانات بجمعها ومعالجتها واستغلالها.

2- ضـرورة إنشـاء هيئة وطنية مسـتقلة ومحايدة – علي غرار اللجنة الوطنية للمعلوماتية والحريات بفرنسـا – تتولي الإشـراف علي موضـوع حماية البيانات الشـخصـية وتتمتع باختصـاصـات تنفيذية ورقابية لإدارة وتنظيم هذا الاسـتخدام بما يكفل التطبيق العملي والفعال لحمايتها قانونيًا.

3- تجريم أي جمع أو استغلال غير مشروع للبيانات الشخصية، كذلك تجريم أي انحراف عن الغرض الذي من أجله تمت معالجة هذه البيانات.

4- تجريم كل إفشاء للبيانات الشخصية علي أن يحدد المشرع نوعية البيانات الشخصية والمعالجات التي تخضع للحماية القانونية، مع مراعاة حقوق الشخص علي بياناته محل المعالجة، وذلك بالنص علي حقه في معرفة الغرض من جمعها ومعالجتها، وحقه في الاعتراض والاطلاع والتصحيح والحذف.

5- عدم الأخذ بالاستثناء الوارد بقانون المعلوماتية الفرنسي المتعلق بالتنازل المسبق للشخص المعني عن ممارسة حقه في الاعتراض علي معالجة بياناته والذي لا يسمح له بممارسة هذا الحق فيما بعد حتي لو توافرت أسباب مشروعة لذلك؛ لأن الأمر يتعلق في النهاية ببيانات شخصية تتعلق بالحياة الخاصة لمن تخصه البيانات. فضلا عن أن الأخذ بهذا الاستثناء علي إطلاقه من شأنه تقويض الحق العام في الاعتراض وهو أحد الحقوق الرئيسية للفرد في مواجهة معالج البيانات الشخصية.

6- تجريم عدم استجابة المسئول عن معالجة البيانات الشخصية للشخص المعني في طلبه بالاطلاع علي بياناته الشخصية أو طلبه بتعديل أو حذف هذه البيانات؛ وذلك حتي نضمن فاعلية هذه الحقوق المقررة للشخص علي بياناته.

7- النص علي مسئولية القائم بمعالجة البيانات الشخصية أو المسئول عنها بحسب الأحوال في المحافظة علي سرية البيانات الشخصية، وتأقيت هذه البيانات بمدة ملائمة لتدخل بعدها في طي النسيان.

8- تجريم القيام بإية إجراءات من إجراءات معالجة البيانات الشخصية دون توافر التدابير الوقائية لحماية هذه البيانات وضمان سريتها.

وأخيرًا يتعين زيادة وعي المواطنين بأهمية بياناتهم الشخصية وعدم الإفراط في افشائها، وذلك بتنبيههم علي المخاطر التي يمكن أن تحيط بتلك البيانات، وما يمكن أن يحدث لهم من أضرار. وفي هذا السياق علي الحكومة، ممثلة في وزارة

الاتصـالات وتكنولوجيا المعلومات الإسـراع بإصـدار دليل إرشـادي لاسـتخدام شـبكة الإنترنت عمومًا وشـبكات التواصـل الاجتماعي خصـوصًـا؛ بحيث يعمم هذا الدليل علي الجهات الحكومية والمؤسـسـات الخاصـة ويتاح عبر وسـائل الإعلام بسـبل الاسـتخدام الأمثل لهذه الشـبكات، وتجنب المخاطر الناجمة عنها ومن أبرزها بطبيعة الحال مخاطر انتهاك خصوصية المستخدمين.

وفي نهاية هذه الدراسـة نهيب بالمشـرع المصـري التدخل بوضـع تشـريع متكامل لمكافحة الجرائم المعلوماتية، أسـوة بما هو عليه الحال في العديد من التشريعات المقارنة، وخصوصًا أن قانون العقوبات الحالي بنصوصه التقليدية أصبح غير قادر علي مواجهة هذه النوعية من الجرائم المستحدثة؛ بحيث يوفر هذا التشريع الحماية الجنائية لحرمة الحياة الخاصـة عبر شـبكات الاتصـال والمعلومات، ويسـد القصـور التشـريعي الذي يحول دون ملاحقة الجناة بما يتواكب مع المسـتجدات. كما نقترح أيضًا وضع النصوص الخاصة بحماية الحياة الخاصة والحق في الخصوصية في فصـل واحد في قانون العقوبات، وذلك لتوحيد القواعد والإجراءات القانونية التي تحكمها.

تم بحمد الله

قائمة المراجع

أولا: المراجع باللغة العربية:

المؤلفات العامة والخاصة

الدكتور/ أحمد فتحي سرور:

- الحماية الدستورية للحقوق والحريات، دار الشروق 2000.

الدكتور/ اسامة عبد الله قايد:

- الحماية الجنائية للحياة الخاصة وبنوك المعلومات، دار النهضة العربية، 1994.

الدكتور/ حسين بن سعيد الغافري:

- السياسة الجنائية في مواجهة جرائم الإنترنت، دراسة مقارنة، دار النهضة العربية، 2009.

الدكتور/ سعيد جبر:

- الحق في الصورة ، دار النهضة العربية، 1986.

الدكتور/ شريف يوسف خاطر:

- حماية الحق في الخصوصية المعلوماتية، دار الفكر والقانون، 2015.

الدكتور/ شمس الدين إبراهيم أحمد:

- وسائل مواجهة الاعتداءات علي الحياة الشخصية في مجال تقنية المعلومات في القانون السوداني والمصري، دراسة مقارنة، دار النهضة العربية، الطبعة الأولي 2005.

الدكتور/ محمد الشهاوي:

- الاعتداء علي الحياة الخاصة بواسطة القنوات الفضائية ووسائل الإعلام والاتصال، دار النهضة العربية، 2015.

الدكتور/ عفيفي كامل عفيفي:

- جرائم الكمبيوتر وحقوق المؤلف والمصنفات الفنية، دراسة مقارنة، منشأة المعارف بالإسكندرية، 2000.

الدكتور/ عمر أبو الفتوح عبد العظيم الحمامي:

- الحماية الجنائية للمعلومات المسجلة إلكترونيًا ، دراسة مقارنة، دار النهضة العربية، 2010.

الدكتور/ عمر فاروق الحسيني:

- المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية، بدون دار نشر، 1995.

الدكتور/ كاظم السيد عطية:

- الحماية الجنائية لحق المتهم في الخصوصية، دار النهضة العربية، 2007.

الدكتور/ محمد حسام محمود لطفي:

- بنوك المعلومات وحقوق المؤلف، بدون دار نشر، 1999.

الدكتور/ محمد سامي عبد الصادق:

- شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية 2016.

الدكتور/ محمد نصر محمد:

- المسئولية الجنائية لانتهاك الخصوصية المعلوماتية– دراسة مقارنة، مركز الدراسات العربية، الطبعة الأولي 2016.

الدكتور/ محمود سلامة جبر:

- الحماية الدستورية والقضائية لخصوصية البيانات الشخصية للعامل، مطبعة أبناء وهبة حسان، الطبعة الأولي 2016.

الدكتور/ مدحت عبد الحليم رمضان:

- الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، دار النهضة العربية، 2001.

الدكتورة/ مروة زين العابدين صالح:

- الحماية القانونية الدولية للبيانات الشخصية عبر الإنترنت، مركز الدراسات العربية، الطبعة الأولي 2016.

الدكتور/ مصطفي أحمد عبد الجواد حجازي:

- المسئولية المدنية للصحفي عن انتهاك حرمة الحياة الخاصة، دار النهضة العربية، 2004.

الدكتور/ هشام محمد فريد رستم:

- قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، 1992.

<u>الرسائل العلمية:</u>

الدكتور/ آدم عبد البديع آدم:

- الحق في حرمة الحياة الخاصة ومدي الحماية التي يكفلها له القانون الجنائي، رسالة دكتوراه – حقوق القاهرة، 2000.

الدكتور/ أسماء حسن سيد محمد رويعي:

- الحق في حرمة الحياة الخاصة في مواجهة الجرائم المعلوماتية، رسالة دكتوراه- حقوق القاهرة، 2013.

الدكتور/ أيمن عبد الله فكري:

- جرائم نظم المعلومات- دراسة مقارنة، رسالة دكتوراه -حقوق المنصورة، 2005.

الدكتور/ علاء محمود يسن حراز:

- الحماية الجنائية للمعلومات المعالجة آليا- دراسة مقارنة بين القانون الوضعى والشريعة الإسلامية ، رسالة دكتوراه – حقوق عين شمس، 2015.

الدكتور/ يسري عبد الله عبد الباري:

- الحماية المدنية للخصوصية المعلوماتية دراسة مقارنة، رسالة دكتوراه – حقوق عين شمس، 2016.

<u>المقالات والبحوث:</u>

الدكتور/أشرف محمد إسماعيل:

- التقنيات المعلوماتية الحديثة وانعكاساتها علي حق العامل في الخصوصية، بحث مقدم لمؤتمر القانون والتكنولوجيا الذي نظمته كلية الحقوق بجامعة عين شمس في الفترة من 9-11 ديسمبر 2017، مجموعة أعمال المؤتمر- الجزء الثاني.

الدكتور/ أيمن مصطفي أحمد:

- الحماية القانونية للبيانات الشخصية في إطار أنشطة البحث العلمي، مجلة الدراسات القانونية، تصدرها كلية حقوق أسيوط، العدد 37 الجزء الأول 2015.

الدكتور/ سامح عبد الواحد التهامي:

- الحماية القانونية للبيانات الشخصية– القسم الأول، مجلة الحقوق الكويتية، العدد 3 س 35، سبتمبر 2011.
- الحماية القانونية للبيانات الشخصية– القسم الثاني، مجلة الحقوق الكويتية، العدد 4 س 36، ديسمبر 2011 .
- ضوابط معالجة البيانات الشخصية– دراسة مقارنة بين القانون الفرنسي والقانون الكويتي، مجلة كلية القانون الكويتية العالمية، العدد 9 السنة الثالثة، مارس 2015.

الدكتور/ محمود عبد الرحمن:

- التطورات الحديثة لمفهوم الحق في الخصوصية "الحق في الخصوصية المعلوماتية" مجلة كلية القانون الكويتية العالمية، العدد التاسع السنة الثالث، مارس 2015.

ثانياً: المؤلفات الانجليزية:

Andru E. Wall:

- Prying Eyes, the legal conseqences of Reading Your Spouses Electronic Mail, 30 FAM. L.Q. 2003.

Angela Choy, Marcia S.Smith & Jane Bortnick Griffith:

- Protecting privacy on the internet: a summary of legislative proposal, CRS Report for Congress, Congressional Reasearch Service, The liberary of Congrsess, 1997.

Atchinson & Daniel M. Fox:

- The Politics of The Health Insurance Portability and Accountability Act. Health Affairs 1997.

Charles A. SHONIREGUN & Stephen CROSIER:

- Securing Biometrics Applications, Éditions Springer, University of East London, United Kingdom, 2008.

Cooper, Marion B, Drinker Biddle & Reath LLP:

- January 1, 2013: New Fair Credit Reporting Act ΈFCRẮ From Required by New Enforcement Agency. TNL 2013.

Duke:

- Privacy: The Development of a Law and the Legal Theory, UK BOOKS, 2011.

Geal RF:

- Federal Trade Commission, Fair Information Practice Principles, (FIPs) Review 2009.

H.M Fenwick & G. Phillipson:

- Privacy and Confidence: A Re-Examination. Cambridge Law Journal, Vol.55, N°. 3, 1996.

Harry A Hammitt, David L Sobel & Mark S Zaid:

- Litigation under the federal open government laws: covering the Freedom of Information Act, the Privacy Act, the Government in the Sunshine Act, and the Federal Advisory Committee Act, Washington, D.C., 2002.

Joan E. Rigdon:

- Internet Users Say They'd Rather Not Share Their "Cookies", Wall Street Journal, (Feb.14,1996).

Jonathan Morgan:

- Privacy, Confidence and Horizontal Effect: "Hello" Trouuble, Cambridge Law Journal, Vol. 62. N°. 2, 2003.

Lanier & Saini:

- Understanding Consumer Privacy: A Review and Future Directions, Academy of Marketing Science, 2008.

Lori Andrews:

- I Know Who You Are and I Saw What You Did: Social networks and the Death of privacy, NY: free press, 2012.

Mendelsohn, Stephen A.:

- ″ U.S. Department of Education Amends its FERPA Regulations to Allow for Certain Additional Student Disclosures″. The National Law Review. 2012.

Narayanan. A, Shmatikov. V:

- Myths and Fallacies of 'personally Identifiable Information'. Communications of the ACM, Vo. 53, N°. 6, June 2010.

Nikolaos KOURKOUMELIS & Margaret TZAPHLIDOU:

- « Eye Safety Related to Near Infrared Radiation Exposure to Biometric Devices », in The Scientific World Journal, Department of Medical Physics, Medical School, University of Ioannina, Ioannina, Greece, March 1st, 2011.

R. Singh & J. Strachan:

- Privacy Postponed, European Human Rights Law Review, 2003.

Scott, Craiag R, HIPA.:

- Privacy Complaint Turns into Federal Criminal Prosecution for frist Time. Compliance Corner (University of Missouri Healthcare. 2012.

Wolf M, Bennett C:

- ″Local perspective of the impact of the HIPAA privacy rule on research″. Cancer, 2006.
- Report, Review of the Implementation of the Human Rights Act, Department of the constitutional Affaires, Justice rights and democracy, July 2006. Available at: https://webarchive.nationalarchives.gov.uk/+/http:/www.dca.gov.uk/peoples-rights/human-rights/pdf/full_review.pdf

- PRIVACY IN AMERICA: SOCIAL SECURITY NUMBERS, Available at: https://www.aclu.org/ other/privacy-america-social-security-numbers
- Online Personal Privacy Act available at: https://www.congress.gov/bill/107th-congress/senate-bill/2201
- The Privacy Act Modernization for the Information Age Act of 2011. Available at: https://www.govtrack.us/congress/bills/112/s1732/text
- Annual Report on the Administration of the Privacy Act 2011-2012. Available at: http://www.esdc.gc.ca/eng/transparency/ati/reports/annual_privacy/2011_2012/index.shtml retrived 162013/5/
- BIOMETRICS INSTITUTE, « Types of biometrics », UK, online: http://www.biometricsinstitute.org/pages/types-of-biometrics.html
- Dutch and Canadian DPAs challenge WhatApp's compliance with their privacy laws. Available at: https://www.privacylaws.com/Publications/enews/

ثالثاً: المؤلفات بالفرنسية:

I- LES OUVRAGES GÉNÉRAUX:

Jean LARGUIER et Marie ANNE-LARGUIER:

- Droit pènal spécial, Dalloz, 10è éd, 1998.

Jean PRADEL et Michel DANTI-JUAN:

- Droit pénal, droit pénal spécial, T. III Edition Cujas, 1995.

Michel VÉRON:

- Droit pènal spécial, Armand Colin, 6è éd 1996.

Patrice GATTEGNO:

- Droit pénal spécial, Dalloz, 1995.

Jean LARGUIER et Marie ANNE-LARGUIER:

- Droit pènal spécial, Dalloz, 10è éd, 1998.

II- LES OUVRAGES SPÉCIAUX:

Alain BENSOUSSAN:

- Informatique et libertés, Editions Francis Lefebvre, 2008.

André Lucas, Jean Devèze, et Jean FRAYSSINET:

- Droit de l'informatique et de l'Internet. P.U.F, 2001.

Christiane FÉRAL-SCHUHL:

- Le droit à l'épreuve de l'internet, Dalloz, 1999.

Claudine GUERRIER:

- Les aspects techniques de la régulation des données personnelles: la question du numéro IP, in La régulation des données personnelles, LEGICOM n° 42 - 2009/1.

Claudine GUERRIER et Merie- Christine MONGET:

- Droit de Sécurité des telecommunications, Collection technique et scientifique des télécommunications, Paris, édition springer, 2000.

Danièle BOURCIER:

- Donnée sensible et risqué informatique de l'intimité menace à l'identité virtueue, CURAPP - Questions sensibles, PUF, 1998.

G. Avoine:

- Sécurité de la RFID: comprendre la technique sans être technicien, in La sécurité de l'individu numérisé, Réflexions prospectives et internationales, sous la direction de S. Lacour, L'Harmattan, 2008.

Isabelle (DE LABERTERIE), Henri (JAQUES- LUCAS):

- Informatique libertés et recherche médicale, Edition CNRS, 2001.

Gauvrit (NICOLAS):

- Statistiques. Méfiez-vous!, Ellipses, 2007.

Grégoire (S):

- Le statut de l'adresse IP: conséquences sur les mécanismes de constat, d'avertissement et de sanction du peer to peer envisagées par les accords de l'Elysée et le projet de loi « Création et Internet », in Les nouvelles frontières de la vie privée. Droits de la personnalité – Protection des données personnelles, LEGICOM, n° 43 – 2009/2.

Jacqueline BOUSSON-PETIT:

- L'identité de la personne humaine. Étude de droit français et de droit comparé, Bruxelles, Bruylant, 2002.

Jean HERVEG:

- « La gestion des risques spécifiques aux traitements de données médicales en droit européen», in Systèmes de santé et circulation de l'information. Encadrement éthique et juridique, Paris, Dalloz, 2006.

Jean MORANGE:

- Manuel des droits de l'homme et libertés publiques, Paris, PUF, 2007.

Marie-Charlotte Roques-Bonnet:

- Le droit peut-il ignorer la révolution numérique? Michalon, 2010.

Marie-Laure LAFFAIRE:

- Protection des données à caractère personnel, Éditions d'Organisation, 2005.

P. Leclercq:

- « La CNIL, garante de la finalité, de la loyauté et de la sé curité des données personnelles », in Les libértes individuelles à l'épreuve des NTIC, Etudes réunies sous la direction de M.-C. Piatti, Presses Universitaires de Lyon, 2001.

Pierre KAYSER:

- La protection de la vie privée par le droit, Economica/Presses universitaires d'Aix-Marseille, 3è éd., 1995.

Pierre PIAZZA et Ayse CEYAN:

- L'Identification biométrique: Champs, acteurs, enjeux et controversies, Éditions de la Maison des sciences de l´homme, 2014.

Serge GUINCHARD, Michèle HARICHAUX et Renaud DE-TOURDONNET:

- Internetpour le droit, Paris, Montchrétien, 1999.

III- THÈSES ET MÉMOIRES:

Benjamin EGERT:

- Les problemes juridiques des logicielsindiscrets, mémoire de D.E.A informatique et droit, faculté de droit, Univesité Montpellier I, 2002.

Brffard WILLIAM:

- Le système de traitment des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier I, 2003.

Cédric CREPIN:

- Le correspondant informatique et libertés: un nouvel outil de régulation pour la protection des données à

caractère personnel, mémoire de master professionnel mention droit de cyberspace, Université de Lille II, Année universitaire 2004-2005. disponiable sur: http://www.droit-tic.com/pdf/correspondant_donnees_personnelles_crepin.pdf

Charlotte HEYLLIARD:

- Le droit à l'oubli sur Internet, Mémoire de Master 2 recherch, Mention DNP, l'Université Paris-Sud, Faculté Jean Monnet-Droit, Économie, Gestion, Année Universitaire 2011-2012.

Claude BOURGEOS:

- L'anonymat et les nouvelles technologies de l'information, Universite Paris V, Thèse, 2003.

Cynthia CHASSIGNEUX:

- L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas (Paris II), 2003.

Frédérique LESAULNIER:

- L'information nominative, Thèse, Paris II, 2005.

Grévin ANTHONY:

- Les rapports entre les secret professionnel et le droit de la protection des des données personnelles, Mémoire de D.E.A informatique et droit, Université Montpellier I, Année Universitaire 2001/ 2002.

Ibrahim COULIBALY:

- La protection des données à caractère personnel dans le domaine de la recherche scientifique. Thèse, Université de Grenoble, 2011.

Julie M-GAUTHIER:

- Cadre juridique de l'utilisation de la biométrie au Québec: sécurité et vie privée, Mémoire présenté à la Faculté de

Droit en vue de l'obtention du grade de Maîtrise (L.L.M.), Droit des technologies de l'information, Université de Montréal, 2014.

Julien LE CLAINCHE:

- La protection des données personnelles nominatives dans le cadre de la recherche dans le domainne de la santé, Comparaison du droit francais et du droit américain, Mémoire de D.E.A., Faculté de droit, des Sciences Economiques et de Gestion, Université Montpellier I, 2000-2001.

Marot (Pierre-Yves):

- Les données et informations à caractère personnel. Essai sur la notion et ses fonctions, Thèse, Université de Nantes, 2007.

N'Da Brigitte Etien-Gnoan:

- L'encadrement juridique de la gestion électronique des données médicales, Thèse, Université Lille II, 2014.

Rosario DUASO CALÉS:

- La protection des données personnelles contenues dans les documents publics accessibles sur Internet: le cas des données judiciaires, Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de Maître en droit (LL.M.), Université de Montréal - Faculté des études supérieures, Décembre, 2002.

Sulliman OMRAJEE:

- Le data mining: Aspects juridiques de l’intelligence artificielle auregard de la protection des données personnelles. Mémoire, Faculté de Droit Université Montpellier I, Année Universitaire 2001-2002.

Yannis ZOUGHAILECH:

- L'Informatisation des données de santé Considérations éthiques: Cas de l'AMP Vigilance, Master 2 Éthique médicale et bioéthique, Universite Paris Descartes, Faculté de Médecine, Année universitaire 2013-2014. Disponiable sur:

  http://www.ethique.sorbonne-paris-cite.fr/sites/default/files/memoire%20zoughailech.pdf

IV- ARTICLE ET NOTES:

Alain BENSOUSSAN:

- Le driot à l'oubli sur Internet, 6 février 2010 Gaz. pal. nº 37.

Agathe LEPAGE:

- Le driot à l'oubli: une Jurisprudence tâtonnante, Recueil Dalloz 2001.

Christian CHARRIERE- BOURNAZEL:

- Propos autour d'Internet: l'histoire et l'oubli, Gaz. pal, 21 avril 2011, nº 111.

Cynthia CHASSIGNEUX:

- La protection des données personnelles en France, Lex Electronica, vol. 6, n°2, hiver 2001.

Guillaume DESGENS-PASANAU:

- Le driot à l'oubli existe-t-il sur Internet?. Expertise nº 343, janvier 2010.

Daniel ACQUARONE:

- L'ambiguïté du droit à l'image, D. 1985, chron.

Delmas Saint-Hilaire:

- Observation sous crim 3 nov. 1987, Rev. Sc.crim. 1988. 295.

D. Huet-Weiller:

- La protection juridique de la voix humaine, Rev. RTD civ. 1982.

DINTILHAC (Jean-Pierrre):

- Observation sous. crim 4 mars. 1997, Rev. Se. crim 1997. 669.

Delphine (ROIGT):

- Appel à une méthode proportionnelle d'évaluation éthique et une réelle réflexion éthique dans le recherche ayant recours à des données et du matériel biologique, in systèmes de santé et circulation de l'information Encadrement juridique et éthique, sous la direction de la HERVE (C), KNOPPERS (B-M), MOLINARI (P-A) et GRIMAUD (M-A), Dalloz, 2007.

Garé:

- Observation sous crim 14 mars 2006, D. 2007. Pan. 404.

Ehrenberg (A):

- Malaise dans l'évaluation de la santé mentale, Esprit, mai 2006.

Elsa SUPIOT:

- Le consommateur de tests génétiques, un patient avisé ou berné? Rev. D.C., octobre 2009.

Fabrice MATTATIA:

- CNIL et tribunaux: concurrence ou complémentarité dans la repression des infractions à la loi informatique et libertés?. Rev. Sc.crim. 2009.

Fatima EL ATMANI:

- Données sensibles: la notion de consentement de la personne concernée, Lamy Droit de l'informatique. 1996. n° 83.1996.1.

Francillon (J):

- Observation sous crim. 19 déc 1995, Rev. Sc.crim. 1996.

Frayssinet (JEAN):

- A propos du droit d'accès des personnes morales, D. 21 mai 1992.
- Atteinte aux droits des personnes résultant des fichiers ou des traitements informatiques, J.-Cl. Code pénal, mai 2006. fasc. 10.
- Loi Loi « Informatique et libertés » et durée de conservation des données personnelles, note sous, CA Douai, 29 déc. 2006, M. Olivier Q., n° 060A 00107 (2), Rev. LDI, n° 28, juin 2007.
- Observation sous crim. Crim 3 nov. 1987, JCP 1988, I.3323.

Frayssinet (J), Pédrot (P):

- La loi du 1er juillet 1994 relative au traitement des données nominatives ayant pour fin la recherche dans le domaine de la santé, JCP 1994.

GAILLARD (E):

- La double nature du droit à l'image et ses conséquences en droit positife française, D. 1984, chron.

GUERRIER (Claudine):

- Protection des données personnelles et application biométriques en Europe, C.C.E., juillet 2003, no 7-8, chron.

Isabelle (FALQUE-PIERROTIN):

- Production et diffusion des données à caractère personnel sur Internet: enjeux nouveaux et questions éthiques, in « Les données personnelles, entre fichiers nominatifs et jungle Internet. Actes de la journée d'études de

l'Association des archivistes français, 17 mars 2009 », Gazette des archives, 2009/3, n° 215, journée d'études de l'Association des archivistes français, 17 mars 2009 », Gazette des archives, 2009/3.

KAYSER (P):

- Les droits de la personnalité aspect théorique et pratique, Rev. trim.dr.civ. 1971.

Louise BERNIER:

- Le développement de la pharmacogénomique. Quelques questions éthiques et légales, in Les pratiques de la recherche biomédicale visitées par la bioéthique, sous la direction de C. Hervé, B. M. Knoppers, P. A. Molinari, Dalloz, Collection pharmacogénomique. Quelques questions éthiques et légales, in Les pratiques de la recherche biomédicale Thèmes et commentaires, 2003.

MARC (VAN- OVERSTRAETEN) et Sébastien (DEPRÉ):

- Le traitement des données à caractère personnel et le droit au respect de la vie privée en Belgique, Rev. trim.dr. h. n° 3- 2003.

Marie-Claire PONTHOREAU:

- La directive 46-95 du 24 octobre 1995 relative à la protection à caractère personnes physiques à l'égard du traitement des données à caractère personel et à la libre circulation des ces données, Rev.F.D.adm., janv-fév. 1997.

Michel VASSEUR:

- Observation sous TGI Rennes 13 janv 1992, Dalloz. 1993. Somm. 54.

Michel VÉRON:

- Observation sous crim. 4 mars. 1997, Dr. pénal 1997. 75.

Mole:

- Observation sous crim. 19 déc 1995, Gaz. Pal. 1996. II. Somm. 418.

Mole et Lebon:

- Note sous crim 30 oct. 2001. Gaz. Pal. 2002. II, 1476.

Proust (OLIVIER):

- Etats des lieux sur la proposition de loi du Sénat visant à modifier la loi « Informatique et libertés », Rev.L.D.I, n° 55, décembre 2009.

J.RAVANAS (J):

- Note sous CA Toulouse, 15 janvier. 1991, D. 1991, 600.

Roseline LETTERON:

- « Le droit à l'oubli », Revue de Droit Public et de la Science Politique. 1996. vol. 112.

Sabine LIPOVESTSKT et Audry YANON- DAUVET:

- Le devnir de la protection des données personnelles sur internet, Gaz. Pal. 12.13 septembre 2001.

Théo HASSLER:

- Droit de la personnalité: rediffusion et droit à l'oubli, Recuiel Dalloz, 2007.

Thiercelin (J-F):

- Place de la bioéthique dans la recherche et le développement d'un nouveau médicament, RGDM, numéro spécial « Dix ans des lois de bioéthique en France », Les Etudes Hospitalières, 2006.

Véron:

- Observation sous crim. 19 déc. 1995, Dr. penal 1996, somm. 126.

Trudo LEMMENS et Lisa AUSTIN:

- « Les défis posés par la réglementation de l'utilisation de l'information génétique ». isponible sur: www.isuma.net, Automne 2001, vol. 2.

Xavier BIOY:

- L'identité de la personne devant le Conseil constitutionnel, Rev. F.D.C, n° 65, janv 2006.

VII- ETUDES, RAPPORTES ET OBSERVATIONS:

Benoit TABAKA et Yann TESAR:

- Loi informatique: un nouveau cadre juridique pour le traitement des données à caractère personnel, Dossier, 2004. Disponible sur: www.foruminternet.org

Blandine POIDEVIN:

- La CNIL et les fichiers e-mails. Disponible sur site suivente: https://www.jurisexpert.net/la_cnil_et_les_fichiers_e_mails/

Cécile DE TERWANGNE:

- La nouvelle loi belge des données à caractère personnel, chapitre 4. Étude Disponible sur: https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr4.pdf

CNIL:

- Guid pour les employeurs et les salaries, 2010. Disponible sur: https://www.cnil.fr/sites/default/files/typo/document/Guide_employeurs_salaries.pdf.pdf

F. Mollo:

- Les notions de données directement nominatives et indirectementnominatives, in Les sciences sociales et leurs données, Rapport au Ministre de l'Education Nationale. R. Silberman, juin 1999, Annexes juridiques. Disponible sur:

http://education.gouv.fr/rapport/silberman/table.htm

Goldberg (M), et Padieu (R):

- Quelles règles déontologiques pour les enquêtes à visée de recherche ou de surveillance? A propos de l'enquête sur la santé physique et mentale des écoles primaires parisiennes. Disponible sur: http://hal.archives-ouvertes.fr/docs/00/22/21/18/PDF/Goldberg_MEdito-RESP-Final.pdf

Julien LE CLAINCHE:

- Le traitement des données à caractère personnel dans le cadre d'un site web. Étude Disponible sur: http://www.droit-tic.com/pdf/dp.pdf

La commission de la protection de la vie privée:

- La protection des données à caractère personnel en Belgique, vie privée- principes de base. Disponible sur: http://www.privacycommission.be/

Liliane DUSSERRE:

- La commercialisation des informations médicales est-elle "déontologiquement correcte"? Rapport adopté par le Conseil de l'Ordre des médecins lors de la Session des 29 et 30 juin 2000. Disponible sur: https://www.conseil-national.medecin.fr/sites/default/files/commercialisation.pdf

Lindon R:

- note sous TGI Paris, 11 juill. 1977, D. 1977, 700.
- note sous TGI Paris, 3 déc. 1975, D. 1977, 211.
- note sous TGI Paris, 25 oct. 1982, D. 1983- 363.

Louise CADOUX:

- Voix, image et protection des données personnelles, Commission nationale de l'informatique et des libertés, La documentation francaise, 1996.

MADEF:

- La protection des données personnelles, un enjeu essentiel pour la confiance des consommateurs et la compétitivité des entreprises, guide pratique à des destination des enterprises et des organization professionnelles, Mars 2001, Disponible sur: http://www.medef.com/fileadmin/www.medef.fr/documents/Donnees_persos/Guide_Protection_des_donnees_personnelles.pdf

Marie LAURE-LAFFAIRE:

- Protection des données à caractère personnel, Éditions d'Organisation, 2005. Étude Disponible sur: http://www.eyrolles.com/Chapitres/9782708132351/chap2_Laffaire.pdf

Murielle CAHEN:

- Utilisation des données personnelles. Disponible sur: http://www.murielle-cahen.com/publications/donnees.asp
- QU'est ce qu'une donnée à caractère personnel? données personnelle. disponible sur: https://se-developper-sur-internet.com/donnee-a-caractere-personnel/

Nathalie MELLET-POUJOL:

- Protection de la vie privée et des données à caractère personnelle, Février 2004, disponible sur: http://eduscol.education.fr/chrgt/guideViePrivee.pdf

P. Leclercq:

- « La CNIL, garante de la finalité, de la loyauté et de la sécurité des données personnelles », in Les libertés individuelles à l'épreuve des NTIC, Etudes réunies sous la direction de M.-C. Piatti, Presses Universitaires de Lyon, 2001.

Pierre PEREZ et Jean DUCHAINE:

- Données à caractère personnel, École supérieure de l'éducation nationale, de l'enseignement supérieur et de la recherche (ESENESR), 2013. Disponible sur: http://www.esen.education.fr/fileadmin/user_upload/Modules/Ress

ources/Themes/management_numerique/internet_responsable/textes_juridiques/5-04-2_donnees_personnelles.pdf

Raoul (DEPOUTOT) et Gérard (LANG):

- Le secret statistique concernant les entreprises: Situation 2000 et perspectives d'évolution, janvier 2002, CNIS, Division environnement juridique de la Statistique, janvier 2002, p. 17. Étude Disponible sur: https://www.cnis.fr/wp-content/uploads/2017/10/RAP_2002_71_secret_statistique_entrprises.pdf

Rosa JULIA-BARCEL, Étienne MONTERO et Anne SALAUN:

- La proposition de directive européenne sur le commerce électronique: questions choisies , in Commerce électronique: le temps des certitudes, Cahiers du CRID., Numéro 17 Bruxelles: Académia Bruylant, 2001.

Thiébaut DEVERGRANNE:

- Donnée sensible CNIL: quelle règlementation? disponiaple sur: https://www.donneespersonnelles.fr/donnee-sensible-cnil
- Droit d'accès et droit de communication des données, Disponible sur: https://www.donneespersonnelles.fr/droit-acces-et-de-communication-des-donnees-personnelles
- L'exactitude et la qualité des données, Disponible sur: http://www.donneespersonnelles.fr/exactitude-et-la-qualite-des-donnees
- Le principe de finalité. Disponiable sur: https://www.donneespersonnelles.fr/le-principe-de-finalite
- Le principe de loyauté et de licéitè de la collecte données. disponiable sur: http://www.donneespersonnelles.fr/le-principe-de-loyaute-et-de-liceite-de-la-collecte-des-donnees

Thierry LEONARD:

- E-Marketing et protection des données à caractère personel. Étude Disponible sur: https://www.droit-technologie.org/wp-content/uploads/.../17-1.pdf

Yves POULLET:

- Protection des données à cractere personnel et obligation de securite, Étude Disponible sur: http://www.crid.be/pdf/public/4674.pdf

CNIL (Commission Nationale Informatique et Libertés), Rapports d'activité 1986-2016.

- CNIL, 38 ème Rapport d'activité 2016, Doc.fr. Paris, 2017.
- CNIL, 36 ème Rapport d'activité 2015, Doc.fr. Paris, 2016.
- CNIL, 24 ème Rapport d'activité 2003, Doc.fr. Paris, 2004.
- CNIL, 21ème Rapport d'activité 2000, Doc.fr.Paris, 2001.
- CINL, 19 ème Rapport d'activité 1998, Doc.fr, Paris, 1999.
- CNIL, 15 ème Rapport d'activité 1994, Doc.fr, Paris, 1995.
- CNIL, 17 ème Rapport d'activité 1996, Doc.fr. Paris, 1997.
- CNIL, 15 ème Rapport d'activité 1994, Doc.fr. Paris, 1995.
- CNIL, 14 ème Rapport d'activité 1993, Doc.fr. Paris, 1994.
- CNIL, 13 ème Rapport d'activité 1992, Doc.fr. Paris, 1993.
- CNIL, 12 ème Rapport d'activité 1991, Doc.fr. Paris, 1992.
- CINL, 11 ème Rapport d'activité 1990, Doc.fr. Paris, 1990.
- CNIL, 09 ème Rapport d'activité 1988, Doc.fr. Paris, 1989.
- CNIL, 08 ème Rapport d'activité 1987, Doc.fr. Paris, 1988.
- CINL, 07 ème Rapport d'activité 1986, Doc.fr. Paris, 1987.
- CNIL, 06 ème Rapport d'activité 1985, Doc.fr. Paris, 1986.

VIII- Délibérations:

CNIL: Délibération n° 2010-229 du 10 juin 2010 dispensant de déclaration les traitements automatisés de données à

caractère personnel mis en œuvre par des organismes à but non lucratif abrogeant et remplaçant la délibération n° 2006-130 du 9 mai 2006 (décision de dispense de déclaration n° 8). Disponible sur: https://www.legifrance.gouv.fr/

CNIL: Deliberation n°2006-048 du 23 février 2006 portant autorisation de la mise en oeuvre par la société ALIS d'un traitement automatisé de données à caractère personnel au suivi des clients en infraction. Disponible sur le site suivant: https://www.legifrance.gouv.fr/

CNIL: Délibération n° 2006-078 du 21 mars 2006 portant refus d'autorisation de mise en œuvre par le conseil représentatif des institutions juives de France d'un traitement automatisé de données à caractère personnel destiné à constituer un échantillon de sondage à partir d'un tri sur le nom des intéressés. Disponible sur le site suivant: https://www.legifrance.gouv.fr/

CNIL: Délibération n° 2006-103 du 27 avril 2006, portant autorisation unique de mise en oeuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire, Disponible sur le site suivant: https://www.cnil.fr/

CNIL: Délibération n° 2000-015 du 21 mars 2000 portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par le collège Jean Rostand de Nice, destiné à gérer à la cantine scolaire par la connaissance des empreintes digitales (demande d'avis n° 636.783).

CNIL: Délibération 99-026 du 22 avril 1999. Deliberation portant modification de la norme simplifee nº 23 concernant les traitements automatises d'information nominatives relatives à la gestion des members des associations a but non-lucrative régies par la loi du 1er juillet 1991, et Disponible sur: www.legifrance.gouv.fr/

CINL: Délibération 98-061 du 16 juin 1998, Délibération portant avis sur la mise en oeuvre, par l'INSEE, d'un traitement automatisé d'informations nominatives à l'occasion de

l'enquête “Handicaps-Incapacités-Dépendance” menée auprès des personnes séjournant en institutions. Disponible sur: https://www.cnil.fr/

CNIL: Délibération 96-009 du 27 fevrier 1996, Délibération portant adoption du rapport intititule˝ Les information personnelles issues de la voix et de l'image et la protection de la vie privee et des libertes fondamentales˝. Disponible sur: https://www.legifrance.gouv.fr.

CNIL: Délibération n° 91-033 du 7 mai. 1991 portant avis relative à la création d’un traitement automatiséd d’informations nominatives concernant une application de gestion des dossiers des ressortissants étrangers en France, CNIL, 12 éme rapport d’activité 1991, La documentation francaise, Paris, 1992, p. 233.

CNIL: Délibération n° 85-050 du 22 oct. 1985 portant recommandation relative aux modalités de collecte d’informations nominatives en milieu scolaire et dans l'ensemble du système de formation, JO 17 nov 1985.

CNIL: Délibération n°80-34 du 21 octobre 1980, relative au traitement automatisé de la comptabilité Générale. Disponible sur le site suivant: https://www.legifrance.gouv.fr

X- Sites Internet:

almohakmoonalarab.ahlamontada.com/
https://www.aclu.org
https://www.cnil.fr
https://www.cnis.fr
https://www.conseil-national.medecin.fr
https://www.congress.gov
http://droit-ntic.com
https://www.droit-technologie.org
www.eia.gov
http://www.ethique.sorbonne-paris-cite.fr
https://www.govtrack.us
http://www.juristic.net
https://www.legifrance.gouv.fr
https://www.legalis.net
https://www.legislation.gov.uk

https://juricaf.org
https://www.privacycommission.be
aws.com/Publications/enews/.https://www.privacyl

رابعاً: قائمة المختصرات:

TABLEAU DES PRINCIPALES ABRÉVIATIONS

AJDA.	Actualité juridique – Droit administrative.
Al.	Alinéa.
Art.	Article.
Art. Préc.	Article précite.
Bull.	Bulletin des arrêts de la cour de cassation.
Bull. Crim.	Bulletin de la cour de cassation (chamre criminelle).
C.A.	Cour d'apple (+ ville).
Crim.	Cour de cassation (chambre criminelle).
CCNE.	Comité consultatif national d'éthique.
CE.	Conseil d'État.
Chron.	Chronique.
CJCE.	Comité consultatif national d'éthique.
CJUE.	Cour de justice de l'Union Européenne.
CNIL.	Commission nationale de l'informatique et des libertés.
CNRS.	Centre national de la recherche scientifique.
D.	Receuil Dalloz.
Doc.	Documentation.
Éd.	Editions.
et s.	Et Suivants.
Fr.	Française.
IP.	Internet protocol.
Gaz. Pal.	Gazette du Palais.
J- Cl. Code. Pén.	Juris-classeur. code pénale**.**
JCP.	Juris- classeur Periodique (Semaine juridique).
Ibid.	Au meme en droit.
Idem.	Renvoie à l'article ou à l'ouvrage cité dans la note précédente.
L.G.D.J.	Librairie Générale de droit et de jurisprudence.
N°- ou n°.	Numéro.

NTIC.	Nouvelles techniques de l'information et de la communication.
Obs.	Observations.
Op.cit.	Ouvrage précite.
p.	Page.
pp.	Pages.
PUF.	Pesses universitaires de France.
Rev.	Revue.
Rev. D.C.	Revue des contrats.
Rev.F.D.adm.	Revue française de droit administratife.
Rev. F.D.C.	Revue française de droit compré.
Rev. DTI.	Revue du Droit des Technologies de l'Information.
Rev. LDI.	Revue Lamy droit de l'immatériel.
Rev. trim. dr. h.	Revue trimestrielle des droits de l'homme.
Rev. Se. crim.	Reuve de sciences criminelles.
Rec. Dalloz.	Recueil Dalloz.
RFID.	Radiofrequency identification.
Somm.	Sommaires commentés.
T.	Tome.
T. corr.	Tribunal correctionnel.
TGI.	Tribunal de grande instance.
Th. préc.	Thése précite.
V.	Voir.
Vol.	Volume.

المحتويات