الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً
"دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي GDPR"

د. ميادة مصطفى محمد المحروقي

أستاذ مشارك القانون الجنائي

كلية العدالة الجنائية- جامعة نايف العربية للعلوم الأمنية

المملكة العربية السعودية- الرياض

(ISSN: 2537 - 0758)

الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً "دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي "GDPR"

د. ميادة مصطفى محمد المحروقي

ملخص باللغة العربية

يسعى البحث إلى تحقيق الأهداف الآتية:

١- التعرف علىم ماهية البيانات الشخصية محل الحماية الجنائية.

٢- بيان مدى إعمال مبدأ التناسب بين الحق في حماية البيانات الشخصية وغيرها من الحقوق الدستورية.

٣- تفسير المبادئ العامة التي تحكم تجميع ومعالجة البيانات الشخصية، خاصة ما يتعلق بمشروعية معالجة تلك البيانات.

٤- تحليل أهم الإشكاليات القانونية التي تواجه الحق في الخصوصية والكشف عن البيانات الشخصية، خاصة مع اختلاف نظرة المجتمعات للحق في حماية الحريات الفردية لاسيما ما يتعلق بالبيانات الشخصية.

٥- تناول صور جرائم الاعتداء على البيانات الشخصية للأفراد المعالجة إلكترونياً والعقوبات المقررة لها.

موضوع هذا البحث هو الحماية الجنائية للبيانات الشخصية المعالجة الكترونيا. وهو يهدف إلى تحقيق الأهداف الآتية:

- التعرف على ماهية البيانات الشخصية محل الحماية الجنائية.
- بيان مدى إعمال مبدأ التناسب بين الحق في حماية البيانات الشخصية وغيرها من الحقوق الدستورية.
- تفسير المبادئ العامة التي تحكم تجميع ومعالجة البيانات الشخصية، خاصة ما يتعلق بمشروعية معالجة تلك البيانات.
- تحليل أهم الإشكاليات القانونية التي تواجه الحق في الخصوصية والكشف عن البيانات الشخصية، خاصة مع اختلاف نظرة المجتمعات للحق في حماية الحريات الفردية لاسيما ما يتعلق بالبيانات الشخصية.
- تناول صور جرائم الاعتداء على البيانات الشخصية للأفراد المعالجة إلكترونياً والعقوبات المقررة لها.

ويعالج هذا البحث المشكلات القانونية التي يثيرها من خلال خطة تتكون من ثلاث مباحث على الوجه التالي:

المبحث الأول: ماهية البيانات الشخصية محل الحماية الجنائية وقوتها القانونية

المبحث الثاني: القواعد التي تحكم تجميع ومعالجة البيانات الشخصية للأفراد.

المبحث الثالث: تجريم العدوان على البيانات الشخصية المعالجة إلكترونياً.

Abstract

This research seeks to achieve the following objectives:

- Identify what personal data is subject to criminal protection.
- An indication of the extent to which the principle of proportionality is implemented between the right to protect personal data and other constitutional rights.
- Interpreting the general principles governing the collection and processing of personal data, particularly with regard to the legality of processing such data.
- Analyzing the most important legal problems facing the right to privacy and disclosure of personal data, especially with the difference in societies' view of the right to protect individual freedoms, especially with regard to personal data.
- Examining the crimes of assaulting the electronically processed personal data of individuals and the penalties prescribed therefor.

This research deals with the legal problems it raises through a plan consisting of three topics as follows:

The first topic: the nature of personal data subject to criminal protection and its legal force

The second topic: the rules governing the collection and processing of personal data of individuals.

The third topic: criminalizing aggression against electronically processed personal data.

(ISSN: 2537 - 0758)

المقدمة

- **موضوع البحث**:

يتجلى الهدف من النظر إلى إشكاليات الاعتداء على بيانات الأشخاص المعالجة إلكترونياً والسعي وراء الحد منها، في كيفية رسم فلسفة التعامل معها في ظل الأطر التنظيمية التي تسعى إلى مواجهتها، لاسيما وأن الحياة الخاصة للأفراد تشكل قيمة ومصلحة تدخل في عداد المصالح العامة الجوهرية التي يُدعى القانون الجنائي إلى التدخل لحمايتها بنصوص تجريم وعقاب تتلاءم وطبيعتها.

ولعل السبب الرئيس في تجريم الاعتداء على البيانات الشخصية، ليس مجرد حماية تلك البيانات فحسب، بل حماية الحقوق والحريات الأساسية للأشخاص أصحاب تلك البيانات، وما صاحب ذلك من ظهور مخاطر عديدة تهدد تلك البيانات وتمس بمصلحة صاحبها؛ كون تلك المخاطر تبدأ في الظهور عند الوقت الذي يبدأ فيه تجميع البيانات من قبل الأشخاص أو الشركات وحتى المؤسسات الإدارية في الدولة ومن ثم مرحلة التعامل فيها. بل قد يتطور الأمر إلى حد الاتجار بها وانتقالها من جهة لأخرى دون موافقة صاحب تلك البيانات. ويزيد الأمر خطورة وتعقيداً عندما يتم فقدان تلك البيانات من المعالج لها أو سرقتها واستخدامها في طرق غير مشروعة قد تضر بصاحبها.

وعليه يتناول موضوع البحث أطر الحماية الجنائية التي أسدلتها التشريعات الجنائية المقارنة، والتي تهدف إلى حماية خصوصية بيانات الأفراد الشخصية المعالجة إلكترونياً؛ حيث إن العبث ببيانات الأفراد الشخصية ألقى بظلاله على النواحي الأمنية، وذلك بظهور جرائم تتناسب والصبغة الخاصة لهذا المجال، لاسيما مع سهولة وجود برامج الاختراق والفيروسات والتي أدت إلى سرعة الدخول إلى أنظمة البيانات واختراق أمن المعلومات، وصولاً إلى بيانات الأشخاص واستغلالها.

لذا يهدف البحث إلى تفسير المبادئ التي تحكم تجميع ومعالجة البيانات الشخصية للأفراد إلكترونياً، ومدى مشروعية تلك المعالجة نظامياً، مع عرض صور الاعتداء على تلك البيانات وكيف تصدت لها التشريعات الجنائية بعقوبات وتدابير تهدف إلى مواجهتها والحد منها.

في ظل هذه المعطيات وإدراكاً لقيمة وسمو الحق في الخصوصية، واستشعار التشريعات الجنائية بوجود خطر يمس حريات الأفراد، لاسيما مع الانتقال إلى العالم

الرقمي وانتشار أجهزة تقنية المعلومات والمواقع الإلكترونية والتي أدت إلى معالجة كميات كبيرة من البيانات، ظهر العديد من التشريعات الجنائية التي عالجت أطر الحماية الجنائية للبيانات الشخصية. من بين أحدث تلك التشريعات قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م. ونظام حماية البيانات الشخصية السعودي رقم (م/١٩) وتاريخ١٤٤٣/٢/٩هـ الموافق ٢٠٢١/٠٩/١٦م، وآخر تعديلاته الصادرة بالمرسوم الملكي رقم (م/١٤٨) وتاريخ ١٤٤٤/٩/٥هـ، الموافق ٢٧ مارس ٢٠٢٣م،

كذلك القانون الفرنسي المتعلق بمعالجة البيانات والملفات والحريات والأحكام المختلفة بشأن حماية البيانات الشخصية رقم ٧٨-١٧ المؤرخ في ٦ يناير ١٩٧٨م، والمعدل بموجب الأمر رقم ٢٠١٨-١١٢٥ المؤرخ في ١٢ ديسمبر ٢٠١٨م الصادر بموجب المادة ٣٢ من القانون رقم ٢٠١٨-٤٩٣ المؤرخ ٢٠ يونيو ٢٠١٨م، والتعديلات التي أدخلت عليه في مايو ٢٠١٩م. بشأن حماية البيانات الشخصية. والقانون الأمريكي لحماية البيانات الصادر ١٩٩٧م.

ونظرا لأهمية حماية بيانات الأفراد الشخصية صدرت اللائحة الأوروبية رقم ٦٧٩/٢٠١٦ الصادرة عن الاتحاد الأوروبي بتاريخ ٢٧ أبريل ٢٠١٦م بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات. والتي دخلت حيز التنفيذ في في ٢٥ مايو/ أيار ٢٠١٨م. كما تم الإعلان عن توجيه الاتحاد الأوروبي ٦٨٠/٢٠١٦ الصادر عن البرلمان الأوروبي والمجلس بتاريخ ٢٧ أبريل ٢٠١٦م بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية من قبل السلطات المختصة لأغراض منع الجرائم الجنائية والكشف عنها.

- **أهداف البحث**:

يسعى البحث إلى تحقيق الأهداف الآتية:

٦- التعرف على ماهية البيانات الشخصية محل الحماية الجنائية.

٧- بيان مدى إعمال مبدأ التناسب بين الحق في حماية البيانات الشخصية وغيرها من الحقوق الدستورية.

٨- تفسير المبادئ العامة التي تحكم تجميع ومعالجة البيانات الشخصية، خاصة ما يتعلق بمشروعية معالجة تلك البيانات.

(ISSN: 2537 - 0758)

٩- تحليل أهم الإشكاليات القانونية التي تواجه الحق في الخصوصية والكشف عن البيانات الشخصية، خاصة مع اختلاف نظرة المجتمعات للحق في حماية الحريات الفردية لاسيما ما يتعلق بالبيانات الشخصية.

١٠- تناول صور جرائم الاعتداء على البيانات الشخصية للأفراد المعالجة إلكترونياً والعقوبات المقررة لها.

- **إشكالية البحث وتساؤلاته**:

تكمن إشكالية البحث في أن معطيات التقنية المعلوماتية أضافت أنماطاً وصوراً إجرامية جديدة خاصة ما يرتبط منها ببيانات الأشخاص الطبيعيين، كما أنها أصبحت وسائل متاحة في يد الجميع. ولأن المساس بخصوصية الأفراد- بوجه عام- في غير الحدود التي رسمها النظام، تمثل انتهاكاً صارخاً لكرامته الإنسانية، لاسيما إذا حدث ذلك بشكل تعسفي ودون مبرر شرعي أو نظامي؛ فكانت حماية خصوصية بياناته لزاماً على الأنظمة والتشريعات. وعليه يكمن التساؤل الرئيس في: **كيف أسدلت التشريعات الجنائية حماية خاصة لبيانات الأفراد الشخصية المعالجة إلكترونياً من صور الاعتداء عليها؟**

كما يرمي البحث إلى الإجابة على عدة تساؤلات فرعية من بينها؛ ما هي البيانات الشخصية محل الحماية الجنائية؟ وهل تختلف البيانات الشخصية عن غيرها من البيانات التي تخص الأفراد؟ وماذا يعني إعمال مبدأ التناسب بهدف التوفيق بين الحقوق وإعطاء أسبقية لحق على حق آخر بحسب الأهداف المشروعة التي تقررها المصلحة العامة؟ وما هي الشروط الواجب اتباعها عند تجميع البيانات المعالجة إلكترونياً؟ وما حقوق الشخص على بياناته؟ وكيف ألزمت التشريعات الجنائية جهة المعالجة بالعديد من الالتزامات أثناء قيامها بمعالجة بيانات الأشخاص؟ وما صور الاعتداء التي يمكن أن تقع على البيانات الشخصية؟ وما هي العقوبات في حالة العدوان على المصلحة محل الحماية المقررة لتلك البيانات؟.

- **أهمية البحث**:

(أ) الأهمية العلمية: يساهم البحث في فهم القضايا ورفع مستوى الوعي لدى أفراد المجتمع، لاسيما فيما يخص أهمية حماية البيانات الشخصية للأفراد، كون الجهل بالقانون يسأل عنه صاحبه. فضلاً عن مناقشة وتفسير الإشكاليات التي تواجه حماية البيانات الشخصية واعتبارها حقاً لصيقاً لا يجوز الاعتداء عليه تحت أي

ذريعة، وبصفة خاصة مع انتشار وسائل التواصل الاجتماعي والعلانية المرتبطة بها. فقد يصبح الاعتداء على تلك البيانات ظاهرة تثير الذعر والثقة في التعامل. إضافة إلى تقديم توصيات من شأنها وضع منظومة حماية لضمان أمن وسلامة المجتمع المعلوماتي، وإيجاد حلول نظامية قد يستند لها المشرعون وكذلك متخذو القرار والتي تكفل حماية حقوق الأفراد في المجتمع.

(ب)الأهمية العملية: تبدو الأهمية العملية نظراً لتزايد التحديات والمشكلات القانونية المتولدة عن استخدام بيانات الأفراد الشخصية، فضلاً عن تحليل الاختلافات الواردة في التشريعات المقارنة وبيان وجهة نظرهم في كيفية إضفاء سبل حماية أكثر فاعلية. كما تزايدت أهمية الموضوع بسبب جائحة كرونا وما ارتبط بها من ضرورة الكشف عن المعلومات الصحية للأشخاص، وطلب تسجيل حالتهم في هواتفهم الخلوية وطلب الاطلاع عليها عند دخول الأماكن العامة بل وتحديد انتقالاتهم بسبب ظروفهم الصحية. ومن ثم كانت الحاجة إلى التعرف على أحكام حماية البيانات الشخصية جنائياً، والتطرق إلى القواعد النظامية التي تحكم تجميع تلك البيانات ومعالجتها إلكترونياً في ظل القوانين والأنظمة التي تحكمها.

- **منهج البحث**:

سوف نعتمد خلال بحثنا على المنهج الوصفي التحليلي المقارن، حيث يتبع المنهج الوصفي في عرض النصوص القانونية والآراء الفقهية والقضائية المرتبطة بحماية البيانات الشخصية للأفراد. كما يتبع المنهج التحليلي بتحليل تلك النصوص وأحدث القضايا التي أثيرت في هذا الشأن. ولأهمية الإشكاليات التي تثيرها الأحكام القانونية للبيانات الشخصية في الأنظمة المختلفة، فقد تمت معالجة الدراسة بالاستعانة بقوانين مقارنة، كالقانون الأمريكي والقانون الفرنسي والقانون المصري والنظام السعودي واللائحة التنظيمية الصادرة عن البرلمان الأوروبي GDPR. فقد تناولت أغلب تلك الإشكاليات في محاولة للتصدي لمخاطرها وهو ما سيتيح لنا الاطلاع على القوانين المقارنة والاجتهادات الفقهية؛ بغية التطرق للسبل التي تبنتها تلك التشريعات في محاولة للاستفادة منها ومعرفة الأسس القانونية التي استندت إليها.

(ISSN: 2537 - 0758)

- **تقسيم البحث**:

تحقيقاً للأهداف التي يسعى البحث إلى تحقيقها، فسوف يتم تناوله في فصليين أساسيين على النحو التالي:-

المبحث الأول: ماهية البيانات الشخصية محل الحماية الجنائية وقيمتها القانونية

المطلب الأول: مفهوم البيانات الشخصية للأفراد.

المطلب الثاني: الحق في الخصوصية وإعمال مبدأ التناسب.

المبحث الثاني: القواعد التي تحكم تجميع ومعالجة البيانات الشخصية للأفراد.

المطلب الأول: المبادئ العامة في تجميع البيانات الشخصية المعالجة إلكترونياً.

المطلب الثاني: ضوابط مشروعية معالجة البيانات الشخصية إلكترونياً.

المبحث الثالث: تجريم العدوان على البيانات الشخصية المعالجة إلكترونياً

المطلب الأول: تجريم مخالفة ضوابط جمع وحفظ البيانات الشخصية والإجراءات الأولية اللازمة لحمايتها.

المطلب الثاني: تجريم الاعتداء على البيانات الشخصية ذاتها.

- **الخاتمة.**

(النتائج– التوصيات)

- **قائمة المراجع**

المبحث الأول
ماهية البيانات الشخصية محل الحماية الجنائية وقيمتها القانونية

تمهيد وتقسيم:

ماهية الشئ تعني استجلاء حقيقة أمره وطبيعته وخصائصه وسماته. ويعد مفهوم حماية البيانات من الحقوق اللصيقة بالشخص، لاسيما وأنها مرتبطة ارتباطاً وثيقاً بالحق في الخصوصية. كلاهما له دور فعال في الحفاظ على الحقوق الأساسية وما يتعلق بها من ممارسة الحقوق والحريات الأخرى كالحق في التعبير وإبداء الرأي على سبيل المثال.

وقد ساهمت ثورة تكنولوجيا المعلومات بشكل فعال في التحكم في كل ما يخص البشر، لاسيما ما يتعلق بخصوصياتهم التي هي محل حماية من الأساس. وقد تطرق الأمر إلى أدق تفاصيل الإنسان، بل ونشرها وانتقالها ليس فقط بشكل محلي بل متجاوزة حدود الدول، دون اعتبار للزمان والمكان وأصناف المطلعين على تلك البيانات[١].

---

[١] وهو ما أكدته محكمة النقض المصرية في حكمها الصادر بتاريخ ١٦ مارس ٢٠٢٢م بقولها "أن البشرية لم تعرف فى أى وقت مضى مثل هذا التزايد الحالى والسرعة فى العلاقات بين الناس، فبعد التلغراف والتليفون والراديو والتليفزيون كانت شبكة المعلومات والاتصالات الدولية المعروفة باسم "الإنترنت" والتى ساهمت بشتى السبل فى نقل وتبادل المعلومات بحيث تسمح بالتعرف الفورى على المعلومة والصورة والصوت والبيانات عبر أنحاء العالم لدرجة يمكن معها القول بتلاشي فروق التوقيت، فالإنترنت أصبح أداة جديدة للمعلوماتية والاتصال وبذلك فهو يمثل ثورة فى الاتصال الإلكتروني، وبهذا التطور السريع جدًا فى نقل وتبادل المعلومات أصبح مجتمع القرن الحادى والعشرين هو مجتمع المعلومات وفى هذا المجتمع ألغت سرعة سير وانتقال المعلومات الزمان والمكان وفسحت المجال أمام الحريات بحيث أصبح لكل شخص يعيش على أرض المعمورة الحق فى الاتصال بغيره وتبادل الأفكار والمعلومات معه، وقد تدعم ذلك بصيرورة حق الاتصال والحصول على المعلومات وتداولها ليس فقط حقًا دستوريًا بل أيضًا حقًا من حقوق الإنسان وحرياته الأساسية، إلا أن هذه التجربة الجديدة "الإنترنت" أظهرت من الخوف بقدر ما أظهرت من الإعجاب، وكان منبع الخوف قادمًا من أن الإنترنت ليس له حدود ولا قياده قانونية وبعبارة أخرى ليس له شخصية قانونية معنوية تمثله فى مواجهة المستعلمين له أو فى مواجهة الغير لأنه عباره عن اتحاد فيدرالي للشبكات فى مجموعها يغطى تقريبًا كل الكرة الأرضية، وكان مما لاشك فيه أن بحث الحماية القانونية ضد هذه الأخطار لا يكون إلا من خلال القانون والذى تطور فى هذا المجال بوضع القواعد القانونية التى تحمى اعتداء أى شخص على الحياة الخاصة لآخرين من خلال الإنترنت".

(ISSN: 2537 - 0758)

بل وقد تستلزم حقوق الخصوصية وحماية البيانات عقد موازنة مع المصالح الخاصة مثل الحق في حرية الصحافة وحرية الوصول إلى المعلومات، وكذلك المصالح العامة كالأمن القومي والتزامات التعاون القضائي والشرطي في المسائل الجنائية، خاصة مايتعلق بمجال الحرية والأمن والعدالة. وهو ما يستلزم معه عقد توازن بين الحقوق الفردية والأمن والعدالة.

وعليه سوف نتناول في هذا المبحث ما يتعلق ببيان مفهوم البيانات الشخصية، إضافة إلى تفسير مبدأ التناسب بين الحقوق وخاصة الحق في الخصوصية. ومن ثم سوف يتم تقسيم هذا المبحث إلى مطلبين على النحو التالي:-

المطلب الأول: مفهوم البيانات الشخصية للأفراد.

المطلب الثاني: الحق في الخصوصية وإعمال مبدأ التناسب.

المطلب الأول
مفهوم البيانات الشخصية للأفراد

أولاً- المقصود بالبيانات الشخصية:

تناول القانون المصري تعريف البيانات الشخصية بأنها "أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر، عن طريق الربط بين هذه البيانات وأي بيانات أخرى، كالاسم أو الصورة، أو الصوت أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية أو الاقتصادية، أو الثقافية، أو الاجتماعية"[٢].

ولم يخالف القانون المصري نظام حماية البيانات الشخصية السعودي رقم (٩٨) لسنة ١٤٤٣هـ (٢٠٢١م) البيانات الشخصية في المادة (الأولى) منه بأنها "كل بيان- مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية

(الحكم الصادر من محكمة النقض بجلسة ٢٠٢٢/٠٣/١٦م في الطعن رقم ٩٥٤٢ لسنة ٩١ ق، طعنًا على الحكم الصادر من الدائرة الاستئنافية بمحكمة القاهرة الاقتصادية في الدعوى المقيدة برقم ١١٩ لسنة ١٢ ق اقتصادي، المقامة من ورثة الطيار الراحل أشرف أبو اليسر ضد الممثل المصري محمد رمضان).

[٢] المادة الأولى من الفصل الأول من نظام حماية البيانات الشخصية المصري.

الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي". وهو ما يتفق مع نص المادة الأولى من قانون حماية البيانات الشخصية المصري.

أما قانون حماية البيانات الشخصية في بريطانيا لسنة ٢٠١٨ م فقد تناول في ثنايا مادته الثالثة، ما يتعلق بتحديد المقصود بالبيانات الشخصية بأنها "المعلومات المتعلقة بشخص حي محدد أو يمكن تحديده بطريقة مباشرة أو غير مباشرة بالإشارة إلى: الاسم، رقم البطاقة، محل الإقامة أو العنوان الإكتروني أو أي محدد آخر بدني أو جيني أو عقلي أو اقتصادي أو ثقافي أو اجتماعي". غير أن بعض التشريعات تولي البيانات الشخصية المتعلقة بأصول الفرد العنصرية وحالته الطبية وسوابقه القضائية عناية خاصة. فلم تقتصر على تنظيم تجميع ومعالجة تلك البيانات ولكنها قررت جزاءً جنائياً في حال نشرها، وذلك على ما سيلي بيانه.

لذا كان اتجاه التشريعات الجنائية المقارنة، إلى ضرورة احترام إرادة الشخص في حرصه على عدم نشر بياناته الشخصية على الرغم من أنها لا تدخل كلها في مجال حرمة الحياة الخاصة. فالاحترام واجب ليس فقط للحياة الخاصة، بل يمتد إلى احترام كل ما يتعلق به، كون ذلك يمثل احتراماً لحريته الشخصية وليس اقتصاراً على حياته الخاصة[٣].

كما تنص المادة ٤ من اللائحة الأوروبية، والمعنونة "التعاريف"، في الفقرة الأولى، على أن مفهوم "البيانات الشخصية" ينبغي أن يفهم على أنه يتعلق "بأي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه "موضوع البيانات"؛ "هو الشخص الطبيعي الذي يمكن التعرف عليه، بشكل مباشر أو غير مباشر، ولا سيما بالإشارة إلى معرف، مثل الاسم أو رقم التعريف أو بيانات الموقع أو معرف على الإنترنت، أو إلى واحد أو

---

[٣] د. محمد عبد المحسن المقاطع، "**نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر**"، مؤتمر جامعة الكويت حول "القانون والحاسب الآلي" مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي، ١٩٩٤ ص ١٦.

-خالد بوعدان، "**الحماية التشريعية والتقنية للحق في الخصوصية عبر شبكة الإنترنت**". مجلة عدالة للدراسات القانونية والقضائية، الناشر: المصطفى الغشام الشعيبي، العدد ١٥، سنة ٢٠٢١م.

(ISSN: 2537 - 0758)

أكثر من العوامل المحددة لهويته الجسدية أو الفسيولوجية أو الوراثية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية.

ومع ذلك فإن النظام السعودي يمد مظلة الحماية إلى البيانات الشخصية أياً كانت الدعامة المدونة عليها دون أن يحصرها في مجال البيانات المعالجة آلياً؛ فهي تشمل إذن البيانات الشخصية المدونة ورقياً بقوله في المادة الأولى " كل بيان –مهما كان مصدره أو شكله". ويقع هذا على عكس ما قرره المشرع المصري الذي قصر مجال تطبيق قانون حماية البيانات الشخصية على البيانات المعالجة آلياً.

أما المادة ٢ الفقرة (أ) من توجيه حماية البيانات[٤] فقد تناولت تعريف البيانات الشخصية بأنها تعني أي معلومات تتعلق بشخص طبيعي محدد الهوية أو يمكن التعرف عليه "صاحب البيانات"؛ ففيما يتعلق بالشخص الذي يمكن التعرف عليه فهو الشخص الذي يمكن تحديد هويته بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى رقم التعريف أو إلى عامل أو أكثر خاص بهويته الجسدية أو الفسيولوجية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية.

ويعرف توجيه حماية البيانات في الفقرة (ج) من نفس المادة نظام حفظ البيانات الشخصية والذي أطلق عليه "نظام حفظ الملفات" بأنه أي مجموعة منظمة من البيانات الشخصية التي يمكن الوصول إليها وفقًا لمعايير محددة، سواء كانت مركزية أو لامركزية أو مشتتة على أساس وظيفي أو جغرافي[٥].

وقد أحال القانون الفرنسي في تعريفه للبيانات الشخصية محل الحماية إلى المادة ٤ من اللائحة الأوروبية، إلا أنه استخدم تعبير "البيانات ذات الطابع الشخصي"، **فهل يعني بذلك اختلافه عن تعبير "البيانات الشخصية" الوارد في التشريعات المقارنة؟.** يرد البعض على ذلك بأن المشرع الفرنسي قد أراد بذلك التمييز بين البيانات الاسمية والتي لا تتغير عن الشخص الطبيعي كاسمه وخصائصه الحيوية، وغيرها من البيانات التي تتصل به كرقم هاتفه ورقم حسابه المصرفي. ويرجح البعض أن التعريف الوارد في اللائحة الأوروبية يستخدم عادة للإحالة إلى بيانات ترتبط بهوية شخص معين، واستثنى

(4) Article 2 (a) of the Data Protection Directive.

(5) Article 2(a) of the Data Protection Direct: (c) “personal data filing system” (“filing system”) shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

من ذلك البيانات التي لا ترتبط بهويته الشخصية ولكنها تساعد في نفس الوقت على تحديد هويته بشكل غير مباشر، كرقم تسجيل السيارة ورقم هاتفه الخلوي[٦].

وفي رأينا؛ أنه لا فرق بين البيانات الشخصية التي ترتبط بهوية شخص معين، أو التي تساعد في الدلالة على هويته؛ ذلك أنه وفقاً للتعريفات السابقة فقد تم تعريف البيانات الشخصية بأنها كل بيان من شأنه أن يؤدي إلى التعرف على شخص على وجه التحديد أو جعل التعرف عليه ممكناً، أي سواء تم تحديده بطريقة مباشرة أو غير مباشرة.

ترتيباً على ما تقدم، يعد بياناً شخصياً خاضعاً للحماية الجنائية، كل بيان يتعلق بالشخص يساعد في التعرف على هويته، كاسمه، ولقبه، وجنسيته، وجنسه، ورقم هاتفه وعنوان منزله، وكل ما يتعلق بأفراد أسرته، وسواء أكان مجال التعرف عليه يشتمل على حروف أو أرقام أو صور أو مقاطع صوتية. كما يشتمل على بياناته المرتبطة بوسائل الاتصال الإلكترونية كعنوان بريده الإلكتروني، وحساباته الإلكترونية، وكذلك البيانات المخزنة عبر هذه الوسائل. وغير ذلك من بياناته الحساسة (كالأصل العرقي، والدين، والفكر، والسياسة، والصحة، وبياناته الائتمانية، والبيومترية،... إلخ).

ونلاحظ أن هذه الصور تم ذكرها على سبيل المثال وليس الحصر، حيث تتسع تشريعات الحماية لتشتمل على صور عديدة حتى ولو لم يتم تناولها ضمن نصوصها صراحة؛ لأن تلك النصوص كانت أوسع نطاقاً من حيث المجال لكي تتضمن أي بيان شخصي قد يظهر في المستقبل، إذا ما أدى إلى التعرف على الشخص بشكل مباشر أو غير مباشر.

ثانياً- التوسع في مفهوم البيانات الشخصية:

اتجهت بعض الأحكام القضائية إلى تبني مفهوم موسع للبيانات الشخصية. من ذلك حكم المحكمة العليا في إيرلندا، الصادر بتاريخ ٢٠ ديسمبر ٢٠١٧م والمتعلق بقضية Nowak v Data Protection Commissioner Peter، والذي انتهت فيه المحكمة إلى أن الإجابات المكتوبة التي يقدمها المرشح في الاختبار المهني تشكل معلومات تتعلق بهذا المرشح؛ بسبب محتواه أو غرضه أو تأثيره، حيث إن إجاباته كانت تعكس

---

[٦] محمد حسن عبدالله علي (٢٠٢١م)، **"النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة"**. مجلة كلية القانون، جامعة عجمان، المجلد ٧، العدد ١٤، ص ١٢.

(ISSN: 2537 - 0758)

طريقة تفكيره وحكمه على الأمور ومن ثم أمكن اعتبارها بيانات شخصية تخضع للحماية التي يقرها التوجيه الأوربي لحماية البيانات(٧).

وقد تعلق ذلك بطلب الطاعن Nowak والذي خضع لاختبار مهني في المحاسبة، الوصول إلى بياناته بموجب قانون حماية البيانات الإيرلندي CAI والمتمثلة في نص إجابته على الاختبار المهني الذي خضع له، إلا أنه تم رفض الكشف عن نص الفحص الخاص به على أساس أن إجابته لا تشكل بيانات شخصية بالمعنى المقصود في تشريعات حماية البيانات الشخصية، وعلى إثر ذلك رفع الطاعن دعوى أثارت التساؤل التالي: هل يعتبر نص الاختبار الكتابي يندرج تحت تعريف البيانات الشخصية في م/٢ (أ) من التوجيه الأوروبي لحماية البيانات.

وفي رأينا أنه بمراجعة المادة ٣ من التوجيه الأوروبي لحماية البيانات، فإن التوجيه ينطبق على معالجة البيانات الشخصية كلياً أو جزئياً بالوسائل التلقائية، وعلى المعالجة بخلاف الوسائل التلقائية للبيانات الشخصية التي تشكل جزءاً من نظام الملفات أو جزءاً من الحفظ في النظام. لذا نلاحظ أن اختبار السيد Nowak لم تتم معالجته بوسائل آلية كإدخاله وحفظه في نظام معالجة بيانات إلكتروني، ومع ذلك فقد اعتبرت المحكمة أنه يشكل جزءاً من نظام حفظ الملفات وفقاً للمادة ٢ من التوجيه الأوروبي. فلا يلزم بالضرورة حفظ نظام الملفات في نظام معالجة إلكترونية، لأن نظام حفظ الملفات يمتد ليشمل أي مجموعة منظمة من البيانات الشخصية، والتي يمكن الوصول إليها وفقاً لمعايير محددة، ولعل هذا ينطبق على مجموعة نصوص الإجابة على الاختبار المهني في شكل ورقي مرتبة أبجدياً أو وفق لمعايير أخرى تفي بهذه المتطلبات.

ثالثاً- الفرد محل الحماية هو الشخص الطبيعي وليس الشخص المعنوي:

تقتصر البيانات محل الحماية على بيانات الأشخاص الطبيعيين- وهو ما أكدته نصوص أغلب التشريعات الجنائية- حيث تضمنت اللائحة الأوروبية النص في فقرتها الأولى من المادة الرابعة على أن" البيانات الشخصية هي أي معلومات تتعلق بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر.....إلخ"(٨). وعرف

(7) Peter Nowak v Data Protection Commissioner. Ireland's Supreme Court - Judgment of the Court (Second Chamber) of 20 December 2017. (Case - 434/16).

(8) Règlement (EU) 2016/679, Art. 4. "Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an

القانون المصري الشخص المعني بالبيانات بأنه "أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونياً تدل عليه قانوناً أو فعلاً، وتمكن من تمييزه عن غيره"(٩). وتضمن نظام حماية البيانات الشخصية السعودي التعريف بصاحب البيانات الشخصية بأنه "الفرد الذي تتعلق به البيانات الشخصية أو من يمثله أو من له الولاية الشرعية عليه"(١٠).

وكان القانون الفرنسي المتعلق بمعالجة البيانات والملفات والحريات، قد اشتملت حمايته على الشخص الطبيعي دون الشخص المعنوي، باعتبار أن المقصود هو حماية الحريات الشخصية، الأمر الذي لا يتوافر فيما يتعلق بالأشخاص المعنوية مثل الشركات والجمعيات وغيرها من التجمعات(١١).

وقد أفصح المشرع الفرنسي عن ذلك صراحة عندما تناول تعريف البيانات الشخصية في المادة الثانية من القانون رقم ٢٠٠٤- ٨٠١ الصادر في ٦ أغسطس سنة ٢٠٠٤م، في خصوص الكمبيوتر والحريات بقوله "البيانات الشخصية هي أي معلومات تتعلق بشخص طبيعي تم تحديده أو يمكن تحديده، بشكل مباشر أو غير مباشر، بالرجوع إلى رقم تعريف أو إلى عنصر أو أكثر خاص به. ومن أجل تحديد ما إذا كان الشخص قابلاً للتحديد أم لا، فمن الضروري النظر في جميع الوسائل التي تمكن من تحديد هويته المتاحة أو التي يمكن لمراقب التحكم أو أي شخص آخر الوصول إليها"(١٢).

---

identifiable natural person is one who can be identified, directly or indirectly....".

(٩) المادة الأولى، الفصل الأول، قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م.

(١٠) المادة الأولى، نظام حماية البيانات الشخصية السعودي.

(11) Jacques FRANCILLON, **" L'adaptation du droit pénal à certaines fromes de délinquance informatiques et audio-visuelles "in" La protection pénale des infromations sur la personne en droit français contemporain, in "Droit pénal contemporain"** Mélanges en l'honneur d'André Vitu, éd. Cujas 1989.

(12) "Law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data and amending Law No. 78-17 of 6 January 1978 on data processing, files and freedoms: "Personal data is any information relating to a natural person identified or which can be identified, directly or indirectly, by reference to an identification number or to one or more elements specific to it. In order to determine whether a person is identifiable, it is necessary to consider all the means to enable his

(ISSN: 2537 - 0758)

كما لم تميز أغلب التشريعات بين الشخص الطبيعي كمواطن أو أجنبي(مقيم). وهو ما أكدت عليه اللائحة الأوروبية بوجوب حماية بيانات الأشخاص الطبيعيين بقولها "بغض النظر على جنسيتهم أو مكان إقامتهم". لاسيما وأن اللائحة الأوروبية لها قوة تنفيذية مباشرة في نطاق الدول الأعضاء، فكل ما يتعلق بمعالجة بيانات الأشخاص الطبيعيين داخل إقليم دولة من دول الاتحاد الأوروبي يخضع لأحكام اللائحة.

أما القانون المصري فقد توسع في اشتماله لبيانات الأشخاص محل الحماية، بأن جعل سريان قانون حماية البيانات الشخصية المصري واجب التطبيق على كل من ارتكب الجرائم المنصوص عليها وفق هذا القانون من المصريين داخل مصر أو خارجها، أو كان من غير المصريين (الأجانب) المقيمين داخل مصر، أو كان أجنبياً ارتكب الفعل المجرم خارج مصر متى كان الفعل معاقباً عليه في الدولة التي وقع فيها تحت أي وصف قانوني شريطة أن تكون البيانات محل الجريمة هي لمصريين أو أجانب مقيمين داخل مصر[١٣].

وهكذا فعل النظام السعودي والذي امتدت حمايته إلى أي عملية مُعالجة لبيانات شخصية تتعلق بالأفراد تتم في المملكة بما فيهم الأفراد المقيمين، بأي وسيلة كانت حتى ولو كانت جهة التحكم أوالمعالجة خارج المملكة[١٤].

ومع ذلك؛ وعلى الرغم من نص لائحة الاتحاد الأوروبي صراحة على أن البيانات محل الحماية الشخصية هي بيانات الأفراد الطبيعيين، وأنها لا تعالج البيانات الشخصية المتعلقة بالأشخاص الاعتباريين، إلا أنها أجازت في فقرتها الأولى من المادة ٢٣ لقانون الاتحاد أو قانون الدولة العضو التي يخضع لها المراقب أو المعالج–عن طريق تدابير تشريعية– أن يحد من نطاق الالتزامات والحقوق المنصوص عليها في المواد من ١٢ إلى ٢٢ والمادة ٣٤ وفي المادة ٥ بقدر ما تتوافق أحكام القانون المعني مع الحقوق والالتزامات المنصوص عليها في المواد من ١٢ إلى ٢٢، عندما يحترم هذا التقييد جوهر الحقوق والحريات الأساسية ويشكل تدبيراً ضرورياً ومتناسباً في مجتمع ديمقراطي خاصة إذا كان لحماية أهداف ذات مصلحة عامة للاتحاد أو لدولة عضو، بما في ذلك المصلحة الاقتصادية أو المالية الهامة سواء في المجالات النقدية والميزانية والمالية

or her identification available to or to which the controller or any other person may have access."

[١٣] المادة/ ٢ قانون حماية البيانات الشخصية المصري.

[١٤] المادة/ ٢ نظام حماية البيانات الشخصية السعودي.

والصحة العامة والضمان الاجتماعي، وضمان الأمن العام ومنع الجرائم أو التحقيق فيها[١٥].

ويعني ذلك قبول اللائحة بوجود تشريعات وطنية تشتمل على أن تكون محل الحماية بيانات الأشخاص الاعتباريين، وهو ما اتجهت إليه محكمة العدل التابعة للاتحاد الأوروبي في قضية LAND NORDRHEIN-WESTFALEN V. D.H.T لسنة ٢٠٢٠م. بشأن التشريعات الوطنية التي توسع نطاق حماية البيانات الشخصية لتشمل الأشخاص الاعتباريين، على الرغم من أن المادة ٢٣ فقرة (١) من اللائحة العامة لحماية البيانات هدفها الأساسي ضمان تحيقيق توازن عادل بين احترام الحقوق الأساسية للأشخاص الطبيعيين المتأثرين بمعالجة البيانات الشخصية والحاجة إلى حماية المصالح المشروعة الأخرى في مجتمع ديمقراطي[١٦].

وكان ذلك بخصوص قضية إفلاس شركة J & S Service، عندما طلبت D.H.T من السلطات الضريبية تقديم معلومات عن الشركة المفلسة والكشف عن بيانات الحساب لجميع أنواع الضرائب والرسوم التي تديرها السلطات الضريبية، إلا أن السلطات الضريبية رفضت تقديم هذه البيانات، فرفعت D.H.T دعوى أمام المحكمة الإدارية بألمانيا، والتي أيدت الطلب المقدم في جوهره، فاستأنفت محكمة LAND NORDRHEIN-WESTFALEN الحكم الصادر من المحكمة الابتدائية، وانتهى حكم المحكمة بقبول تقديم معلومات عن الشركة المفلسة، ومعاملة السلطات الضريبية نفس المعاملة التي يخضع لها الدائنون والمدينون الطبيعيون في حالة مطالبات القانون المدني، بهدف تشجيع تحصيل الضرائب وحماية الإيرادات الضريبية، والتي تدخل ضمن حماية المصلحة العامة[١٧]. وهنا تظهر فكرة التوازن بين الاحترام الواجب للبيانات الشخصية والمصلحة العامة المتمثلة في فرض الضرائب.

رابعاً- اختلاف البيانات الشخصية عن البيانات السرية:

تختلف البيانات الشخصية عن البيانات السرية في مفهوم أغلب القوانين الجنائية، ومن أمثلة ذلك ما يتعلق بصحيفة الحالة الجنائية والتي تُعد من الأسرار لدى الإدارة

---

[١٥] راجع في ذلك المادة/ ٢٣ من لائحة الاتحاد الأوروبي.

[16] LAND NORDRHEIN-WESTFALEN V. D.H.T (10/12/2020). Court of Justice of the European Union (CJE). No: C-620/1 https://curia.europa.eu/juris/document/document.jsf?text=&docid=235346

[17] ibid.

(ISSN: 2537 - 0758)

المختصة بها بوزارة الداخلية. وكذلك الأمر بالنسبة لدخل الفرد والذي يعتبر من الأسرار لدى مأموري الضرائب ولايجوز الإفصاح عنه خارج نطاق الوظيفة. بناء على ذلك، فإن هؤلاء الأشخاص يسألون في حالة إفشاء هذه المعلومات، وهو ما تضمنه صراحة نص المادة ٣١٠ من قانون العقوبات المصري، والتي نصت على أن "كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم مودعاً إليه بمقتضى صناعته أو وظيفته سر خصوصي ائتمن عليه فأفشاه في غير الأحوال التي يلزمه القانون فيها بتبليغ ذلك يعاقب بالحبس مدة لا تزيد على ستة شهور أو بغرامة لا تتجاوز خمسمائة جنيه مصري ....."[١٨].

تلك البيانات الشخصية تستحق الحماية التي يقررها القانون لكفالة حرمة الحياة الخاصة. ومع ذلك؛ فإن هذه الفكرة تعتبر من الأفكار الحديثة بالنسبة للقواعد التقليدية في قانون العقوبات، هذا القانون لا يمد حمايته للحياة الخاصة إلاّ بالنظر إلى المكان الخاص الذي يرتبط بالحياة الخاصة للشخص[١٩]. لذا نصت المادة ٣٠٩ مكرراً عقوبات مصري، على عقاب من استرق السمع أو سجّل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون. وكذلك يعاقب بنفس العقوبة كل من التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص، فحرمة الحياة الخاصة مرتبطة وفقاً للمفهوم التقليدي بحرمة المكان الخاص. ومن هنا ظهر التجديد الذي ساهم في وجوده أنظمة البيانات المبرمجة.

وفي المقابل؛ خالفت المحكمة الأوروبية لحقوق الإنسان ذلك في قضية L.B. v. HUNGARY لسنة ٢٠٢١م، بشأن انتهاك الحق في احترام الحياة الخاصة بسبب نشر السلطات الضريبية في دولة المجر على بوابة الإنترنت معلومات تسمح بتحديد هوية شخص لم يف بالتزاماته الضريبية، وانتهت المحكمة في حكمها إلى أن النشر

---

[١٨] غنام محمد غنام، "**الحماية الجنائية لأسرار الأفراد لدى الموظف العام**"، دار النهضة العربية، مصر، ١٩٨٨م، ص ٤٢.

انظر كذلك:- محمد أحمد سلامة، "**الحق في محو البيانات الشخصية: دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية**". مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات- كلية الحقوق، المجلد ٣، العدد ٢، ص ٣٠.

[١٩] عمر الفاروق الحسيني، "**المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية**"، ١٩٩٥م، ص ٦٠.

المبرر على بوابة السلطات الضريبية على شبكة الإنترنت فيما يتعلق بالمعلومات التي تساعد في التعرف على هوية مقدم الطلب، بما فيها عنوان منزله بسبب عدم وفائه بالتزاماته الضريبية، لم تنتهك حق مقدم الطلب في احترام حياته الخاصة[٢٠].

ويبدو في رأي المحكمة أن النشر المتعلق بمخالفة القانون هو أمر مبرر إذا كان يخدم غاية عامة وكان متناسباً معها.

خامساً- مفهوم معالجة البيانات إلكترونياً (Electronic data processing):

تناولت المادة الأولى من نظام حماية البيانات الشخصية السعودي مفهوم المعالجة بأنها "أي عملية تجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف"[٢١]. وهو ما اتفق مع القانون المصري المعني بحماية البيانات الشخصية، غير أن القانون الأخير اقتصر في تعريفه للمعالجة على العمليات التي تتم معالجتها باستخدام أي وسيط من الوسائط الإلكترونية أو التقنية، وسواء أتمت المعالجة بشكل جزئي أم كلي، وهو ما يعني اقتصاره على البيانات المعالجة بشكل إلكتروني دون المعالجة يدوياً أو ورقياً.

ويتفق هذا التعريف مع ما قررته المادة ٢ من التوجيه الخاص بحماية البيانات في الفقرة (ب) بأن "معالجة البيانات الشخصية" هي أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية، سواء بالوسائل الآلية أم لا، مثل الجمع أو التسجيل أو التنظيم أو التخزين أو التكييف أو التغيير، الاسترجاع أو الاستشارة أو الاستخدام أو

---

(20) L.B. v. HUNGARY (12/1/2021). European Court of Human Rights. (Application no. 36345/16). https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-207132%22].

(٢١) كما حددت المادة الثالثة من قانون حماية البيانات الشخصية البريطاني لسنة ٢٠١٨م، المقصود بمعالجة البيانات بأنها "عملية أو أكثر ترد على بيان أو مجموعة من البيانات وتتمثل في: التجميع لهذه البيانات، التسجيل، التنظيم، الهيكلة، التخزين، الملاءمة، التغيير، الاستعادة، الاستشارة، الاستعمال، الكشف عنها بطريق النقل أو التوزيع أو إتاحة تلك البيانات بأي طريقة، الارتباط، التقييد، الحذف أو الاتلاف".

(ISSN: 2537 - 0758)

الكشف عن طريق الإرسال أو النشر أو الإتاحة أو المحاذاة أو الدمج أو الحجب أو المحو أو التدمير".

أما المعالجة اليدوية فيقصد بها وضع البيانات الشخصية في ملفات ورقية عادية، دون أن تتم معالجتها بوسائل تقنية ودون الاستعانة ببرامج آلية وإلكترونية[٢٢].

ولكن ما يخصنا في هذا الصدد هو المعالجة الإلكترونية للبيانات[٢٣]، والتي تشير إلى استخدام الوسائل الآلية لمعالجة البيانات، والتي تستخدم عادة بغرض حفظ أو جمع أو تنظيم أو تخزين كميات كبيرة من المعلومات المتشابهة، كما هو الحال في المعاملات المصرفية التي تطبق على حسابات العملاء في البنوك، والنظام الخاص بإصدار تذاكر في شركة حجز تذاكر طيران.

ويعد من قبيل المعالجة الإلكترونية، تلك البيانات المبرمجة التي يتم إدخالها إلى نظام الكمبيوتر وتسجيلها على دعامة مادية مثل الشريط الممغنط أو في داخل الجهاز نفسه، كما تشمل عملية البرمجة للمعلومات كل ما يتعلق بحفظ تلك البيانات في الذاكرة أو إعدادها وتنسيقها ونقلها إلى علم الغير communication[٢٤]. تطبيقاً لذلك قُضي في فرنسا بأن مجرد إدخال البيانات في الكمبيوتر لا يتحقق به وصف البيانات بأنها "مبرمجة"، إذا كان ذلك لا يعدو أن يكون كتابة لتلك البيانات وكان الغرض منها طبعها

---

[٢٢] مشار إليه: سامح عبدالواحد التهامي "**الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي**" القسم الأول. مجلس النشر العلمي، جامعة الكويت، كلية الحقوق. سنة ٢٠١١م، ص٤١٢.

(23) Frederick G. Bohme, "**100 Years of Data Processing: The Punchcard Century**" Volume 3, U.S. Department of Commerce, Bureau of the Census, Data User Services Division. 1991, p. 87.

(24) Gassin Raymond, "**La protection pénale des informations sur la personne en droit français contemportain**", in "Droit pénal contemporain", Mélanges en l'honneur d'André Vitu, éd. Cujas, 1989, p.237.

– وفقاً لتقارير مكتب الإحصاء في الولايات المتحدة الأمريكية، فقد بدأ استعمال مصطلح المعالجة التلقائية للبيانات عند استخدام هيرمان هوليريث لمعدات البطاقات المثقوبة لتعداد سكان الولايات المتحدة لعام ١٨٩٠م، حيث تمكن مكتب التعداد من إكمال جدولة معظم بيانات التعداد السكاني لعام ١٨٩٠ مستغرقاً من سنتين إلى ثلاث سنوات، مقارنة بالتعداد السكاني لعام ١٨٨٠م والذي تم يدوياً واستغرق من سبع إلى ثماني سنوات.

على ورق وليس الاحتفاظ بها في جهاز الكمبيوتر[٢٥]. وقد تعلق الأمر في هذه القضية ببيانات نُقلت من بعض ملفات المرضى وأراد الطبيب طباعتها على ورق لتسهيل تجميعها.

كما يعتبر إدخال بيانات على مواقع شبكة الإنترنت نوعاً من معالجة البيانات الذي يجعلها خاضعة لقوانين تنظيم تجميع ومعالجة البيانات الشخصية. ومع ذلك اتجهت بعض أحكام القضاء إلى اعتبار أن معالجة البيانات بوسائل تلقائية بالمعنى المقصود في توجيه حماية البيانات الشخصية في سياق الأنشطة الخيرية أو الدينية، لا يدخل ضمن نطاق الاستثناءات الواردة في التوجيه الأوروبي، مادام أنها لا تندرج ضمن فئة الأنشطة المتعلقة بالأمن العام أو كانت من فئة الأنشطة الشخصية البحتة ومن ثم فهو خارج نطاق التوجيه.

ودل على ذلك ما أقره الحكم الصادر في قضية Lindqvist لعام ٢٠٠٣م، وهي متطوعة في الكنيسة البروتستانية في دولة السويد، أنشأت على جهاز الكمبيوتر الخاص بها صفحات إنترنت ونشرت عليها بيانات شخصية تتعلق بعدد من الأشخاص الذين يعملون معها على أساس تطوعي، وتم الحكم عليها بغرامة مالية على أساس استخدامها لبيانات شخصية بالوسائل التلقائية دون تقديم إشعار كتابي مسبق إلى السلطة الرقابية على حماية البيانات المنقولة إلكترونياً، واعتبار أن ما ارتكبته من قبيل معالجة لبيانات حساسة. فقدمت تلك السيدة استئناف على قرار المحكمة، وصدر قرار محكمة الاستئناف بأن إجراء نقل بيانات على صفحة الإنترنت إلى أشخاص مختلفين وتحديد هويتهم بالاسم ومعلومات متعلقة بظروف عملهم وإن كان يشكل معالجة لبيانات شخصية بوسائل آلية بالمعنى المقصود في توجيه حماية البيانات، إلاّ أن المحكمة اعتبرت أن معالجة البيانات في سياق الأنشطة الخيرية أو الدينية لا يدخل ضمن نطاق البيانات المحمية بموجب التوجيه الأوروبي لحماية البيانات[٢٦].

وفي قرار صادر عن المحكمة العليا الأسبانية، اعتبرت أن نشاط محرك البحث المتمثل في العثور على المعلومات المنشورة أو الموضوعة على الإنترنت من قبل أطراف ثالثة، وفهرستها تلقائيًا، وتخزينها مؤقتًا، وأخيراً، إتاحتها لمستخدمي الإنترنت وفقًا

(25) Crim. 6 juill. 1994 cite par Jacques FRANCILLON, "Infractions relevant du droit de l'information et de la communication "Rev.sc. crim.1996, chronique de jurisprudence, p. 676.

(26) Judgment of 6 November 2003 (Grand Chamber), Lindqvist (C-101/01, EU:C:2003:596).

(ISSN: 2537 - 0758)

لترتيب تفضيلي معين يجب اعتبارها معالجة للبيانات الشخصية عندما تحتوي تلك المعلومات على بيانات شخصية. كما أشارت المحكمة إلى أن العمليات المشار إليها في التوجيه يجب تصنيفها على أنها معالجة حيث تتعلق حصريًا بمواد تم نشرها بالفعل بهذا الشكل في وسائل الإعلام. كما أن من شأن عدم التقيد العام بتطبيق التوجيه في مثل هذه الحالة أن يجرد التوجيه إلى حد كبير من تأثيره[٢٧].

كما تعرضت المحكمة الدستورية بجمهورية لاتفيا في عام ٢٠٢١م، وذلك في الطعن المقدم أمامها بخصوص قانون حركة المرور على الطرق، والذي يسمح بالوصول إلى ٢١ معلومة تتعلق بنقاط العقوبة المفروضة على سائقي المركبات المُدرجة في سجل للجمهور ويتم الكشف عنها من قبل دائرة الأحوال المدنية لأي شخص يطلب ذلك، دون أن يثبت هذا الشخص وجود مصلحة محددة للحصول على تلك المعلومات. وانتهت المحكمة إلى أن معالجة البيانات الشخصية المتعلقة بنقاط العقوبة تشكل "معالجة للبيانات الشخصية المتعلقة لالجرائم الجنائية وأحكام الإدانة" التي تنص اللائحة العامة لحماية البيانات (GDPR) فيما يتعلق بها على حماية معززة بسبب حساسية خاصة للبيانات المعنية. كما أن المعلومات المتعلقة بنقاط العقوبة هي بيانات شخصية وأن إفصاحها من قبل CSDD إلى أطراف ثالثة يشكل معالجة تندرج ضمن النطاق المادي للائحة العامة لحماية البيانات (GDPR). وهذه المعالجة غير مشمولة بالاستثناءات التي تطبقها اللائحة الأوروبية[٢٨].

سادساً: المقصود بمعالج البيانات الشخصية (Data processor):

يعرف معالج البيانات (جهة المعالجة) بأنه "أي جهة عامة، أو أي شخص طبيعي أو اعتباري مختص بطبيعة عمله بمعالجة البيانات الشخصية لصالحه أو لمصلحة المتحكم أو نيابة عنه"[٢٩]. وبالتالي قد تكون جهة المعالجة هي نفسها جهة التحكم، وقد تكون جهة منفصلة تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابة عنها.

---

(27) Judgment of 13 May 2014 (Grand Chamber), Google Spain and Google (C-131/12, EU:C:2014:317). Court of justice of the European union, "PROTECTION OF PERSONAL DATA". November 2021, p 15.

(28) Judgment of the Court (Grand Chamber) of 22 June 2021 (request for a preliminary ruling from the Satversmes tiesa– Latvia).(Case C-439/19). https://curia.europa.eu/juris/document/document.jsf?text=&docid=244575&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=8508699. Retrieved 30/8/2022.

[٢٩] المواد الأولى من النظام السعودي والقانون المصري لحماية البيانات الشخصية.

بناء على ذلك؛ يعد معالجاً للبيانات الشخصية كل شخص طبيعي أو اعتباري قام لصالحه أو لمصلحة المتحكم، بإجراء من الإجراءات التالية (التجميع، التسجيل، الحفظ، التنظيم، الاستخلاص، التعديل، الاطلاع، الاستخدام، النشر، المنع، التحديث، الدمج، الاسترجاع، الفهرسة، الترتيب، التنسيق، المحو والتدمير). فأي إجراء يتم اتخاذه من قبل الجهة المعالجة يتضمن أحد الأنشطة السابق ذكرها، تعد في نظر التشريعات الجنائية معالجة لهذه البيانات، لاسيما إذا ما تم ذلك باستخدام أي وسيط من الوسائط أو الوسائل الإلكترونية أو التقنية، وسواء أتم ذلك جزئياً أم كلياً.

ويعد من قبيل جهات المعالجة، الجهات القائمة بتجميع عناوين البريد الإلكتروني للعملاء بهدف إرسال رسائل دعائية، كذلك قيام جهة بحث علمي بتجميع بيانات عن الحالة الصحية لبعض المرضى النفسيين، بهدف إجراء أبحاث علمية.[٣٠] كما تعد جهة معالجة الشركات التي تقوم بإنشاء نظام لمراقبة أجهزة الحاسوب الخاصة بموظفي الشركة داخل مكان العمل، وشركات الطيران التي تحتفظ ببيانات المسافرين على خطوطها.

وقد أتيح للمحاكم فرصة بيان مفهوم معالج البيانات الشخصية، ومنها ما تضمنه الحكم الصادر من المحكمة الإقليمية العليا في "Düsseldorf" ألمانيا، في ٢٩ يوليو ٢٠١٩م في قضية شركة Fashion ID، وذلك فيما يتعلق بتضمين مكون إضافي اجتماعي على موقع ويب. حيث قامت شركة Fashion ID، وهي شركة ألمانية لبيع الملابس بالتجزئة عبر الإنترنت، بتضمين المكوّن الإضافي الاجتماعي "أعجبني" على موقع الويب الخاص بها من شبكة التواصل الاجتماعي Facebook. وكان تضمين المكون الإضافي قد مكّن Facebook Ireland من الحصول على البيانات الشخصية لزوار موقع Fashion ID على الويب، وذلك بغض النظر عما إذا كان الزائر على علم بهذه العملية أم لا، أو أنه عضو في شبكة التواصل الاجتماعي Facebook أو كونه قام بالنقر فوق الزر "أعجبني" على Facebook. وقد انتقدت منظمة Verbraucherzentrale NRW، – وهي جمعية خدمات عامة ألمانية مكلفة بحماية مصالح المستهلكين – شركة Fashion ID لإرسالها إلى Facebook Ireland بيانات

---

[٣٠] التهامي سامح عبد الواحد، "الحماية القانونية للبيانات الشخصية: دراسة القانون الفرنسي – القسم الأول" مجلة الحقوق، جامعة الكويت – مجلس النشر العلمي، المجلدة ٣٢، العدد ٣، سنة ٢٠١١م، ص ٤١١.

(ISSN: 2537 - 0758)

شخصية تخص زوار موقعها على الويب، وذلك لسببين: تمثل الأول في عدم موافقتهم، أما السبب الثاني في انتهاك للواجبات تجاه الإبلاغ المنصوص عليه في الأحكام المتعلقة بحماية البيانات الشخصية.[٣١]

وانتهت المحكمة أولاً؛ إلى أن مشغل موقع ويب مثل Fashion ID، يمكن اعتباره معالجاً بالمعنى المقصود في المادة ٢ (د) من التوجيه ٤٦/٩٥. ومع ذلك؛ يقتصر هذا الوضع على العملية أو مجموعة العمليات التي تنطوي على معالجة البيانات الشخصية التي تحدد بالفعل الأغراض والوسائل، أي الجمع والإفصاح عن طريق نقل البيانات المعنية.

على النقيض من ذلك؛ قررت المحكمة أنه يبدو من المستحيل أن تحدد شركة FashionID أغراض ووسائل العمليات اللاحقة التي تنطوي على معالجة البيانات الشخصية التي يقوم بها Facebook Ireland بعد إرسالها إلى الأخير، مما أدى إلى أن Fashion ID لا يمكن اعتباره مراقبًا فيما يتعلق بهذه العمليات بالمعنى المقصود في المادة/ ٢ (د).

علاوة على ذلك، أشارت المحكمة إلى أنه من الضروري أن يسعى كل من المشغل والمزود إلى تحقيق مصلحة مشروعة، بالمعنى المقصود في المادة ٧ (و) من التوجيه ٤٦/٩٥، من خلال عمليات المعالجة من أجل تبرير تلك العمليات فيما يتعلق بكل منهم.

سابعاً: **بيانات شخصية لا يجوز معالجتها**:

تضمنت أغلب التشريعات المعنية بحماية البيانات الشخصية النص صراحة على حظر معالجة نوع خاص من البيانات والتي أطلق عليها مصطلح "البيانات الحساسة"، وفي الأحوال الضرورية التي تتطلب معالجتها يستلزم أن يتم ذلك وفق شروط وقيود معينة.

ويعد من بين تلك البيانات، ما يتعلق البيانات الصحية ويعد من بينها (البيانات النفسية والعقلية والبدنية والجينية والوراثية)، والبيانات البيومترية "بيانات القياسات

(31) Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV. Court of Justice of the European Union: PRESS RELEASE No 99/19.. Judgment in Case C-40/17. Luxembourg, 29 July 2019. https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf.

الحيوية"، والبيانات المالية، والبيانات ذات الطبيعة الخاصة كالمتعلقة (بالأصل والدين والعرق والمعتقد الفكري والسياسي)، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو إحداهما، وبيانات الأطفال.

تلك البيانات أسدلت عليها التشريعات الجنائية –كما سنرى لاحقاً– حماية خاصة، نظراً لطبيعتها الحساسة والماسة بصفة أصيلة بخصوصية الأفراد. والتي تستلزم لها التشريعات حماية أكبر بالمقارنة بنظيراتها من البيانات الشخصية الأخرى. ويشترط لإجراء معالجة أي نوع من هذه البيانات عدد من الشروط على النحو التالي:–[٣٢]

- أن تكون البيانات محل المعالجة محددة ودقيقة ومحدثة.
- أن تكون كافية وذات صلة، ولا تتجاوز الغرض من المعالجة.
- ألا تتجاوز فترة الاحتفاظ بها المدد الزمنية المحددة قانوناً، باستثناء حالات الضرورة.
- موافقة صاحب البيانات على إجراء معالجته.

المطلب الثاني
الحق في الخصوصية وإعمال مبدأ التناسب

أولاً- مفهوم مبدأ التناسب:

يعرف مبدأ التناسب بأنه "آلية توازن بين المبادئ القانونية ذات القيمة المتساوية، والقابلة للتطبيق في وقت واحد، ولكنها متعارضة"[٣٣]. وعليه؛ فإن فالتناسب ضامن للحريات الفردية وللأهداف المشروعة الأخرى، والتي من بينها حماية المصالح العامة.

ترتيباً على ذلك، فإذا كان مبدأ التناسب يهدف إلى إعمال التوازن بين "وزن" الحق و"ثقل" الأسباب التي دعت المشرع إلى اتخاذ قرار بتقييد هذا الحق لتحقيق أهداف مشروعة، فهو يهدف إلى السعي من أجل التوفيق بين الحقوق وإعطاء أولوية لحق على حق آخر بحسب الأهداف المشروعة التي يسعى إليها الحق الأول[٣٤]. وهو ما ورد النص عليه في المواد من ٨ إلى ١١ من الاتفاقية الأوروبية لحقوق الإنسان، والتي

(32) European Court of Human Rights: (Drelon c. France - 3153/16 et 27758/18 Arrêt 8.9.2022 [Section V]). Septembre 2022.

(33) G. Xynopoulos, «Proportionnalité», in D. Alland et S. Rials (dir), Dictionnaire de la culture juridique, PUF, 2003, p. 1251.

(34) Al-Mahrouky Mayada.,"Hate Crimes and Freedom of Speech". International Review of law and Economics. Article submission No. 109069. ISSN: 01448188, Chicago- (USA),٢٠٢٣ .

(ISSN: 2537 - 0758)

تضمنت إمكانية الحد من ممارسة الحقوق التي تحميها عندما يشكل هذا التقييد "تدبيراً ضرورياً، في مجتمع ديمقراطي، لحماية أهداف معينة، بما في ذلك الأمن القومي، حفظ النظام، وحماية حقوق الآخرين وحرياتهم".

وهو ما انتهت إليه محكمة العدل التابعة للاتحاد الأوروبي في قضية Human Rights League V Council of Ministers لسنة ٢٠٢٢م. باعتبار أن نقل بيانات سجلات أسماء المسافرين ومعالجتها آلياً بشكل معمم، يتفقان مع الحقوق الأساسية في احترام الحياة الخاصة وحماية البيانات الشخصية في بلجيكا ولم يخالفه(٣٥).

وفي حكم آخر صادر عن المحكمة الأوروبية لحقوق الإنسان في قضية CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA في مارس ٢٠٢٢م، قضت بانتهاك المادة ١٠ من الاتفاقية الأوروبية لحقوق الإنسان، والمتعلقة بالحق في حرية التعبير. حيث تعلقت القضية بقرارات قضائية تأمر وسائل الإعلام بالكشف عن بيانات تسجيل المستخدمين الذين نشروا تعليقات على إحدى المواقع الإلكترونية ترتبط ببعض الشخصيات السياسية المتعلقة بالفساد، وكانت الشركة مقدمة الطلب قد سحبت تلك التعليقات بينما رفضت الكشف عن معلومات تتعلق بمؤلفيها. وعلى الرغم من اعتبار المحكمة أن بيانات المستخدمين لا تغطيها حماية المصادر الصحفية، ولا يوجد حق مطلق في عدم الكشف عن هويتهم على الإنترنت، غير أنها وجدت أن المحاكم الوطنية المذكورة لم توازن بين مصالح المدعين ومصالح الشركة الطالبة في الحفاظ على عدم الكشف عن هوية مستخدميه، بهدف تعزيز التبادل الحر للأفكار والمعلومات والمحمية بموجب المادة ١٠، بناء على ذلك قررت المحكمة أن هذه القرارات القضائية ليست ضرورية في مجتمع ديمقراطي(٣٦).

---

(35) Human Rights League V Council of Ministers, Case C-817/19. Court of Justice of the European Union (CJE). OPINION OF THE ADVOCATE GENERAL MR GIOVANNI PITRUZZELLA., 27 january 2022.

(36) CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA (07/03/2022). Application no. 39378/15. European Court of Human Rights, (Fourth Section).
https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-213914%22]}

ثانياً- إعمال مبدأ التناسب بين الحق في خصوصية البيانات الشخصية والحق في المعلومة:

لا تختلف التشريعات كافة في ضمان حق الشخص في الخصوصية، واعتبارها حق لصيق به له حرمة وقدسية– مع مراعاة أن مفهوم الخصوصية نسبي يختلف من مجتمع لآخر بحسب الثقافات المختلفة– بل وشرعت العديد من الدساتير والقوانين التي تضمنت النص صراحة على كفالته، وأفردت له الاتفاقيات والمواثيق الدولية نصوصاً تحميه من أي انتهاك أو تعدٍ.[٣٧] ولعل الحق في الخصوصية لا يشمل الفرد بذاته، بل يشمل كل ما يتعلق به، بما فيها بياناته الشخصية. ومع ظهور وسائل التقنية الحديثة وأنظمة الاتصال التي تستخدم لنقل البيانات على نطاق أوسع، كانت الحاجة إلى وضع قواعد قانونية تحكم وتنظم جمع ومعالجة تلك البيانات الخاصة[٣٨].

ولعل الحق في الخصوصية والحق في الحصول على المعلومة حقان دستوريان، ويؤكد ميثاق الحقوق الأساسية للاتحاد الأوروبي أنه يجب عندما يكون للتدابير التي تنطوي على التدخل في الحقوق الأساسية التي أرساها الميثاق مصدرها في قانون تشريعي للاتحاد الأوروبي، فإن الأمر متروك للهيئة التشريعية للاتحاد الأوروبي لتحديد العناصر الأساسية التي تحدد نطاق تلك التدخلات. لاسيما الأحكام التي تتطلب أو تسمح بنقل البيانات الشخصية للأشخاص الطبيعيين إلى طرف ثالث –مثل السلطة العامة– يجب أن تصنف، في غياب موافقة هؤلاء الأشخاص الطبيعيين وأياً كان

---

[٣٧] المادة ١٢ من الإعلان العالمي لحقوق الإنسان سنة ١٩٤٨م، المادة ١٧ العهد الدولي للحقوق السياسية والمدنية سنة ١٩٦٦م، المادة ٨ الاتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية سنة ١٩٥٠م. والمادة ٥٧ من الدستور المصري الصادر سنة ٢٠١٤م. والنظام الأساسي للحكم، المملكة العربية السعودية، الصادر بأمر ملكي رقم أ/٩٠ بتاريخ ١٤١٢/٨/٢٧هـ.

[٣٨] صدر أول تشريع لحماية البيانات عام ١٩٧٠م في ألمانيا، وسن أول قانون وطني لحماية البيانات الشخصية في السويد عام ١٩٧٣م، تبعته في ذلك الولايات المتحدة الأمريكية عام ١٩٧٤م، أما فرنسا فأصدرت قانون معالجة البيانات والملفات والحريات عام ١٩٧٨م. وتبعهم الكثير من الدول بعد ذلك.

- انظر: شريف يوسف حلمي خاطر، "**حماية الحق في الخصوصية المعلوماتية :دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا**"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة – كلية الحقوق، العدد ٥٧، سنة ٢٠١٥م.

(ISSN: 2537 - 0758)

الاستخدام اللاحق للبيانات المعنية، على أنها تدخل في حياتهم الخاصة وفي الحق الأساسي في حماية البيانات الشخصية. ولا يمكن تبرير هذا التدخل إلا إذا نص عليه القانون، واحترم جوهر تلك الحقوق، وكان ضرورياً امتثالاً لمبدأ التناسب، ويحقق بالفعل أهداف المصلحة العامة التي يعترف بها الاتحاد الأوروبي أو الحاجة إلى حماية حقوق الآخرين وحرياتهم(٣٩).

ومن قبيل التأكيد على ذلك؛ قرار مفوضي المعلومات والخصوصية على المستوى الاتحادي والإقليمي الصادر في ٢٠٢١م بشأن جائحة كرونا، والذي جاء فيه، أن تشريعات الخصوصية تنص على استثناءات للسماح بجمع هذه المعلومات واستخدامها والكشف عنها لأسباب تتعلق بالصحة العامة أثناء الجائحة وغيرها من الحالات الطارئة. ويجب ألا ينظر إلى هذه القوانين من قبل الخاضعين لها على أنها عقبة أمام جمع المعلومات واستخدامها والكشف عنها بصورة مشروعة ومناسبة. بل على العكس من ذلك؛ ينبغي النظر إلى قوانين الخصوصية وأفضل ممارساتها باعتبارها وسيلة لضمان الاستخدام المسؤول للبيانات والكشف عنها بما يدعم أهداف الصحة العامة ويعزز الثقة في نظام الرعاية الصحية(٤٠).

كما أكدت المحكمة الأوروبية لحقوق الإنسان في الكثير من أحكامها على ضرورة إعمال مبدأ التناسب بين الحقوق، وكان من بينها الحكم الصادر في قضية LIEBSCHER v. AUSTRIA لسنة ٢٠٢١م، بشأن الحكم بانتهاك الحق في احترام الحياة الخاصة؛ بسبب الالتزام بتقديم اتفاق الطلاق بأكمله إلى السجل العقاري حيث يكون متاحاً للجمهور، وأوضح أن الطلب الذي قدمته محكمة السجل العقاري لتقديم تسوية الطلاق الكاملة لا يتوافق مع قوانين حماية البيانات، حيث سيعني ذلك أن بياناته الشخصية مثل أسماء وأماكن إقامة أطفاله القصر وبيانات زوجته السابقة، ومقدار مدفوعات النفقة، واتفاقيات الحضانة ستكون متاحة للجمهور في أرشيف

(39) CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA, op.cit

(٤٠) الموقع الرسمي CNI "اللجنة الوطنية لحماية البيانات": استرجاع بتاريخ ٢٠٢٢/٥/٢٠م، https://www.cnil.fr/en

المستندات. وانتهت المحكمة إلى وجود انتهاك للمادة ٨ من الاتفاقية والخاصة باحترام الحياة الخاصة والأسرية(٤١).

فمن المستقر عليه أن الحقوق الأساسية في احترام الحياة الخاصة وحماية البيانات الشخصية ليست امتيازات مطلقة، بل يجب أن يؤخذ في الاعتبار ما يتعلق بوظيفتها في المجتمع، وأن تتوازن مع الحقوق الأساسية الأخرى. ومن ثم يجوز فرض قيود تحد من ممارسة تلك الحقوق، شريطة أن ينص القانون عليها، وأن تحترم جوهر الحقوق الأساسية ومبدأ التناسب. وبموجب المبدأ الأخير، لا يجوز فرض القيود إلا إذا كانت ضرورية وتفي حقاً بأهداف المصالح العامة المعترف بها أو الحاجة إلى حماية حقوق الآخرين وحرياتهم. كما يجب أن يتم تنفيذها في حدود ما هو ضروري للغاية، وأن يضع التشريع الذي ينطوي على التدخل قواعد واضحة ودقيقة تحكم نطاق وتطبيق التدبير المعني(٤٢).

ثالثاً- استثناءات ترد على الحق في الخصوصية (الحق في الاطلاع على بعض أنواع البيانات الشخصية):

على الرغم من الحماية التي تسدلها التشريعات والاتفاقيات الدولية للحق في الخصوصية، لاسيما خصوصية البيانات الشخصية، إلا أنه يسمح في بعض الأحيان بالاطلاع على تلك البيانات، متى توافرت ضرورة تستدعي ذلك خاصة، لاسيما إذا ماتعلقت هذه الضرورة بالمصلحة العامة والأمن القومي. ويعد من بين تلك الاستثناءات، والتي سوف نذكرها على سبيل المثال وليس الحصر:

(41) CASE OF LIEBSCHER v. AUSTRIA (06/07/2021). European Court of Human Rights, (Application, no. 5434/17). https://hudoc.echr.coe.int.

(42) Court of Justice of the European Union (CJEU). REQUEST for a preliminary ruling under Article 267 TFEU from the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia),Case C-439/19. 22 june 2021.
https://curia.europa.eu/juris/document/document.jsf?text=&docid=243244&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=65509.

(ISSN: 2537 - 0758)

١- البيانات الشخصية المتعلقة بمحاضر الضبط الجنائي والتحقيقات والبيانات المتوافرة لدى الأمن القومي:

تتناول التشريعات المقارنة ما يتعلق بتعريف بيانات أحكام الإدانة الجنائية، على أنها معلومات تتعلق بشخص "ارتكب جريمة، أو أدين من المحكمة في قضية جنائية، أو خضع لأحد التدابير الجنائية القسرية، كالاحتجاز أو حظر السفر، أو كان مشتبه في ارتكابه جريمة".

وقد تطلب ذلك عدم جواز معالجة بيانات الإدانة الجنائية إلا من جانب السلطات العامة فقط، ومع ذلك يجوز معالجة تلك البيانات عن طريق معالجي البيانات الآخرين، متى كانت تلك المعالجة ضرورية وامتثالاً لأحكام الأرشفة، أو لإنشاء مطالبات قانونية أو الدفاع عنها. وكذلك متى كانت المعالجة ضرورية للامتثال لالتزام قانوني بموجب نص في قانون أو لائحة. وفي جميع الأحوال لا يمكن السماح بمعالجة بيانات الإدانة الجنائية بناء على موافقة صاحب البيانات، كون هذا الأمر تخص السلطة العامة وحدها، فيما عدا بعض الاستثناءات المحددة بموجب القانون[٤٣].

يعني ذلك؛ جواز الاطلاع على البيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم أو التدابير الاحترازية المتصلة بها، شريطة ألا يتم ذلك إلا تحت رقابة السلطة العامة في الدولة. أو إذا كانت المعالجة مصرح بها بموجب قانون أو لائحة، على أن يشتمل هذا القانون على ضمانات مناسبة لحماية حقوق وحريات أصحاب البيانات. بل

---

[٤٣] وفقاً للقانون السويدي، توجد استثناءات تجيز معالجة بيانات الإدانة الجنائية لسلطات غير السلطة العامة، حيث تنطبق تلك الاستثناءات في الحالات الآتية:

- في حالة الضرورة امتثالاً للقوانين المطبقة على الخدمات الاجتماعية.
- في مجال رعاية بعض المنظمات التعليمية للطلاب.
- إذا كانت جزء من عمليات التحقق من نزاع يتم إجراؤه داخل مكاتب المحاماه أو الحالات القانونية المماثلة.
- الحالات المتعلقة بالأفراد في المناصب الرئيسية والقيادية المدرجة في تقارير نظام الإبلاغ عن المخالفات.

وفي جميع الأحوال السابقة، يتم تقديم طلب لمنح إذن المعالجة المحددة لبيانات الإدانة الجنائية المتعلقة بفحص الأفراد، مقابل قوائم عقوبات بعض الدول، مثل العقوبات التي تفرضها الولايات المتحدة الأمريكية.

ولا يجوز الاحتفاظ بملف كامل عن الإدانات الجنائية إلا تحت رقابة السلطة العامة أيضاً[٤٤].

وعلى الرغم من نص القانون المصري صراحة، على عدم تطبيق أحكام قانون حماية البيانات الشخصية على البيانات المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية، وكذلك البيانات الشخصية المتوافرة لدى جهات الأمن القومي[٤٥]. إلا أنه أجاز لاعتبارات يقدرها مركز حماية البيانات الشخصية بناء على طلب جهات الأمن القومي، إخطار جهة المعالجة بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، وذلك خلال مدة زمنية محددة، وعلى جهة المعالجة الالتزام بما ورد بالإخطار خلال المدة المحددة.

وقد أيدت المحكمة الأوروبية لحقوق الإنسان ذلك، في قضية Uzun v. Germany بقرارها بعدم انتهاك نص المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان، فيما يتعلق بطلب الطاعن – والمشتبه في ضلوعه في عمليات إرهابية– بانتهاك حرمة حياته الخاصة، بقيام السلطات العامة بمراقبته، وذلك عن طريق استخدام جهاز تحديد المواقع GPS واستخدام البيانات التي يتم الحصول عليها عبر هذه الجهاز في الإجراءات الجنائية المقامة ضده، كون ذلك يمثل انتهاكاً لحقه في الخصوصية. فقد قضت المحكمة بأن معالجة واستخدام البيانات التي تتم معالجتها في هذه الحالة، إنما

---

[٤٤] راجع في ذلك المادة ١٠ من اللائحة الأوروبية، ونص المادة ٣ من قانون حماية البيانات الشخصية المصري

-Article 10 - Processing of personal data relating to criminal convictions and offences: The processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) may be carried out only under the control of public authority, or if the processing is authorised by Union or Member State law which provides for appropriate safeguards for the rights and freedoms of data subjects. Any complete register of criminal convictions may be kept only under the control of public authority.

[٤٥] راجع الفقرة ٥ من نص المادة ٢ من قانون حماية البيانات الشخصية المصري.

– جهات الأمن القومي يعني بها رئاسة الجمهورية ووزارة الدفاع ووزارة الداخلية وجهاز المخابرات العامة وهيئة الرقابة الإدارية المصرية.

(ISSN: 2537 - 0758)

يهدف إلى تحقيق المصلحة العامة المتمثلة في حماية الأمن القومي وحماية الجمهور، وكان هذا التدبير ضرورياً في مجتمع ديمقراطي(٤٦).

على النقيض من ذلك؛ انتهت المحكمة الأوروبية في قضية S. and Marper v. the United Kingdom إلى حدوث انتهاك للمادة ٨ من الاتفاقية، فيما يتعلق بالاحتفاظ في قاعدة بيانات ببصمات الأصابع وملفات الحمض النووي لأشخاص مشبته بهم ولكنهم غير مدانيين، واعتبرت المحكمة أن ذلك يمثل تدخلاً في احترام الحياة الخاصة، ولا يمكن اعتباره ضرورياً في مجتمع ديمقراطي. وأكدت المحكمة أنه وإن كان من الضروري استخدام تقنيات العلم الحديث في نظام العدالة الجنائية، إلا أن ذلك يتطلب الموازنة الدقيقة بين المزايا المحتملة لاستخدام مثل هذه التقنيات والحق في الخصوصية، حيث لم تحقق السلطات في هذه القضية توازناً عادلاً بين المصالح العامة والمصالح الخاصة(٤٧).

٢- البيانات الشخصية المعالجة حصراً للأغراض الإعلامية، أو أغراض البحث العلمي أو التاريخي:

تضمنت التشريعات المعنية بحماية البيانات الشخصية، إمكانية معالجة البيانات الشخصية حصراً للأغراض الإعلامية، شريطة أن تكون صحيحة ودقيقة، وألا يتم استخدامها في أغراض أخرى، ودون الإخلال بالتشريعات المنظمة للصحافة والإعلام(٤٨).

---

(46) European Court of Human Rights: Uzun v. Germany, 02.09.2010. (application no. 35623/05). https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-3241790-3612154%22]}. Also:

- Kennedy v. the United Kingdom, 18.05.2010. (application no. 26839/05)
- Privacy International and Others v. the United Kingdom, 4 September 2020. (Application no. 46259/16)
- Ben Faiza v. France, 08.02.2018. (application no. 31446/12).

(47) European Court of Human Rights : S. And Marper v. the United Kingdom, 4 December 2008 (Grand Chamber). https://hudoc.echr.coe.int/eng-press?i=003-2571936-2784147

(٤٨) الفقرة الثالثة من المادة ٣ من قانون حماية البيانات الشخصية المصري.

- للمزيد انظر: رزق سعد، "**الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في ضوء القانون رقم ١٥١ لسنة ٢٠٢٠م**". ورقة بحثية مقدمة للمؤتمر العلمي الدولي الأول لكلية الحقوق

واشترطت اللائحة الأوروبية لضمان لحماية تلك البيانات، ضرورة التوفيق بين الحق في حماية البيانات الشخصية والحق في حرية التعبير والمعلومة، بما ذلك المعالجة التي تتم لأغراض صحفية أو أغراض التعبير الفني أو الأدبي(٤٩). كما يجب أن تتوافق معالجة البيانات الشخصية للأغراض العلمية أيضًا مع التشريعات الأخرى ذات الصلة مثل التجارب السريرية.

إلا أن المحكمة الدستورية النمساوية قضت بعدم دستورية المادة ٨٥/أ من اللائحة الأوروبية، والتي تسمح للدول الأعضاء بتطبيق استثناءات على قواعد اللائحة العامة لحماية البيانات، والتي من بينها عدم خضوع معالجة البيانات الشخصية بواسطة وسائل الإعلام وموظفوا الشركات الإعلامية بما يعرف "بالإعفاء الصحفي" لشرط موافقة صاحب البيانات، كون ذلك يمثل انتهاكاً للحق في حماية البيانات الشخصية، وعدم تحقيق التوازن بين الحق في حرية التعبير والحق في حماية البيانات(٥٠).

يستفاد مما سبق أن معالجة البيانات الشخصية التي تتم لأغراض إعلامية، يجب أن تتم بشكل حصري، ولا يجوز أن تنسحب تلك المعالجة لخدمة أغراض أخرى غير تلك المحددة في القانون، وأن يتم ذلك وفق الشروط والضمانات المعنية المحددة لأصحاب البيانات، لتمكينهم من ممارسة حقوقهم إذا كان ذلك مناسبًا، وفي ضوء الأغراض التي تسعى إليها المعالجة المحددة إلى جانب التدابير الفنية والتنظيمية التي تهدف إلى تقليل معالجة البيانات الشخصية وفقًا لمبدأي التناسب والضرورة.

جامعة مدينة السادات بعنوان "**الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي "رؤية مصر ٢٠٣٠– في المجال الصحي**". عدد خاص بالمؤتمر.

(49) Article 85 - Treatment and freedom of expression and information:
"Member States shall, by law, reconcile the right to the protection of personal data under this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and for the purposes of academic, artistic or literary expression".

(50) Austrian Constitutional Court (Verfassungsgerichtshof - VfGH). 14. Dec.2022, (G 287/2022-16, G 288/2022-14). https://gdprhub.eu/index.php?title=VfGH_-_G_287/2022-16,_G_288/2022-14 .

(ISSN: 2537 - 0758)

٣- البيانات الشخصية المعالجة بغرض الحصول على البيانات الإحصائية الرسمية أو بغرض الأرشفة للمصلحة العامة:

صرح القانون المصري بعدم خضوع البيانات الشخصية المعالجة بغرض الحصول على البيانات الإحصائية الرسمية لأحكام قانون البيانات الشخصية، وهذا يعني شرعية الحق في الاطلاع عليها.

غير أنه يجب أن تخضع المعالجة لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو للأغراض الإحصائية، للضمانات التي تتناسب وحقوق وحريات صاحب البيانات. على أن تشتمل هذه الضمانات تنفيذ التدابير الفنية والتنظيمية، وذلك لضمان الامتثال لمبدأ تقليل الاطلاع على البيانات. ويمكن أن تشتمل هذه التدابير على استخدام أسماء مستعارة، بالقدر الذي يحمي حقوق صاحب البيانات.

تطبيقاً لذلك قضت المحكمة الأوروبية لحقوق الإنسان في قضية And others Glavna direktsia za borba s في يناير ٢٠٢٣م، بأن معالجة البيانات البيومترية والجينية من قبل سلطات الشرطة بهدف تحقيق أغراض الأرشفة للمصلحة العامة فيما يتعلق بمكافحة الجريمة والحفاظ على القانون والنظام، وبشأن حرية نقل هذه البيانات. مصرح به بموجب المادة ١٠/ أ من اللائحة الأوروبية لحماية البيانات، والمواد ٤٧ و٤٨ من ميثاق الحقوق الأساسية للاتحاد الأوروبي. ويستبعد أي تشريع يسمح بشكل منتظم على جمع البيانات البيومترية لأي شخص كان قد اتهم بارتكاب جريمة، دون وجود رقابة من السلطة المختصة بالتحقق مما إذا كان جمع تلك البيانات ضرورياً للغاية التي جمع من أجلها، وإثبات ذلك يتم من خلال التحقق من أن الهدف المحدد يتعلق بالمصلحة العامة. كما أنه يجب التأكد من أن تحقيق هذا الهدف، يتم من خلال اتخاذ تدابير أقل خطورة في حال المساس بحقوق وحريات الأشخاص"[٥١].

(51) European Court of Human Rights: JUDGMENT OF THE COURT (Fifth Chamber). Ministerstvo na vatreshnite raboti ،Glavna direktsia za borba s Organiziranata prestapnost. 26 January 2023. (C-205/21). https://curia.europa.eu/juris/document/document.jsf?text=&docid=269704&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1

المبحث الثاني
القواعد العامة في تجميع ومعالجة البيانات الشخصية للأفراد

تمهيد وتقسيم:-

الثابت أنه كلما تدفقت كمية البيانات المخزنة والمعالجة، ازدادت أهمية حمايتها. وترجع أهمية تلك الحماية للأشخاص أصحاب تلك البيانات، كما ترجع أيضاً إلى المؤسسات القائمة على المعالجة من أوجه الأنشطة غير المشروعة والاحتيالية التي يمكن أن تقع عليها- كالدخول غير المشروع على أنظمة المؤسسة والتصيد والاحتيال- ومن ثم كان لابد من توافر معايير فعّالة لضمان أمن وسلامة تلك البيانات من التهديدات التي يمكن أن تتعرض لها في ظل ظروف مختلفة.

ترتيباً على ما تقدم؛ تبنت أغلب التشريعات الجنائية المختلفة، وضع قوانين خاصة لحماية البيانات، بموجبها يعطى الحق للأفراد في ممارسة حقوقهم على بياناتهم، مع إلزام المؤسسات -سواء ذات الطابع العام أو الخاص- التي تعالج تلك البيانات باحترام حقوق هؤلاء الأشخاص على بياناتهم وحمايتها. وهو ما سنتناوله من خلال المطالب الآتية:-

المطلب الأول: القواعد العامة في تجميع البيانات الشخصية المعالجة إلكترونياً.

المطلب الثاني: ضوابط مشروعية معالجة البيانات الشخصية إلكترونياً.

المطلب الأول
القواعد العامة في تجميع البيانات الشخصية المعالجة إلكترونياً

نظرا لأن هذا المطلب يتطلب نوعاً من التعمق، ومناقشة العديد من الإشكاليات، وعدم الوقوع في خلط بين الالتزامات التي تقع على عاتق جهة المعالجة نحو البيانات الشخصية نفسها، وبين التزاماتها في تمكين صاحب البيانات من ممارسة حقوقه على بياناته. فسوف يتم عرضه وبيانه في فرعين مستقلين. يتناول **الفرع الأول:** التزامات جهة المعالجة نحو البيانات الشخصية. أما **الفرع الثاني** فيتناول: حقوق صاحب البيانات المعالجة على بياناته.

الفرع الأول
التزامات جهة المعالجة نحو البيانات الشخصية

أولاً: ضمان المعالجة العادلة الشفافة:

اعتنقت أغلب التشريعات المقارنة ما يعرف بمبدأ "الشرعية والإنصاف والشفافية" في مجال حماية البيانات الشخصية. والذي يُعنى بألا تتم معالجة البيانات الشخصية إلا

(ISSN: 2537 - 0758)

بناء على اتباع أسس وأساليب تتسم بالشفافية، دون استخدام طرق احتيالية أو أساليب غير واضحة وغير صريحة للحصول على موافقة صاحب البيانات دون علمه الواضح بما سيجرى على بياناته.

ولعل من أبرز النصوص الصريحة على ذلك، ما تضمنته الفقرة الثانية من المادة ١٥ من القسم الثاني للائحة الأوروبية، والتي نصت على أنه:

"بالإضافة إلى المعلومات المشار إليها في الفقرة الأولى، فيجب على وحدة التحكم، في وقت الحصول على البيانات الشخصية، تزويد صاحب البيانات بالمعلومات الإضافية التالية والضرورية لضمان المعالجة العادلة والشفافة":

(أ) الفترة التي سيتم فيها تخزين البيانات الشخصية أو –إذا تعذر ذلك– المعايير المستخدمة لتحديد تلك الفترة.

(ب) أن لصاحب البيانات الشخصية الحق في أن يطلب من وحدة التحكم الوصول إلى بياناته أو تصحيحها أو محوها، أو تقييد المعالجة المتعلقة بها، أو الحق في الاعتراض على المعالجة والحق في إمكانية نقل البيانات.

(ج) الاعتراف بحقه في سحب الموافقة على معالجة البيانات في أي وقت، دون التأثير على قانونية المعالجة القائمة على الموافقة قبل سحبها.

(د) الحق في تقديم شكوى إلى سلطة الإشرافية على حماية البيانات.

(هـ) تقديم معلومات عما إذا كان شرط تقديم البيانات الشخصية ذا طبيعة تنظيمية أو تعاقدية أو كشرط لإبرام عقد، وما إذا كان صاحب البيانات ملزماً بتقديم البيانات الشخصية، وكذلك عن العواقب المحتملة لعدم تقديم تلك البيانات.

(و) وجود عملية صنع قرار آلية، بما في ذلك عملية التنميط[٥٢]، فضلاً عن أهمية هذه المعالجة والعواقب المترتبة عليها بالنسبة لصاحب البيانات.

أما عن قانون حماية البيانات البريطاني لسنة ٢٠١٨م، فقد تضمنت الفقرة الأولى من المادة ٥ منه، ما أكدت عليه اللائحة الأوروبية لحماية البيانات، من وجوب أن تتم

---

[٥٢] التنميط هو: "أي شكل من أشكال المعالجة الآلية للبيانات الشخصية، والتي تستخدم لتقييم جوانب شخصية معينة تتعلق بشخص طبيعي، خاصة ما يتعلق بتحليل أو التنبؤ بالجوانب المتعلقة بأداء ذلك الشخص الطبيعي في العمل، والوضع الاقتصادي والصحة، والتفضيلات الشخصية، والمصالح والسلوك وموقعه وتحركاته". راجع في ذلك نص المادة ٢ الفقرة ٤ من اللائحة الأوروبية لحماية البيانات.

معالجة البيانات بشكل قانوني وعادل وشفاف، وهو ما أُطلق عليه مبدأ "الشرعية والانصاف والشفافية"[٥٣]. والذي من خلاله يتم تحديد أسباب محددة للمعالجة (الأساس القانوني للمعالجة).

ويعد من بين أمثلة المعالجة غير القانونية في التشريع البريطاني، ما يتعلق بخرق واجب الثقة، أو حالات تجاوز جهة المعالجة السلطات القانونية، أو ممارسة سلطاتها بشكل غير صحيح، كذلك حالات التعدي على حقوق المؤلف، أو مخالفة اتفاق تعاقدي واجب النفاذ، أو فيما يتعلق بمخالفة التشريعات أو اللوائح الخاصة بحقوق النشر والصناعة.

ثانياً: أن تتم المعالجة بشكل يضمن أمن وسلامة البيانات (تأمين وسرية البيانات):

يعرف أمن البيانات بأنه "عبارة عن إجراءات وعمليات تقنية وتنظيمية من شأنها الحفاظ على خصوصية البيانات الشخصية وسريتها وسلامتها ووحدتها وتكاملها فيما بينها"[٥٤].

وقد عُنيت تشريعات حماية البيانات الشخصية بفرض التزام على جهة المعالجة، يتضمن إجراء المعالجة للبيانات بشكل يضمن سلامتها وأمنها. ومن بينها قانون حماية البيانات الشخصية البريطاني، حيث أشارت المادة ٦٦ منه إلى أنه يقع على الجهة القائمة بتجميع ومعالجة البيانات الشخصية أن توفر من الوسائل الفنية ما يكفل أمن تلك البيانات، بما يحول دون أن اطلاع الغير غير المسموح له بالاطلاع عليها أو العبث بها أو إجراء تعديلات عليها دون وجه حق. ومن أجل ذلك يتعين عليه أن يستعمل أنظمة دقيقة توفر ذلك. كما يقع عليه واجب تدوين ما يطرأ عليها من تعديلات[٥٥].

---

(53) "1. Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness, transparency')".

(٥٤) المادة الأولى، قانون حماية البيانات الشخصية المصري.

(55) UK Public General Acts 2018: PART 3 CHAPTER 4 Obligations relating to security Section 66.

(ISSN: 2537 - 0758)

وتضمن القسم الثاني من اللائحة الأوروبية لحماية البيانات في المادة ٣٢ منها على أنه يجب على المعالج تنفيذ الالتزام بالتدابير الفنية والتنظيمية المناسبة، لضمان مستوى من الأمن يناسب المخاطر التي يمكن أن تتعرض لها البيانات بما في ذلك[٥٦]:

(أ) الأسماء المستعارة وتشفير البيانات الشخصية.

(ب) وسائل لضمان استمرار سرية نظم وخدمات التجهيز وسلامتها وتوافرها ومرونتها.

(ج) القدرة على استعادة البيانات الشخصية والوصول إليها في الوقت المناسب في حالة وقوع حادث مادي أو تقني.

(د) تحليل وتقييم فعالية التدابير التقنية والتنظيمية بانتظام لضمان أمن المعالجة.

يُضاف إلى ذلك؛ أوجبت اللائحة الأوروبية أنه يلزم عند تقييم المستوى المناسب من الأمان، يجب مراعاة المخاطر التي تشكلها المعالجة بشكل خاص، والتي تنتج على وجه الخصوص عن تدمير البيانات الشخصية المنقولة أو المخزنة أو المعالجة أو فقدانها أو

---

(56) CHAPTER IV- Controller and processor: Section 2- Security of personal data. Article 32- Security of processing:

1- Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, inter alia, as appropriate:

(a) pseudonymisation and encryption of personal data;

(b) means to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services;

(c) means to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident;

(d) A procedure for regularly testing, analyzing and evaluating the effectiveness of technical and organizational measures to ensure the security of processing.

2- When assessing the appropriate level of security, particular account shall be taken of the risks posed by the processing, resulting in particular from the destruction, loss, alteration, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise processed, accidentally or unlawfully.

4-The controller and the processor shall take measures to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them, except on instructions from the controller, unless obliged to do so by Union or Member State law.

تغييرها أو الكشف غير المصرح به عنها أو الوصول غير المصرح به إليها، عن طريق الخطأ أو بشكل غير قانوني. كما أوجبت على وحدة التحكم والمعالج اتخاذ تدابير لضمان عدم قيام أي شخص طبيعي يتصرف تحت سلطة وحدة التحكم أو المعالج الذي لديه حق الوصول إلى البيانات الشخصية بمعالجتها، إلا بناء على تعليمات من وحدة التحكم، ما لم يكن ملزماً بذلك بموجب قانون الاتحاد أو الدولة العضو[٥٧].

ترتيباً على ذلك؛ فرضت اللجنة الوطنية لحماية البيانات CNIL في ٣٠ نوفمبر ٢٠٢٢م غرامة مالية قدرها ٣٠٠,٠٠٠ يورو ضد شركة FREE؛ بسبب عدم احترامها لحقوق الأفراد وأمن بيانات مستخدميها، بأن تم خرق الالتزام بضمان أمن البيانات الشخصية (وفقاً للمادة ٣٢ من اللائحة العامة لحماية البيانات)، حيث إنه[٥٨]:

أولاً: كانت كلمة المرور التي تم إنشاؤها عند إنشاء حساب مستخدم على موقع الشركة على الويب أو أثناء إجراء الاسترداد أو عند تجديد كلمة المرور غير قوية بما فيه الكفاية.

ثانياً: تم تخزين جميع كلمات المرور التي تم إنشاؤها عند إنشاء حساب مستخدم على موقع الشركة على الويب، بنص عادي في قاعدة بيانات المشتركين الخاصة بالشركة.

ثالثاً: تم إرسال كلمات مرور المستخدمين من قبل الشركة عن طريق البريد الإلكتروني أو البريد العادي، إلى المستخدمين عند إنشاء حساباتهم على الموقع، دون أن تكون كلمات المرور هذه مؤقتة وأن الشركة تطلب تغييرها. وبالمثل، تم إرسال كلمة المرور المرتبطة بحساب البريد الإلكتروني "free.fr" من قبل الشركة عن طريق البريد الإلكتروني أو البريد العادي إلى المستخدم والمشار إليها بنص عادي في نص الرسالة.

رابعاً: لم تمنع التدابير الفنية والتنظيمية لعملية التجديد حوالي ٤١٠٠ صندوق مجاني يحتفظ به المشتركون السابقون من إعادة تخصيصها لعملاء جدد، دون حذف بيانات هؤلاء المشتركين السابقين المخزنة هناك بشكل صحيح. هذه البيانات قد تكون صوراً أو مقاطع فيديو منزلية أو تسجيل برامج تلفزيونية.

---

(57) ibid.

(58) Délibération de la formation restreinte n°SAN-2022-022 du 30 novembre 2022 concernant la société FREE. Délibération SAN-2022-022 du 30 novembre 2022 - Légifrance (legifrance.gouv.fr) Revised 8 Jan 2023.

(ISSN: 2537 - 0758)

وفي حكم صادر عن محكمة العدل التابعة للاتحاد الأوروبي في قضية Human Rights League V Council of Ministers لسنة ٢٠٢٢م، أقرت بأن نقل بيانات سجلات أسماء المسافرين ومعالجتها آلياً بشكل معمم وعشوائي، يتفقان مع الحقوق الأساسية في احترام الحياة الخاصة وحماية البيانات الشخصية؛ ذلك أن إجراءات نقلها كانت كافية وغير مفرطة، وراعت الأهداف التي يسعى إليها التوجيه الأوروبي، وأن نطاقها لا يتجاوز ما هو ضروري للغاية لتحقيق تلك الأهداف. وعلاوة على ذلك، رأت المحكمة أن ذلك النقل محاط بضمانات كافية ترمي إلى ضمان عدم نقل سوى البيانات المشار إليها صراحة، وضمان أمن وسرية البيانات المنقولة[٥٩].

- **ولكن التساؤل الذي يطرح نفسه الأن، ماذا عن حالة استخدام كل من تقنية إخفاء الهوية وتقنية الاسم المستعار في معالجة البيانات الشخصية؟**

تثير معالجة البيانات باستخدام كل من تقنية إخفاء الهوية وتقنية الاسم المستعار إشكاليات عديدة من بينها؛ هل تطبيق مثل هذه التقنيات يخفف من المخاطر التي قد تلحق بالبيانات الشخصية أثناء المعالجة، وهل يمكن باستخدام هذه التقنيات الامتثال لقوانين حماية البيانات فيما يتعلق بالالتزام بالسرية وتأمين البيانات؟

عرفت اللائحة الأوروبية الاسم المستعار في الفقرة ٣ من المادة ٤ بأنه "معالجة البيانات الشخصية بطريقة لا يمكن أن تُعزى البيانات إلى صاحب بيانات معين دون استخدام معلومات إضافية، طالما يتم الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل، وتخضع للتقنية والتدابير التنظيمية لضمان عدم الإسناد إلى فرد محدد أو يمكن التعرف عليه"[٦٠].

ويعني ذلك أن استخدام تقنية الاسم المستعار تعني أن تتم معالجة البيانات الشخصية بطريقة لا يمكن نسبتها إلى صاحب بيانات معين، دون استخدام معلومات

---

(59) Human Rights League V Council of Ministers, Case C-817/19. Court of Justice of the European Union (CJE). OPINION OF THE ADVOCATE GENERAL MR GIOVANNI PITRUZZELLA., 27 january 2022. https://curia.europa.eu/juris/document/document.jsf?text=&docid=252841.

(60) GDPR. (Article 4(3b)) :"the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution to an identified or identifiable individual".

إضافية، بشرط أن يتم الاحتفاظ بهذه المعلومات الإضافية بشكل منفصل، وتخضع لتدابير تقنية وتنظيمية، وذلك لضمان عدم نسبة هذه البيانات لشخص طبيعي محدد أو يمكن التعرف عليه.

وهو ما يعني أيضاً أن البيانات الشخصية التي تخضع لأسماء مستعارة، والتي يمكن أن تُنسب إلى شخص طبيعي من خلال استخدام معلومات إضافية، يجب اعتبارها معلومات عن شخص طبيعي يمكن التعرف عليه. ومن ثم يمكن خضوعها ضمن نطاق اللائحة العامة لحماية البيانات.

أما إخفاء الهوية فهي عملية إزالة المعرفات الشخصية– المباشرة وغير المباشرة–[٦١] والتي قد تؤدي إلى تحديد هوية الفرد. تلك المعلومات لا تتعلق بشخص طبيعي محدد أو قابل للتحديد، أو بالبيانات الشخصية التي تم جعلها مجهولة بطريقة تجعل صاحب البيانات غير قابل للتحديد أو لم يعد قابلاً للتحديد.

يقصد من ذلك، أنه بمجرد أن تصبح البيانات مجهولة الهوية، ولم يعد الأفراد قابلين للتحديد، فلن تندرج البيانات ضمن نطاق اللائحة العامة لحماية البيانات (GDPR) وتصبح أسهل في الاستخدام[٦٢].

وتظهر أهمية هذه الوسائل في حماية البيانات الشخصية من مخاطر العبث بالبيانات وإساءة استخدامها، بمنع الوصول غير المشروع إليها، كون ذلك يحقق تنظيم استخدام تكنولوجيا تشفير المعلومات التي يتم نقلها عبر وسائل المعالجة الإلكترونية، بحيث لا يمكن قراءتها أو فهمها إلا من قبل القائمين على المعالجة. كما قد تضمن تلك الوسائل ضمان نقل البيانات لطرف ثالث دون أن يستطع التعديل عليها أو إعادة نقلها مرة أخرى[٦٣]، وهو ما أباحته اللائحة الأوروبية.

---

[٦١] ويتم التعرف على الفرد مباشرة من اسمه أو عنوانه أو رمزه البريدي أو رقم هاتفه أو صورته أو صورته أو بعض السمات الشخصية الفريدة الأخرى. كما يمكن التعرف على الفرد بشكل غير مباشر عندما يتم ربط معلومات معينة مع مصادر أخرى للمعلومات مثل مكان العمل، والمسمى الوظيفي، والراتب، والرمز البريدي أو حتى حقيقة أن لديهم تشخيصًا أو حالة معينة.

[62] The UK Anonymisation Network (UKAN): https://ukanon.net/.Retrieved 12/12/2022.

[٦٣] محسن عبد الحميد البيه "**الإثبات الجنائي في المواد المدنية والتجارية، وفقاً لقانون الإثبات وقانون التوقيع الإلكتروني**"، بدون دار نشر، طبعة ٢٠٠٧، ص ٢١٥.

(ISSN: 2537 - 0758)

ثالثًا- الالتزام بالإخطار بأي انتهاك قد يحدث للبيانات الشخصية[٦٤]:

يتعلق هذا الالتزام في حالات تصحيح البيانات أو محوها أو خرقها، فيجب إبلاغ صاحبها بأي انتهاك قد يحدث لها. خاصة وأنه في حال اختراق البيانات الشخصية فقد يؤدي ذلك إلى وجود مخاطر تهدد حقوق وحريات الأشخاص أصحاب تلك البيانات. لذلك؛ يجب إبلاغ صاحب البيانات بهذا الخرق بلغة واضحة وصريحة- وفقاً لما تضمنته اللائحة الأوروبية لحماية البيانات- خاصة ما يتعلق بما يلي[٦٥]:

- وصف طبيعة اختراق البيانات الشخصية إن أمكن ذلك.
- نقل اسم وتفاصيل الاتصال بمسؤول حماية البيانات، للحصول على المزيد من المعلومات حول طبيعة الاعتداء على البيانات.
- وصف العواقب المحتملة التي قد تترتب على خرق البيانات أو الاعتداء عليها.
- وصف التدابير المتخذة أو المقترح اتخاذها من قبل المراقب لمعالجة البيانات الشخصية. بما في ذلك تدابير التخفيف من أثاره السلبية المحتملة.

ومع ذلك أجازت اللائحة الأوروبية جواز عدم الإخطار، إذا استوفت جهة التحكم أو المعالجة أحد الشروط التالية[٦٦]:

أولاً: إذا اتخذت جهة التحكم تدابير الحماية التقنية والمناسبة، وتم تطبيق تلك التدابير على البيانات الشخصية المتأثرة بانتهاك البيانات الشخصية، خاصة ما يجعل

- انظر كذلك: شول بن شهرة، "**برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الإلكترونية**". المركز الجامعي غرداية، بدون سنة نشر.

(64) Regulation (EU) of the European) Article 19:" Notification obligation regarding rectification or erasure of personal data or restriction of processing":

The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

(65) Regulation (EU) of the European. (Article 33) "Notification of a personal data breach (3)".

(66) Regulation (EU) of the European. (Article 34): "Communication of a personal data breach to the data subject".

تلك البيانات غير مفهومة لأي شخص لم يكن مصرح له بالوصول إليها، مثل استخدام تقنية تشفير البيانات.

ثانياً: أن وحدة التحكم قد اتخذت تدابير لاحقة تضمن من خلالها، أنه لم يعد من المحتمل وقوع مخاطر عالية تمس حقوق وحريات صاحب البيانات.

ثالثاً: إذا تطلب إبلاغ صاحب البيانات بخرق بياناته جهد غير متناسب.

الفرع الثاني
حقوق صاحب البيانات المعالجة على بياناته

تضمنت أغلب التشريعات التي عُنيت بحماية البيانات الشخصية، النص على حقوق صاحب البيانات وضوابط تطبيقها واحترامها عند القيام بمعالجة بياناتهم. فلم تقتصر الحماية على وضع نصوص تجريم تتعلق بالاعتداء على تلك البيانات، بل امتد الأمر إلى وضع ضوابط يعطى من خلالها الأشخاص الطبيعين الحق في ممارساتها في مواجهة جهة المعالجة، **وتتمثل تلك الحقوق فيما يلي:**

(أ) الحق في العلم والوصول والاطلاع:

تضمنت الفقرة الأولى من المادة الثانية من القانون المصري الاعتراف بحق صاحب البيانات في "العلم بالبيانات الشخصية الخاصة به والموجودة لدى حائز أو متحكم أو معالج، والاطلاع عليها والوصول إليها أو الحصول عليها". كما نصت المادة الرابعة من نظام حماية البيانات الشخصية السعودي صراحة على حق صاحب البيانات في العلم، والذي يشتمل على "إحاطته علماً بالمسوغ النظامي أو العملي المعتبر لجمع بياناته الشخصية، والغرض من ذلك، وألاَّ تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها...إلخ".

وعبر المنظم السعودي عن تفسير حق صاحب البيانات في الوصول إلى بياناته المتوفرة لدى جهة التحكم أو المعالجة، بمنحه حق الحصول على نسخة منها، وأن تكون تلك النسخة واضحة ومطابقة لمضمون السجلات، وأن يتم ذلك بلا مقابل مادي ودون إخلال بما يقضي به نظام المعلومات الائتمانية فيما يخص المقابل المالي. فمن حق صاحب الشأن أن يعلم وأن يطلع على ما يخصه من بيانات[٦٧].

---

[٦٧] وتتطلب القانون الفرنسي لحماية البيانات من صاحب البيانات وفقاً للمادة ٣٩/١-٢ أن يتقدم بطلب إلى معالج البيانات، يطلب فيه الاطلاع على بياناته الشخصية، شريطة أن يكشف طالب الاطلاع

(ISSN: 2537 - 0758)

واشترطت اللائحة الأوربية في القسم الثاني منها والوراد تحت عنوان "المعلومات والوصول إلى البيانات الشخصية"، بأنه يجب أن يعلم صاحب البيانات عند تجميع بياناته ما يلي:

(1) هوية جهة المعالجة وتفاصيل الاتصال بها، وممثل وحدة التحكم.
(2) عند الاقتضاء، تفاصيل الاتصال بمسؤول حماية البيانات.
(3) أغراض المعالجة التي تهدف إليها البيانات الشخصية والأساس القانوني للمعالجة.
(4) بيان المصالح المشروعة التي يسعى إليها المعالج أو أي طرف ثالث.
(5) مستلموا البيانات الشخصية أو فئاتهم، إن وجدت.
(6) عند الاقتضاء، حقيقة أن جهة التحكم تعتزم نقل البيانات الشخصية إلى بلد ثالث أو منظمة دولية، ووجود أو عدم وجود قرار يسمح لها بذلك من الجهة المختصة، مع ذكر الضمانات المناسبة أو المناسبة ووسائل الحصول على نسخة منها أو المكان الذي أتيحت فيه.

أما في الحالة التي تنوي فيها وحدة المعالجة مواصلة معالجة البيانات الشخصية لغرض آخر غير الغرض الذي تم جمع البيانات الشخصية من أجله، يجب عليها في هذه الحالة تزويد صاحب البيانات بمعلومات حول الغرض الآخر وأي معلومات أخرى ذات صلة بموضوع المعالجة.

ولعل من بين العقوبات التي وردت في هذا الشأن، ما فرضته اللجنة الوطنية لحماية البيانات "CNIL" في ٢١ يناير عام ٢٠١٩م، من غرامة مالية قدرها ٥٠ مليون يورو ضد شركة GOOGLE LLC، وفقًا للائحة العامة لحماية البيانات(GDPR)، وتم تبرير المبلغ الذي تم تحديده والإعلان عن الغرامة بسبب خطورة الانتهاكات التي لوحظت فيما يتعلق بالمبادئ الأساسية للائحة العامة لحماية البيانات والمتعلقة بالافتقار إلى الشفافية وعدم كفاية المعلومات[٦٨]. وكان ذلك بسبب ملاحظة اللجنة أن المعلومات التي تقدمها GOOGLE لا يمكن الوصول إليها بسهولة للمستخدمين، كما أن بعض المعلومات ليست دائمًا واضحة ولا شاملة، كما لا يستطيع المستخدمون فهم مدى

عن هويته، حتى يتسنى لمعالج البيانات التأكد من أن هذه البيانات تخصه. كما يحق لمعالج البيانات أن يفرض رسوماً نظير الحصول على نسخة من هذه البيانات بشرط ألا تزيد عن تكلفة إعدادها.

[٦٨] الموقع الرسمي "اللجنة الوطنية لحماية البيانات"CNIL https://www.cnil.fr/en، استرجاع بتاريخ ٢٠٢٢/١١/٢٣م.

عمليات المعالجة التي تجريها GOOGLE بشكل كامل، فضلاً عن أن أغراض المعالجة موصوفة بطريقة عامة وغامضة للغاية. وبالمثل، فإن المعلومات التي يتم إرسالها ليست واضحة بما يكفي بحيث يمكن للمستخدم أن يفهم أن الأساس القانوني لعمليات المعالجة لتخصيص الإعلانات هو الموافقة وليس المصلحة المشروعة للشركة. أخيرًا، تلاحظ اللجنة المقيدة أن المعلومات المتعلقة بفترة الاحتفاظ ببعض البيانات غير متوفرة[٦٩].

يبدو أن الحق في الاطلاع لم يرد مطلقاً، بل ألحقت به عدة قيود عددتها المادة ١٦ من نظام حماية البيانات الشخصية السعودي بقولها: على جهة التحكم ألاّ تفصح عن البيانات الشخصية، **متى اتصف الإفصاح بأيٍّ مما يأتي:**

١. أن يمثل خطراً على الأمن، أو يسيء إلى سمعة المملكة، أو يتعارض مع مصالحها.
٢. أن يؤثر على علاقات المملكة مع دولة أخرى.
٣. أن يمنع من كشف جريمة أو يمس حقوق متهم في الحصول على محاكمة عادلة أو يؤثر في سلامة إجراءات جنائية قائمة.
٤. أن يعرض سلامة فرد أو أفراد للخطر.
٥. أن يترتب عليه انتهاك خصوصية فرد آخر غير صاحب البيانات الشخصية وفق ما تحدده اللوائح.
٦. أن يتعارض مع مصلحة ناقص أو عديم الأهلية.
٧. أن يخل بالتزامات مهنية مقررة نظاماً .
٨. أن ينطوي عليه إخلال بالتزام أو إجراء أو حكم قضائي.
٩. أن يكشف عن مصدر سري لمعلومات تحتم المصلحة العامة عدم الكشف عنه.

كما أعطى المشرع الفرنسي في مادته ٢/٣٩ الحق لجهة المعالجة أن ترفض طلب صاحب البيانات في الاطلاع على البيانات التي تخصه؛ إذا اتسم هذا الطلب بالتعسف بالطلب المتكرر أو المنتظم، ويقع عبء الإثبات على عاتق معالج البيانات بوجود

---

[٦٩] ورأى البعض المبالغة في مبلغ الغرامة المفروضة على GOOGLE LLC، إلا أن اللجنة ردت على هذه التعليقات بأنه يجب أن يؤخذ في الاعتبار المكانة الهامة التي يتمع بها نظام Android حيث يقوم آلاف الفرنسيين يومياً بإنشاء حساب في GOOGLE عند استخدام هواتفهم الخلوية، وتشير اللجنة إلى أن النموذج الاقتصادي للشركة يعتمد جزئياً على تخصيص الإعلانات، فكان على GOOGLE LLC المسؤولية القصوى للامتثال للإلتزامات المتعلقة بهذا الشأن.

(ISSN: 2537 - 0758)

تعسف في ممارسة الحق في الاطلاع على البيانات. كما نص في مادته ٦٧ من قانون المعلوماتية والحريات، على أنه لا يحق لمن تخصه البيانات الشخصية الحق في الاطلاع إذا كان معالج البيانات يقوم بذلك في إطار مهنة الصحافة، بشرط مراعاة القواعد المهنية لهذه المهنة. وهذا يعني أن المشرع الفرنسي لم يرد أن يضع قيوداً على حرية الصحفي مادام قد التزم بواجبات وأخلاقيات مهنة الصحافة.

(ب)الحق في التصحيح[٧٠]:

يعطي هذا الحق لصاحب البيانات الشخصية سلطة تصحيح بياناته إذا ارتأى عدم دقتها، أو إكمال بياناته غير المكتملة، أو التعديل أو المحو أو الإضافة أو التحديث. على أن يتم ذلك مع مراعاة أغراض المعالجة.

ونصت المادة ٤٠ من قانون حماية البيانات الفرنسي على أنه يشترط كي يمارس صاحب البيانات حقه في التصحيح، أن تكون البيانات التي تتم معالجتها غير دقيقة أو ناقصة أو غامضة أو أن تم تجميعها أو استخدامها أو حفظها بطريقة غير مشروعة.

ولم تحدد أغلب القوانين المدة الزمنية التي يلتزم بها معالج البيانات بإجراء التصحيح الذي يطلبه صاحب البيانات، بينما يجب على معالج البيانات التزام تصحيح البيانات وتحديثها بصفة مستمرة، وأن يجيب طلب صاحب البيانات في مدة زمنية معقولة دون تأخير متعمد.

(ج) الحق في المحو "الحق في النسيان":

تبنت تشريعات حماية البيانات الشخصية حق صاحب البيانات في طلب إتلاف بياناته الشخصية المتوفرة لدى جهة المعالجة متى انتهت الحاجة إليها. وقررت أنه " إذا اتضح أن البيانات الشخصية التي تجمع لم تعد ضرورية لتحقيق الغرض من حجمها، فعلى جهة التحكم التوقف عن جمعها، وإتلاف ما سبق أن جمعته منها دون تأخير".[٧١]

---

[٧٠] للمزيد عن هذا الحق راجع: المادة ٤ من نظام حماية البيانات الشخصية السعودي، والمادة ٢ من الفصل الثاني من قانون حماية البيانات الشخصية المصري، والمادة ٤٠ من قانون المعلوماتية والحريات الشخصية الفرنسي، والمادة ١٦ من اللائحة الأوروبية لحماية البيانات.

[٧١] راجع نص المادة ٤/١١ من نظام حماية البيانات الشخصية السعودي.

- وانظر كذلك: طارق جمعة السيد راشد، "**الحماية القانونية لخصوصية البيانات الشخصية في القانون القطري والمقارن**"، المجلة القانونية والقضائية، وزارة العدل – مركز الدراسات القانونية والقضائية، العدد ٢، سنة ٢٠١٧م.

إعمالاً لذلك؛ نص قانون حماية البيانات البريطاني لسنة ٢٠١٨ م، على حذف البيانات وكذلك على تقييد استعمالها من جانب الجهة الرقابية. وللمحكمة أن تصدر أمراً إلى الجهة المشرفة والمراقبة لتجميع البيانات أن تقوم بذلك في حالة مخالفة مواد القانون (مادة ١٠٠). من تلك الحالات أن يطلب صاحب البيانات هذا المحو لعدم دقة تلك البيانات أو عدم قانونيتها في التجميع أو المعالجة أو الاستعمال أو عدم رضاء صاحب البيان بعملية التجميع أو المعالجة أو لم تراع في المعالجة مبدأ الملاءمة والتناسب مع الغاية منها، أو تم الاحتفاظ بها بعد فوات المدة المناسبة لتجميعا أو معالجتها أو عدم الحفاظ على سرية تلك البيانات (مادة ٤٥).

وبررت اللائحة الأوروبية لحماية البيانات حق الشخص في طلب محو بياناته، وكان من بين الحالات التي نصت عليها اللائحة ما يلي[٧٢]:

(أ) إذا لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها أو معالجتها بطريقة أخرى.

(ب) العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها، ولا يوجد أساس قانوني آخر للمعالجة.

(د) إذا تمت معالجة البيانات الشخصية بشكل غير قانوني.

(هـ) يجب محو البيانات الشخصية من أجل الامتثال لالتزام قانوني بموجب قانون الاتحاد أو الدولة العضو التي تخضع لها وحدة التحكم أو المعالجة.

وتستثني اللائحة الأوروبية من تطبيق نص المادة ١٧ في حال توافرات حالة من حالات المعالجة الضرورية **والتي تتمثل فيما يلي:**

- ممارسة الحق في حرية التعبير والصحافة والإعلام.
- الامتثال لالتزام قانوني يتطلب المعالجة بموجب قانون الاتحاد أو الدولة العضو التي يخضع لها معالج البيانات، أو أداء مهمة تنفذ للمصلحة العامة أو في ممارسة السلطة الرسمية المخولة لجهة المعالجة.
- لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة.
- لأغراض الأرشفة للمصلحة العامة أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية.
- إقامة مطالبات قانونية أو ممارستها أو الدفاع عنها.

[٧٢] المادة ١٧ من اللائحة الأوروبية لحماية البيانات.

(ISSN: 2537 - 0758)

وفي رأينا أن قوانين حماية البيانات في أوروبا تهدف إلى تأمين المعلومات الخاصة التي قد تضر ببعض الأفراد؛ لذا كانت فكرة الحق في المحو. وهو أمر راسخ لدى الأوروبين منذ قانون إعادة تأهيل المجرمين في انجلترا، والذي يقرر أنه بعد فترة زمنية معينة لا ينبغي الكشف عن معلومات مرتبطة بالأحكام التي أدين بها شخص جنائياً عند طلبه الحصول على تأمين أو بحث عن عمل. كما اعترفت فرنسا بهذا الحق رسمياً منذ عام ٢٠١٠م.

ونلاحظ اختلاف الآراء بين الولايات المتحدة الأمريكية ودول الاتحاد الأوروبي، حيث تتجه الآراء في الولايات المتحدة إلى ترجيح الحق في الشفافية وحرية التعبير، وكذلك الحق في المعرفة عند إزالة أو زيادة الصعوبة في الوصول إلى المعلومات المنشورة فيما يتعلق بالأفراد أو الشركات، مادام أن هذه المعلومات كانت صحيحة.

أما نظام حماية البيانات الشخصية السعودي فقد أكد على تأقيت مدة الاحتفاظ بالبيانات الشخصية لدى جهة التحكم فور الانتهاء من الغرض من جمعها. ومع ذلك استثنى بعض الحالات التي يجوز فيها احتفاظ جهة التحكم بتلك البيانات حتى بعد انتهاء الغرض من جمعها، وذلك في حالتين: **الأولى،** إذا توافر سبب نظامي يوجب الاحتفاظ بها لمدة محددة، وفي هذه الحالة يتم إتلاف تلك البيانات بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها أيهما كان أطول. **أما الحالة الثانية،** فتتمثل في الفرض الذي يتكون فيه تلك البيانات متصلة اتصالاً وثيقاً بأحد القضايا المنظورة أمام جهة قضائية، وفي هذه الحالة يتم إتلافها بعد انتهاء الإجراءات القضائية المتعلقة بالقضية سبب الاحتفاظ بالبيانات[٧٣].

وعلى الرغم من أن الحق في النسيان فكرة حديثة نسبياً، إلا أن محكمة العدل الأوروبية أكدت على اعتباره أحد أهم حقوق الإنسان وجدير بالحماية، وهو ما ظهر جلياً في حكمها في قضية Google Spain v AEPD and Mario Costeja Gonzalez لسنة ٢٠١٤م، حيث أجبرت المحكمة موقع Google على حذف الروابط المتنازع عليها ومحو اسم Costeja Gonzalez من فهرس نتائج البحث Google فيما يتعلق بإجراءات الإعسار المرتبطة بديون الضمان الإجتماعي، والتي تم نشرها من

[٧٣] مادة ١٨ نظام حماية البيانات الشخصية السعودي.

قبل صحيفة أسبانية في عام ١٩٩٨م. ذلك أن إجراءات الإعسار قد انتهت ولم تعد ذات أهمية[٧٤].

- **ولكن التساؤل الذي يثار في أذهاننا الآن، ماذا عن الموت الرقمي، أو بمعنى آخر هل بالإمكان طلب محو بيانات شخص متوفي؟**

باستقراء النصوص التشريعية، وجدنا المنظم السعودي قد أدخل ضمن البيانات الشخصية للأفراد محل المعالجة، بيانات المتوفي إذا كانت ستؤدي إلى معرفته أو إلى معرفة أحد أفراد أسرته بشكل محدد[٧٥].

كما أتاح القانون الفرنسي المتعلق بمعالجة البيانات والحريات، لورثة المتوفي ممارسة بعض الحقوق على بياناته والتي منها[٧٦]:

- الحق في الوصول إلى بيانات الشخص المتوفي في حالة تنظيم وتسوية تركة المتوفي، فيجوز لهم معالجة البيانات الشخصية المتعلقة بهم بهدف تحديد أو الحصول على معلومات تفيد في تصفية أو تقسيم التركة.
- حقهم في محو البيانات الشخصية المتعلقة بالمتوفي، بجواز طلب إغلاق حسابات المتوفي، أو معارضة المعالجة المستمرة للبيانات الشخصية المتعلقة به أو حتى تحديثها.

وفي هذه الحالة، على جهة المعالجة الاستجابة لطلب الورثة دون فرض أي تكلفة على مقدم الطلب. بل أوجبت الفقرة ٣ من المادة آنفة الذكر على أي مزود لخدمة اتصالات عبر الانترنت، الإلتزام بإبلاغ المستخدم بمصير البيانات المتعلقة به عند وفاته، ويسمح له باختبار ما إذا كان سينقل بياناته إلى طرف ثالث يقوم بتعيينه أم لا. وبالفعل اتجهت بعض شبكات التواصل الاجتماعي إلى إضافة ميزات تأخذ في الاعتبار حالة وفاة الشخص، ومن بينهم face book فيعرض على أقارب المتوفي تحويل حسابه

---

(74) Lynskey, Orla, "**Control over personal data in a digital age**" Google Spain v AEPD and Mario Costeja Gonzalez. Modern Law Review, 78 (3). (2015) pp. 522-534. ISSN 0026-7961, DOI: 10.1111/1468-2230.12126. This version available at: http://eprints.lse.ac.uk/61944.

(٧٥) المادة ٢ من نظام حماية البيانات الشخصية السعودي.

(٧٦) راجع نص المادة ٨٥ من قانون البيانات والحريات الفرنسي المعدل في ٢٠١٩م، ونلاحظ أنه وفقاً للمادة ٣٦ من الأمر رقم ٢٠١٩-٩٦٤ المؤرخ في ١٨ سبتمبر ٢٠١٩ م، تدخل أحكام هذه المادة حيز التنفيذ في ١ يناير ٢٠٢٠م، على الرغم من أن القانون في صورته الجديدة دخلت حيز النفاذ في ١ يونيو ٢٠١٩م.

(ISSN: 2537 - 0758)

إلى نصف تذكاري للسماح لعائلته وأصدقائه بالتجمع والتبادل مع بعضهم البعض، والشعور بوجود المتوفي من خلال إدارة صفحته. مع ملاحظة أنه في حال عدم وجود تعليمات من المتوفي بخلاف ذلك، فإن للورثة أن يطلبوا حذف حساب المتوفي.

يتضح مما سبق، أنه يجوز لورثة المتوفي بعد إثبات هويتهم أن يطلبوا من الجهة المسؤولة عن المعالجة لبيانات فقيدهم أن ينبهوا لوفاة هذا الشخص، والقيام بتحديث بياناته. كما أنه في الحالة التي تستمر فيها جهة المعالجة باستخدام بيانات الشخص المتوفي فيجوز للورثة التقدم بطلب إلى المحكمة للمطالبة بتعويض عن الضرر الذي لحق بهم. كما يجوز لهم اللجوء إلى القضاء في حالة استخدام البيانات الشخصية للشخص المتوفي بشكل يؤدي إلى الإضرار بسمعته أو شرفه أو أي ضرر آخر قد يلحق بهم.

(د) الحق في تقييد المعالجة أو نقلها:

يعد من بين حقوق صاحب البيانات "تخصيص المعالجة في نطاق محدد"[٧٧]. وأوضحت اللائحة الأوروبية لحماية البيانات في نص المادة ١٨ منها تحت بند "الحق في تقييد المعالجة" على أنه يحق لصاحب البيانات أن يطلب تقييد معالجة بياناته متى توافرت أحد الإجراءات الآتية:

- إذا تم الطعن في دقة البيانات الشخصية من قبل صاحب البيانات، لفترة زمنية تمكّن جهة المعالجة من التحقق من دقة بياناته الشخصية.
- إذا كانت معالجة بياناته غير قانونية، وعارض صاحب البيانات محوها، وطلب بدلاً من ذلك تقييد استخدامها.
- لم تعد هناك حاجة لأغراض معالجة البيانات الشخصية، ولكن تلك البيانات مازالت ضرورية لإنشاء حقوق قانونية أو الدفاع عنها.
- إذا اعترض صاحب البيانات على المعالجة، بينما يتم التحقق مما إذا كانت الأسباب المشروعة التي تتبناها وحدة التحكم تتعدى الأسباب الخاصة بصاحب البيانات.

وفي الحالة التي يتم فيها تقييد المعالجة، لا يجوز معالجة البيانات الشخصية محل التقييد، باستثناء التخرين، إلا بموافقة صاحب البيانات، أو لحماية حقوق شخص طبيعي أو اعتباري أخر، أو لأسباب تتعلق بالمصلحة العامة للاتحاد أو لدولة عضو. وفي

[٧٧] الفقرة ٤ من نص المادة ٢ من قانون حماية البيانات الشخصية المصري.

الحالة التي تنوي فيها جهة المعالجة رفع قيود المعالجة، يجب عليها إبلاغ صاحب البيانات الذي سبق وطلب تقييدها(٧٨).

وفيما يتعلق بنقل البيانات فلصاحب البيانات الحق في تلقي البيانات الشخصية المتعلقة به، والتي سبق أن قدمها إلى وحدة تحكم معينة، إلى وحدة تحكم أخرى دون عوائق من وحدة التحكم التي تم الكشف عن بياناته الشخصية لها في المرة الأولى. ويستثنى من هذا الحق المعالجة التي تتم لأداء مهمة للمصلحة العامة أو ممارسة الاختصاصات الرسمية المخولة لوحدة التحكم(٧٩).

- **ولكن ماذا عن الحالة التي يتم فيها نقل البيانات إلى خارج إقليم الدولة (عبر الحدود)، سواء إلى أشخاص أو جهات تحكم أو معالجة أو حتى مجرد الإفصاح؟**

وللإجابة عن هذا التساؤل؛ يلاحظ أن الفصل السابع من قانون حماية البيانات الشخصية المصري قد تضمن النص صراحة في الماده ١٤ منه، على حظر إجراء عمليات نقل للبيانات الشخصية التي يتم جمعها أو إعدادها للمعالجة إلى دولة أجنبية أو مشاركتها. وقصد بحركة البيانات الشخصية عبر الحدود (نقلها أو إتاحتها أو تسجيلها أو تخزينها أو تداولها أو نشرها أو استخدامها أو عرضها أو إرسالها أو استقبالها أو استرجاعها أو معالجتها، من داخل النطاق الجغرافي لجمهورية مصر العربية إلى خارجه أو العكس). وقد أورد عدة استثناءات على هذا الحظر تتمثل فيما يلي(٨٠):

أولاً: الحصول على تصريح أو ترخيص من مركز حماية البيانات الشخصية.

ثانياً: الموافقة الصريحة من الشخص صاحب البيانات أو من ينوب عنه، يصرح فيها بنقل أو مشاركة أو تداول أو معالجة بياناته الشخصية إلى دولة لا يتوافر فيها

---

(78) CHAPTER III - Rights of the data subject. Article 18 - Right to restriction of processing:

2. Where processing has been restricted pursuant to paragraph 1, such personal data may, with the exception of storage, be processed only with the consent of the data subject, or for the establishment, exercise or defense of legal claims, or for the protection of the rights of another natural or legal person, or for important reasons of public interest of the Union or of a Member State.
3. A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

(79) Article 20 - Right to data portability.

(٨٠) راجع المواد ١٤، ١٥، ١٦ من نظام حماية البيانات الشخصية المصري.

(ISSN: 2537 - 0758)

مستوى الحماية الذي يتضمنه القانون المصري، وذلك في حال توافر حالة من الحالات الآتية:

١) المحافظة على حياة شخص صاحب البيانات، وتوفير الرعاية الطبية أو علاجه أو إدارة خدماته الصحية.
٢) مراعاة التزامات معينة تتضمن إثبات حق له أمام جهات العدالة أو في حالة الدفاع عنه.
٣) في حالة إبرام عقد أو تنفيذ لعقد مبرم فعلياً، أو سيتم إبرامه بين المسؤول عن المعالجة والغير، على أن يتم ذلك لمصلحة شخص صاحب البيانات.
٤) ضرورة وجود تعاون قضائي دولي. أو وفقاً لتنفيد اتفاق دولي ثنائي أو متعدد الأطراف تكون جمهورية مصر العربية طرفاً فيه.
٥) الحالة التي تتوافر فيها ضرورة لصالح المصلحة العامة
٦) في حال إجراء تحويلات نقدية إلى دولة أخرى وفقاً لتشريعاتها المحددة والسارية.

ولم يختلف المنظم السعودي مع ما أقره المشرع المصري فيما يتعلق بإجراءات وضوابط نقل البيانات، ففي الماده ٢٩ من نظام حماية البيانات الشخصية السعودي، أوضحت أنه لا يجوز لجهة التحكم أو المعالجة نقل البيانات الشخصية إلى خارج المملكة أو الإفصاح عنها لجهة خارجها، إلاَّ إذا كان ذلك تنفيذاً لالتزام بموجب اتفاقية تكون المملكة طرفاً فيه، أو لخدمة مصالح المملكة، أو لأغراض أخرى وفقاً لما تحدده اللوائح، **وذلك بعد أن تتوافر الشروط الآتية:**

١. ألاَّ يترتب على النقل أو الإفصاح مساس بالأمن الوطني أو بمصالح المملكة الحيوية.
٢. أن تقدم ضمانات كافية للمحافظة على البيانات الشخصية التي سَيُجرى نقلها أو الإفصاح عنها وعلى سريتها، بحيث لا تقل معايير حماية البيانات الشخصية عن المعايير الواردة في النظام واللوائح.
٣. أن يقتصر النقل أو الإفصاح على الحد الأدنى من البيانات الشخصية الذي تدعو الحاجة إليه.
٤. موافقة الجهة المختصة على النقل أو الإفصاح وفقاً لما تحدده اللوائح.

واستثنى المنظم السعودي من استيفاء هذه الشروط، "حالات الضرورة القصوى للمحافظة على حياة صاحب البيانات خارج المملكة أو مصالحه الحيوية أو الوقاية من عدوى مرضية أو فحصها أو معالجتها".

أما عن موقف المحكمة الأوروبية لحقوق الإنسان، فقد ظهر في الحكم الصادر في قضية AFFAIRE BIG BROTHER WATCH ET AUTRES c. ROYAUME- UNI لسنة ٢٠٢١م، بشأن الاعتراض الجماعي للاتصالات في المملكة المتحدة، وتبادل المعلومات الاستخبارية مع الدول الأجنبية والحصول على البيانات من مقدمي خدمات الاتصالات. فقد استند مقدمو الشكوى إلى أنه بالنظر إلى طبيعة أنشطتهم، فإن اتصالاتهم الإلكترونية وبيانات اتصالاتهم ربما تكون قد اعترضتها أو جمعتها أجهزة الاستخبارات البريطانية(٨١).

خلصت المحكمة- في هذه القضية- إلى أن نظام الاعتراض الجماعي ينتهك المادتين ٨ والمتعلقة بالحق في احترام الحياة الخاصة والأسرية والاتصالات، والمادة ١٠ والمرتبطة بحرية التعبير على أساس أن كل من نظام الاعتراض الجماعي ونظام الحصول على بيانات الاتصالات صدر من مقدمي خدمات الاتصالات. ولكنها وجدت أن نظام تلقي المواد المعترضة التي يتم الحصول عليها من الحكومات الأجنبية أو دوائر الاستخبارات الأجنبية يتفق مع الاتفاقية.

وتتجه المحكمة إلى أنه بالنظر إلى كثرة التهديدات التي تواجهها الدول في المجتمعات الحديثة، فإن استخدام نظام اعتراض جماعي لا يتعارض في حد ذاته مع الاتفاقية. وهذا يعني أنها ترى أن هذا النظام يجب أن يحاط "بضمانات شاملة"، أي أنه ينبغي على الصعيد الوطني تقييم ضرورة وتناسب التدابير المتخذة في كل مرحلة من مراحل العملية، وأن أنشطة الاعتراض الجماعي ينبغي أن تخضع لإذن من سلطة مستقلة منذ البداية- بمجرد تحديد موضوع العملية ونطاقها- وأن العمليات ينبغي أن تخضع للإشراف من جهة مستقلة.

وقد بررت المحكمة قولها بأن نظام الاعتراض الجماعي الساري في المملكة المتحدة في ذلك الوقت، كان يعاني من أوجه قصور عديدة، من بينها؛ أن عمليات الاعتراض الجماعي صدرت بإذن من وزير، وليس من قبل هيئة مستقلة عن السلطة التنفيذية، كما لم يرد ذكر ضوابط التفتيش التي حددت أنواع الاتصالات التي يمكن فحصها في طلبات إصدار أمر اعتراض، وكذلك مصطلحات التفتيش المتعلقة ببيانات شخصية للأفراد (أي معرفات محددة مثل عناوين البريد الإلكتروني) خاضعين لإذن داخلي مسبق من عدمه.

(81) Case C-207/16; ECLI:EU:C: 2018:788.

(ISSN: 2537 - 0758)

كما قررت أن آلية الحصول على بيانات الاتصالات من مقدمي خدمات الاتصالات تتعارض مع المادتين ٨ و١٠ من حيث كونها غير منصوص عليها في القانون.

واستندت في رأيها إلى ما سبق وقضت به الغرفة الكبرى لاتحاد الصحفيين الأوروبيين، بأن المادة ١٥ (١) من التوجيه EC/٥٨/٢٠٠٢ في ضوء المادتين ٧ و٨ من ميثاق الحقوق الأساسية للاتحاد الأوروبي، يجب أن تُفسَّر على أنها تقصد أن وصول السلطات العامة إلى البيانات بغرض التعرف على أصحاب بطاقات SIM التي تم تفعيلها بهاتف محمول مسروق، مثل الألقاب، والأسماء الأولى، وإذا لزم الأمر، عناوين المالكين، يستلزم التدخل في بياناتهم. فالحقوق الأساسية التي لم تكن خطيرة بما فيه الكفاية بحيث تستلزم تقييد الوصول في مجال منع الجرائم الجنائية والتحقيق فيها وكشفها ومحاكمة مرتكبيها، بهدف مكافحة الجرائم الخطيرة. وأشارت بصفة خاصة إلى أنه وفقاً لمبدأ التناسب، لا يمكن تبرير التدخل الجاد في مجالات المنع والتحقيق والكشف عن الجرائم الجنائية ومقاضاة مرتكبيها، إلا بهدف مكافحة الجرائم الخطيرة.

على النقيض من ذلك؛ عندما يكون التدخل الذي يستتبعه هذا الوصول غير خطير، فيمكن تبرير هذا الوصول بهدف منع "الجرائم الجنائية" والتحقيق فيها وكشفها ومحاكمة مرتكبيها بشكل عام. ولذلك لا تسمح هذه البيانات باستخلاص استنتاجات دقيقة فيما يتعلق بالحياة الخاصة للأشخاص المعنيين ببياناتهم.

كما اعتمدت المحكمة على السوابق القضائية الذي صدرت في هذا الشأن من محكمة العدل التابعة للاتحاد الأوروبي، ومنها قضية Privacy International والتي أقرت في أكتوبر ٢٠٢٠م، أن التشريع الوطني يعطي الحق لسلطات الدولة في مطالبة مقدمي خدمات الاتصالات الإلكترونية من إرسال بيانات حركة المرور وبيانات الموقع، إلى وكالات الأمن والاستخبارات؛ بهدف الحفاظ على الأمن في نطاق التوجيه الخاص بالخصوصية والاتصالات الإلكترونية. ونبهت على أنه يجب لتفسير هذا التوجيه الأخذ في الاعتبار حماية الحق في الخصوصية والحق في حماية البيانات الشخصية والحق في حرية التعبير[٨٢].

(82) Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others (Case C-623/17; ECLI:EU:C: 2020:790) and La Quadrature du Net and Others, French Data Network and Others and Ordre des barreaux francophones et germanophone and Others (Cases C‑511/18, C‑512/18 and C-520/18; ECLI:EU:C:2020:791).

وفي الحالة التي تفرض فيها قيوداً على ممارسة تلك الحقوق، يجب أن ينص عليها القانون وأن تكون مناسبة وضرورية، وتفي بتحقيق أهداف المصلحة العامة التي يعترف بها الاتحاد الأوروبي. كما يجب أن تطبق تلك القيود في حدود الضرورة القصوى، ومن أجل إعمال مبدأ التناسب. بحيث يكون للأشخاص الذين تمس بياناتهم الشخصية ضمانات كافية، بأن بياناتهم سوف تكون في حماية متكاملة ضد مخاطر سوء استخدامها.

أما في الولايات المتحدة الأمريكية، وبموجب الأمر التنفيذي رقم ١٢٣٣٣ والذي تم التوقيع عليه عام ١٩٨١م، يتم جمع وحفظ ونشر المعلومات التي يتم الحصول عليها بسبب تحقيق استخباراتي أجنبي، أو لمكافحة التجسس أو تمرير المخدرات أو الإرهاب الدولي. ولم يُخضع هذا الأمر التنفيذي مراقبة الرعايا الأجانب للوائح المحلية بموجب قانون مراقبة الاسخبارات الأجنبية FISA، ولم يعرف آنذاك مقدار البيانات التي يتم جمعها بموجب هذا الأمر التنفيذي(٨٣).

وقبل إبريل ٢٠١٧م، كان النائب العام ومدير المخابرات الوطنية يصدر شهادات سنوية تسمح بالمراقبة التي تستهدف أشخاص غير أمريكيين يعتقد –بشكل معقول– أنهم خارج الولايات الأمريكية، ويوجد سبب محتمل للاعتقاد بأنهم يعملون لصالح جهات أجنبية. بموجب هذه الشهادات يتم تحديد المعلومات التي يجب جمعها، والتي يجب أن تفي بمفاهيم المعلومات الاستخباراتية الأجنبية، خاصة في الحالة التي تشتمل فيها تلك الشهادات على معلومات تتعلق بالإرهاب الدولي أو أسلحة دمار شامل.

وبناء على تلك الشهادات تقوم وكالة الأمن القومي الأمريكية بإلزام مقدمي الخدمات بنسخ وبحث حركات الإنترنت، وذلك أثناء تدفق البيانات عبر الإنترنت، ويتم جمع المكالمات التليفونية واتصالات الإنترنت. أما بعد إبريل ٢٠١٧م، فلم تحصل وكالة الأمن القومي على اتصالات انترنت أو جمعها، بل أعلنت أنها سوف تقلص من مثل هذه العمليات(٨٤).

(83) CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM. (Applications no. 58170/13, 62322/14 and 24960/15). 25 May 2021.

(84) CASE OF BIG BROTHER WATCH AND OTHERS, op.cit

(ISSN: 2537 - 0758)

(و) الحق في الاعتراض:

يقصد بحق الاعتراض السماح للأفراد بالحق في الاعتراض على معالجة بياناتهم الشخصية أو أي إجراء من إجراءات المعالجة. ويكون للأفراد الحق في الاعتراض في أي مرحلة تكون عليها بياناتهم، فقد يتم الاعتراض في مرحلة جمع البيانات وذلك برفضهم الإفصاح عنها، أو في مرحلة المعالجة والنقل بأن يفصح الفرد برفضه نقل بياناته إلى جهة أخرى.

وتضمنت نصوص قانون حماية البيانات الشخصية المصري ذلك صراحة بقولها يحق للشخص "الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات...إلخ"[٨٥]. وهو ما نصت عليه أيضاً المادة ٥٦ من قانون حماية البيانات الفرنسي، بمنح الشخص الحق في ممارسة الاعتراض على معالجة بياناته، ويستثنى من تطبيق هذا القانون المعالجة التي تتم امتثالاً للقانون ولم توجد أسباب مشروعة للاعتراض. أو وفقاً للشروط المنصوص عليها في المادة ٢٣ من لائحة الاتحاد الأوروبي[٨٦].

واستثنت اللائحة الأوروبية من ذكر المبررات المشروعة، وجواز الاعتراض على المعالجة دون ذكر أسباب، **الحالات الآتية:**

١- إذا كان المعالجة تتجاوز مصالح وحقوق وحريات صاحب البيانات أو لإنشاء مطالبات قانونية أو ممارستها أو الدفاع عنها.

٢- إذا كانت معالجة البيانات الشخصية لأغراض التسويق المباشر.

٣- في سياق استخدام البيانات الشخصية في مجتمع خدمات المعلومات.

٤- أما إذا كانت معالجة بيانات الفرد في مجال البحث العلمي الطبي أو التاريخي أو لأغراض إحصائية، والتي تتناول حالته الصحية وتهدد حياته الخاصة، فله في ذلك

---

[٨٥] الفقرة ٦ من المادة ٢ قانون حماية البيانات الشخصية المصري.

[86] The Data Protection Act. Chapter II: Rights of the data subject. Section 56: "The right to object is exercised under the conditions provided for in Article 21 of Regulation (EU) 2016/679 of 27 April 2016. That right does not apply where the processing complies with a legal obligation or, under the conditions laid down in Article 23 of that regulation, where the application of those provisions has been excluded by an express provision of the act establishing the processing".

الوقت الاعتراض دون إبداء مبررات مشروعة، ما لم تكن المعالجة ضرورية للمصلحة العامة(٨٧).

- **وتظهر إشكالية تتعلق بأوامر ملفات الارتباط Cookies والتي باتت تطلبها أغلب المواقع الإلكترونية أثناء تصفح الإنترنت، فهل القبول الإجباري لهذه الأوامر يعد اعتداءً على البيانات الشخصية والمتمثل في عدم الالتزم بحق الفرد في الاعتراض؟**

قامت بعض الشركات بالسطو على البيانات الخاصة بملايين المشتركين في فيسبوك إضافة إلى أصدقاء هؤلاء الأخيرين. وتسبب ذلك في توجيه اللوم إلى Mark Zuckerberg المسئول عن فيسبوك أثر استجوابه من جانب الكونجرس الأمريكي عام ٢٠١٦م، وإقراره بأنه أخطأ في الحفاظ على بيانات المشتركين كما وعد في ٢٥ مارس ٢٠١٨م، بتعديل سياسة فيسبوك واحترام القواعد الأوروبية بما يضمن مزيداً من حماية بيانات المشتركين، ليس فقط في نطاق البلاد الأوربية ولكن أيضاً على المستوى العالمي(٨٨).

وهو كذلك الأمر الذي دعا اللجنة الوطنية لحماية البيانات CNIL، فرضت غرامة إدارية مقدارها ١٥٠ مليون يورو على جوجل و٦٠ مليون يورو على فيسبوك لمخالفتها للقواعد الأوربية. بأن جعلوا قبول أوامر "الكوكيز" أسهل من رفضها، وذلك بقرارها الصادر في نوفمبر ٢٠٢٠م، حيث صدر القرار بغرامة ٦٠ مليون يورو على شركة GOOGLE LLC و٤٠ مليون يورو على شركة GOOGLE IRELAND LIMITED. وقد تمثل الخطأ المنسوب إليهما في أنهما وضعا "Cookies" على محرك البحث google.fr دون موافقة المستخدمين له ودون تقديم ما يكفي من معلومات(٨٩). هذه الأوامر والتي تسمى"Cookies" تسمح بتسجيل بيانات المشترك ومنها الاحتفاظ بالمواقع التي يدخل عليها وبالتالي تحديد افضلياته واتجاهاته التي تستفيد منها شركات التسوق في توزيع منتاجاتها.

---

(٨٧) انظر المادة ٢١ من القسم الرابع من الفصل الثالث من اللائحة الأوروبية لحماية البيانات.

(88) Royal Courts of Justice, Strand, London, WC2A 2LL, Case No: B2/2002/2636, Monday 8th December 2003: http://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003

(89) https://www.cnil.fr/en/cookies-financial-penalties-60-million-euros-against-company-google-llc-and-40-million-euros-google-ireland

(ISSN: 2537 - 0758)

وقد أيد مجلس الدولة الفرنسي القرار السابق والصادر من لجنة حماية البيانات في ٦ يناير ٢٠٢٢م. ورأى أن هناك عمداً من جوجل وفيسبوك في وضع زر لكي يضغط عليها المستخدم للدخل على صفحات يريده، وأنه كي يرفض يتعين عليه أن يضغط أكثر من زر لبلوغ هذه الغاية. هذا الدخول كان يترتب عليه تسجيل بياناته على هذا المحرك.

وأعطت اللجنة هذه الشركات مهلة ثلاثة أشهر كي تقوم بتعديل موقفها بأن تتيح للمستخدمين في فرنسا إمكانية رفض "الكوكيز" وإلاّ تم الحكم عليها بغرامة ١٠٠ ألف يورو عن كل يوم تأخير.

علاوة عل ذلك؛ ظهر ما يسمى بالحق في إلغاء الإشارة في قرارات مجلس الدولة الفرنسي، هذا الحق لم يكن معروفاً ولم تقرره اللائحة الأوروبية لحماية البيانات، وتم الانتباه إلى هذا الحق في السوابق القضائية من قبل محكمة العدل التابعة للاتحاد الأوروبي (CJEU) والتي كرسته في حكم Google Spain الصادر في ١٣ مايو ٢٠١٤م. ويتمثل هذا الحق، في أنه في ظل ظروف معينة يلتزم محرك البحث Google بناء على طلب الطرف المعني، بأن يحذف من قائمة النتائج التي يتم الحصول عليها نتيجة للبحث الذي أجري "باسم شخص ما" روابط إلى صفحات ويب نشرتها أطراف ثالثة وتحتوي على معلومات تتعلق بذلك الشخص.

وهو ما تم تكريسه في الحكم الصادر عن مجلس الدولة الفرنسي في قضية GOOGLE V. CNIL لسنة ٢٠١٩م. والذي طالبت فيه شركة Google، بدفع الغرامة التي ألزمتها بها CNIL بقيمة ١٠٠٠٠٠ يورو؛ وذلك بسبب عدم امتثالها للإشعار الرسمي الذي تم إرساله إليها للاستجابة لطلبات إلغاء الإشارة إلى الأشخاص الطبيعيين عن طريق إزالة جميع الروابط المؤدية إلى الصفحات من قائمة النتائج المنشورة.

وفي مناقشات مجلس الدولة لم يجدوا في الوضع الحالي، التزام بموجب قانون الاتحاد الأوروبي على مشغل محرك البحث Google الذي يوافق على طلب إلغاء الإحالة المرجعية الذي يقدمه صاحب البيانات، بناء على أمر قضائي من سلطة إشرافية أو سلطة قضائية في دولة عضو، بتنفيذ مثل هذا الإلغاء المرجعي على جميع إصدارات محركه.

وبالرغم من ذلك صدر الحكم بأنه وإن كان قانون الاتحاد الأوروبي لا يشترط بصيغته الحالية إلغاء الإشارة إلى جميع إصدارات محرك البحث، فإنه لا يحظره أيضاً.

وبناء على ذلك تظل سلطات الدول الأعضاء مختصة بأن تقيم في ضوء المعايير الوطنية لحماية الحقوق الأساسية، توازناً بين حق صاحب البيانات المعالجة في احترام حياته الخاصة وحماية البيانات الشخصية المتعلقة به، من ناحية، والحق في حرية المعلومات من ناحية أخرى، وفي نهاية عملية التوازن هذه، أن تأمر عند الاقتضاء، مشغل محرك البحث بإلغاء الإشارة إلى جميع إصدارات ذلك المحرك(٩٠).

ترتيباً على ما سبق بيانه؛ فلكل شخص طبيعي الحق في ممارسة العديد من الحقوق التي منحتها إياه القوانين والتشريعات على اختلافها، وأدرجتها صراحة في ثنايا نصوصها حفاظاً منها على بياناته الشخصية والتي هي حق لصيق به واجب حمايته. ولكن يبدو أن الأمر لم يقف عند ذلك، ولم يترك تطبيق تلك الحقوق على عنانه، بل وجدت نصوص عديدة تضع قيوداً على ممارسة الشخص لحقوقه على بياناته. **والتساؤل الآن ماذا عن تلك القيود وهل حقاً تمس بحقوق الشخص على بياناته، أم أنها تطبق وفق آليات محددة سلفاً، متى ما توافرت ضرورة وغايات تفرض تطبيقها؟**

نص المادة ٢٣ من اللائحة الأوروبية لحماية البيانات من القسم الخامس منها، نص صراحة على أنه يجوز لقانون الاتحاد أو قانون الدولة العضو التي يخضع لها المتحكم أو المعالج–عن طريق تدابير تشريعية– أن يحد من نطاق الالتزامات والحقوق المنصوص عليها في هذه اللائحة، متى كان هذا القيد يحترم جوهر الحقوق والحريات الأساسية، ويكون تدبيراً ضرورياً ومتناسباً في مجتمع ديمقراطي(٩١)، وذلك لضمان ما

(90) Google LLC, coming to the rights of Google Inc. V, Commission nationale de l'informatique et des libertés (CNIL). In Case C-507/17. 24/9/2019. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=99559

(91) Article 23– Limitations:-

1. Union law or the law of the Member State to which the controller or processor is subject may, by means of legislative measures, limit the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34 and Article 5 to the extent that the provisions of the law in question correspond to the rights and obligations provided for in Articles 12 to 22, where such a limitation respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to ensure.

(a) national security;
(b) national defense;
(c) public safety;

(ISSN: 2537 - 0758)

يمس الأمن القومي، الدفاع الوطني، السلامة العامة، كذلك منع الجرائم الجنائية أو التحقيق فيها أو كشفها أو مقاضاة مرتكبيها أو تنفيذ عقوبات جنائية، بما في ذلك الحماية من الأخطار التي تهدد الأمن العام بل ومنعها، وحماية استقلال القضاء والإجراءات القضائية.

ومن القيود أيضا ما قد يمكن أن يمس الأهداف الهامة الأخرى ذات المصلحة العامة للاتحاد أو لدولة عضو، بما في ذلك مصلحة اقتصادية أو مالية هامة، والتي منها المسائل النقدية والمتعلقة بالميزانية والمالية والصحة العامة والضمان الاجتماعي.

وأضافت إلى ذلك إمكانية تطبيق قيود معينة، لمنع الانتهاكات الأخلاقية في المهن الخاضعة للأنظمة معينة، وكشفها والتحقيق فيها ومقاضاة مرتكبيها. كذلك وجود مهمة رقابية أو تفتيشية أو تنظيمية، وأخيراً إنفاذاً لمطالبات القانون المدني.

واشترطت اللائحة لتطبيق تلك القيود، أن يلتزم أي تشريع قانوني بأن يتضمن أحكاماً محددة تتعلق– عند الاقتضاء– **بما يلي:**–

(أ) أغراض المعالجة أو فئات المعالجة.

(ب) فئات البيانات الشخصية.

(ج) مدى القيود المدخلة.

(د) ضمانات لمنع إساءة الاستخدام أو الوصول أو النقل غير المشروعين.

(هـ) تحديد جهة المعالجة أو فئات وحدات التحكم.

(و) فترات التخزين والضمانات المنطبقة، مع مراعاة طبيعة المعالجة ونطاقها وأغراضها.

(d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including protection against and prevention of threats to public security;

(e) other important objectives of general public interest of the Union or of a Member State, including an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and fiscal matters, public health and social security;

(f) the protection of the independence of the judiciary and judicial proceedings;

(g) the prevention, detection, investigation and prosecution of breaches of ethics in regulated professions;

(h) a control, inspection or regulatory task linked, even occasionally, to the exercise of official authority, in the cases referred to in points (a) to (e) and (g);

(i) the protection of the data subject or the rights and freedoms of others;

(j) The enforcement of civil law claims.

(ز) المخاطر التي تهدد حقوق وحريات أصحاب البيانات.
(ح) حق أصحاب البيانات في أن يتم إبلاغهم بالتقييد، ما لم يكن من شأن ذلك أن يخل بالغرض من التقييد.

وهذا يعني أنه جائز– متى توافرت حالة من الحالات المنصوص عليها– أن يتم فرض قيود على ممارسة الشخص لحقوقه على بياناته، كون هناك دوافع تجيز فرض قيود على الحقوق والحريات. وكون الأصل عدم جواز المساس بحقوق وضمانات الأشخاص في سبيل الحفاظ على بياناتهم الشخصية، فقد أتيح ذلك بموجب قانون تشريعي يحدد حالات تلك القيود سلفاً، لاسيما إذا ما توافرت حالة ضرورة، مع مراعاة إعمال مبدأ التناسب بين الحقوق.

ويحدث بالفعل في كثير من الدول، والتي أتاحت استخدام بيانات موقع الهاتف المحمول كطريقة ممكنة لرصد انتشار COVID-19 أو احتوائه أو التخفيف من حدته. فعن طريق استخدام تطبيقات معينة– منها تطبيق توكلنا في المملكة العربية السعودية– يتم تحديد الموقع الجغرافي للأفراد أو إرسال رسائل الصحة العامة إلى الأفراد في منطقة معينة عن طريق الهاتف أو الرسائل النصية.

فقد تم تطبيق مبدأ التناسب؛ حيث طبقت بعض القيود، مع مراعاة الغرض المحدد الذي يتعين تحقيقه من فرضها. فتتّبع الأفراد ومعالجة بياناتهم للكشف عن حالات انتشار الوباء، متناسبة في ظل ظروف استثنائية. ومع ذلك؛ يجب أن يخضع لتدقيق وضمانات معززة لضمان احترام الحق في حماية البيانات، أي البحث في مدى تناسب التدبير من حيث المدة والنطاق، والاحتفاظ المحدود بالبيانات وتحديد الغرض، ومحو تلك البيانات متى انتهى الغرض من المعالجة.

وهو ما أكده المنظم السعودي في نصوصه المعنية بحماية البيانات، في اعتبار أن الوقاية من العدوى المرضية أو فحصها أو معالجتها، تعد من بين الحالات الضرورية القصوى، التي تجيز لجهة التحكم نقل البيانات والإفصاح عنها[٩٢]. بل أجازت الإفصاح عن البيانات الشخصية لشخص معين، متى كان هذا الإفصاح ضرورياً لحماية الصحة أو السلامة العامة أو حماية حياة الأفراد وحماية صحتهم[٩٣].

---

[٩٢] مادة ٢٩ من نظام حماية البيانات الشخصية السعودي.
[٩٣] مادة ١٥ من نظام حماية البيانات الشخصية السعودي.

(ISSN: 2537 - 0758)

المطلب الثاني
ضوابط مشروعية معالجة البيانات الشخصية إلكترونياً

أولاً- أن يكون تجميع البيانات الشخصية مشروعاً:

تستلزم الأنظمة والتشريعات الجنائية المقارنة، واجب أن يتم تجميع البيانات ابتداءً بطريقة مشروعة، ويمكن القول بأن تجميع البيانات قد يتم بطرق غير مشروعة في الحالة التي يتم فيها خداع الشخص أو تضليله عن الحصول على بياناته. بل قد يكون التجميع تم بشكل مشروع، بينما تم استخدام تلك البيانات بطرق تؤثر سلباً على حقوق وحريات صاحب البيانات المعالجة.

ولا يحدث ذلك إلاّ إذا تم ذلك بإخطار الجهة الإدارية المختصة بحماية البيانات الشخصية في بعض التشريعات، بينما تشترط تشريعات أخرى أن يتم ذلك بعلم من صاحب البيانات نفسه وقبوله بذلك صراحة.

في ذلك تفرض المادة ١٦ من القانون الفرنسي، التزاماً على كل شخص يقوم بتسجيل معلومات شخصية عن الأفراد أن يخطر لجنة إدارية خاصة أنشأها القانون لمراقبة مدى احترام الحياة الخاصة للأفراد، وهي "اللجنة الوطنية للمعلوماتية والحريات" بكل ما ستقوم به جهة المعالجة. على أن يتم هذا الإخطار قبل القيام بإنشاء نظام المعالجة وليس بعد جمع البيانات المراد معالجتها. ولعل السبب في ذلك هو؛ تمكين اللجنة من ممارسة سلطاتها في العلم بعمليات المعالجة التي تتعلق ببيانات شخصية، وتطبيق أحكام الرقابة عليها والتأكد من مطابقتها للقانون، فضلاً عن كون هذا الإخطار يحقق شفافية عملية المعالجة وسبق الإخطار بها للجنة المختصة.

ويشارك القانون الفرنسي تشريعات أوربية عديدة في اشتراطها أن يتم هذا النوع من الإخطار إلى جهة تتولى مهمة المراقبة والمتابعة، حماية للحياة الخاصة للأفراد[٩٤]. ويعد من بين تلك القوانين القانون الدنمركي[٩٥]، والقانون السويدي[٩٦]، وقانون لكسمبورج[٩٧]، والقانون الإيطالي[٩٨].

---

(94) Ulrich Sieber, The international Handbook on Computer Crime, John Wiley & Sons, New York, 1986, at 107.
(95) section 8, 20 (1) and (2), 21 (2) and 27 (2) n° 4.
(96) section 20 (1) and (2), Swedish Data Act.
(97) section 32, Luxembourgian Act Regulating the Use of Nominal Data
(98) section 23.

غير أن القواعد التي أقرها المجلس الأوربي قد عدلت في هذا الصدد بحيث لم يعد الأمر قاصراً على الإخطار، بل أصبح ملزماً على جهة التحكم في البيانات وجهة المعالجة واجب الحصول على رضاء صاحب الشأن(٩٩).

ولعل من بين البيانات الواجب الإخطار بها لإضفاء مشروعية تجميع البيانات لمعالجتها، هوية وعنوان المسؤول عن المعالجة، والهدف من المعالجة، وإذا كان هناك صلة بين نظام المعالجة الجديد وبين أي نظام آخر موجود بالفعل، كذلك أنواع البيانات التي يتم معالجتها بصفة خاصة، والمدة التي يتم الاحتفاظ بها بالبيانات محل المعالجة، والأشخاص المخول لهم بمقتضى وظيفتهم الاطلاع على هذه البيانات، إضافة إلى التدبير التي سيتم اتخاذها لضمان أمان وسرية المعالجة.

وعليه فرضت اللجنة الوطنية لحماية البيانات **CNIL** بتاريخ ٢٩ ديسمبر ٢٠٢٢م، غرامة إدارية قدرها ٨,٠٠٠,٠٠٠ (ثمانية ملايين) يورو على شركة APPLE DISTRIBUTION INTERNATIONAL لمخالفة المادة ٨٢ من قانون حماية البيانات، والتي بموجبها "يجب إبلاغ أي مشترك أو مستخدم لخدمة الاتصالات الإلكترونية بطريقة واضحة وكاملة– ما لم يتم إبلاغه مسبقاً– من قبل المعالج أو ممثله بالغرض من أي إجراء يهدف إلى الوصول، عن طريق الإرسال الإلكتروني، إلى المعلومات المخزنة بالفعل في معدات الاتصالات الإلكترونية الخاصة به، أو لإدخال معلومات في هذا الجهاز. كذلك الوسائل المتاحة لصاحب الشأن للاعتراض على ذلك". فلا يجوز أن يتم هذا الوصول أو التسجيل إلا شريطة أن يكون المشترك أو المستخدم قد أعرب بعد تلقي هذه المعلومات عن موافقته.

وكانت ذلك بسبب أنه بموجب الإصدار القديم ios١٤.٦ من نظام تشغيل iPhone، عندما يذهب المستخدم إلى متجر التطبيقات، كانت المعرفات التي تسعى إلى أغراض التخصيص للإعلانات التي يتم بثها على App Store، تتم قراءتها تلقائياً على الجهاز دون الحصول على موافقة. حيث وجدت أن هذه المعرفات ليست ضرورية لتوفير الخدمة (متجر التطبيقات). وبالتالي؛ يجب ألا تكون قابلة للقراءة أو الإيداع دون موافقة مسبقة من المستخدم. إضافة إلى ذلك وجدت اللجنة أنه كان على المستخدم تنفيذ عدد كبير من الإجراءات لتعطيل هذا الإعداد، نظراً لعدم دمج هذا الاحتمال في مسار تهيئة الهاتف، فكان على المستخدم النقر على أيقونة "الإعدادات" في iPhone، ثم

(99) https://www.europarabct.com

(ISSN: 2537 - 0758)

الانتقال إلى قائمة "الخصوصية" وأخيراً إلى القسم المعنون "إعلانات Apple". ولم تسمح هذه العناصر بالموافقة المسبقة للمستخدمين(١٠٠).

- **حالات المعالجة غير المرئية "Invisible Processing"**:

يقصد بها الحالات التي يتم فيها تجميع البيانات من مصدر آخر غير صاحبها. في هذا الخصوص استخدمت اللائحة الأوروبية مصطلح الشفافية في تجميع البيانات، والذي يعني أن تتم المعالجة في ظل وجود شفافية مع أصحاب تلك البيانات، ومن أهمها بيان سبب تجميع بياناتهم الشخصية والمدة التي سيتم الاحتفاظ بها، خاصة في حالات المعالجة غير المرئية. ففي هذه الحالة يكون للشفافية أهمية بالغة خاصة وأنه في الحالة الأخيرة، قد لا يكون لدى الأشخاص أي دراية عن تجميع بياناتهم، وهو ما يؤثر على قدرتهم على ممارسة حقوقهم على بياناتهم.

يستتبع ذلك أن تلتزم جهة المعالجة بإخبار الأشخاص المراد تجميع بياناتهم بطريقة تسهل الوصول إليها وفهم مضمونها، مع ضرورة استخدام لغة واضحة وصريحة، خاصة ما يتعلق بالمعلومات الموجهة إلى طفل(١٠١).

غير أنه يجوز في حالة الحصول على بيانات شخصية من مصادر أخرى غير صاحبها استثناء عدم تزويد أصحاب هذه البيانات بمعلومات تخص أسباب تجميع البيانات ومعالجتها؛ وذلك متى توافرت حالة من الحالات الأتية، شريطة أن تتخذ جهة المعالجة التدابير المناسبة لحماية حقوق صاحب البيانات وحرياته ومصالحه المشروعة، **هذه الحالات هي**(١٠٢):

---

(100) Deliberation of the restricted formation n ° SAN-2022-025 of December 29, 2022 concerning the company APPLE DISTRIBUTION INTERNATIONAL.
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046907077. Retrieved: 8 Jan 2023.

(101) Regulation (EU) of the European Parliament and of the Council. (Article 12): "Transparent information, communication and modalities for the exercise of the rights of the data subject".

(102) Regulation (EU) of the European. Article 14: Information to be provided where personal data have not been obtained from the data subject
- the individual already has the information;
- providing the information to the individual would be impossible;
- providing the information to the individual would involve a disproportionate effort;

- أن يكون لدى الفرد بالفعل تلك المعلومات وعلى دراية بها.
- إذا كان من المستحيل توفير تلك المعلومات لصاحب البيانات.
- إذا كان توفير تلك المعلومات يتطلب جهداً كبيراً وغير متناسب، خاصة ما يتعلق بأغراض الأرشفة للمصلحة العامة، أو أغراض البحث العلمي أو الأغراض الإحصائية.
- إذا كان توفير المعلومات للشخص سيجعل من المستحيل أو يضعف بشكل يمثل خطورة تحقيق أهداف المعالجة.
- إذا كانت جهة المعالجة بموجب القانون تخضع لالتزام السرية المهنية التي ينظمها القانون والتي تغطي البيانات محل المعالجة.

أما القانون الإنجليزي فقد اتخذ خطوة أوسع عندما حصر الجهات التي لها أن تقوم بتجميع بيانات شخصية عن الأفراد، وهي وفقاً للمادة الثامنة من Data Protection Act لسنة ٢٠١٨م:

- أجهزة العدالة
- مجلس النواب
- قيام شخص بتجميع البيانات بتصريح قانوني بذلك
- أجهزة الحكومة
- قيام جهات بهذا التجميع دعماً للديمقراطية
- **وتظهر إشكالية قانونية عن الحالة التي يتم فيها استخدام الكاميرات الذكية أو الكاميرات الحرارية "Smart or Thermal cameras"، فهل يعد ذلك تجميعاً لبيانات شخصية لأشخاص طبيعيين بطريق غير مشروع؟**

طرحت إشكاليات عديدة بشأن استخدام الكاميرات الذكية، وهو مصطلح يشير إلى الأجهزة التي تستخدم خوارزميات تسمح بالتحليل التلقائي للصور الرقمية، وذلك بإنتاج معلومات تخص هذه الصور، وتمكن من التعرف على بعض السمات والخصائص مثل (تصنيف السيارات– أو تحديد الجنس– أو الفئة العمرية للأفراد... إلخ). حيث يتم وضع

- providing the information to the individual would render impossible or seriously impair the achievement of the objectives of the processing;
- you are required by law to obtain or disclose the personal data; or
- You are subject to an obligation of professional secrecy regulated by law that covers the personal data.

(ISSN: 2537 - 0758)

هذه الكاميرات وتثبيتها في الأماكن العامة أو الأماكن المفتوحة، والتي تكون عادة لتحقيق مصالح عامة[١٠٣].

وتختلف كاميرات الفيديو الذكية عن أجهزة معالجة البيانات الحيوية أو الحرارية (مثل كاميرات التعرف على الوجه)؛ وذلك لأن الكاميرات الذكية لا تعالج دائماً الخصائص الجسمانية أو الفسيولوجية أو السلوكية، ذلك أن هذه الكاميرات مهمتها الأساسية نقل صور عن المكان العام كحركة مرور السيارات في الشارع أو رصد تجمع للجمهور في مكان معين...إلخ. فلا تهدف تلك الكاميرات إلى تحديد هوية أشخاص معينيين.

ولكن إذا ما تم إضافة أنواع معينة من البرامج إلى أنظمة حماية الفيديو الموجودة مسبقاً فيمكن أن تتحول تلك الكاميرات إلى أجهزة قادرة على التعرف على الخصائص الجسمانية كما هو الحال للكاميرات الحرارية، والتي عن طريقها يتم قياس درجة الحرارة الأتوماتيكية، واكتشاف ارتداء القناع والامتثال لتدابير التباعد الاجتماعي (كما كان الحال أثناء انتشار وباء كرونا). والتي تعد من بين البيانات البيومترية التي يحظر معالجتها من الأساس[١٠٤]، ما لم تكن المعالجة ضرورية لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة، مثل الحماية من التهديدات الخطيرة عبر الحدود للصحة، أو لغرض ضمان معايير عالية لجودة وسلامة الرعاية الصحية والمنتجات الطبية أو الأجهزة الطبية، على أساس قانون الاتحاد أو الدولة العضو الذي ينص على تدابير مناسبة ومحددة لحماية حقوق وحريات صاحب البيانات، بما في ذلك السرية المهنية[١٠٥].

---

(103) CNIL., **"CAMÉRAS DITES «INTELLIGENTES» OU «AUGMENTÉES» DANS LES ESPACES PUBLICS".** POSITION SUR LES CONDITIONS DE DÉPLOIEMENT. Juillet 2022., p 9.

[١٠٤] تضمنت المادة/٩ من اللائحة العامة لحماية البيانات الأوروبية النص صراحة على أنه: "تحظر معالجة البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية، وكذلك معالجة البيانات الجينية أو البيانات البيومترية لغرض تحديد هوية الشخص الطبيعي بشكل فريد أو البيانات المتعلقة بالصحة أو البيانات المتعلقة بالحياة الجنسية للشخص الطبيعي أو التوجه الجنسي".

(105) Article 9- Processing of special categories of personal data:(i) "The processing is necessary for reasons of public interest in the area of public health, such as protection against serious cross-border threats to health, or for the purpose of ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, on the basis of

ولكن الأمر الأكثر إشكالية وتعقيداً في حالات استخدام الكاميرات الذكية، هو الانتقال من المراقبة المعممة إلى خطر التحليل المعمم، فعلى الرغم من أن كاميرات الفيديو الذكية تقوم بالتقاط وتسجيل الصور بشكل عشوائي، إلا أن المعالجة الخوارزمية في أنظمة كاميرات الفيديو هذه، قد تأخذ بعداً أوسع في جميع بيانات يمكن استنتاجها بشكل كبير، ومن ثم يمكن أن تؤدي تلك الكاميرات إلى معالجة البيانات الشخصية بما فيها البيانات الحساسة.

هذه الكاميرات يمكن أن توفر لمستخدميها التعرف على معلومات تخص بعض الأشخاص الذين يتم تصويرهم، حتى ولو كان ذلك من أجل اتخاذ قرار أو تدبير يتعلق بالمكان أو الجهة العامة التي وضعت بها الكاميرات.

يضاف إلى ذلك إشكالية أكبر كون نشر مثل هذه الكاميرات في الأماكن العامة، ينطوي على مخاطر تمس حقوق وحريات الأشخاص والتي منها (الحق في الخصوصية- حرية التعبير والتجمع- الحق في التظاهر- حرية ممارسة العبادة وغير ذلك من الحريات)؛ ذلك أن الحفاظ على المجهولية في الفضاء العام- أي عدم الكشف عن الهوية في الأماكن العامة- يمثل بعداً أساسياً لممارسة تلك الحريات[١٠٦]. وهو ما يستدعي أن يتوافق استخدام تلك الكاميرات مع اللوائح والقوانين المعمول بها في شأن البيانات الشخصية، حتى ولو تم إخفاء هوية الصور أو إتلافها بعد التقاطها وتحليلها، ذلك هذه العمليات تشكل معالجة لبيانات شخصية.

لذلك يجب أن تنص التشريعات على وجود ضمانات كافية لاستخدام مثل هذه الكاميرات، خاصة إذا قامت بمعالجة بيانات حساسة مثل التقاط البيانات الصحية الشخصية أو البيانات البيومترية، مع مراعاة حقوق أصحاب تلك البيانات في الاعتراض، ومن ثم يجب وضع إطار قانوني مناسب لاستخدامها، وتحديد المخاطر غير المقبولة التي يمكن أن تقع في مجتمع ديمقراطي.

وإذا ما طبقنا مبدأ الضرورة والتناسب على هذه الحالة، فيجب نشر هذه الكاميرات بموافقة الأفراد، ما لم تكن ضرورية لتحقيق أهداف معينة تفيد الصالح العام، وبناء على

Union or Member State law which provides for appropriate and specific measures to safeguarding the rights and freedoms of the data subject, including professional secrecy".

(106) CNIL., "CAMÉRAS DITES «INTELLIGENTES» OU «AUGMENTÉES» DANS LES ESPACES PUBLICS. Ibdi.

(ISSN: 2537 - 0758)

ذلك يجب ألا تنتهك الخصوصية على نحو غير متناسب، ومن ثم فيمكن إثبات ضرورة وتناسب استخدام الكاميرات الذكية في الحالات الآتية:

- عدم وجود وسائل أخرى أقل تدخلاً واعتداءً على حقوق وحريات أصحاب البيانات لتحقيق الأهداف المبتغاه من نشرها.
- تحديد أهمية البيانات المعالجة.
- الكشف عما يتعلق بنطاق نشر تلك الكاميرات في المكان والزمان، وذلك فيما يتعلق (بعدد الكاميرات– مدى نطاقها– مدة نشرها).
- ما يتعلق بردود الفعل على مراقبي البيانات.

كذلك الحال إذا ما تم استخدام الكاميرات الحرارية، والتي تسمح بتحديد هوية الأشخاص خاصة ما يتعلق (بتحديد الوجه والجسم ودرجة الحرارة)، فتعد من بين البيانات الشخصية وتحديداً الصحية، والتي يحظر معالجتها من الأساس، ما لم يرد أحد الاستثناءات التي يلزم أن ينص عليها القانون صراحة. كما هو الحال في اللائحة الأوروبية لحماية البيانات، التي تبرر معالجة البيانات الصحية وفقاً لنص المادة ٩/٢ والتي تضمنت ما يلي[١٠٧]:

- وجود أسباب ذات أهمية تحقيق المصلحة العامة بوجه عام.
- وجود أسباب تتعلق بالصحة العامة.
- وجود نص صريح ومحدد يأذن بوجود مثل هذه الأجهزة في حالات الضرورة.
- كما يمكن معالجة مثل هذه البيانات في حالة موافقة الشخص على ذلك.

وفي جميع الأحوال؛ يجب مراعاة حق الشخص في أن يعترض على أن يكون موضوعاً لالتقاط صور له في الفضاء العام[١٠٨]. ومراعاة حقه في الاعتراض عندما يستند إلى مصلحة عامة أو مصلحة مشروعة، خاصة وأن استخدام مثل هذه الأجهزة

---

[107] Article 9 - Processing of special categories of personal data.

[١٠٨] راجع نص المادة ٢١ من اللائحة الأوربية لحماية البيانات والتي نصت على أنه:

- Article 21 - Right to object: "The data subject shall have the right to object at any time, on grounds relating to his or her particular situation, to the processing of personal data concerning him or her based on point (e) or (f) of Article 6 (1), including profiling based on those provisions. The controller shall no longer process personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

في الأماكن العامة والأماكن المفتوحة يتعارض مع الالتزام بمراعاة حق الاعتراض والاعتداء على احترامه بشكل فعّال. هذه الكاميرات تلتقط تلقائياً صورة الأشخاص شكل عام عن طريق طيف المسح الضوئي دون إمكانية تجنب الأشخاص الذين سبق وأعربوا عن معارضتهم، لذلك إذا تعذر تطبيق الحق في الاعتراض في الواقع العملي، فيجب أن يخضع استخدام تلك الكاميرات في إطار قانوني منظم ومحدد وفق نصوص تشريعية واضحة.

وقد أكدت اللائحة الأوروبية لحماية البيانات ذلك عندما أوجبت أن يشتمل أي تشريع قانوني أحكاماً محددة وصريحة– عند الاقتضاء– **على ما يلي**[١٠٩]:

(أ) أغراض المعالجة أو فئات المعالجة.

(ب) أنواع البيانات الشخصية.

(ج) مدى القيود المدخلة.

(د) ضمانات تمنع إساءة الاستخدام أو الوصول أو النقل غير القانونيين.

(هـ) تحديد المراقب أو فئات المراقبين.

(و) تحديد فترات التخزين والضمانات المعمول بها، مع مراعاة طبيعة ونطاق وأغراض المعالجة.

(ز) المخاطر التي يمكن أن تهدد حقوق وحريات أصحاب البيانات.

(ح) حق أصحاب البيانات في إبلاغهم بتلك القيود، ما لم يكن ذلك من شأنه أن يخل بالغرض من هذه القيود.

---

(109) Article 23– Limitations: In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions concerning, at least, where appropriate:
(a) the purposes of the processing or categories of processing;
(b) categories of personal data;
(c) the extent of the limitations introduced;
(d) safeguards to prevent misuse or unlawful access or transfer;
(e) the determination of the controller or categories of controllers;
(f) the applicable storage periods and safeguards, taking into account the nature, scope and purposes of the processing or categories of processing;
(g) risks to the rights and freedoms of data subjects; and
(h) The right of data subjects to be informed of the restriction, unless this would prejudice the purpose of the restriction.

(ISSN: 2537 - 0758)

خلاصة ما تقدم؛ ففي الحالة التي يتم فيها معالجة البيانات الشخصية بشكل غير مشروع وغير قانوني، يلزم أن يمنح الحق لأصحاب هذه البيانات في محو تلك البيانات أو تقييد معالجتها، وفي حال مخالفة ذلك، فإن انتهاكاً لحقوق الأفراد على بياناتهم يتوافر، حتى ولو كان الأمر يستند إلى مصلحة عامة ومشروعة(١١٠).

ثانياً- أن يكون مصدر البيانات هو صاحبها (موافقة صاحب البيانات):

نصت المادة ٤ من اللائحة الأوروبية لحماية البيانات على أن مفهوم الموافقة يعني "إشارة حرة ومحددة ومستنيرة ولا لبس فيها، عبر عنها صاحب البيانات بإرادته عن رغبته بالموافقة على معالجة البيانات الشخصية المتعلقة به من خلال بيان أو إجراء إيجابي واضح"(١١١).

وتم التعبير عن ذلك صراحة في قضية ORANGE ROMANIA لسنة ٢٠٢٠م، والذي قدمت فيها محكمة رومانية طلباً للحصول على حكم أولي في إجراءات بين مشغل هاتف والسلطة الإشرافية الوطنية لمعالجة البيانات الشخصية، فيما يتعلق بدعوى لإلغاء قرار فرضت بموجبه هذه الأخيرة غرامة على المشغل لقيامه بجمع وتخزين نسخ من وثائق هوية عملائه دون موافقتهم الصحيحة، وطلبت منه إتلاف هذه النسخ(١١٢).

---

(١١٠) أصدرت اللجنة الوطنية CNIL تقريرها المعنون "بأخلاقيات الخوارزميات والذكاء الاصطناعي" المنشور في ديسمبر ٢٠١٧م، أهمية وضرورة حماية مبادئ اليقظة (والتي تهدف إلى الحماية من إغراءات التقنيات الحديثة وعدم تفويض أكثر الأمور إلى تلك الأدوات) كذلك حماية مبدأ الولاء والذي يعني (ضمان استخدام الأدوات بما يتوافق مع ما هو متوقع. كون استخدام مثل هذه التقنيات قد يؤدي إلى ما يسمى بأتمتة التمييز؛ كون هذه التقنيات يمكنها استهداف خصائص الأفراد ومن ثم إمكانية تعرضهم للتمييز، فيما يتعلق (بالهوية الجنسية– المظهر الجنسي– العمر...إلخ). انظر موقع النت أدناه، استرجاع بتاريخ ٢٠٢٣/١/٢٤م.

-Algorithmes: prévenir l'automatisation des discrimination» sur defenseurdesdroits. fr.

(111) "consent" of the data subject means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject consents, by a statement or by a clear affirmative action, to the processing of personal data relating to him or her.

(112) Orange România SA V, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP). Court of Justice of the European Union.Case-no:C-61/19. (11/11/2020). Retrieved: 2/10/2022.

وظهر موقف محكمة العدل التابعة للاتحاد الأوروبي في تفسيرها لمفهوم الموافقة بقولها؛ أن التوجيه EC٤٦/٩٥، واللائحة الأوروبية ٦٧٩/٢٠١٦ (GDPR) التي تلغي هذا التوجيه، يجب تفسيرهما على أنهما يعنيان أنه يتعين على وحدة التحكم أن تثبت أن صاحب البيانات قد أعرب بشكل صريح عن موافقته على معالجة بياناته الشخصية. وأنه قد حصل مسبقاً على المعلومات الكافية في ضوء جميع الظروف المحيطة بتلك المعالجة، بشكل مفهوم ويسهل الوصول إليه وصياغته بعبارات واضحة وبسيطة، مما يمكنه من تحديد عواقب تلك الموافقة بسهولة. وأقرت بأن عقد تقديم خدمات الاتصالات السلكية واللاسلكية الذي يتضمن بنداً تم بموجبه إبلاغ صاحب البيانات وموافقته على جمع نسخة من وثيقة هويته والاحتفاظ بها لأغراض تحديد الهوية، ليس من شأنه أن يثبت أن ذلك الشخص قد أعطى موافقته بشكل صحيح، بالمعنى المقصود في تلك الأحكام، بما في ذلك الجمع والتخزين، **حيث أنه:**

- تم وضع علامة في المربع الذي يشير إلى هذا البند من قبل مراقب البيانات قبل توقيع ذلك العقد.
- أو من المحتمل أن تضلل الأحكام التعاقدية لذلك العقد صاحب البيانات فيما يتعلق بإمكانية إبرام العقد المعني حتى لو رفض الموافقة على معالجة بياناته.
- أو عندما يتأثر الاختيار الحر للاعتراض على هذا الجمع والتخزين بشكل غير مبرر من قبل وحدة التحكم، من خلال مطالبة صاحب البيانات، من أجل رفض إعطاء الموافقة، بإكمال نموذج إضافي ينص على هذا الرفض.

وفي حكم لاحق لمحكمة العدل التابعة للاتحاد الأوروبي، أقرت بأنه وفيما يتعلق بموافقة صاحب البيانات الورادة في المادة/ ٢ فقرة (ح) والمادة/ ٧ فقرة (أ) من التوجيه الأوروبي ٤٦/٩٥، يجب من خلالها أن يحصل عليها مشغل موقع الويب فقط فيما يتعلق بالعمليات التي تنطوي على معالجة البيانات الشخصية التي يحدد المشغل أغراضها ووسائلها. في مثل هذه الحالة، فإن واجب الإبلاغ المنصوص عليه في المادة ١٠ من هذا التوجيه يقع أيضًا على عاتق ذلك المشغل، مع مراعاة أن المعلومات التي يجب أن يقدمها هذا الأخير إلى صاحب البيانات لا تتعلق إلا بالعمليات التي تنطوي

https://curia.europa.eu/juris/document/document.jsf?text=&docid=233544&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1

(ISSN: 2537 - 0758)

على معالجة البيانات الشخصية التي يحدد المشغل بالفعل الأغراض والوسائل المتعلقة بها[١١٣].

أما القانون السويدي لحماية البيانات فقد تضمن في القسم العاشر منه في الفصل الثالث، فإنه لا يجيز معالجة أرقام الهوية الشخصية إلا دون موافقة صريحة من صاحب البيانات إذا كان لها ما يبررها بوضوح، مع مراعاة الغرض وأهمية تحديد الهوية[١١٤].

وقد ذهب المنظم السعودي إلى أبعد من ذلك، عندما اشترط موافقة صاحب الشأن– بصفة أساسية– على تجميع ومعالجة البيانات الخاصة به بقوله في المادة الخامسة "فيما عدا الأحوال المنصوص عليها في النظام، لا تجوز معالجة البيانات الشخصية أو تغيير الغرض من معالجتها إلاَّ بعد موافقة صاحبها. وتُبين اللوائح شروط الموافقة، والأحوال التي يجب فيها أن تكون الموافقة كتابية، والشروط والأحكام المتعلقة بالحصول على الموافقة من الولي الشرعي إذا كان صاحب البيانات الشخصية ناقص أو عديم الأهلية. في جميع الأحوال، يجوز لصاحب البيانات الشخصية الرجوع عن الموافقة المشار إليها في الفقرة (١) من هذه المادة في أي وقت، وتحدد اللوائح الضوابط اللازمة لذلك".

وقد أفرد النظام السعودي وضعاً خاصاً للبيانات الائتمانية؛ باستلزامه ضرورة الموافقة الصريحة للجمع وتغيير الغرض من الجمع والإفصاح عنها أو نشرها. كما نصت المادة السابقة على ضرورة إبلاغ صاحب البيانات عند وجود طلب الإفصاح عن تلك البيانات[١١٥]. ومع ذلك فقد استغنى عن تلك الموافقة في بعض الحالات عددتها المادة السادسة من النظام، **وهي:**

١– عندما تُحقق المعالجة مصلحة متحققة لصاحب البيانات وكان الاتصال به متعذراً أو كان من الصعب تحقيق ذلك.

---

(113) Judgment of 29 July 2019, Fashion ID (C-40/17, EU:C: 2019:629) (Higher Regional Court, Düsseldorf, Germany). JUDGMENT OF THE COURT (Second Chamber)29 July 2019. Retrieved 30/8/2022. https://curia.europa.eu/juris/document/document.jsf?text=&docid=244575&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=8508699.

(114) Chapter 3, Section 10 of Swedish Data Act: personal identity numbers may only be processed without the data subject's explicit consent if it is clearly justified, taking into account the purpose, the importance of identification and other significant reasons.

(١١٥) المادة ٢٤ من نظام حماية البيانات الشخصية السعودي.

٢- عندما تكون المعالجة بمقتضى نظام آخر أو تنفيذاً لاتفاق سابق يكون صاحب البيانات الشخصية طرفاً فيه.

٣- في الحالة التي تكون فيها جهة التحكم جهة عامة، وكانت تلك المعالجة مطلوبة لأغراض أمنية أو لاستيفاء مُتطلبات قضائية.

وحرص هذا النظام على أن تبدى الموافقة بحرية فلا يعلق قبول خدمة معينة على أداء تلك الموافقة بقولها "لا يجوز أن تكون الموافقة المشار إليها في الفقرة الأولى من المادة ٥ من النظام شرطاً لإسداء خدمة أو تقديم منفعة، ما لم تكن الخدمة أو المنفعة ذات علاقة بمعالجة البيانات الشخصية التي صدرت الموافقة عليها"[١١٦].

- **ويثار تساؤل عن الحالات التي يتم فيها جمع بيانات شخصية تتعلق بأطفال، فهل يلزم الحصول على موافقتهم أو موافقة ذويهم؟**

تضمن القانون الفرنسي المتعلق بمعالجة البيانات والملفات والحريات، مستنداً للائحة الأوروبية لحماية البيانات النص صراحة على أن "لا تكون المعالجة قانونية لبيانات قاصر أقل من خمس عشر عاماً، إلا إذا تم الحصول موافقة من قبل القاصر أو صاحب الولاية عليه"[١١٧]. ويجوز للقاصر الموافقة بمفرده على معالجة البيانات الشخصية فيما يتعلق بالعرض المباشر لخدمات مجتمع المعلومات من سن الخامسة عشرة. على أن تتولى جهة المعالجة وضع عبارات واضحة وبسيطة، يسهل على القاصر فهمها عند إخطاره بالمعلومات المتعلقة بالمعالجة الخاصة به.

أما القانون السويدي فقد نص الفصل الثاني منه في القسم الرابع، على أنه عندما يتم تقديم خدمات مجتمع المعلومات مباشرة للأطفال الذين يعيشون في السويد، فإن معالجة البيانات الشخصية قد تستند إلى موافقة الطفل إذا كان الطفل يبلغ من العمر ١٣ عامًا أو أكبر. أما إذا كان عمر الطفل أقل من ١٣ عامًا، فلا يُسمح بمعالجة البيانات الشخصية بناءً على الموافقة صريحة من الوصي القانوني للطفل[١١٨].

---

[١١٦] المادة السابعة من النظام السعودي.

[117] Section 45 :"When the minor is under fifteen years of age, processing is lawful only if consent is given jointly by the minor concerned and the holder(s) of parental authority over that minor". (Pursuant to Article 1(8) of Regulation (EU) 2016/679 of 27 April 2016).

[118] Chapter 2, Section 4 of the Act: contains a provision which states that when information society services are offered directly to children living in Sweden, the processing of personal data may be based on a child's consent if the child is 13 years or older. If a child is below 13 years of age, the

(ISSN: 2537 - 0758)

ويتمتع الأطفال السويديون الذين تزيد أعمارهم عن ١٦ عامًا أيضًا بأهلية قانونية معينة للدخول في اتفاقات. وبالتالي، بناء على ذلك يجب أن يكون الأطفال الذين تزيد أعمارهم عن ١٦ عامًا قادرين على إعطاء الموافقة على معالجة بياناتهم الشخصية.

أما الأطفال الذين تتراوح أعمارهم بين ١٣ و١٦ عامًا، فيجب تقييم صلاحية موافقتهم على أساس كل حالة على حدة. وفيما يتعلق بالجوانب التي يجب مراعاتها أثناء هذا التقييم هي، على سبيل المثال: عمر صاحب البيانات، ومدة المعالجة، والغرض منها. يضاف إلى ذلك فمن أجل أن يفهم الأطفال بشكل صحيح ما تستلزمه معالجة بياناتهم الشخصية والسماح لاتخاذ قرار مستنير، يجب أن تكون المعلومات المتعلقة بمعالجة بياناتهم الشخصية واضحة، ويمكن الوصول إليها وسهلة الفهم من منظور الطفل.

ويتفق مع القانون السويدي ما أقرته لجنة التجارة الفيدرالية الأمريكية، بتغريم شركة EPIC games المنتجة للعبة Fortnite غرامة قدراها ٥٢٠ مليون دولار، وأيدها في ذلك حكم المحكمة الفيدرالية لشمال ولاية كالورنيا في ديسمبر ٢٠٢٢م. حيث انتهكت هذه الشركة خصوصية الأطفال وجمعت معلومات شخصية بطريقة غير مشروعة، ودون الحصول على موافقة من ذويهم. وكانت رئيسة لجنة التجارة الفيدرالية قد أوضحت أن الشركة استخدمت إعدادات افتراضية تنتهك الخصوصية، بل واستخدمت واجهات خادعة أوقعت ضحاياها من مستخدمي هذه اللعبة بما في ذلك المراهقون والأطفال[١١٩].

ثالثًا- أن يكون تجميع البيانات لغاية مشروعة:

يتعين أن يتم تجميع البيانات لتحقيق مصلحة مشروعة، فلا يسمح بمجرد تجميع معلومات عن الأشخاص بلا غاية ظاهرة. كما يجب أن يتم هذا الأسلوب بعيداً عن استخدام أساليب الغش والخداع. بل ويتعين احترام مبدأ التناسب بأن يكون تجميع البيانات بما يتماشى مع الغاية من هذا التجميع بلا تعسف أو زيادة عما يحقق تلك الغاية، بمعنى أن يكون هذا التجميع متناسباً ويحقق التوازن بين مصالح الشخص وحقوقه وحرياته.

---

processing of personal data based on consent is permitted only if consent is given or approved by the person who is the child's legal guardian.

(119) United States of America, Plaintiff, v. Epic Games, Inc. (FTC Matter/File Number 2223087), Civil Action Number 5:22-CV-00518-BO. Enforcement Type Civil Penalties Federal Injunctions. 12/19/22022. https://www.ftc.gov/legal-library

ولعل الهدف من تطلب اشتراط تجميع البيانات إلا لأغراض محددة ومشروعة؛ هو تقييد معالجة البيانات الشخصية على قدر الهدف والغاية التي تم جمعها من أجلها. فيظل هذا الهدف هو الحاكم والمقيد لكل إجراء من إجراءات معالجة البيانات من قبل جهة المعالجة(١٢٠).

بناء على ذلك؛ يلزم توافر ثلاث عناصر أساسية للقول بأن المصالح والغايات مشروعة، كي يتم الحكم على أن تجميع البيانات الشخصية للأشخاص الطبيعيين كان لأغراض مشروعة، **والتي تتمثل فيما يلي:**

- تحديد المصلحة المشروعة.
- أن تكون المعالجة ضرورية لتحقيق تلك الغاية.
- إعمال مبدأ التناسب بين مصالح الفرد وحقوقه وحرياته.

واعتبرت المادة ٧ من اللائحة الأوروبية لحماية البيانات أن المعالجة لبيانات الأشخاص الطبيعيين تكون في نطاق المشروعية، إذا توافرت حالة من الحالات الآتية(١٢١):

١- إذا وافق صاحب البيانات على معالجة بياناته الشخصية لغرض واحد أو أكثر من الأغراض المحددة والمعلن عنها صراحة له.

٢- إذا كانت المعالجة ضرورية لتنفيذ عقد، يكون أحد أطرافه صاحب البيانات، أو من أجل تنفيذ شرط أو أمر بناء على طلب صاحب البيانات قبل إبرام العقد.

٣- إذا كانت المعالجة التزاماً لأمر قانوني تخضع له جهة التحكم.

٤- إذا كانت المعالجة ضرورية لحماية المصالح الحيوية لصاحب البيانات أو لشخص طبيعي آخر.

٥- إذا كانت المعالجة ضرورية لأداء مهمة يتم تنفيذها للمصلحة العامة.

وعلى وحدة المعالجة أن تتخذ كافة التدابير الفنية والتنظيمية المناسبة لضمان معالجة البيانات الشخصية- فقط بشكل افتراضي- والتي تكون ضرورية لكل غرض محدد من المعالجة. ويجب أن تتناسب تلك التدابير مع كمية البيانات الشخصية التي تم جمعها، ومدى معالجتها، وفترة تخزينها وإمكانية الوصول إليها. وهذا يعني أن تتضمن

---

(١٢٠) أحمد كمال، "حماية البيانات الشخصية على شبكة الإنترنت"، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، المجلد ٥٢، العدد ٢، سنة ٢٠٠٩م، ص ٨٤.

(121) Regulation (EU) of the European. (Article 6): "Lawfulness of processing".

(ISSN: 2537 - 0758)

تلك التدابير بصفة أساسية عدم إتاحة البيانات الشخصية بشكل افتراضي، دون حاجة لتدخل الفرد في الحصول عليها(١٢٢).

ولكن يبدو أن الأمر على خلاف ذلك في أحكام المحكمة الأوروبية لحقوق الإنسان، وذلك عندما أصدرت حكمها في قضية P.N. v. GERMANY لسنة ٢٠٢٠م، بعدم انتهاك المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان والمتعلقة (بالحق في احترام الحياة الخاصة والأسرية والمنزل والمراسلات). وكان ذلك بمناسبة جمع العناصر التي تهدف إلى التعرف على المشتبه به، بأمر من الشرطة الألمانية– استناداً إلى قانون الإجراءات الجنائية الألماني– مثل صور الوجه وصور جسده والوشم الموجود به، فضلاً عن بصمات أصابعه؛ على أساس أن هناك إجراءات جنائية قد أقيمت ضد مقدم الطلب المشتبه فيه. مبررة ذلك بأن لديه سجلاً جنائياً، وتعتقد الشرطة أن تدابير تحديد الهوية التي أمرت بها ستيسر التحقيق في الجرائم التي ستقع في المستقبل(١٢٣).

وكانت المحكمة الإدارية قد رفضت الطعن في قرار المشتبه به، والذي تم جمع بياناته دون تحديد الغرض من ذلك بشكل واضح وصريح، واعتمد القاضي أن لديه سجلاً جنائياً سابقاً. وبموجب قانون الإجراءات الجنائية الألماني، فإنه يجوز جمع بيانات تحديد الهوية إذا كان من الممكن أن يساعد في إجراء تحقيق مستقبلي، وقضت بأن إسقاط التهم في سجل المتهم عام ٢٠١٢م، لا يحول دون هذا الجمع الذي تم في عام ٢٠١٧م. وعندما دفع مقدم الطلب بانتهاك حقوقه وفق المادة ٨ من الاتفاقية، قضت المحكمة الأوروبية بأنه لم يحدث انتهاك لتلك المادة(١٢٤).

أما القانون المصري فقد اشترط على جهة المعالجة أن يكون تجميعها للبيانات لأغراض معالجة مشروعة ولا تخالف النظام العام أو الآداب العامة. بل والالتزام بعدم تجاوز الغرض المحدد للمعالجة وبعدم التعارض مع غرض المتحكم ونشاطه. باستثناء إذا كان ذلك لغرض إحصائي أو تعليمي لا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة(١٢٥).

---

(122) Regulation (EU) of the European. (Article 25).

(123) CASE OF P.N. v. GERMANY 11/06/2020 ((Application no. 74440/17). European Court of Human Rights. https://hudoc.echr.coe.int/. Retrieved 10/12/2022.

(124) ibdi.

(١٢٥) راجع المادة ٥ من قانون حماية البيانات الشخصية المصري، خاصة ما يتعلق بالفقرات ٢، ٦.

وفيما يتعلق بموقف المنظم السعودي؛ فإنه وعلى الرغم من إقراره بعدم جواز مُعالجة البيانات الشخصية إلاَّ لتحقيق الغرض الذي جُمعت من أجله. فقد استثنى حالات معينة يجوز فيها لجهة التحكم أو المعالجة مُعالجة البيانات الشخصية لغرض آخر غير الذي جمعت من أجله، **وذلك في الأحوال الآتية**[١٢٦]:

١. إذا وافق صاحب البيانات الشخصية على ذلك.
٢. إذا كانت البيانات الشخصية متاحة للعموم، أو جرى جمعها من مصدر متاح للعموم.
٣. إذا كانت جهة التحكم جهة عامة، وكان جمع البيانات الشخصية من غير صاحبها مباشرةً، أو مُعالجتها لغرض آخر غير الذي جمعت من أجله؛ مطلوباً لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء مُتطلبات قضائية وفق الأحكام التي تحددها اللوائح .
٤. إذا كان التقيد بهذا الحظر قد يُلحق ضرراً بصاحب البيانات الشخصية أو يؤثر على مصالحه الحيوية.
٥. إذا كان جمع البيانات الشخصية أو معالجتها ضروريًّا لحماية الصحة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم. وتبيّن اللوائح الضوابط والإجراءات المتعلقة بذلك.
٦. إذا كانت البيانات الشخصية لن تُسجل أو تُحفظ في صيغة تجعل من الممكن تحديد هوية صاحبها ومعرفته بصورة مباشرة أو غير مباشرة.

رابعاً- ألا يتم الاحتفاظ بالبيانات مدد زمنية أطول من المدد المحددة للوفاء بالغرض من جمعها:

لعل من أهم الإجراءات التي استلزمتها التشريعات الجنائية المعنية بحماية البيانات الشخصية، ما يتعلق بالمدد الزمنية اللازمة للاحتفاظ بالبيانات محل الحماية، والتي بموجبها تلتزم جهات المعالجة بحفظ البيانات محل المعالجة لمدة زمنية لا تزيد على ما هو ضروري لتحقيق الغرض من جمع تلك البيانات. الأمر الذي يوجب على المعالج أن يراجع بشكل دوري البيانات المخزنة وطبيعة الهدف من جمعها. فإذا تبين له انتهاء الغرض من جمعها فيجب عليه القيام بتدميرها متى تحقق هذا الغرض ولم يعد للاحتفاظ بها أية أهداف أخرى.

[١٢٦] راجع المادة/١٠ من نظام حماية البيانات الشخصية السعودي.

(ISSN: 2537 - 0758)

وقد تضمن النص على ذلك صراحة قانون حماية البيانات الشخصية المصري، بأن أقر بألا يتم الاحتفاظ بالبيانات المعالجة لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها، على أن تتولى اللائحة التنفيذية لهذا القانون تحديد السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات[١٢٧]. وفي الحالة التي يتم الاحتفاظ بها لأي سبب من الأسباب المشروعة بتلك البيانات، يجب ألا تبقى في صورة تسمح بتحديد الشخص المعني بالبيانات، كما يجب إخطار هذا الشخص بالمدة الزمنية الأخرى اللازمة لحفظ هذه البيانات.

ولحقه المنظم السعودي بإلزام جهة المعالجة باتلاف البيانات الشخصية فور انتهاء الغرض من جمعها؛ إلا أنه أجاز الاحتفاظ بتلك البيانات بعد انتهاء الغرض من جمعها إذا تمت إزالة كل ما يؤدي إلى معرفة صاحبها على وجه التحديد وفق الضوابط التي تحددها اللائحة. ويقصد بالإتلاف كل عمل يؤدي إلى إزالة البيانات الشخصية، ويجعل من المتعذر الاطلاع عليها أو استعادتها مرة أخرى.

غير أن المنظم السعودي توسع في إجازته لجهة المعالجة الاحتفاظ بالبيانات الشخصية حتى بعد انتهاء الغرض منها في حالتين، هما[١٢٨]:

الأولى: إذا توافر مسوغ نظامي يوجب الاحتفاظ بها مدة محددة. وفي هذه الحالة يتم اتلافها بعد انتهاء هذه المدة أو انتهاء الغرض من جمعها، أيهما أطول.

الثانية: إذا كانت البيانات الشخصية متصلة اتصالاً وثيقاً بأحد القضايا المنظورة أمام الجهات القضائية، وكان الاحتفاظ بها لازماً لهذا الغرض. وفي هذه الحالة يتم تلافها بعد استكمال الإجراءات القضائية المتعلقة بتلك القضية.

أما المشرع الفرنسي فقد اتفق مع ما ورد في نصوص اللائحة الأوروبية لحماية البيانات، وأكد على أنه لا يمكن الاحتفاظ بالبيانات الشخصية إلى أجل غير مسمى، بل يجب تحديد مدة الاحتفاظ بتلك البيانات عن طريق وحدة التحكم أو وحدة المعالجة؛ وذلك اعتماداً على الغرض الذي أدى إلى جمع تلك البيانات وهو ما يعرف بمبدأ "الاحتفاظ المحدود بالبيانات الشخصية".

---

[١٢٧] فقرة ٤ من المادة ٣، قانون حماية البيانات الشخصية المصري.

[١٢٨] راجع المادة/ ١٨ من نظام حماية البيانات الشخصية السعودي.

وقد يتم تحديد المدة الزمنية اللازمة لحفظ البيانات بموجب القوانين واللوائح بالنص عليها صراحة، كما هو الحال في قانون العمل الفرنسي خاصة ما يتعلق بالمادة L ٣٢٤٣/٤ والتي أجازت لصاحب العمل الاحتفاظ بنسخة مكررة من قسيمة رواتب الموظف لمدة خمس سنوات(١٢٩). أو قد يترك الأمر لتقدير جهة المعالجة متى انتهت من الغرض من المعالجة.

- **التوفيق بين فترات الاحتفاظ والمحفوظات:**

يتم الاحتفاظ بالبيانات الشخصية طوال مدة المعالجة، لكن قد يكون لتلك البيانات استخدامات أخرى توجب الاحتفاظ بها لفترات زمنية مختلفة. الأمر الذي دعى اللجنة الأوروبية لحماية البيانات إلى التطرق لدورة حياة البيانات الشخصية، وقامت بتقسيمها إلى ثلاث مراحل متتالية على النحو الأتي(١٣٠):

المرحلة الأولى: والتي تسمى بالاستخدام الحالي أو "قاعدة البيانات النشطة": في هذه المرحلة تكون مدة الاستخدام الحالية للبيانات هي المدة اللازمة لتحقيق الغرض من المعالجة، كاستخراج شهادة ميلاد على سبيل المثال. في هذه المرحلة يمكن الوصول إلى البيانات بشكل عام على أساس يومي للموظفين القائمين على تلك المعالجة، وذلك داخل المؤسسة المسئولة عن الأحوال المدنية. في هذه الحالة الأمر متروك للشخص المسؤول عن ملف البيانات محل المعالجة، ومدى احترامه لمدة المعالجة اللازمة.

المرحلة الثانية: وهي مرحلة "الأرشفة المتوسطة" والتي تتوافق مع مدة الاستخدام الإداري: ففي بعض الأحيان قد يتم تخزين البيانات الشخصية بعد استخدامها، وتكون قاعدة تخزينها منفصلة عن قاعدة البيانات النشطة، ويكون الوصول إليها مقيد وفي حدود معينة. ولا يتم ذلك إلا إذا كان هناك التزام قانوني بالاحتفاظ بالبيانات لفترة زمنية محددة. أما في الحالة التي لا يتوافر فيها التزام بالاحتفاظ، فيلزم أن تكون هذه البيانات ذات أهمية إدارية، خاصة ما يتعلق بحالة التقاضي، وهو ما يبرر الاحتفاظ بها طوال مدة التقادم.

---

(129) Code du travail. Partie législative (Article L3243-4): “L'employeur conserves un double des bulletins de paie des salariés pendant cinq ans”.

(130) "Article: ”How to reconcile retention periods and archives?” 18 September 2019. https://www.cnil.fr/fr/comment-concilier-les-durees-de-conservation-et-les-archives. Retrieved 9 Jan 2023.

(ISSN: 2537 - 0758)

المرحلة الثالثة: وهي مرحلة الأرشفة النهائية: ويتم فيها الاحتفاظ بالبيانات والوثائق ذات الأهمية التاريخية وأرشفتها وفقاً للشروط التي تحددها القوانين. ومن أبرز الأمثلة على ذلك ما أقره قانون التراث الفرنسي، خاصة ما تضمنته المادة R٢١٢-١٣ حيث أنه وفقاً لمدونة التراث، يجوز للمحافظ تقديم إشعار رسمي للبلدية لاتخاذ التدابير المناسبة للاحتفاظ بالوثائق ذات الأهمية التاريخية المعينة والتي ثبت أن ظروف حفظها تعرضها للخطر. وإذا لم تتخذ البلدية هذه التدابير، يجوز للمحافظ أن يفرض الإيداع الإلزامي لهذه الوثائق في محفوظات الدائرة، بغض النظر عن حجم البلدية وتاريخ الوثائق(١٣١).

وبالمثل فقد تبنى القانون السويدي نفس الاتجاه (في القانون المتعلق بمسك الدفاتر لسنة SFS1999) والذي نص على أن بعض المعلومات والوثائق المالية- على سبيل المثال الفواتير- يجب الاحتفاظ بها لمدة سبع سنوات. كما أن هناك أيضًا متطلبات قانونية للاحتفاظ بالمعلومات المتعلقة بالتوظيف(١٣٢).

ويلاحظ أنه في كل مرحلة من هذه المراحل الثلاث، يجب على جهة المعالجة المسؤولة عن البيانات، توفير تدابير تقنية وتنظيمية لحماية تلك البيانات، باتخاذها تدابير أمنية تتناسب مع المخاطر وطبيعة تلك البيانات. حيث يجب عليها حمايتها من التدمير أو الفقد أو التغيير أو النشر أو الوصول غير المصرح به. كما يجب إبلاغ صاحب البيانات الذي يمارس حقه في الوصول إلى جميع البيانات المتعلقة به، سواء كانت مخزنة في قاعدة بيانات نشطة أو مؤرشفة.

وأيدت المحكمة الأوروبية لحقوق الإنسان الالتزام بحفظ البيانات محل المعالجة لمدة زمنية محددة، وظهر ذلك في حكمها الصادر في يونيو ٢٠٢٠م، في قضية GAUGHRAN v. THE UNITED KINGDOM، وإقرارها بانتهاك الحق في

---

(131) **Code du patrimoine.** (Article L212-13): Lorsqu'il s'agit de documents présentant un intérêt historique certain et dont il est établi que les conditions de leur conservation les mettent en péril, le préfet peut mettre en demeure la commune de prendre toutes mesures qu'il énumère.

- Si la commune ne prend pas ces mesures, le préfet peut prescrire le dépôt d'office de ces documents aux archives du département, quelles que soient l'importance de la commune ET la date des documents.

(132) **Swedish Bookkeeping Act (SFS 1999):** stipulates that certain financial information and documents, e.g. Invoices must be retained for seven years. There are also legal requirements to retain information related to employment.

الخصوصية؛ بسبب الاحتفاظ إلى أجل غير مسمى بملف تعريف الحمض النووي وبصمات الأصابع، وصورة رجل أدين بالقيادة في حالة سكر في أيرلندا الشمالية، وحذفت إدانته من سجله الجنائي في نهاية المهلة القانونية(١٣٣).

وخلصت المحكمة الأوروبية بالإجماع إلى حدوث انتهاك للمادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان، والمعنية بالحق في احترام الحياة الخاصة والأسرية. وبررت المحكمة رأيها بأن مدة الاحتفاظ بالبيانات المعنية لم تكن حاسمة، بل وعدم وجود ضمانات كافية. وفي القضية محل النظر، قررت السلطات الاحتفاظ ببياناته الشخصية لفترة غير محدودة من الزمن، دون مراعاة خطورة الجريمة المرتكبة أو الحاجة إلى الاحتفاظ بالبيانات المعنية لفترة غير محدودة من الزمن، ودون أن تتيح له إمكانية حقيقية للمراجعة.

كما علقت المحكمة على أن التكنولوجيا المستخدمة اليوم باتت أكثر تعقيداً مما تصورته المحاكم المحلية في هذه القضية، ولا سيما فيما يتعلق بالاحتفاظ بالصور الفوتوغرافية وتحليلها، فإنها ترى أن الاحتفاظ بالبيانات الشخصية لمقدم الطلب لا يعكس توازناً عادلاً بين المصالح العامة والخاصة.

وفي ١٠ نوفمبر لعام ٢٠٢٢م، فرضت اللجنة الوطنية لحماية البيانات CNIL غرامة قدرها ٨٠٠٠٠٠ يورو ضد شركة DISCORD INC لعدم الامتثال للعديد من التزامات اللائحة الأوروبية لحماية البيانات، لا سيما فيما يتعلق بفترات الاحتفاظ وأمن البيانات الشخصية. وDISCORD هي خدمة صوتية عبر بروتوكول الإنترنت (تقنية تسمح للمستخدمين بالدردشة عبر الميكروفون أو كاميرا الويب عبر الإنترنت) والرسائل الفورية، حيث يمكن للمستخدمين إنشاء خوادم وغرف نصوص وصوت وفيديو. هذه الخدمة تقدمها شركة DISCORD IN ومقرها الولايات المتحدة الأمريكية.

فقد انتهت اللجنة إلى ضرورة الالتزام بتحديد فترة الاحتفاظ بالبيانات المناسبة للغرض المقصود من المعالجة، وتوصلت إلى أن هناك حسابات ٢,٤٧٤,٠٠٠ للمستخدمين الفرنسيين الذين لم يستخدموا حساباتهم لأكثر من ثلاث سنوات و٥٨,٠٠٠ حساب لم يتم استخدامها لأكثر من خمس سنوات في قاعدة بيانات DISCORD. إضافة إلى تأكيد الشركة بأن ليس لديها سياسة مكتوبة للاحتفاظ بالبيانات(١٣٤).

---

(133) CASE OF GAUGHRAN v. THE UNITED KINGDOM. 13/06/2020 (Application no.45245/15). Cour européenne des droits de l'homme. Retrieved., 10 NOV 2022. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]}

(١٣٤) الموقع الرسمي للجنة الوطنية لحماية البيانات CNIL، استرجاع بتاريخ ١ديسمبر ٢٠٢٢م.

(ISSN: 2537 - 0758)

المبحث الثالث
تجريم العدوان على البيانات الشخصية المعالجة إلكترونياً

تمهيد وتقسيم:-

بعد أن بات العالم يعيش في إطار تحركه البيانات وتدفق في الاستخدامات اليومية لها، لاسيما بعد التوسع في استخدامات التطور التقني والتكنولوجي، ظهر في مقابل ذلك تحديات عديدة تتعلق بالاستخدامات غير المشروعة لتلك البيانات، والتي تمثل أضراراً على الأفراد والمؤسسات بل وعلى المجتمع بأكمله. سواء فيما يخص البيانات التي يتم معالجتها، أو المخزنة للمعالجة، أو حتى المهملة التي انتهى الغرض من معالجتها بينما مازال الاحتفاظ بها مستمراً. وقد دفع ذلك قوانين حماية البيانات والتشريعات المختلفة إلى التصدي لتلك الممارسات، وتجريم كل ما يمثل اعتداءً على ما يعد بياناً شخصياً.

ونظراً لكون جرائم الاعتداء على البيانات الشخصية من الجرائم الشكلية (جرائم الخطر) فلم نتعرض سوى للسلوك الإجرامي محل التجريم، دون الحاجة لتناول النتيجة الإجرامية، أو إثبات علاقة السببية. والركن المعنوي المتطلب توافره في هذه الجرائم، إضافة إلى تناول العقوبات التي قررتها بعض التشريعات الجنائية في مواجهة تلك الجرائم. وهو ما سنتطرق له من خلال مبحثيين على النحو التالي:

المطلب الأول: تجريم مخالفة ضوابط جمع وحفظ البيانات الشخصية والإجراءات الأولية اللازمة لحمايتها.

المطلب الثاني: تجريم الاعتداء على البيانات الشخصية ذاتها.

المطلب الأول
تجريم مخالفة ضوابط جمع وحفظ البيانات الشخصية والإجراءات الأولية اللازمة لحمايتها

تمهيد وتقسيم:-

يتبين من الطرح السابق، أن لجمع وحفظ البيانات الشخصية محل المعالجة شروط وضوابط حددتها التشريعات الجنائية المختلفة، سواء فيما يتعلق بالإجراءات الأولية اللازم على جهة المعالجة اتخاذها لحماية تلك البيانات، أو في مراحل جمعها وحفظها وإعدادها للمعالجة. لاسيما فيما يتعلق بالبيانات ذات الطبيعة الخاصة كالبيانات الحساسة أو البيانات الصحية وغير ذلك.

---

https://www.cnil.fr/fr/sanction-de-800-000-euros-lencontre-de-la-societe-discord-inc

ورتبت تشريعات حماية البيانات الشخصية جزاءات خاصة، إثر مخالفة جهة المعالجة التزاماتها سواء السابقة على عملية المعالجة (الإجراءات الأولية لعملية المعالجة) أو المتزامنة مع عملية المعالجة والمتعلقة بشروط وضوابط جمع وحفظ البيانات الشخصية، أو فيما يتعلق بالبيانات ذات الطبيعة الخاصة كالمرتبطة بالعرق أو الدين أو الصحة أو الآراء السياسية. وعليه؛ سوف نتناول بشيء من التفصيل صور الاعتداء التي قد تقع على البيانات الشخصية في تلك المراحل وعقوباتها، وذلك من خلال المطالب التالية:-

الفرع الأول: عدم اتخاذ الإجراءات والاحتياطات الأولية لإجراء معالجة البيانات.

الفرع الثاني: مخالفة الشروط الخاصة بجمع وحفظ البيانات الشخصية.

الفرع الثالث: مخالفة ضوابط معالجة البيانات ذات الطبيعة الخاصة.

الفرع الأول

عدم اتخاذ الإجراءات والاحتياطات الأولية لإجراء معالجة البيانات

أولاً: مخالفة القواعد السابقة على معالجة البيانات.

اشترطت أغلب التشريعات المعنية بحماية البيانات الشخصية ومن بينها اللائحة الأوروبية لحماية البيانات، عدد من القواعد التي يجب على جهة المعالجة اتباعها في حال القيام بمعالجة بيانات شخصية للأفراد.

فقد ألزم القانون المصري مزاول نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها، الحصول على ترخيص من مركز حماية البيانات الشخصية، وهو عبارة عن وثيقة رسمية تحدد التزامات المرخص له وتكون محددة الصلاحية، حيث حددها القانون لمدة ثلاث سنوات قابلة للتجديد لمدد أخرى.

وفرق القانون المصري بين الترخيص والتصريح، فأما عن التصريح فهو وثيقة تصدر عن مركز البيانات الشخصية للشخص الطبيعي أو الاعتباري تمنحه الحق في ممارسة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها، وكذلك التعامل عليها بأية صورة. وتحدد هذه الوثيقة التزامات المصرح له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة، وذلك لمدة مؤقتة لا تتجاوز سنة قابلة للتجديد لمدد أخرى.

تطبيقاً لذلك قضت المحكمة "بأن الأدلة التي أخذت بها المحكمة واطمأنت إليها في شأنها مجتمعة أن تحقق ما رتبه عليها من استدلال على صحة ما نسب إلى الطاعنين من استيراد أجهزة الاتصالات بدون الحصول على ترخيص من الجهة المختصة وإنشاء

(ISSN: 2537 - 0758)

شبكة اتصالات بغير ترخيص من الجهاز القومي التنظيم الاتصالات واستخدام وسائل غير مشروعة لإجراء الاتصالا، فإن ما يثيره الطاعنان بشأن تعويل الحكم المطعون فيه في الإدانة على ما أورده من التقرير الفني للجهاز القومي لتنظيم الاتصالات وما رتبه عليه لا يكون سديداً"[١٣٥].

أما القانون الفرنسي فقد تطلب في الفصل الثاني من قانون حماية المعلوماتية والحريات، وبخاصة المادة ٦١ منه– والمتضمنة الإجراءات الشكلية قبل تنفيذ عمليات المعالجة– أن تحدد اللجنة القومية للحريات نماذج للإعلانات وطلبات الآراء والمشاورات وطلبات الترخيص وتضع قائمة بالمرفقات التي يجب إرفاقها عند الاقتضاء. وتقدم الإعلانات وطلبات الرأي وطلبات الترخيص من قبل المعالج أو من يحق له تمثيله، عندما يكون المعالج شخصاً طبيعياً أو معنوياً. وترسل البيانات والطلبات إلى اللجنة إلكترونياً.

وتضمن قانون العقوبات الفرنسي النص صراحة– في القسم الخامس الوارد تحت بند انتهاكات حقوق الإنسان الناتجة عن ملفات الحاسوب أو معالجتها– تجريم حالات عدم اتخاذ الاجراءات الأولية للمعالجة في نص المادة ١٦/٢٢٦ بعقاب كل من يقوم ولو بطريق الإهمال بتنفيذ معالجة للبيانات الشخصية دون الامتثال للإجراءات الشكلية قبل تنفيذها بموجب القانون[١٣٦].

بناء على ذلك يتمثل الركن المادي في هذه الجريمة، بارتكاب جهة المعالجة سلوكاً يمثل عدم الإلتزام بإجراء المعالجة طبقاً للقواعد المنظمة لذلك والمحددة في القانون، ووفقاً للحالات المشروعة والقانونية. وبناء على التعليمات والقواعد المكتوبة والواردة إليه من مركز حماية البيانات أو من المتحكم أو من أي ذي صفة حسب الأحوال، خاصة

---

[١٣٥] الطعن رقم٦٦٧٤ لسنة٨٧ ق–جلسة ٢٠١٩/٠٤/٠٢م، والطعن رقم٣٧١٩ لسنة ٨٦ ق– جلسة٢٠٢٠/٠٧/٠٧م. المكتب الفني، المجموعة الجنائية". مجموعة المبادئ القانونية التي قررتها محكمة النقض في جرائم الاتصالات" بدون سنة نشر.

[136] **Penal code:(**Section 5: Human rights violations resulting from computer files or processing) Article 226-16: "The fact, including negligence, of carrying out or having carried out processing of personal data without having complied with the formalities prior to their implementation provided for by law is punishable by five years' imprisonment and a fine of 300,000 euros". (Amended by Ordinance No. 2018-1125 of 12 December 2018).

ما يخص عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية واتفاقها مع الأغراض المحددة للمعالجة.

ويعني ذلك أن هذه الجريمة تعد من الجرائم السلبية، كون السلوك المرتكب من جانب جهة المعالجة في هذه الحالة هو سلوك سلبي، حيث يمتنع الفاعل عن اتباع التعليمات والقواعد المخولة له حق القيام بمعالجة البيانات الشخصية للأفراد.

لذلك اعتبرت اللجنة القومية للحريات أن بيع أو تأجير البيانات الشخصية لأغراض البحث التجارية التي تتم عن طريق الوسائل الإلكترونية، يتطلب إخطار اللجنة القومية للحريات وموافقتها أولاً على هذا الاستخدام. كما يتعين على المعالج اتخاذ جميع التدابير مع مزود الخدمة لضمان عدم اعتراض أصحاب تلك البيانات، أو موافقتهم على استخدام بياناتهم لأغراض تجارية(١٣٧).

تطبيقاً لما ورد، قضت محكمة النقض الفرنسية بتأييد الحكم الصادر ضد شركة Allied Signal Industrial Fibers، التي أصبحت فيما بعد شركة Honeywell Longlaville والتي قامت بإنشاء نظام يتم إدارته بوسائل آلية ويسمح بتحديد هوية الموظفين عند دخولهم ومغادرتهم مقر الشركة، وذلك دون إبلاغ اللجنة الوطنية للمعلوماتية والحريات بإنشاء هذا النظام. وذلك على الرغم من أن الشركة بررت تصرفها بأن من حق صاحب العمل استخدام جهاز تحكم إلكتروني لدخول وخروج الموظفين شريطة إبلاغ الموظفين بذلك مسبقاً، ومع ذلك رفضت المحكمة تبرير الشركة، وانتهت إلى أنه في حال عدم وجود إخطار إلى اللجنة القومية للمعلومات والحريات بشأن المعالجة الآلية للمعلومات الشخصية للموظفين، فلا يتم إلقاء اللوم على الموظف في حال رفضه الامتثال لمتطلبات صاحب العمل(١٣٨).

وفيما يتعلق بالركن المعنوي فلم تتطلب أغلب القوانين سوى توافر القصد الجنائي العام، بعنصريه العلم والإرادة، غير أن المشرع الفرنسي ساوى بين صورتي العمد والخطأ (الإهمال) في العقوبة. والواضح أن الفارق بينهما هو مقدار سيطرة الجاني على ماديات الجريمة، ففي صورة العمد فإن الجاني يعلم بكل ماديات الجريمة وتتجه إرادته نحو

(137) Délibération n°2010-229 du 10/06/2010 dispensant de déclaration les traitements automatisés de données à caractère personnel mis en oeuvre par des organismes à but non lucratif, abrogeant et remplaçant la délibération n°2006-130 du 9 mai 2006. https://www.cnil.fr. Retrieved 03/02/2023.

(138) Cour de Cassation, Chambre sociale, du 6 avril 2004, 01-45.227, Publié au bulletin, https://www.legifrance.gouv.fr Retrieved 03/02/2023.

(ISSN: 2537 - 0758)

تحقيق نتيجتها أو حتى قبولها، وأما في صورة الخطأ غير العمدي فإنه كان يستطيع أن يتوقع النتيجة ويحول دون وقوعها، ولكنه اعتمد على احتياط وطرق غير كافية للحيلولة دون وقوع نتائجها(١٣٩).

أما إذا لم يُنسب إليه خطأ، فإن الجريمة لا تقوم عندئذ وذلك لعدم توافر الركن المعنوي. ويخالف ذلك ما سبق أن قضت به محكمة النقض الفرنسية من وقوع الجريمة بناء على النشاط فقط، ودونما تطلب للركن المعنوي. فقد اعتبرتها المحكمة من الجرائم المادية في ظل قانون العقوبات الفرنسي قبل تعديله في سنة ١٩٩٢(١٤٠). وقد سبق أن قضت المحكمة بأنه لا يلزم توافر القصد الجنائي في هذه الجريمة وبأنه لا يجدي المتهم إلاّ التمسك بالقوة القاهرة لإعفائه من المسؤولية الجنائية(١٤١).

وتتنوعت العقوبات الواردة في حق مرتكب هذه الجريمة، ففي قانون العقوبات الفرنسي تنوعت العقوبات بين الحبس لمدة خمس سنوات وغرامة ٣٠٠٠٠٠ يورو. أما القانون المصري فقد عاقب على مخالفة أحكام التراخيص أو التصاريح أو الاعتمادات المنصوص عليها في القانون بالغرامة التي لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه(١٤٢).

وقرر المشرع المصري جزاءً إدرايا ولم يخالفه المشرع الفرنسي في ذلك– مع عدم الإخلال بأحكام المسؤولية المدنية والجنائية– يتمثل في تولي مركز حماية البيانات إنذار المخالف بالتوقف عن المخالفة وإزالة أسبابها خلال فترة زمنية محددة، فإذا انقضت تلك المدة دون الإلتزام بتنفيذ مضمون الإنذار، فلمجلس إدارة المركز إصدار قرار مسبب بما يلي(١٤٣):

- الإنذار بإيقاف الترخيص أو التصريح أو الاعتماد جزئياً أو كلياً لمدة محددة.

---

(١٣٩) محمود نجيب حسني "**شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي**" دار النهضة العربية، الطبعة الثامنة، سنة ٢٠١٨م، ص ٦٨٩.

(140) Crim. 3 nov. 1987, Bull. crim. nº 382; Rev. sc. crim. 1988. 295, obs. Delmas Saint- Hilaire; J. C. P. 1988. 1. 3323.

(141) Crim 3 nov. 1987, D. 1988. J. 17, note Herbert Maisl.

(١٤٢) المادة/ ٤٥ من قانون حماية البيانات الشخصية المصري.

(١٤٣) راجع نص المادة/٣٠ من قانون حماية البيانات الشخصية المصري. كذلك نص المادة/ ٢٠ من قانون معالجة البيانات والحريات الفرنسي.

- إيقاف أو سحب الترخيص أو التصريح أو الاعتماد أو إلغاؤه جزئياً أو كلياً. وحدد القانون الفرنسي مدة انقطاع المعالجة بثلاثة أشهر.
- نشر بياناً بالمخالفات التي ثبت وقوعها في وسيلة إعلام أو أكثر على نفقة المخالف.
- إخضاع المعالج المخالف للإشراف الفني للمركز؛ لتأمين حماية البيانات الشخصية على نفقته بحسب الأحوال.
- دفع غرامة لا تتجاوز مائة ألف يورو لكل يوم تأخير من التاريخ الذي يتم فيه إنذار جهة المعالجة وعدم امتثالها، وفقاً للقانون الفرنسي. ودفع غرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه في القانون المصري(١٤٤).

يتبين من التنظيم القانوني لهذه الجريمة، أنها تقع اعتداء على المصلحة العامة التي تقتضي ضرورة اتباع إجراءات معينة قبل معالجة البيانات. ومع ذلك فإن المجني عليه في هذه الجريمة أيضاً هو الأفراد المقصودين بالمعلومات الشخصية. خاصة أن النص على الجريمة ورد في القانون الفرنسي ضمن ثنايا نصوص الفصل الخامس تحت عنوان "انتهاكات حقوق الإنسان الناتجة عن ملفات الحاسوب أو معالجتها". ويترتب على ذلك أن للفرد المقصود بالبيانات الشخصية أن يدعي مدنياً أمام القضاء الجنائي عن ضرر شخصي ومباشر. وهو ما انتهت إليه أحكام القضاء الفرنسي بالفعل(١٤٥).

ثانياً: معالجة البيانات الشخصية دون اتخاذ الاحتياطات اللازمة لإجراء المعالجة.

تطلب قانون حماية البيانات الشخصية المصري لحماية وتأمين البيانات الشخصية محل المعالجة، اتخاذ عدد من الاحتياطات الضرورية لتأمين تلك البيانات، وكان من بينها تعيين مسؤول يسمى "مسؤول حماية البيانات الشخصية"، حيث يتولى إنشاء سجل خاص بمركز حماية البيانات(١٤٦) لقيد مسئولي حماية البيانات.

---

(١٤٤) المادة/ ٢١ من القانون الفرنسي لمعالجة البيانات والحريات. المادة /٣٩ من قانون حماية البيانات الشخصية المصري.

(145) Paris 13 sept. 1996. 677. Francillon; Dr. Pénal 1996, 32.

(١٤٦) مركز حماية البيانات الوارد النص عليه في نظام حماية البيانات الشخصية المصري، هو "هيئة عامة اقتصادية تتبع الوزير المعني بشؤون الاتصالات وتكنولوجيا المعلومات، لها شخصية اعتبارية، ومقرها الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، ويهدف هذا المركز إلى

(ISSN: 2537 - 0758)

وألزم الممثل القانوني للشخص الاعتباري لأي متحكم أو معالج بتعيين موظف مختص داخل المنشأة الاعتبارية، يكون مسؤولاً عن حماية البيانات الشخصية، ويتولى هذا الأخير مسؤولية تنفيذ القواعد والأنظمة الصادرة إليه من مركز حماية البيانات، **وبصفة خاصة ما يلي:**

- إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية، ومنع اختراقها وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها.
- إخطار مركز حماية البيانات بأي خرق أو انتهاك قد يحدث للبيانات الشخصية المسؤول عنها.
- متابعة القيد والتحديث لسجل البيانات الشخصية لدى المتحكم أو المعالج، بما يضمن دقة البيانات والمعلومات المقيدة به.
- إزالة أية مخالفة تتعلق بالبيانات الشخصية يكون مسؤولاً عنها، واتخاذ الإجراءات التصحيحية تجاهها.

كما يلتزم مسؤول حماية البيانات وتابعوه لدى جهة المعالجة، باتباع واستيفاء السياسات والإجراءات التأمينية اللازمة لعدم مخالفة البيانات الشخصية وبصفة خاصة البيانات الحساسة أو انتهاكها. وفي حال إتاحة البيانات الشخصية لمتحكم أو معالج آخر خارج البلاد، يجوز ذلك بشرط إصدار ترخيص من مركز حماية البيانات متى توافرت شروط معينة من بينها، توافر المصلحة المشروعة لديهما أو لدى الشخص صاحب البيانات، ألا يقل مستوى الحماية القانونية والتقنية للبيانات لدى المتحكم أو المعالج عن الموجودة داخل البلاد[١٤٧].

حماية البيانات الشخصية وتنظم معالجتها وإتاحتها، ولها أن تضع وتطور السياسات والخطط الاستراتيجية والبرامج اللازمة لحماية البيانات الشخصية. كذلك توجيه سياسات وخطط حماية البيانات الشخصية داخل جمهورية مصر العربية، ووضع وتطبيق القرارات والضوابط والتدابير والإجراءات والمعايير الخاصة بحماية البيانات الشخصية، وكذلك اعتماد الجهات والأفراد ومنحهم التصاريخ اللازمة التي تتيح لهم تقديم استشارات في إجراءات حماية البيانات". ويتولى هذا المركز إصدار التراخيص والتصاريخ لكل من يقوم بإجراء عمليات معالجة أو حفظ أو التعامل في البيانات بما فيها الجمعيات والنقابات أو النوادي، وفيما يتعلق بوسائل المراقبة البصرية في الأماكن العامة". (راجع الفصل العاشر م/٢٦ من قانون حماية البيانات الشخصية المصري).

[١٤٧] راجع نص المادة/ ١٣ من نظام حماية البيانات الشخصية المصري.

ولم تختلف اللائحة الأوروبية لحماية البيانات عما تم ذكره في ثنايا نصوص القانون المصري، فقد تطلبت من جهة المعالجة– مع مراعاة أحدث التقنيات وتكاليف التنفيذ وطبيعة المعالجة ونطاقها ومدة الاحتفاظ بها وتوقع المخاطر بحسب شدتها واحتمالية وقوعها– اتخاذ التدابير الفنية والتنظيمية اللازمة والمناسبة لضمان معالجة البيانات الشخصية للأفراد، بما يكفل عدم إتاحة تلك البيانات للغير من غير ذي الصفة القانونية.

وفي الحالة التي يتم فيها إجراء المعالجة نيابة عن جهة التحكم، فيجب على الأخيرة استخدام جهات المعالجة التي تضمن أن تقوم بتقديم ضمانات كافية، فيما يتعلق بتنفيذ التدابير والأنظمة المناسبة التي تفي بضمان سلامة وأمن البيانات وحماية حقوق أصحابها(١٤٨). **ولكن التساؤل الآن، هل يترك لمعالج البيانات خيار الكشف عن هوية المستلمين أو فئاتهم لصاحب البيانات، أو بمعنى آخر هل لصحاب البيانات الحق في معرفة هوية المستفيدين من بياناته؟**

تلتزم جهة المعالجة بتزويد صاحب البيانات عند طلبه ذلك، بهوية المستفيدين والمستلمين لبياناته. وهو ما أكده القضاء في النمسا في قضية Österreichische Post لسنة ٢٠٢٣م، بأن لصاحب البيانات الحق في معرفة هوية المستفيدين من بياناته، ما لم يكن من المستحيل معرفة هوياتهم، ويعد هذا أمراً ضرورياً لتمكينه من ممارسة حقوقه على بياناته والتي منحها إياه القانون(١٤٩).

يضاف إلى ذلك أن اللائحة الأوروبية، أوجبت على جهة المعالجة اتخاذ إجراءات وتدابير مناسبة لضمان مستوى أمن مناسب ومستمر لحماية البيانات، والتي من بينها(١٥٠):–

---

(148) CHAPTER IV - Controller and processor. Article 28– Subcontractor:
1. Where processing is to be carried out on behalf of a controller, the controller shall only use processors who provide sufficient guarantees as to the implementation of appropriate technical and organisational measures so that the processing meets the requirements of this Regulation and ensures the protection of the rights of the data subject.

(149) Judgment of the Court (First Chamber) of 12 January 2023, (request for a preliminary ruling from the Oberster Gerichtshof– Austria)– RW v Österreichische Post AG, (Case C-154/21).

(150) Section 2 - Security of personal data. Article 32 - Security of processing:
a) pseudonymisation and encryption of personal data؛
b) means to ensure the continued confidentiality, integrity, availability and resilience of processing systems and services؛

(ISSN: 2537 - 0758)

- استخدام الأسماء المستعارة وتشفير البيانات.
- استخدام وسائل متناسبة لضمان استمرار سرية نظم وخدمات التأمين وتوافرها ومرونتها.
- إجراء اختبارات وتقييم فعالية التدابير التقنية والتنظيمية المتخذة، لضمان أمن المعالجة بصفة منتظمة.

ويراعى في هذه الحالات توقع المخاطر التي يمكن أن تشكلها المعالجة، وبصفة خاصة ما يترتب عليها من تدمير لتلك البيانات المنقولة أو المخزنة أو المعالجة أو تغييرها أو فقدانها أو إفشاؤها، سواء أتم ذلك عن طريق الخطأ أم بشكل قانوني.

بناء على ما تقدم؛ يتمثل الركن المادي في هذه الجريمة، في كل فعل من شأنه إجراء معالجة لبيانات شخصية إلكترونية، دون اتخاذ التدابير والاحتياطات اللازمة والمحددة مسبقاً وفق نصوص القوانين التي تحكم تجميع ومعالجة البيانات الشخصية للأفراد. وكذلك عدم اتخاذ جهة المعالجة التقنيات والأدوات التي تكون جديرة بحماية البيانات الشخصية سواء أثناء تخزينها أو معالجتها بما يضمن سريتها وتأمينها.

كذلك يعد سلوكاً مجرماً عدم إجراء التقييم والفحص الدوري لنظم حماية البيانات الشخصية ومنع اختراقها، وتوثيق نتائج التقييم وإصدار التوصيات اللازمة لحمايتها، بما في ذلك إمكانية توقع المخاطر التي يمكن أن تشكلها المعالجة بما فيها ما قد ينتج عن تدمير البيانات الشخصية. كذلك التقاعس عن إخطار جهة الإشراف بأي خرق أو انتهاك قد يحدث للبيانات الشخصية المسؤول عنها.

ولعل تجريم مثل هذه الصور يعد التزاماً على عاتق جهة المعالجة، ذلك أن تأمين البيانات الشخصية ووضع أنظمة حماية أولية قبل البدء في المعالجة، يعد حجر الأساس

---

c) means to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident؛

d) A procedure for regularly testing, analysing and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

-When assessing the appropriate level of security, particular account shall be taken of the risks posed by the processing, resulting in particular from the destruction, loss, alteration, unauthorised disclosure of, or unauthorised access to, personal data transmitted, stored or otherwise processed, accidentally or unlawfully.

في ضمان توفير مستوى حماية ملائم لها، مع الأخذ في الاعتبار طبيعة هذه البيانات، والأخطار التي من المحتمل أن تتصل بها.

وفيما يتعلق بالركن المعنوي لهذه الجريمة يستوي فيها القصد الجنائي أو الخطأ غير العمدي (الإهمال). وعليه قُضي بأن المجني عليه في هذه الجريمة هو من يصاب بضرر مباشر منها، بسبب عدم اتخاذ ما يلزم من إجراءات تكفل عدم مساسها بشخص الغير. لذا فإن الجريمة تقوم إذا قام مسئول بشركة ائتمان بتدوين بيانات عن شخص بوصفه من المدينين السيئيين، وترتب على عدم تدوين بيان محل الميلاد أن اختلط اسمه مع اسم شخص آخر يتشابه معه في الاسم، ويختلف معه في بيان محل الميلاد. وقد انتهى القضاء الفرنسي في هذه القضية إلى أن هذا الشخص غير المقصود أصلاً يعد مجنياً عليه ومضروراً أيضاً من الجريمة(١٥١).

كما وقضت محكمة النقض المصرية بأنه "لما كان الحكم الابتدائي المؤيد والمعدل بالحكم المطعون فيه، بيَّن واقعة الدعوى بما تتوافر به كافة العناصر القانونية للجريمة، وهي إنشاء شبكة اتصالات لتوزيع خدمة الإنترنت للغير بدون تصريح من الجهاز القومي لتنظيم الاتصالات، وإعادة بث مصنفات فنية سمعية وبصرية محمية دون إذن كتابي من صاحب الحق، والتي دان الطاعن بها وأورد علي ثبوتها في حقه أدلة سائغة من شأنها أن تؤدي إلى ما رتبه عليها، وكان ما أورده الحكم كافياً لإثبات توافر هذه الجريمة بأركانها بما فيها ركناها المادي والمعنوي، ولا يلزم أن يتحدث الحكم عنهما على استقلال متى كان فيما أورده من وقائع وظروف ما يكفي للدلالة على قيامها"(١٥٢).

ولم تختلف عقوبة هذه الجريمة في التشريع المصري عن سابقتها، بينما في القانون الفرنسي نصت المادة ٢٢٦-١٧ من قانون العقوبات الفرنسي، على معاقبة كل من يقوم بإجراء معالجة إلكترونية دون تنفيذ التدابير الفنية والتنظيمية المناسبة لضمان وحماية تلك البيانات، خاصة ما يتعلق بالمخاطر التي يمكن أن تلحق بها، بما في ذلك إتاحتها بشكل تلقائي للغير غير المصرح لهم بذلك بالسجن لمدة خمس سنوات وغرامة قدرها

(151) Manon Leblond."**Le principe d'individualisation de la peine en droit pénal français**". Droit. Université Montpellier, 2021. Français.
- Crim 19 déc. 1995; Bull. Crim. nº 387; Rev. Sc. crim.1996. 679. Francillon; Dr. Pénal 1996.

(١٥٢) أحكام محكمة النقض، الطعن رقم٦٦٧٤ لسنة ٨٧ ق-جلسة ٢٠١٩/٠٤/٠٢م، والطعن رقم٣٧١٩ لسنة ٨٦ ق – جلسة٢٠٢٠/٠٧/٠٧م. المكتب الفني، المجموعة الجنائية، "مجموعة المبادئ القانونية التي قررتها محكمة النقض في جرائم الاتصالات" بدون سنة نشر.

(ISSN: 2537 - 0758)

٣٠٠ يورو. وقرر المشرع الفرنسي نفس العقوبة في حالة لم تخطر جهة المعالجة، اللجنة الوطنية للمعلوماتية والحريات أو صاحب البيانات، بخرق البيانات الشخصية(١٥٣).

الفرع الثاني
مخالفة الشروط الخاصة بجمع وحفظ البيانات الشخصية

يعاقب على الأفعال التي تشكل مخالفة لشروط جمع وحفظ البيانات الشخصية– والتي أسلفنا الحديث عنها في الفصل الأول من بحثنا– وكذلك عدم تمكين الشخص المعني بالبيانات بممارسة حقوقه على بياناته الشخصية محل الحفظ أو المعالجة وفقاً لما تضمنته نصوص القانون. ولجميع الأشخاص المعنيين ببيانات شخصية الحق في التحكم في بياناتهم والتمتع بكامل حقوقهم عليها، لأنها ملك خاص لهم، ولا يجوز مخالفة هذا الحق إلا وفق الشروط والقيود التي حددتها القوانين. بل يجب على جهة المعالجة عند ممارستها لأحد إجراءات المعالجة ضرورة إخطار الشخص ليس فقط بإجراء المعالجة فحسب، بل بحقوقه التي له حق ممارستها على بياناته الشخصية.

وعليه تتخذ هذه الجريمة عدة صور للسلوك الإجرامي المعاقب عليه، والتي سنتناولها على النحو التالي:–

الصورة الأولى: مخالفة مشروعية الحصول على البيانات الشخصية.

لكي يتم معالجة بيانات شخصية بشكل قانوني، يجب أن تستند تلك المعالجة إلى أساس قانوني. ويتخذ السلوك الإجرامي في هذه الصورة عدة أنشطة من بينها ارتكاب غش أو احتيال أو الجمع بصورة خفية وبشكل غير مشروع لبيانات شخصية. وقد يأخذ السلوك صورة عدم الاعتداد بحق الشخص في اعتراضه على عملية المعالجة أو مخالفة حقه في المحو أو التعديل.

تطبيقاً لذلك قضت المحكمة الأوروبية لحقوق الإنسان في قضية Dragan Petrović v. Serbia. بأن تفتيش شقة مقدم الطلب، وأخذ عينة من لعابة لتحليل الحمض النووي أثناء إجراء التحقيق في جريمة قتل، لم يمثل انتهاكاً للمادة ٨ من

(153) Penal Code: Art. 226-17: "Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites aux articles 24, 25, 30 et 32 du règlement (UE) 2016/679 du 27 avril 2016 précité ou au 6° de l'article 4 et aux articles 99 à 101 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

الاتفاقية فيما يتعلق بإجراء التفتيش كونه تم بصورة قانونية ومشروعة. إلا أنها قضت بوقوع مخالفة للمادة ٨ فيما يتعلق بأخذ عينة من لعابة، لأن ذلك لم يتم وفق القانون، ومن ثم فقد شرعيته، حيث تم تنفيذ هذا الإجراء في ظل قانون سابق للإجراءات الجنائية، والذي أجاز فقط أخذ عينة دم أو إجراءات طبية أخرى، دون أن يتضمن النص على أخذ عينة من لعاب المشتبه فيه(١٥٤).

كما فرضت اللجنة الوطنية لحماية البيانات CNIL في ٢٠ نوفمبر ٢٠٢٢م غرامة مالية قدرها ٢٠ مليون يورو ضد شركة CLEARVIEW للذكاء الاصطناعي، وأصدرت أمراً بالتوقف عن جمع واستخدام بيانات الأشخاص في فرنسا دون أساس قانوني وحذف تلك التي تم جمعها بالفعل. ذلك أنها كانت تقوم بجمع الصور من مجموعة واسعة من مواقع الإنترنت– بما في ذلك وسائل التواصل الاجتماعي– كما تقوم باستخراج الصور كذلك من مقاطع الفيديو التي يمكن الوصول إليها بغض النظر عن منصات التوزيع. وتستخدم الشركة تقنية التعرف على الوجه للاستعلام عن محرك البحث والعثور على شخص من صورته. وتقوم الشركة بتسويق الوصول إلى قاعدة بياناتها لصور الأشخاص في شكل محرك بحث يمكن من خلاله البحث عن الفرد باستخدام صوره. كما تقدم الشركة هذه الخدمة لوكالات إنفاذ القانون من أجل تحديد مرتكبي الجريمة أو ضحاياها(١٥٥).

واعتبرت اللجنة أنه قد تم انتهاك اللائحة الأوروبية لحماية البيانات، حيث إن المعالجة كانت غير القانونية للبيانات الشخصية، وهذا يمثل انتهاكاً للمادة ٦ من اللائحة العامة لحماية البيانات؛ لأن جمع واستخدام البيانات البيومترية يتم دون أساس قانوني. ذلك إضافة إلى عدم مراعاة حقوق الأفراد بشكل مرض وفعال (المواد ١٢ و١٥ و١٧ من اللائحة العامة لحماية البيانات)، خاصة ما يتعلق بطلبات الوصول والاطلاع والمحو.

(154) European Court of Human Rights: Dragan Petrović v. Serbia, 14 April 2020. (application no. 75229/10). file:///C:/Users/hp/Downloads/Judgment%20Dragan%20Petrovic%20v.%20Serbia%20%20rights%20violation%20owing%20to%20DNA%20mouth%20swab%20in%20absence%20of%20clear%20law.pdf.

(155) Facial recognition: €20 million penalty against CLEARVIEW AI October 20, 2022.
https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai

(ISSN: 2537 - 0758)

الصورة الثانية: مخالفة حقوق صاحب البيانات على بياناته.

فرضت التشريعات الجنائية حماية خاصة لحقوق صاحب البيانات على بياناته محل المعالجة، ولا يمثل هذه الفرض إنشاء لتلك الحقوق، بل تأكيداً على حمايتها من أوجه الانتهاك التي قد تتعرض لها، وهو ما يعني أن النصوص التي اشتملت على حماية تلك الحقوق الوارادة بقوانين حماية البيانات الشخصية كاشفة وليست منشئة لها[١٥٦].

بناء على ذلك؛ فقد عاقب القانون المصري كل معالج امتنع دون مقتضى من القانون عن تمكين الشخص المعني بالبيانات محل المعالجة، ممن ممارسة حقوقه المنصوص عليها بموجب القانون، ولم تخالفه التشريعات الجنائية المقارنة في ذلك.

وعليه يتمثل السلوك الإجرامي في هذه الجريمة في ارتكاب سلوك سلبي، يتمثل في منع صاحب البيانات من ممارسة حق من حقوقه المقررة له على بياناته، **وتتمثل تلك الحقوق فيما يلي:**

(أ) تجميع ومعالجة البيانات الشخصية دون الحصول على موافقة صاحبها:

يقع السلوك الإجرامي في هذه الصورة بسلوك تجميع البيانات الشخصية لأحد الأفراد أو معالجتها دون سبق الحصول على موافقته. ويؤخذ في الاعتبار الحالات المستثناه من الحصول على رضاء من يتم معالجة بياناته كما في حالات حماية حياة الشخص الصحية، أو أن هناك التزام قانوني يقع على جهة المعالجة، وكذلك حالات تنفيذ عقد

---

[١٥٦] حيث قضت المحكمة الدستورية المصرية بأن "الدساتير المصرية المتعاقبة قد حرصت جميعها منذ دستور سنة ١٩٢٣م، على تقرير الحريات والحقوق العامة في صلبها، قصداً من الشارع الدستوري أن يكون النص عليها في الدستور قيداً على المشرع العادي فيما يسنه من قواعد وأحكام، وفي حدود ما أراده الدستور لكل منها من حيث إطلاقها أو جواز تنظيمها تشريعياً. فإذا خرج المشرع فيما يقرره من تشريعات على هذا الضمان الدستوري، بأن قيد حرية أو حقاً ورد في الدستور مطلقاً، أو أهدر أو انتقص من أيهما تحت ستار التنظيم الجائز دستورياً، وقع عمله التشريعي مشوباً بعيب مخالفة الدستور". الدعوى رقم ٣٧ لسنة ٩ قضائية المحكمة الدستورية العليا "دستورية"، بالجلسة العلنية المنعقدة ١٩ مايو سنة ١٩٩٠م.

- **راجع كذلك:**
- La Cour des marchés: Décision quant au fond 46/2022 du 1er avril 2022. Numéro de dossier: DOS-2020-02892. (01/04/2022). https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-46-2022.pdf

يكون أحد أطرافه صاحب البيانات كشركة الاتصالات التي تتعاقد مع أحد عملائها وتقوم بمعالجة بياناته في سبيل توصيل خدمات الإنترنت لمنزله.

ونلاحظ أنه في الحالة التي تنوي فيها وحدة المعالجة مواصلة معالجة البيانات الشخصية لغرض آخر غير الغرض الذي تم جمع البيانات الشخصية من أجله، يجب عليها في هذه الحالة تزويد صاحب البيانات بمعلومات حول الغرض الآخر وأي معلومات أخرى ذات صلة بموضوع المعالجة.

وترجع علة تجريم هذه السلوك، في الحفاظ على حرمة الحياة الخاصة للأفراد، وفي ذلك اعتبرت المحكمة أن نشر أو توزيع أو عرض صور تم التقاطها دون إذن صاحبها، لا يكون مشروعاً إلا إذا كان هذا الشخص ذو صفة رسمية أو شخصية عامة أو مشهورة محلياً أو عالمياً، أو سمحت بذلك النشر السلطات العامة في الدولة بهدف خدمة الصالح العام. في غير تلك الحالات يعد نشر صور بدون إذا وموافقة صاحبها ارتكاباً لخطأ في حقه ويثبت به توافر الضرر المادي والأدبي ويلتزم مرتكبه بالتعويض، متى ثبت حدوث ضرر، وأن الإذن بالتصوير لا يتضمن النشر والتوزيع والاستغلال إلا برضاء صريح صادر عن صاحبه[١٥٧].

ولمحكمة الموضوع سلطة استخلاص توافر الخطأ الموجب للمسئولية والضرر وعلاقة السببية بينهما، ولا رقابة عليها فى ذلك من محكمة النقض طالما جاء استخلاصها سائغًا وتبين لها الحقيقة التى اقتنعت بها وأن تقيم قضاءها على أسباب تكفى لحمله. كما أن تقدير التعويض هو من اختصاصات محكمة الموضوع وبحسب ما تراه مناسبًا مستهدية فى ذلك بكافة الظروف والملابسات فى الدعوى، ولا عليها إن هى قدرت التعويض الذى رأته مناسبًا بدون أن تبين أو ترد على ما أثاره الطاعن من ظروف. وإذا لم يكن التعويض مقدرًا بالاتفاق أو بنص القانون فإن لمحكمة الموضوع السلطة التامة فى تقديره دون رقابة عليها من محكمة النقض، ويستلزك أن يكون الحكم قد بين عناصر الضرر الذى يقدر التعويض عنه[١٥٨].

وقد تضمنت نصوص اللائحة الأوروبية لحماية البيانات خاصة ما يتعلق بالمادة ٨٢ منها، في إحالتها للمادة ٣/٥ من توجيه الخصوصية الإلكترونية، وجوب إبلاغ أي مشترك أو مستخدم لخدمة اتصالات إلكترونية بطريقة واضحة وصريحة، ما لم يتم

---

[١٥٧] الطعن رقم ٩٥٤٢ لسنة ٩١ القضائية. جلسة ١٦ من مارس سنة ٢٠٢٢م، مرجع سابق.

[١٥٨] نفس الحكم السابق.

(ISSN: 2537 - 0758)

إبلاغه بها مسبقاً، من قبل جهة المعالجة خاصة ما يتعلق بالغرض من المعالجة، كي يتمكن من حقه في الوصول والاطلاع، إضافة إلى إخطاره بالوسائل المتاحة لمعارضتها. ولا يجوز أن يتم هذا الوصول أو التسجيل إلا بشرط أن يكون المشترك أو المستخدم قد أعرب بعد تلقي هذه المعلومات عن موافقته، والتي قد تنتج عن المعلمات المناسبة لجهاز الاتصال الخاص به أو أي جهاز آخر تحت سيطرته[١٥٩].

تطبيقا لذلك فرضت اللجنة الوطنية لحماية البيانات CNIL في ٦ يناير ٢٠٢٢م، غرامة مالية قدرها ١٥٠ مليون يورو ضد شركة google و٦٠ مليون يورو ضد شركة FACEBOOK، لعدم الامتثال لأحكام اللائحة العامة لحماية البيانات. حيث قامت المواقع الإلكترونية google.fr, facebook.com, youtube.com. بإنشاء زر لقبول ملفات تعريف الارتباط على الفور. ولم بتم إنشاء زر أخر يسمح للمستخدم برفض إيداع ملفات تعريف الارتباط بسهولة. بل كان الأمر يحتاج إلى النقر عدة نقرات لرفض جميع ملفات تعريف الارتباط، مقارنة بنقرة واحدة فقط لقبولها. هذه العملية تنتهك حرية الموافقة وتشكل انتهاكاً للمادة ٨٢ من اللائحة العامة لحماية البيانات[١٦٠].

(ب)انتهاك حق صاحب البيانات في الاعتراض على معالجة بياناته:

أكدت تشريعات حماية البيانات الشخصية على حق صاحب البيانات في الاعتراض على معالجة البيانات المرتبطة به أو نتائجها متى تعارضت مع حقوقه وحرياته الأساسية. ويكون للأفراد الحق في الاعتراض في أي مرحلة تكون عليها بياناتهم، فقد يتم الاعتراض في مرحلة جمع البيانات وذلك برفضهم الإفصاح عنها، أو في مرحلة المعالجة والنقل بأن يفصح الفرد برفضه نقل بياناته إلى جهة أخرى على سبيل المثال. ويعد مخالفة ذلك سلوكاً إجرامياً معاقباً عليه، ويستثنى من تطبيق ذلك المعالجة التي تتم امتثالاً للقانون ولم توجد أسباب مشروعة للاعتراض.

---

(159) Deliberation of the restricted formation n ° SAN-2022-027 of December 29, 2022 concerning the companies TIKTOK INFORMATION TECHNOLOGIES UK LIMITED and TIKTOK TECHNOLOGY LIMITED. (Commission Nationale de l'Informatique et des Libertés-Deliberation SAN-2022-027 of December 29, 2022).
https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046977994?init=true&page=1&query=SAN-2022-027&searchField=ALL&tab_selection=all

(160) Cookies: the CNIL fines GOOGLE €150 million and FACEBOOK €60 million for non-compliance with the law 06 January 2022.
https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions

تطبيقاً لذلك قضت المحكمة الأوروبية لحقوق الإنسان في قضية L.B. v. Hungary لسنة ٢٠٢٣م. بانتهاك المادة ٨ من الاتفاقية؛ فيما يتعلق بنشر البيانات الشخصية لدافعي الضرائب المحكوم عليهم، من خلال نشر أسماء وعناوين منازلهم على قائمة "كبار الممولين" على الموقع الإلكتروني لمصلحة الضرائب. حيث رأت المحكمة عدم التوازن بين المصلحة العامة في ضمان الانضباط الضريبي وحقوق الخصوصية للأفراد، ودون الأخذ في الاعتبار خطر إساءة استخدام الجمهور لعنوان منزل الممول والاعتداء على حقه في الاعتراض(١٦١).

(ج) حق صاحب البيانات في الوصول والاطلاع على بياناته:

إن إعمال الحق في الاطلاع، لا يتوافر إلاّ إذا تعلق الأمر بمعلومات شخصية تتعلق بالفرد. ويتمثل السلوك الإجرامي في هذه الصورة في تطلب إحاطة صاحب البيانات علماً بالمسوغ القانوني لجمع بياناته الشخصية، والغرض من تلك المعالجة. ومنعه من ممارسة حقه في الوصول إلى بياناته والاطلاع عليها وحقه في تصحيحها ومحوها.

تطبيقاً لذلك قضت محكمة Royal Court of Justice, Strand, London. وقد تعلق الأمر بشكوى قدمها Durant إلى أحد البنوك، وعندما لم ينل إجابة مرضية لشكواه قدم شكوى أخرى للجهة المشرفة على البنوك وهي Financial Service Authority FSA)) وفقاً لقانون ١٩٩٨ في بريطانيا، والذي يسمح للأفراد بالاطلاع على بياناتهم الشخصية. وقد رفضت الجهة المشرفة على البنوك إطلاع الشاكي على شكواه والإجراءات التي اتخذت في مواجهته، إلا أنه طعن في قرارها أمام المحكمة باعتبار أن من حقه الاطلاع على ما يخصه من بيانات شخصية. وقد أيدت المحكمة في هذه القضية موقف الجهة المشرفة باعتبار أن الأمر لا يتعلق ببيانات شخصية يمكن أن

(161) L.B. v. Hungary, 09.03.2023, (application no. 36345/16). European Court of Human Right. Retrieved 2 April 2023.
file:///C:/Users/hp/Downloads/Grand%20Chamber%20judgment%20L.B.%20v.%20Hungary%20%20systematic%20publishing%20of%20tax%20debtors%E2%80%99%20personal%20data%20breached%20the%20Convention.pdf.

(ISSN: 2537 - 0758)

تتعلق بشخصه أو بحياته الخاصة، وأن الأمر لا يتعلق ببيانات مبرمجة ولا بيانات يدوية يمكن أن تسري عليها أحكام القانون سابق الذكر[١٦٢].

واستندت المحكمة في حكمها إلى أن البيانات الشخصية التي يسمح لصاحبها الاطلاع عليها، يتعين أن تجتمع فيها الشروط التالية: ١- أن تتعلق بالأشخاص، ٢- أن تكون مرتبة بطريقة أوتوماتيكية وفقاً لمعايير معينة مثل الاسم، السن، الحالة الوظيفية، الحالة الاجتماعية، إلخ... ٤- وأن تكون من اليسير الرجوع إليها في ظل المعايير السابقة.

وبتطبيق هذه المعايير على موقف السيد Durant خلصت المحكمة إلى أن الأمر يتعلق بطلب المدعي الاطلاع على الشكوى وما اتخذ فيها من قرارات لتعزيز موقفه في مواجهة البنك، ولم يكن الأمر متعلقاً ببيانات شخصية تم تجميعها وفقاً للمعايير السابقة ومن ثم فإن المدعي ليس له الحق في الاطلاع.

أما فيما يتعلق بالركن المعنوي لصور الجرائم آنفة الذكر، فتتطلب القوانين توافر القصد الجنائي العام بعنصريه العلم والإرداة، بأن يعلم الجاني أن إجراء تجميع البيانات ومعالجة يتم دون الإلتزامات المفروضة على جهة المعالجة أثناء عملية التجميع والمعالجة، وكذلك أنه يعلم بعدم تمكين صاحب البيانات من ممارسة حقوقه المقررة له قانوناً على بياناته، وتتجه إرادته إلى إتيان هذا الفعل وتحقيق نتيجته.

وقد نص المشرع المصري على عقوبة تلك الأفعال في المادتين ٣٧ و٣٨ من قانون حماية البيانات الشخصية، بقوله "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، كل حائز أو متحكم أو معالج امتنع دون مقتضى من القانون، عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه المنصوص عليها في المادة ٢ من هذا القانون. ويعاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة ٣ من هذا القانون". "ويعاقب بغرامة لا تقل عن ٣٠٠ ألف جنيه ولا تجاوز ٣ ملايين جنيه، كل

(162) Royal Courts of Justice Strand, London. THE EDMONTON COUNTY COURT: Durant v Financial Services Authority, 8 Dec 2003. (Case No: B2/2002/2636).
https://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf.

متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في المواد ٤- ٥- ٧ من هذا القانون".

أما المشرع الفرنسي فقد عاقب على تلك الأفعال في مواده من ٢٢٦-١٦ إلى ٢٢٦-٢٢-٢. خاصة ما يتعلق بعقوبات السجن لمدة ٥ سنوات وغرامة ٣٠٠ يورو، لأي شخص يحتفظ ببيانات شخصية في وقت تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة، بهدف تحويل هذه المعلومات عن غرضها المحدد في النص التشريعى أو القانون التنظيمى أو قرار اللجنة الوطنية للمعلوماتية والحريات الذي يأذن بالمعالجة الآلية، أو من خلال الإخطارات قبل تنفيذ هذه المعاملة(١٦٣). وقرر نفس العقوبة في حالات جمع البيانات الشخصية بوسائل أو غير قانونية(١٦٤).

وأجاز في جميع الأحوال للجنة الوطنية للمعلوماتية والحريات إصدار أمر بمحو كل أو جزء من البيانات الشخصية الخاضعة للمعالجة، والتي تعرضت لانتهاك(١٦٥).

الفرع الثالث

مخالفة ضوابط معالجة البيانات ذات الطبيعة الخاصة

تضمنت المادة ٦ من قانون حماية المعلوماتية والحريات الفرنسي والمعدلة بموجب الأمر (رقم ٢٠١٨-١١٢٥ المؤرخ ١٢ ديسمبر ٢٠١٨م)، النص على أنه "يحظر

(163) **Code penal**:" Section 5 - Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques: Art. 226-21: "Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

(164) Art. 226-18: "Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende".

(165) Art. 226-23: "Dans les cas prévus aux articles 226-16 à 226-22-2, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné. Les membres et les agents de la Commission nationale de l'informatique et des libertés sont habilités à constater l'effacement de ces données".

(ISSN: 2537 - 0758)

معالجة البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية لشخص طبيعي، أو معالجة البيانات الجينية أو البيانات البيومترية لغرض تحديد هوية الشخص الطبيعي بشكل فريد، أو البيانات المتعلقة بالصحة أو البيانات المتعلقة بالحياة الجنسية للشخص أو توجهه الجنسي"[١٦٦]. ولم يخالفه في ذلك التشريعات الجنائية التي عنيت بحماية البيانات الشخصية كالتشريع المصري[١٦٧]، والتشريع الإنجليزي والتشريع السويدي، والنظام السعودي[١٦٨].

وتندرج هذه البيانات تحت مسمى "البيانات الحساسة"، والتي حظرت تشريعات حماية البيانات معالجتها، إلا **إذا توافرت حالة من الحالات الآتية:**

- صدور موافقة صريحة من صاحب البيانات– من الأفضل أن تكون الموافقة في شكل كتابي–، وصادرة عنه بإرادته الحرة والصريحة.
- إذا تم نشر تلك المعلومات بشكل صريح من قبل صاحب البيانات.

---

(166) Article 6 :"Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique" (Modifié par Ordonnance n°2018-1125 du 12 décembre 2018).

[١٦٧] ورد مفهوم البيانات الحساسة ضمن ثنايا قانون حماية البيانات الشخصية المصري بأنها "البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة".

[١٦٨] عرفت المادة الأولى من نظام حماية البيانات الشخصية السعودي البيانات الحساسة بأنها "كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو أصله القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية. وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو البيانات الصحية، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما".

- إذا كان نشر هذه البيانات ضروري لحماية حياة الإنسان.
- إذا كان استخدامها مبررًا بالمصلحة العامة وتم إصدار إذن بذلك من الجهة صاحبة الصلاحية بذلك.
- إذا تعلقت البيانات بأعضاء أو أتباع جمعية أو منظمة سياسية أو دينية أو فلسفية أو سياسية أو نقابية.

كما تضمن القانون الفرنسي النص صراحة على أنه، لا يجوز معالجة البيانات الشخصية المتعلقة بالأحكام الجنائية أو الجرائم أو التدابير الأمنية ذات الصلة إلا من خلال جهات معينة تضمنها القانون صراحة[١٦٩].

بناء على ما تقدم، يتمثل الركن المادي في هذه الجريمة في مخالفة ضوابط معالجة البيانات الحساسة، كالمعلومات المتعلقة بالأصل العنصري للشخص أو بآرائه السياسية أو الدينية أو الفلسفية أو تتعلق بانتماءاته النقابية أو أخلاقياته العامة، إذا حدث ذلك بدون موافقة صريحة من صاحب الشأن.

---

[١٦٩] **تتمثل هذه الجهات كالأتي:-**

(١) المحاكم والسلطات العامة والأشخاص الاعتباريون الذين يديرون خدمة عامة، ويتصرفون في إطار صلاحياتهم القانونية، بما في ذلك الأشخاص الاعتباريون بموجب القانون الخاص الذين يتعاونون في الخدمة العامة للعدالة، وينتمون إلى فئات تحدد قائمتها بموجب مرسوم صادر عن مجلس الدولة، وذلك بعد رأي مسبب ومنشور من اللجنة الوطنية للمعلوماتية والحريات، بالقدر اللازم للمهام الموكولة إليهم.

(٢) مساعدو جهات العدالة، لتلبية الاحتياجات الصارمة لممارسة المهام الموكلة إليهم بموجب القانون.

(٣) الأشخاص الطبيعيون أو الاعتباريون، لتمكينهم من إعداد وممارسة ومتابعة الإجراءات القانونية عند الاقتضاء، كضحية أو متهم أو نيابة عنهم وإنفاذ القرار الصادر بحقهم، لفترة تتناسب مع الأغراض المحددة. مع مراعاة أنه لا يمكن الاتصال بطرف ثالث إلا في ظل نفس الظروف وبالقدر الضروري للغاية لتحقيق تلك الأغراض.

(٤) الأشخاص الاعتباريون المذكورون في المادتين L.321-1 وL.331-1 من قانون الملكية الفكرية، الذين يتصرفون بموجب الحقوق التي يديرونها أو نيابة عن ضحايا انتهاكات الحقوق المنصوص عليها في الكتاب الأول والثاني والثالث من نفس القانون، لغرض ضمان الدفاع عن هذه الحقوق.

(٥) إعادة استخدام المعلومات العامة الواردة في القرارات المذكورة في المادة L.10 من قانون القضاء الإداري، والمادة L.111-13 من قانون التنظيم القضائي، شريطة ألا يكون للمعالجة المنفذة غرض أو إمكانية السماح بإعادة تحديد هوية الأشخاص المعنيين.

(ISSN: 2537 - 0758)

وترجع العلة من ذلك في استبعاد أي تمييز ممنهج ضد الأشخاص، بما يهدد الحق في المساواة في حرية الفكر والمعتقد والعقيدة والدين، ومن ثم يحظر معالجة تلك البيانات من قبل أي جهة من الجهات غير المخولة قانوناً، وفي حدود اختصاصها معالجتها. وساوى القانون الفرنسي في هذه الجريمة بوقوع السلوك الإجرامي على البيانات المعالجة إلكترونياً والمعالجة غير الآلية للبيانات، حتى ولو لم يقتصر تنفيذها على ممارسة الأنشطة الشخصية فقط[١٧٠].

بل واعتبر القانون المصري لحماية البيانات الشخصية أنه في جميع الأحوال، تعد بيانات الأطفال بيانات حساسة لا يجوز معالجتها إلا بموافقة المعني بذلك. بل وتوسع المنظم السعودي واشتمل في تجريمه، البيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما وكذلك البيانات الوراثية كتحليل الحمض النووي.

وفيما يتعلق بالركن المعنوي لجريمة معالجة البيانات ذات الطبيعة الحساسة، فإنه يتحقق بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، أي أن القائم بالمعالجة يعلم بكونها بيانات شخصية حساسة وتتم المعالجة دون موافقة صاحبها أو السلطات المخولة قانوناً بالموافقة، وتتجه إرادته نحو ارتكاب هذا الفعل.

بينما تطلب المنظم السعودي قصداً جنائياً خاصاً إلى جانب القصد الجنائي العام، لإخضاع مثل هذه الصورة للعقاب، وهو ما يستفاد من نص التجريم الوارد بالمادة ٣٥ من نظام حماية البيانات بقوله "إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية". كالإضرار بسمعته أو ماله أو شرفه، أو تحقيق منفعة شخصية سواء أكانت مادية أو أدبية.

ويعاقب المشرع الفرنسي وفق المادة ١٩/٢٢٦– فيما عدا الحالات المستثناه من تطبيق هذا النص والمنصوص عليها ضمن المادة ٦ من قانون حماية المعلوماتية والحريات الفرنسي– كل من يقوم بإجراء معالجة بوضع أو حفظ في ذاكرة إلكترونية، دون موافقة صريحة من الشخص المعني، خاصة ما يتعلق بالبيانات الشخصية التي تكشف بشكل مباشر أو غير مباشر، عن الأصول العرقية أو الإثنية، أو الآراء السياسية أو الفلسفية أو الدينية، أو العضوية النقابية للأشخاص، أو التي تتعلق بالصحة أو

(170) Art. 226-19: "Les dispositions du présent article sont applicables aux traitements non automatisés de données à caractère personnel dont la mise en œuvre ne se limite pas à l'exercice d'activités exclusivement personnelles".

التوجه الجنسي أو الهوية الجنسية، بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠٠٠٠ يورو.

وفي الحالات التي يتم فيها معالجة البيانات الشخصية لغرض البحث في مجال الصحة، يعاقب القانون الفرنسي وفق المادة ٢٢٦-١٩-١ بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠٠٠٠ يورو إذا تمت المعالجة في الحالات الآتية[١٧١]:

١- دون إخطار فردي مسبقًا للأشخاص الذين يتم جمع بياناتهم، أو نقلها نيابة عنهم، بحقهم في الوصول والتصحيح والاعتراض، وطبيعة البيانات المرسلة والمتلقين لها.

٢- في حالة معارضة الشخص المعني، أو في حالة عدم وجود موافقة مستنيرة وصريحة من الشخص المعني. أو في حالة الشخص المتوفى على الرغم من الرفض الذي أعرب عنه خلال حياته.

أما القانون المصري فتنوعت عقوباته بين الحبس والغرامة، حيث قضت المادة ٤١ بعقاب كل معالج جمع أو أتاح أو تداول أو عالج أو أفشى أو خزن أو نقل أو حفظ بيانات شخصية حساسة، وكان ذلك بدون موافقة الشخص المعني بالبيانات، أو في غير الأحوال المصرح بها قانوناً، بالحبس مدة لا تقل عن ثلاثة شهور وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز خمسة ملايين جنيه، أو بإحدى هاتين العقوبتين.

وعاقب المنظم السعودي "كل من أفصح عن بيانات حساسة أو نشرها مخالفاً أحكام النظام: يعاقب بالسجن مدة لا تزيد على سنتين وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية"[١٧٢].

---

[171] Art. 226-19-1: En cas de traitement de données à caractère personnel ayant pour fin la recherche dans le domaine de la santé, est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende le fait de procéder à un traitement:

1° Sans avoir préalablement informé individuellement les personnes sur le compte desquelles des données à caractère personnel sont recueillies ou transmises de leur droit d'accès, de rectification et d'opposition, de la nature des données transmises et des destinataires de celles-ci؛

2° Malgré l'opposition de la personne concernée ou, lorsqu'il est prévu par la loi, en l'absence du consentement éclairé et exprès de la personne, ou s'il s'agit d'une personne décédée, malgré le refus exprimé par celle-ci de son vivant.

[١٧٢] راجع المادة ٣٥ من نظام حماية البيانات الشخصية السعودي.

(ISSN: 2537 - 0758)

- موقف المحكمة الأوروبية لحقوق الإنسان من معالجة البيانات على أساس التمييز:

قضت المحكمة الأوروبية لحقوق الإنسان في قضية Heinz Huber v Deutschland Bundesrepublik. بأنه وعلى الرغم من أن حق الإقامة لمواطن من الاتحاد الأوروبي في دولة عضو ليس من رعاياها، غير مشروط ولكنه يحكمه قيود معينة، فإن الاختلاف في المعاملة بين هؤلاء المواطنين ومواطني الاتحاد بسبب المعالجة المنهجية للبيانات الشخصية المتعلقة فقط بمواطني الاتحاد بغية مكافحة الجريمة، يشكل تمييزاً محظوراً بموجب المادة/ ١٢ (١) من الاتحاد الأوروبي[١٧٣]. وقد تعلق ذلك الأمر بطلب المدعي Heber وهو مواطن نمساوي مقيم في ألمانيا، حذف بياناته من السجل المركزي للأجانب(AZR)، والمتعلقه(باسمه، مكان ميلاده، جنسيته، جنسه، حالته الاجتماعية، وغير ذلك من البيانات)، والتي تم استخدامها لأغراض إحصائية وفي ممارسة أجهزة الأمن والشرطة والسلطات القضائية لصلاحيتها فيما يتعلق بالأنشطة التي تهدد الأمن العام، ونتيجة لذلك تم تعريضه للتمييز على أساس الجنسية.[١٧٤]

ولكن المحكمة اعتبرت أن تخزين ومعالجة البيانات الشخصية، التي تحتوي على معلومات شخصية فردية في مثل هذا السجل للأغراض الإحصائية، ليس ضرورياً بالمعنى المقصود لمفهوم الضرورة الوارد في نص المادة e/٧ من التوجيه الأوروبي لحماية البيانات.

وفي الحالات التي يتم فيها الاستناد إلى استخدام البيانات الواردة في السجل لأغراض مكافحة الجريمة، فيتم ذلك بغض النظر عن جنسية مرتكبيها. كما أن ما يتعلق بالدولة العضو فليس من المقبول أن يكون وضع مواطنيها فيما يتعلق بمكافحة الجريمة

---

[١٧٣] تضمنت المادة ١٢/(١) المفوضية الأوروبية منع قيام دولة عضو بغرض مكافحة الجريمة، بوضع نظام لمعالجة البيانات الشخصية الخاصة بمواطني الاتحاد الذين ليسوا من مواطني تلك الدولة العضو.

[174] Judgment of the Court (Grand Chamber) of 16 December 2008. Heinz Huber v Bundesrepublik Deutschland. Case C-524/06. European Court Reports 2008 I-09705. Retrieved 14/03/2023. https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62006CJ0524.

مختلفاً عن حالة مواطني الاتحاد الذين ليسوا من مواطني تلك الدولة العضو ويقيمون في أراضيها.

أما الحكم الصادر في سبتمبر ٢٠٢٢م، في قضية **Drelon c. France**. فقد انتهت المحكمة الأوروبية إلى أن جمع وتخزين البيانات الشخصية المتعلقة بنتائج إجراءات المرشحين للتبرع بالدم، وإن كان يساهم في ضمان النقل الآمن وضرورياً لحماية الصحة العامة، إلا أن التدخل في الخصوصية؛ يجب أن ينص عليه القانون، وأن يكون ضرورياً ومتناسباً مع الهدف المنشود من المعالجة، خاصة وإن كان يتعلق بحساسية البيانات المخزنة[١٧٥].

وكان ذلك حينما اتخذت الحكومة الفرنسية تدابير خاصة بالرجال الذين مارسوا الجنس مع أطراف من نفس النوع، لمجرد رفض أحدهم (مقدم الطلب) الإجابة عن التساؤل المتعلق بحياته الجنسية. ورأت المحكمة أنه من غير المناسب جمع بيانات شخصية تتعلق بممارسات وتوجهات جنسية على أساس التخمين أو الافتراض فقط. فكان يكفي من أجل تحقيق الهدف المبتغى من ضمان سلامة الدم وحماية الصحة العامة، اعتبار رفض مقدم الطلب الإجابة على الأسئلة المتعلقة بحياته الجنسية يبرر رفضه بالتبرع بالدم.

وعليه قررت المحكمة انتهاك المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان، ومطالبة فرنسا بدفع مبلغ ٣٠٠٠ يورو لمقدم الطلب مقابل الأضرار غير المادية التي لحقت به.

في ذلك يلاحظ أن المحكمة الأوروبية لحقوق الإنسان، تطلب شروطاً لتخزين ومعالجة البيانات– لاسيما البيانات الحساسة–، **تتمثل فيما يلي:**

- أن تكون البيانات محل المعالجة محددة ودقيقة ومحدثة.
- أن تكون كافية وذات صلة، ولا تتجاوز الغرض من المعالجة.
- ألا تتجاوز فترة الاحتفاظ بها المدد الزمنية المحددة قانوناً، باستثناء حالات الضرورة.
- موافقة صاحب البيانات على إجراء معالجتها.

(175) European Court of Human Rights: (Drelon c. France - 3153/16 et 27758/18 Arrêt 8.9.2022 [Section V]). Septembre 2022. Retrieved 14/03/2023. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13775%22]}

(ISSN: 2537 - 0758)

المطلب الثاني
تجريم الاعتداء على البيانات الشخصية ذاتها

تمهيد وتقسيم:-

تعد هذه الصور من الجرائم الماسة بالبيانات الشخصية أشد خطورة من سابقتها، لأنها تمثل اعتداء على حرمة الحياة الخاصة. حيث تضمنت المادة ١٢ من الإعلان العالمي لحقوق الإنسان النص صراحة على أن "لا يجوز تعريض أحد للتدخل التعسفي في خصوصياته، شؤونة العائلية، المنزلية، أو مراسلاته ولا المساس بشرفه وسمعته، فكل الأشخاص لهم حق حماية القانون لهم ضد التدخلات أو الانتهاكات". ولا يتم ذلك إلا في ظل قيود وضوابط تحددها القوانين المعنية. وعليه سوف نتناول هذا المطلب من خلال ثلاثة فروع على النحو التالي:

الفرع الأول: معالجة البيانات الشخصية بطريقة تنافي الغرض من جمعها.

الفرع الثاني: إفشاء البيانات الشخصية إلى شخص غير ذي صفة قانونية.

الفرع الثالث: الاستغلال غير المشروع للبيانات الشخصية أو التهديد به.

الفرع الأول
معالجة البيانات الشخصية بطريقة تنافي الغرض من جمعها

تطلبت قوانين حماية البيانات الشخصية– كما سبق وأسلفنا– التزامات عديدة تقع على عاتق جهة المعالجة، من أهمها تحديد الغرض من المعالجة مسبقاً. وكان الهدف من تطلب اشتراط تجميع البيانات لأغراض محددة ومشروعة؛ هو تقييد معالجة البيانات الشخصية على قدر الهدف والغاية التي تم جمعها من أجله. فيظل هذا الهدف هو الحاكم والمقيد لكل إجراء من إجراءات معالجة البيانات من قبل جهة المعالجة.

وأوضحنا أنه يشترط تجميع البيانات الشخصية لأغراض مشروعة، وأن يتم تحديد المصلحة المشروعة، وأن تكون المعالجة ضرورية لتحقيق تلك الغاية. فضلاً عن إعمال مبدأ التناسب بين مصالح الفرد وحقوقه وحرياته وبين الغرض الذي تمت المعالجة لأجله، والذي يكون محدداً أثناء الموافقة الصادرة من صاحب البيانات على معالجة بياناته.

لذلك؛ جرم قانون العقوبات الفرنسي الأفعال التي تمثل تغيير للغرض من جمع البيانات بقوله "يعاقب كل شخص يمتلك بيانات شخصية أثناء تسجيلها أو تصنيفها أو نقلها أو أي شكل آخر من أشكال المعالجة، بتغيير هذه البيانات من غرضها على النحو

المحدد في النص التشريعي أو اللائحة التنظيمية أو قرار اللجنة الوطنية، أو موافقته بالمعالجة الآلية، أو بإلإعلان المسبق لتنفيذ هذه المعالجة....."[١٧٦].

ويتمثل السلوك الإجرامي في هذه الجريمة، بمجرد تغيير الغاية التي جمعت من أجلها البيانات، والخروج عن الهدف الأساسي من المعالجة. ففي هذه الحلة تحصل جهة المعالجة على بيانات الأشخاص بطريق مشروع، وبمحض إرادتهم وموافقتهم على إجراء المعالجة على بياناتهم، ثم بعد ذلك تقوم باستخدامها في غايات لم يتم الاتفاق عليها مسبقاً، سواء أكانت مشروعة أم غير مشروعة.

لذلك قضي بأن قيام الشركة بنشر عناوين البريد الإلكتروني المرتبطة بالعاملين بها، وذلك خارج نطاق العمل، يعد معالجة غير مشروعة للبيانات الشخصية ولا تتلاءم مع الهدف من جمع عناوين البريد الإلكتروني الخاص بالموظفين، والذي كان غرضها في الأساس تداول هذه العناوين بهدف تسهيل العمل بين العاملين في الشركة[١٧٧].

كذلك يعد معالجة غير مشروعة ما يتعلق بجمع البيانات الشخصية لأغراض تنبؤية، وهو ما ورد في رأي المحام العام في قضية Ligue des droits humains v Conseil des ministre لسنة ٢٠٢٢م. بقوله كيف يمكن تطبيق التوازن بين الفرد والمجتمع أثناء تجميع البيانات الشخصية، خاصة عندما مكنت التقنيات الرقمية من جمع وتخرين ومعالجة وتحليل كميات هائلة من البيانات الشخصية لأغراض تنبؤية. فإذا كان الهدف هو تعزيز وحماية المصالح الأساسية للمجتمع ومكافحة الإرهاب ومنع الجريمة لاسيما الجرائم الخطيرة، فإنه ينبغي إعمال التوازن بين مصالح المجتمع وحقوق

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

(177) Tribunal de grande instance de Paris 3ème chambre, 2ème section 25 avril 2003.

(ISSN: 2537 - 0758)

الأفراد، وتطبيق الضمانات الكافية لعدم الإخلال بضمانات حماية بيانات الأفراد، ومن بينها أية تجاوزات تتعلق بمعالجة تلك البيانات[١٧٨].

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

وبناء عليه، عاقب المشرع الفرنسي كل من ارتكب هذا الفعل، بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠٠٠٠ يورو. أما المشرع المصري فقد عاقب بموجب المادة ٣٨ من قانون حماية البيانات الشخصية عن تلك الأفعال بالغرامة التي لا تقل عن ٣٠٠ ألف جنيه ولا تجاوز ٣ ملايين جنيه، كل متحكم أو معالج لم يلتزم بواجباته المنصوص عليها في القانون، والتي من بينها الالتزام أثناء المعالجة بالغرض المحدد مسبقاً من المعالجة.

الفرع الثاني
إفشاء البيانات الشخصية إلى غير ذي صفة قانونية

تضمن النص على هذه الجريمة صراحة قانون حماية البيانات الشخصية المصري في مادته ٣٦، وذلك عندما أقر معاقبة كل حائز أو متحكم أو معالج للبيانات الشخصية جمع أو عالج أو أفشى أو أتاح أو تداول بيانات شخصية معالجة إلكترونياً، بأي وسيلة من الوسائل، دون تصريح قانوني بذلك، أو بدون موافقة صاحبها. وعرف المنظم السعودي الإفصاح بأنه "تمكين أي شخص– عدا جهة التحكم أو جهة المعالجة بحسب الأحوال– من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض"[١٧٩].

أما قانون العقوبات الفرنسي، فقد تضمنت المادة ٢٢/٢٢٦ عقاب كل شخص يقوم أثناء نقله أو معالجته أو تصنيفه أو بأي شكل من أشكال المعالجة، بالإفصاح عن تلك

(178) CONCLUSIONS DE L'AVOCAT GÉNÉRAL M. GIOVANNI PITRUZZELLA. Ligue des droits humains v Conseil des ministre (Affaire C-817/19)27 janvier 2022.

(١٧٩) المادة الأولى من نظام حماية البيانات الشخصية السعودي والمعدلة بتاريخ وذلك بموجب المرسوم الملكي الصادر بتاريخ ٢٧ مارس ٢٠٢٣م.

البيانات للغير من غير ذي الصفة القانونية لتلقي تلك البيانات، وترتب على ذلك انتهاك لاعتبار صاحب البيانات وتعدي على حرمة حياته الخاصة، وتم ذلك دون موافقة أو تصريح من الشخص المعني بالبيانات.

ترتيباً على ذلك، يتمثل الركن المادي في هذه الجريمة بفعل الإفشاء أو الإفصاح، والإفصاح هنا ينطوي على إفشاء بيانات يحرص صاحبها على ألا يطلع عليها أحد، أو أنه أراد حصر العلم بها في عدد محدود من الأشخاص. فقبوله الصريح باطلاع عدد محدد على بياناته يرتبط بنطاق استقلال كل فرد ببعض قراراته الهامة، والتى تمثل بالنظر إلى خصائصها وآثارها أكثر ارتباطاً بمصيره، وأكثر تأثيرًا فى أوضاع حياته التى اختار أنماطها. مما يرتب على إفشاء تلك البيانات ضرر بسمعة أو كرامة أو مال أو نفس صاحبها.

ومن ثم اتجه البعض إلى المساواة بين هذه الصورة وبين إفشاء السر[١٨٠]، والذي يكون من شأن الإفصاح عنه إلحاق ضرر بشخص صاحبه، كالمريض بمرض معين ولا يريد أن يعلم بمرضه سوى طبيبه فقط، وأن إفصاح أو الكشف عن هذا المرض سوف يضر به مهنياً وعائلياً على سبيل المثال.

واعتبر المنظم السعودي من قبيل الإفشاء سلوك النشر، والذي من خلاله يتم بث أي من البيانات الشخصية عبر وسيلة نشر مقروءة أو مسموعة أو مرئية، أو إتاحتها للغير بدون موافقة صاحبها.

لذلك قضي بأنه إذا كانت البيانات الشخصية للأفراد، تتمثل في بيانات عن حالة الشخص العائلية، والتي أودعها صاحبها في إحدى الوكالات المتخصصة في التعارف بين الرجال والنساء بغرض الزواج، وقد حدث انقسام cession للشركة إلى شركتين، فإن وجود هذه البيانات لدى الشركة الوليدة لا يحقق الركن المادي في جريمة الإفشاء؛ ذلك أنها ليست من الغير. يُضاف إلى ذلك أن الاتفاق مع صاحب هذه البيانات يخول الوكالة الحق في أن يقوم الغير بإخبار المهتم بمسألة الزواج حتى يتم التعارف بين

---

[١٨٠] دياب محمد فتحي إبراهيم "**تجريم الاعتداء على المعلومة الإلكترونية ذات الطابع الشخصي بين الواقع والمأمول**"، مجلة الفقه والقانون، الناشر: صلاح الدين دكداك، العدد ٦٢، سنة ٢٠١٨م، ص١٩.

(ISSN: 2537 - 0758)

الطرفين[١٨١]. وبالتالي فإن رضاء صاحب البيانات الشخصية يرفع عن الفعل صفة التجريم.

بناء على ما تقدم، يشترط لقيام السلوك الإجرامي في هذه الصورة توافر عدة شروط تتمثل فيما يلي:

١. أن يتم فعل الإفشاء دون موافقة صاحب البيانات، وبدون رضاه صراحة على ذلك.
٢. أن يكون الإفشاء تم إلى شخص ليس له حق الاطلاع، وليس لديه أي صفة قانونية تسمح له بذلك.
٣. أن يترتب على إفشاء تلك البيانات، الإضرار بالمجني عليه، بأن يترتب على فعل الإفشاء أو الإفصاح اعتداء على اعتباره وحرمة حياته الخاصة. حتى ولو وقع ذلك بطريق الخطأ أو الإهمال.

تطبيقاً لذلك؛ فرضت اللجنة المعنية بحماية البيانات CNIL في فرنسا في ٢٩ ديسمبر ٢٠٢٢م، غرامة قدرها ثلاثة ملايين يورو على شركة VOODOO، التي تقوم بنشر ألعاب الفيديو للهواتف الذكية، لاستخدامها معرفًا تقنيًا بشكل أساسي للإعلانات التجارية دون موافقة المستخدم. حيث أنه عندما يقدم ناشر تطبيقًا على App Store، تزوده APPLE بمعرّف تقني يسمى "Identifier For Vendors" أو (IDFV)، مما يسمح لهذا الناشر بتتبع استخدام المستخدمين لتطبيقاته. ويتم تعيين IDFV لكل مستخدم وهو مطابق لجميع التطبيقات الموزعة بواسطة ناشر واحد، وبالتالي فإن لجميع تطبيقات VOODOO. أن تجمع بين المعلومات الأخرى من الهاتف الذكي، حيث يسمح IDFV بتتبع عادات تصفح الأشخاص، بما في ذلك فئات الألعاب التي يختارونها، من أجل تخصيص الإعلانات التي يشاهدها كل منهم، ويتم ذلك دون موافقة صريحة، وبما يتعارض مع ما يشير إليه في شاشة المعلومات التي يعرضها، وهو ما يمثل خرقًا للمادة ٨٢ من قانون حماية البيانات الفرنسي[١٨٢].

---

(181) Jacques Ghestin et Le Centre de droit des obligations de l'Université catholique de Louvain. "LA PROTECTION DE LA PARTIE FAIBLE DANS LES RAPPORTS CONTRACTUELS". Direction: Marcel Fontaine. Librairie générale de droit et de jurisprudence, E.J.A., 1996.

(182) Commission Nationale de l'Informatique et des Libertés. "Deliberation of restricted formation No SAN-2022-026 of 29 December 2022 concerning VOODOO". (Date of publication on Légifrance: January 17, 2023). https://www.legifrance.gouv.fr/cnil.

وفيما يتعلق بالركن المعنوي فإنه يلوم توافر القصد الجنائي العام بعنصريه العلم والإرداة؛ بأن يعلم الجاني أن فعل التسجيل أو المعالجة أو الفهرسة يترتب عليه إفشاء لبيانات شخصية، ويقوم بذلك دون علم صاحبها وموافقته، وتتجه إرادته إلى إتيان هذا الفعل وتحقق النتيجة. وساوى المشرع الفرنسي بين القصد الجنائي والخطأ غير العمدي، مع اختلافه في تقرير العقوبة بينهما.

أما المنظم السعودي فقط تطلب وجود قصد جنائي خاص إضافة إلى القصد الجنائي العام، يتمثل في تعمد الجاني الإضرار بصاحب البيانات أو تحقيق منفعة شخصية من جراء سلوك الإفشاء. ويدلل على ذلك ما اتجه إليه جانب من الفقه بقوله أن القصد الجنائي الخاص لا يقتصر على أركان الجريمة وعناصرها بل يمتد ليشمل وقائع لا تعد في ذاتها من أركان الجريمة. وهذا يعني أن الفارق بين القصد العام والقصد الخاص في جريمة إفشاء بيانات شخصية ليس اختلافاً في طبيعتهما فهما علم وإرادة، ولكن هذا العلم والإرادة أوسع نطاقاً في القصد الخاص عنه في القصد العام. فالنية إرادة يقوم بها القصد الخاص، الذي هو في الأساس مستند إلى العلم[١٨٣].

وعاقب المشرع المصري على تلك الجريمة بالغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه. وتشدد العقوبة لتصبح الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه، ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكبت هذه الجريمة مقابل الحصول على منفعة مادية أو معنوية، أو ارتكبت بقصد تعريض صاحب البيانات للخطر.[١٨٤] وعاقب المشرع الفرنسي بالسجن خمس سنوات وبغرامة ٣٠٠ ألف يورو في حالة العمد، وبالسجن ثلاث سنوات وبغرامة ١٠٠ ألف يورو في حال ارتكاب سلوك الإفشاء عن طريق الإهمال وعدم الاحتياط أي بطريق الخطأ.

---

[١٨٣] محمود نجيب حسني "**شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي**" دار النهضة العربية، يالطبعة الثامنة، سنة ٢٠١٨م، ص٧٥١-٧٥٢.

[١٨٤] راجع المادة ٣٦ من قانون حماية البيانات الشخصية المصري.

(ISSN: 2537 - 0758)

ولحقه في ذلك المنظم السعودي عندما عاقب على تلك الجريمة ضمن ثنايا المادة ٣٥/ فقرة أ بقوله، "كل من أفصح عن بيانات حساسة أو نشرها مخالفاً أحكام النظام: يعاقب بالسجن مدة لا تزيد على سنتين وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية".

وفيما يتعلق بالإفصاح خارج حدود المملكة العربية السعودية، ففيما عدا حالات الضرورة القصوى، ومن أجل المحافظة على حياة صاحب البيانات أو مصالحه الحيوية أو الوقاية من عدوى مرضية أو فحصها أو معالجتها، لا يجوز الإفصاح عن بياناته إلا إذا كان ذلك تنفيذاً لالتزام بموجب اتفاقية تكون فيها المملكة طرفاً، أو لخدمة مصالح المملكة متى **توافرت الشروط الآتية:**

١- ألا يترتب على النقل أو الإفصاح مساس بالأمن الوطني أو بمصالح المملكة الحيوية.
٢- أن تقدم ضمانات كافية للمحافظة على البيانات الشخصية التي سيجرى نقلها أو الإفصاح عنها وعلى سريتها، بحيث لا تقل معايير حماية البيانات الشخصية عن المعايير الواردة في النظام واللوائح.
٣- أن يقتصر النقل أو الإفصاح على الحد الأدنى من البيانات الشخصية الذي تدعو الحاجة إليه.
٤- موافقة الجهة المختصة على النقل أو الإفصاح وفقاً لما تحدده اللوائح. ويعاقب كل من خالف ذلك يعاقب بالسجن مدة لا تزيد على سنةوبغرامة لا تزيد على مليون ريال، أو بإحدى هاتين العقوبتين.

وعاقب قانون العقوبات الفرنسي بموجب المادة ٢٢٦-١/٢٢ على حالة الإفشاء أو نقل البيانات الشخصية محل المعالجة إلى دولة لا تنتمي إلى الاتحاد الأوروبي أو إلى منظمة دولية، حيث تمثل انتهاك للفصل الخامس من اللائحة الأوروبية لحماية البيانات الصادرة بتاريخ ٦٧٩/٢٠١٦ للبرلمان الأوروبي، والمجلس بتاريخ ٢٧ أبريل ٢٠١٦ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، وإلغاء التوجيه EC٤٦/٩٥ حيث يعاقب القانون رقم ١١٢ إلى ١١٤ من القانون رقم

١٧-٧٨ الصادر في ٦ كانون الثاني/ يناير ١٩٧٨ سالف الذكر بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠ ألف يورو(١٨٥).

وقد انتهت محكمة العدل الأوروبية إلى أنه يجوز لسلطة إشرافية وطنية، في ظل ظروف معينة، أن تمارس سلطتها في تقديم أي انتهاك مرتبط بالقانون العام لحماية البيانات (GDPR) إلى محكمة دولة عضو، حتى لو لم تكن هي صاحبة السلطة في هذه المعالجة(١٨٦).

---

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

(186) Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA V, Gegevensbeschermingsautoriteit. (15/6/2021). Court of Justice of the European Union (CJEU). C-645/19. https://curia.europa.eu/juris/document/document.jsf?text=&docid=242821

– وأوضحت محكمة العدل الأوروبية، أنه "يجب تفسير المادة ٥٨ (٥) من اللائحة ٦٧٩/٢٠١٦ على أنها تعني أنه عندما تقوم سلطة إشرافية تابعة لدولة عضو ليست "السلطة الإشرافية الرائدة"، بالمعنى المقصود في المادة ٥٦ (١) من تلك اللائحة، برفع دعاوى قانونية قبل ٢٥ مايو ٢٠١٨ لمعالجة البيانات الشخصية عبر الحدود، وهذا يعني أنه يجوز قبل التاريخ الذي تصبح فيه تلك اللائحة قابلة للتطبيق، الإبقاء على هذا الإجراء، من وجهة نظر قانون الاتحاد، على أساس أحكام التوجيه EC/٤٦/٩٥ الصادر عن البرلمان الأوروبي والمجلس المؤرخ ٢٤ تشرين الأول/أكتوبر ١٩٩٥ بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة هذه البيانات، التي تظل سارية فيما يتعلق بانتهاكات القواعد المنصوص عليها فيها الملتزمة حتى تاريخ إلغاء ذلك التوجيه. وبالإضافة إلى ذلك، يجوز لتلك السلطة أن ترفع تلك الدعوى فيما يتعلق بالتعديات المرتكبة بعد ذلك التاريخ، استنادا إلى المادة ٥٨ (٥) من اللائحة التنظيمية ٦٧٩/٢٠١٦، شريطة أن يكون ذلك في إحدى الحالات التي تخول فيها، على سبيل الاستثناء، سلطة إشرافية تابعة لدولة عضو ليست "السلطة الإشرافية الرائدة" سلطة اتخاذ قرار يخلص إلى أن معالجة البيانات المعنية. ينتهك القواعد الواردة في تلك اللائحة فيما يتعلق بحماية حقوق الأشخاص الطبيعيين فيما يتعلق

(ISSN: 2537 - 0758)

المطلب الثالث
الاستغلال غير المشروع للبيانات الشخصية أو التهديد به

ورد النص على هذه الجريمة، تحت مفهوم "خرق وانتهاك البيانات الشخصية" الوراد ضمن تعريفات المادة الأولى من قانون حماية البيانات الشخصية المصري، بقولها يعد خرق وانتهاك للبيانات الشخصية كل دخول غير مرخص به إلى البيانات الشخصية أو وصول غير مشروع أو أية عملية غير مشروعة، لنسخ أو إرسال أو توزيع أو تبادل أو نقل أو تداول، يهدف إلى الكشف أو الإفصاح عن البيانات الشخصية، أو إتلافها أو تعديلها أثناء تخزينها أو نقلها أو معالجتها.

ويتمثل الركن المادي في هذه الجريمة، في أفعال الاستغلال غير المشروع للبيانات الشخصية، ويتم ذلك بخرق أو انتهاك أو الدخول غير المشروع لحاسب آلي أو موقع إلكتروني أو نظام معلوماتي، من أجل الحصول على البيانات أو نسخها أو تبادلها أو نقلها بغرض الإفصاح أو الكشف عنها للغير.

وكانت محكمة النقض المصرية، قد انتهت إلى أن جريمة إساءة استعمال أجهزة الاتصالات وتكنولوجيا المعلومات، لا تقتصر فقط على مجرد السب أو القذف، بل تتسع لتشمل كل قول أو فعل يتعمده الجاني يضيق به صدر المجني عليه أياً كان هذا الفعل[١٨٧]. كما في حالة التهديد باستغلال تلك البيانات، والذي يقع عن طريق التوعد والضغط على إرادة المجني عليه أو ابتزازه من أجل الحصول على فائدة معينة. ويكفي أن يقوم الجاني بإرسالة رسالة التهديد لتصل إلى علم المراد تهديده، سواء أرسلها إليها فتلقاها مباشرة، أم بعث بها إلى شخص آخر فتلقاها ثم بلغها إياه أو لم يبلغها مادام أنه

بمعالجة البيانات الشخصية والامتثال لإجراءات التعاون والاتساق المنصوص عليها في تلك اللائحة، والتي يعود إلى محكمة الإحالة أن تقررها".

[١٨٧] الطعن رقم ١١٤٥٦ لسنة ٩٠ قضائية- جنح النقض- جلسة ٢٠٢١/٠٩/١١م.

توقع حتماً أن المرسل إليه بحكم وظيفته أو بسبب علاقته أو صلته بالشخص المقصود بالتهديد سيبلغه الرسالة(١٨٨).

فعلة التجريم تنطوي على حماية بيانات الشخص من الاعتداء عليها باستغلالها أو التهديد بها، ومن ثم إلقاء الشعور بالطمأنينة والأمن بداخله؛ كونها تمثل جزءاً من مستودع حياته الخاصة، وهي مصونة ولا يجوز مساسها بدون مصوغ قانوني، فالنشر والتوزيع والإفصاح لا يتم إلا بإذن من صاحب البيانات.

وهو ما أكدته محكمة النقض المصرية بقولها "توجد مناطق من الحياة الخاصة لكل فرد تُمثل أغوارًا لا يجوز النفاذ إليها، وهذه المناطق من خواص الحياة ودخائلها وينبغى دومًا– ولاعتبار مشروع– ألا يقتحمها أحد ضمانًا لسريتها وصونًا لحرمتها ودفعًا لمحاولة التلصص عليها أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التى بلغ تطورها حدًا مذهلًا وكان لتنامى قدراتها على الاختراق أثر بعيد على الناس جميعهم، حتى فى أدق شئونهم وما يتصل بملامح حياتهم بل وببياناتهم الشخصية، والتى غدا الاطلاع عليها والنفاذ إليها كثيرًا ما يُلحق الضرر بأصحابها"(١٨٩).

أما عن الركن المعنوي لهذه الجريمة، فيتحقق بتوافر القصد الجنائي العام بعنصريه العلم والإرادة، بأن يعلم القائم بالمعالجة أن سلوكه يمثل استغلالاً للبيانات الشخصية على نحو غير مشروع، ودون موافقة صاحبها أو السلطات المخولة قانوناً بالموافقة، وتتجه إرادته نحو ارتكاب هذا الفعل.

وفي ذلك قضت محكمة النقض المصرية بأن "ما أورده الحكم المطعون فيها لواقعة الدعوى ورداً على ما دفع به الطاعن من انتفاء أركان جريمة الاعتداء على حرمة الحياة الخاصة بغير رضاء المجني عليها، بالتقاط صور لها في مكان خاص وهي عارية، مهددين بها إياها، تتحقق به كافة العناصر القانونية للجريمة التي دان الطاعن بارتكابها،

(١٨٨) الطعن رقم ٢٢٨٣٠ لسنة ٨٨ ق، جلسة ٢٠٢١/٠٩/١١م. (المكتب الفني، المجموعة الجنائية– المستحدث من المبادئ الصادرة من الدوائر الجنائية بمحكمة النقض– بداية من أول أكتوبر ٢٠٢٠م، حتى نهاية سبتمبر ٢٠٢١) ص ٧٨.

(١٨٩) حكم النقض بجلسة ١٦/٠٣/٢٠٢٢ في الطعن رقم ٩٥٤٢ لسنة ٩١ق، مرجع سابق.

(ISSN: 2537 - 0758)

كما هي معرفة به في القانون، ومن ثم فإن النعي على الحكم في هذا الخصوص يكون غير سديد"[١٩٠].

وعليه عاقب قانون حماية البيانات الشخصية المصري على الاستغلال غير المشروع للبيانات الشخصية في مادته ٣٦، بالغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، وشدد العقوبات لتصل للحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحداهما، إذا ارتكبت هذه الجريمة مقابل الحصول على منفعة مادية أو أدبية أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.

أما قانون العقوبات الفرنسي، فيعاقب على جمع البيانات الشخصية التي تتم بوسائل احتيالية أو غير قانونية، بالسجن لمدة خمس سنوات وغرامة قدرها ٣٠٠٠٠٠ يورو[١٩١].

خلاصة ما تقدم؛ فقد اتجهت العديد من التشريعات الجنائية إلى توخي الحذر مما ترتب على التحول الرقمي وتداول استخدام تكنولوجيا المعلومات وبرامجها وتطبيقاتها، وما نتج على ذلك من آثار سلبية ألحقت بخصوصية الأفراد، لاسيما ما يتعلق ببياناتهم الشخصية. محاولة بذلك التصدي لتلك الأدوات الإلكترونية التي قد يتم إساءة استخدامها وعلى نحو غير مشروع. بل وتنبهت تلك التشريعات إلى ضرورة سن أنظمة صارمة قد لا تؤدي إلى منع تلك الانتهاكات، ولكنها تساعد في الحد منها، والحفاظ على كينونة الإنسان وحماية أهم حقوقه في هذه الحياة.

---

[١٩٠] الطعن رقم ١٩٥٥ لسنة ٨٨ ق، جلسة ٢٠٢٠/١٠/١١م. (المكتب الفني، المجموعة الجنائية– المستحدث من المبادئ الصادرة من الدوائر الجنائية بمحكمة النقض– بداية من أول أكتوبر ٢٠٢٠م، حتى نهاية سبتمبر ٢٠٢١) ص ٧٤.

[191] Code penal. Art. 226-18: “Le fait de collecter des données à caractère personnel parun moyen frauduleux, déloyal ou illicite EST puni de cinq ans d'emprisonnement ET de 300 000 euros d'amende”.

الخاتمة

بعد أن انتهينا من عرضنا لأحكام الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً، ومناقشتها في عدد من التشريعات الجنائية المقارنة والحديثة نسبياً في هذا الشأن، تبين لنا مدى أهمية اتساق البيانات الشخصية بحرمة الحياة الخاصة، التي هي الإطار السري والخفي لحياة الإنسان والتي لا يجوز الولوج إليها دون سند قانوني أو أسباب مشروعة. الأمر الذي دعى التشريعات الجنائية إلى سن نظم حماية، ووضع العديد من الأطر والممارسات وأحكام التجريم التي تتناسب والصبغة الخاصة لهذه الخصوصية، لاسيما ما يتعلق بالبيانات الشخصية للأفراد.

فالحماية لا تحقق فاعليتها وجدواها إلا من خلال توقيع العقوبات الجنائية على الجاني، سواء أكانت عقوبات سالبة للحرية أم أنها تتمثل في توقيع الغرامة والمنع من مزاولة النشاط. وسواء ارتكبت عن عمد أو خطأ كما أقرت بعض التشريعات الجنائية.

وفي خلاصة بحثنا توصلنا إلى عدد من النتائج من هذه الدراسة تحقيقا للغاية منها، ورداً على التساؤلات التي أثيرت بداية في إشكاليات البحث، ومن ثم الخروج بتوصيات قد تفيد القائمين على صنع القرار والباحثين في هذا الشأن، **وذلك على النحو التالي:-**

أولاً: النتائج:

١- حماية حرمة الحياة الخاصة، لاسيما ما يتعلق بحماية البيانات الشخصية للأفراد، تعد أحد أهم الحقوق التي أقرتها التشريعات الوطنية والقواعد الدولية، لما لها من أهمية في الوقت الراهن، وبخاصة مع انتقال العالم إلى عصر الرقمنة.

٢- تنوعت البيانات الشخصية للأفراد محل الحماية، وارتبطت بجميع أنواع البيانات مادامت قد تساهم في التعرف على الشخص بشكل مباشر أو غير مباشر، وسواء أكانت بيانات حساسة، أم بيانات خاصة مرتبطة بالفرد نفسه ولم يشتملها الحالات الجوازية للإفصاح كالبيانات الإحصائية أو المرتبطة بالأمن القومي.

٣- تتمتع البيانات الحساسة بنوع خاص من الحماية؛ ويرجع ذلك إلى طبيعتها الخاصة. وهو ما اتفقت عليه التشريعات المعنية بحماية البيانات الشخصية، بتحديد ما يعد من قبيل البيانات الحساسة والتي لا يجوز معالجتها إلا في ظل شروط وقيود محددة في القانون.

(ISSN: 2537 - 0758)

٤- يلزم إعمال مبدأ التناسب بين الحقوق، وإعطاء الأولوية لحق على حق آخر بحسب الأهداف المشروعة، متى كان ذلك يعد تدبيراً ضرورياً، وفي مجتمع ديمقراطي، ولحماية المصلحة العامة كالأمن القومي وحفظ النظام، وحماية حقوق الآخرين وحرياتهم.

٥- تلتزم جهة المعالجة بمراعاة الشروط والضوابط الواجب اتباعها عند تجميع ومعالجة البيانات، خاصة ما يتعلق بمشروعية تجميعها، والحصول على موافقة صريحة من صاحب تلك البيانات، وأن تتم المعالجة وفقاً للغاية التي جمعت من أجلها، فضلاً عن عدم الاحتفاظ بتلك البيانات لمدد زمنية أطول من المدد المحددة للوفاء بالغرض منها.

٦- اعترفت القوانين المعنية بحماية البيانات الوطنية والدولية، بوجود التزامات تقع على عاتق جهة المعالجة، تتمثل في تمكين صاحب البيانات الشخصية من ممارسة حقوقه على بياناته، في ظل ضوابط تنظم هذه الحقوق، كالحق في العلم والوصول والاطلاع، وحقه في تصحيح معلوماته، وحقه في المحو والنسيان، والحق في تقييد المعالجة أو نقلها، وكذلك حقه في الاعتراض.

٧- تجرم التشريعات الجنائية المعنية بحماية البيانات الشخصية، صور الاعتداء على البيانات الشخصية محل المعالجة، سواء في الفترة التي تسبق عملية المعالجة كتجريم عدم الإلتزام بالإجراءات الأولية اللازم على جهة المعالجة اتخاذها لحماية وتأمين تلك البيانات، أو في مراحل جمعها وحفظها وإعدادها للمعالجة. أم أثناء عملية معالجتها وجمعها بخلاف الغرض التي جمعت من أجله، أو حال إفشائها، وكذلك تجريم الاستغلال غير المشروع لها أو حتى التهديد به.

٨- تنوعت صور السلوك الإجرامي المرتكب في جرائم الاعتداء على البيانات الشخصية، فمنها ما يرتكب بشكل إيجابي ومنها ما يرتكب بشكل سلبي. كما اختلفت طبيعتها ما بين جرائم خطر وجرائم ضرر.

٩- تتطلب جرائم الاعتداء على البيانات الشخصية، توافر القصد الجنائي العمدي، ومع ذلك عاقبت بعض التشريعات كالتشريع الفرنسي على ارتكاب تلك الجرائم بصورة غير عمدية أي بطريق الخطأ أو الإهمال.

١٠- تنوعت العقوبات الورادة على الاعتداء على البيانات الشخصية للأفراد أو مخالفة ضوابط حمايتها، ولم تكتف بعض التشريعات بالجزاء الجنائي فحسب، بل أقرت جزاءً إدارياً وآخر مدنياً إلى جانب الجزاء الجنائي، ومنها من اقتصر على الجزاءات الجنائية التي تطبق من جانب القضاء الجزائي.

١١- اختلفت العقوبات الجنائية التي قُررت لمعاقبة مرتكب جرائم الاعتداء على البيانات الشخصية للأفراد، ما بين عقوبات سالبة للحرية كالحبس، ومنها ما اكتفى بعقوبة الغرامة، والبعض الآخر أخذ بالعقوبتين معاً أياً كانت صور الجرائم المرتكبة.

ثانياً: التوصيات:

١- نوصي في الحالات التي يقع فيها التزام قانوني على الجهة القائمة بالمعالجة، ولا يتطلب ذلك الحصول على رضاء الشخص المعني بمعالجة بياناته، يتم تبصير هذا الأخير بنوع هذا الالتزام وغرضه ومصدره القانوني.

٢- أن ينص التشريع المصري والسعودي على وقوع جرائم العدوان على البيانات الشخصية، حتى في حالات الخطأ والإهمال غير العمدي أسوة بالمشرع الفرنسي، حتى لا يكون عدم التبصر والإهمال ذريعة تنفي عن مرتكبها المسؤولية الجنائية.

٣- عند تحديد الاستثناءات التي تتعلق بالبيانات الشخصية التي يمكن إتاحتها حتى مع عدم توافر الرضا من صاحبها، أن تخضع لتقييم المصلحة والضرر المترتب على إتاحتها. بمعنى أن تكون المصلحة التي ستتحقق من علانيتها تفوق المصلحة التي ستتحقق من عدم إفشاؤها.

٤- وضع معايير محددة للقاضي أن يستدل منها على احترام التوازن بين المصلحة المشروعة لجهة المعالجة ومصلحة الشخص المعالج بياناته، بما يضمن كفالة حقوقه وحرياته الخاصة، حيث أن فكرة المصلحة المشروعة واسعة للغاية، ويمكن التذرع بها من أجل معالجة بيانات الشخص دون موافقة مسبقة منه.

٥- نوصي الجهات المعنية ومؤسسات الدول وهيئاتها بما فيها وسائل الإعلام، تبصير الأفراد بأهمية حماية بياناتهم الشخصية، وأنواع تلك البيانات الجديرة بالحماية. مع إلقاء الضوء على أهم الحقوق التي لهم ممارستها في حال طلب معالجة بياناتهم الشخصية.

(ISSN: 2537 - 0758)

٦- عند الدخول لمواقع أو تطبيقات إلكترونية أياً كان نوعها، من الضروري التأكد وقراءة الشروط التي تطلبها من أجل إتمام الموافقة على استخدامها أو الدخول إليها.

٧- أن تتضمن التشريعات المعنية بحماية البيانات الشخصية، نصوصاً صريحة ودقيقة، تحدد فيها ضوابط ممارسة الشخص حقوقه على بياناته دون أن ترد النصوص عامة وواسعة، **ونقترح من قبيل هذه النصوص على سبيل المثال:**

المادة الأولى: "أن يتقدم الشخص المعني بالبيانات بطلب (وفق نموذج محدد) إلى جهة المعالجة، محدداً فيه اعتراضه على البيانات المعالجة أو المعدة للمعالجة أو جزءاً منها، خلال مدة زمنية معينة، وللجهة أن تفحص طلبه والتأكد من إعمال التوازن بين حقه في الاعتراض وبين الحالات الاستثنائية التي يجيزها القانون لإجراء المعالجة دون حق الشخص المعني في إبداء اعتراضه، وإخطاره بما توصلت إليه من قرارات. وفي حال مخالفة جهة المعالجة تلك الإجراءات يتم رفع الأمر إلى المراكز والجهات المعنية بالإشراف على أعمال جهة المعالجة".

المادة الثانية: "إخطار الشخص المعني بالبيانات، بالمسوغ القانوني لجمع بياناته ومعالجتها، وأن يكون هذا الإخطار مكتوباً وموقعاً من الجهة المصدرة له، ويتم إرساله عبر الوسائل الإلكترونية كالبريد الإلكتروني، أو الوسائل اليدوية كالبريد العادي، ولا تقوم الجهة بالمعالجة إلى بعد استلام ما يفيد موافقة الشخص المعالج بياناته على تلك المعالجة".

المادة الثالثة: "يتطلب في موافقة الشخص على إجراء معالجة بياناته، أن تكون تلك الموافقة مكتوبة وصريحة وبعيدة عن أي عبارات يشوبها الغموض، وأن تكون مجانية ومحددة بالغرض الذي ستتم المعالجة من أجله. خاصة في الحالات التي تتعلق بالبيانات الحساسة أو إعادة استخدام بياناته في أغراض أخرى".

المادة الرابعة: "لصاحب البيانات الحق في تقديم تظلم أمام الجهات المعنية بالإشراف على تنظيم معالجة البيانات- كاللجنة القومية للحريات في القانون الفرنسي، ومركز حماية البيانات في القانون المصري- خلال مدة زمنية محددة في القانون، يبين فيه منعه من حقه في ممارسة حقوقه على بياناته، وأسباب هذا المنع، ولجهة التظلم أن تحدد إجراءات سير التظلمات المقدمة وطريقة البت فيها".

المادة الخامسة: "جواز فصل البيانات في حال وجود بيانات شخصية في سجلات تضم بيانات لأشخاص آخرين، وكانت بيانات الآخرين محظور إتاحتها، فيجوز فصل تلك البيانات لإتاحتها لطالب الإطلاع عليها وتمكينه من ممارسة، دون الاطلاع على البيانات الأخرى للأشخاص الآخرين، وأن يتم ذلك تحت رقابة الجهة القائمة على المعالجة".

٨- أن يرد نص صريح في تشريعات حماية البيانات الشخصية يتضمن إلزام المواقع الإلكترونية ومواقع التواصل الاجتماعي بنشر سياسة استخدامها، بما يضمن كفالة حقوق الأفراد المستخدمين لهذه المواقع، كذلك نشر ما يضمن إعلام المستخدم بحقوقه على بياناته في حال معالجتها، وأن يحدد لذلك عقوبة جنائية في حال مخالفتها ذلك.

٩- تشديد العقوبات في حال إفشاء بيانات شخصية محظور إفشاؤها، إذا كان الغرض من ذلك الإضرار بالنظام العام أو الأمن القومي، أو سيترتب عليها تعريض سلامة وأمن المجتمع للخطر، أو الإضرار بمركز الدولة السياسي أو الاقتصادي أو تقويض السلام الاجتماعي.

١٠- التمييز في العقوبات المترتبة على الإخلال بحماية البيانات الشخصية حال ارتكابها عن عمد أو عن غير عمد بطريق الخطأ.

١١- الحكم بمصادرة المواد محل الجريمة كالأجهزة الإلكترونية محل الجريمة في حال الحكم بعقوبة جنائية على مرتكبها.

(ISSN: 2537 - 0758)

قائمة المراجع

أولاً: المراجع العربية:

(أ) المراجع العامة:

- محمود نجيب حسني "**شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي**". دار النهضة العربية، الطبعة الثامنة، سنة ٢٠١٨م.

(ب)المراجع المتخصصة:

- أحمد كمال، "**حماية البيانات الشخصية على شبكة الإنترنت**"، المجلة الجنائية القومية، المركز القومي للبحوث الاجتماعية والجنائية، المجلد ٥٢، العدد ٢، سنة ٢٠٠٩م.
- تامر محمد محمد صالح، "**الحماية الجنائية للحق في المعلومات الرسمية، دراسة مقارنة**"، مجلة القانون والاقتصاد– ملحق خاص العدد (الثانى والتسعون)، بدون سنة نشر.
- خالد بوعدان، "**الحماية التشريعية والتقنية للحق في الخصوصية عبر شبكة الإنترنت**". مجلة عدالة للدراسات القانونية والقضائية، الناشر: المصطفى الغشام الشعيبي، العدد ١٥، سنة ٢٠٢١م.
- دياب محمد فتحي إبراهيم، "**تجريم الاعتداء على المعلومة الإلكترونية ذات الطابع الشخصي بين الواقع والمأمول**"، مجلة الفقه والقانون، الناشر: صلاح الدين دكداك، العدد ٦٢، سنة ٢٠١٨م.
- رزق سعد، "**الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في ضوء القانون رقم ١٥١ لسنة ٢٠٢٠م**". ورقة بحثية مقدمة للمؤتمر العلمي الدولي الأول لكلية الحقوق جامعة مدينة السادات بعنوان "**الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي** "**رؤية مصر ٢٠٣٠– في المجال الصحي**". عدد خاص بالمؤتمر.
- سامح عبد الواحد التهامي، "**الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي**" القسم الأول. مجلس النشر العلمي، جامعة الكويت، كلية الحقوق. سنة ٢٠١١م.
- شريف يوسف حلمي خاطر، "**حماية الحق في الخصوصية المعلوماتية :دراسة تحليلية لحق الاطلاع على البيانات الشخصية في فرنسا**"، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة– كلية الحقوق، العدد ٥٧، سنة ٢٠١٥م.
- شول بن شهرة، "**برنامج الحماية الجنائية للبيانات الشخصية في معاملات التجارة الإلكترونية**". المركز الجامعي غرداية، بدون سنة نشر.
- عمر الفاروق الحسيني، "**المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي**

وأبعادها الدولية"، بدون دار نشر، سنة ١٩٩٥م.

- غنام محمد غنام، "**الحماية الجنائية لأسرار الأفراد لدى الموظف العام**"، دار النهضة العربية، مصر، سنة ١٩٨٨م.
- طارق جمعة السيد راشد، "**الحماية القانونية لخصوصية البيانات الشخصية فى القانون القطري والمقارن**"، المجلة القانونية والقضائية، وزارة العدل- مركز الدراسات القانونية والقضائية، العدد ٢، سنة ٢٠١٧م.
- محسن عبد الحميد البيه "**الإثبات الجنائي في المواد المدنية والتجارية، وفقاً لقانون الإثبات وقانون التوقيع الإلكتروني**"، بدون دار نشر، طبعة ٢٠٠٧.
- محمد أحمد سلامة، "**الحق في محو البيانات الشخصية: دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي GDPR وأحكام المحاكم الأوروبية**". مجلة الدراسات القانونية والاقتصادية، جامعة مدينة السادات- كلية الحقوق، المجلد ٣، العدد ٢.
- محمد حسن عبدالله علي، "**النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة**". مجلة كلية القانون، جامعة عجمان، المجلد ٧، العدد ١٤، سنة ٢٠٢١م.
- محمد عبد المحسن المقاطع، "**نحو صياغة جديدة لمفهوم الحياة الخاصة للأفراد وضماناتها في مواجهة تهديدات الكمبيوتر**"، مؤتمر جامعة الكويت حول "القانون والحاسب الآلي" مطبوعات جامعة الكويت ومؤسسة الكويت للتقدم العلمي، سنة ١٩٩٤.

(ج) أحكام قضائية:

- حكم المحكمة الدستورية العليا المصرية، في الدعوى رقم ٣٧ لسنة ٩ قضائية، بجلسة ١٩ مايو سنة ١٩٩٠م.
- الطعن رقم٦٦٧٤ لسنة ٨٧ ق-جلسة ٢٠١٩/٠٤/٠٢م، والطعن رقم٣٧١٩ لسنة ٨٦ق- جلسة٢٠٢٠/٠٧/٠٧م. المكتب الفني، المجموعة الجنائية". مجموعة المبادئ القانونية التي قررتها محكمة النقض في جرائم الاتصالات" بدون سنة نشر.
- الطعن رقم ١٩٥٥ لسنة ٨٨ق، جلسة ٢٠٢٠/١٠/١١م. (المكتب الفني، المجموعة الجنائية- المستحدث من المبادئ الصادرة من الدوائر الجنائية بمحكمة النقض- بداية من أول أكتوبر ٢٠٢٠م، حتى نهاية سبتمبر ٢٠٢١).

(ISSN: 2537 - 0758)

- الطعن رقم ٩٥٤٢ لسنة ٩١ق- جلسة ٢٠٢٢/٠٣/١٦م في، طعنًا على الحكم الصادر من الدائرة الاستئنافية بمحكمة القاهرة الاقتصادية في الدعوى المقيدة برقم ١١٩ لسنة ١٢ ق اقتصادي.
- الطعن رقم ١١٤٥٦ لسنة ٩٠ قضائية- جنح النقض- جلسة ٢٠٢١/٠٩/١١م.
- الطعن رقم ٢٢٨٣٠ لسنة ٨٨ق، جلسة ٢٠٢١/٠٩/١١م. (المكتب الفني، المجموعة الجنائية- المستحدث من المبادئ الصادرة من الدوائر الجنائية بمحكمة النقض- بداية من أول أكتوبر ٢٠٢٠م، حتى نهاية سبتمبر ٢٠٢١).
- الطعن رقم ٩٥٤٢ لسنة ٩١ق- جلسة ١٦ مارس ٢٠٢٢، محكمة النقض المصرية.

(د) القوانين والتشريعات والأنظمة والاتفاقيات الدولية:

- الإعلان العالمي لحقوق الإنسان سنة ١٩٤٨م.
- الاتفاقية الأوروبية لحقوق الإنسان وحرياته الأساسية سنة ١٩٥٠م.
- العهد الدولي للحقوق السياسية والمدنية سنة ١٩٦٦م.
- القانون الأمريكي لحماية البيانات الصادر ١٩٩٧م.
- النظام الأساسي للحكم، المملكة العربية السعودية، الصادر بالأمر الملكي رقم أ/٩٠ بتاريخ ١٤١٢/٨/٢٧هـ الموافق ١ مارس ١٩٩٢م.
- الدستور المصري الصادر سنة ٢٠١٤م.
- توجيه الاتحاد الأوروبي ٦٨٠/٢٠١٦ الصادر عن البرلمان الأوروبي والمجلس بتاريخ ٢٧ أبريل ٢٠١٦م.
- القانون الفرنسي المتعلق بمعالجة البيانات والملفات والحريات رقم ٧٨-١٧ المؤرخ في ٦ يناير ١٩٧٨م، والمعدل بموجب الأمر رقم ٢٠١٨-١١٢٥ المؤرخ في ١٢ ديسمبر ٢٠١٨م الصادر بموجب المادة ٣٢ من القانون رقم ٢٠١٨-٤٩٣ المؤرخ ٢٠ يونيو ٢٠١٨ م بشأن حماية البيانات الشخصية.
- اللائحة الأوروبية رقم ٦٧٩/٢٠١٦ الصادرة عن الاتحاد الأوروبي بتاريخ ٢٧ أبريل ٢٠١٦م بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقل هذه البيانات. والتي دخلت حيز التنفيذ في في ٢٥ مايو/ أيار ٢٠١٨م.
- المرسوم رقم ٢٠١٩-٥٣٦ المؤرخ في ٢٩ مايو ٢٠١٩ المتعلق بتطبيق القانون رقم ٧٨-١٧ المؤرخ ٦ يناير ١٩٧٨ المتعلق بمعالجة البيانات والملفات والحريات
- قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠م.
- نظام حماية البيانات الشخصية السعودي رقم (م/١٩) وتاريخ١٤٤٣/٢/٩هـ ٢٠٢١/٠٩/١٦م. وآخر تعديلاته الصادرة بالقرار رقم (٦٠٤) وتاريخ ١٤٤٤/٨/٢٩هـ، الموافق ٢٠٢٣/٣/٢١م.

(هـ) المواقع الإلكترونية:

- https://www.cnil.fr/en
- https://ukanon.net
- https://curia.europa.eu
- https://www.legifrance.gouv.fr/cnil

ثانياً: المراجع الأجنبية:

***Books and Articles:**

- Al-Mahrouky Mayada, "**Hate Crimes and Freedom of Speech**". International Review of law and Economics. Article submission No. 109069. ISSN: 01448188, Chicago- (USA),2023.
- Commission Nationale de l'Informatique et des Libertés. "**Deliberation of restricted formation No SAN-2022-026 of 29 December 2022 concerning VOODOO**". (Date of publication on Légifrance: January 17, 2023). https://www.legifrance.gouv.fr/cnil.
- David Harrington. "**U.S. Privacy Laws: The Complete Guide". September 2, 2022.** https://www.varonis.com/blog/us-privacy-laws.
- Frederick G. Bohme, "**100 Years of Data Processing: The Punchcard Century**" Volume 3, U.S. Department of Commerce, Bureau of the Census, Data User Services Division, 1991.
- Gassin Raymond, "**La protection pénale des informations sur la personne en droit français contemportain**", in "Droit pénal contemporain", Mélanges en l'honneur d'André Vitu, éd. Cujas, 1989.
- Lynskey, Orla, "**Control over personal data in a digital age**" Google Spain v AEPD and Mario Costeja Gonzalez. Modern Law Review, 78 (3). (2015). ISSN 0026-7961. DOI:10.1111/1468-2230.12126. This version available at: http://eprints.lse.ac.uk/61944.
- Manon Leblond." **Le principe d'individualisation de la peine en droit pénal français**". Droit. Université Montpellier, 2021.
- Rials (dir), **Dictionnaire de la culture juridique**, PUF, 2003.
- Jacques FRANCILLON, "**L'adaptation du droit pénal à certaines fromes de délinquance informatiques et audio-**

(ISSN: 2537 - 0758)

visuelles "in" La protection pénale des infromations sur la personne en droit français contemporain, in "Droit pénal contemporain" Mélanges en l'honneur d'André Vitu, éd. Cujas 1989.

- Jacques Ghestin et Le Centre de droit des obligations de l'Université catholique de Louvain. "**LA PROTECTION DE LA PARTIE FAIBLE DANS LES RAPPORTS CONTRACTUELS**". Direction: Marcel Fontaine. Librairie générale de droit et de jurisprudence, E.J.A., 1996.
- Ulrich Sieber**, "The international Hand book on Computer Crime".** John Wiley & Sons, New York, 1986.

***Decisions of Courts:**

- Crim. 3 nov. 1987, Bull. crim. nº 382; Rev. sc. crim. 1988. 295, obs. Delmas Saint- Hilaire; J. C. P. 1988. Crim 3 nov. 1987, D. 1988. J. 17, note Herbert Maisl.
- Crim. 6 juill 1994 cite par Jacques FRANCILLON, "Infractions relevant du droit de l'information et de la communication", 1996. Chronique de Jurisprudence.
- Crim 19 déc. 1995; Bull. Crim. nº 387; Rev. Sc.1996. Francillon; Dr. Pénal 1996.
- Tribunal de grande instance de Paris 3ème chambre, 2ème section 25 avril 2003.
- Judgment of 6 November 2003 (Grand Chamber), Lindqvist (C-101/01, EU: C 2003:596).
- Royal Courts of Justice Strand, London.THE EDMONTON COUNTY COURT: Durant v Financial Services Authority. (Case No: B2/2002/2636). 8 Dec 2003. https://www.5rb.com/wp-content/uploads/2013/10/Durant-v-Financial-Services-Authority-CA-8-Dec-2003.pdf.
- Cour de Cassation, Chambre sociale, du 6 avril 2004, 01-45.227, Publié au bulletin, https://www.legifrance.gouv.fr.
- Délibération n°2010-229 du 10/06/2010 dispensant de déclaration les traitements automatisés de données à caractère personnel mis en oeuvre par des organismes à but non lucratif, abrogeant et remplaçant la délibération n°2006-130 du 9 mai 2006. https://www.cnil.fr.

- European Court of Human Rights: S. and Marper v. the United Kingdom, 4 December 2008 (Grand Chamber). https://hudoc.echr.coe.int/eng-press?i=003-2571936-2784147
- Judgment of the Court (Grand Chamber) Heinz Huber v Bundesrepublik Deutschland, (Case C-524/06). European Court Reports 2008 I-09705. 16 December 2008.
- https://eurlex.europa.eu/legalcontent/EN/TXT/?uri=CELEX%3A62006CJ0524.
- European Court of Human Rights: Uzun v. Germany, (application no. 35623/05). 2 September 2010. https://hudoc.echr.coe.int/engpress#{%22itemid%22:[%22003-3241790-3612154%22]}.
- Kennedy v. the United Kingdom, 18.05.2010. (Application no. 26839/05), 15 May 2010.
- Peter Nowak v Data Protection Commissioner. Ireland's Supreme Court -Judgment of the Court (Second Chamber), (Case -434/16), 20 December 2017.
- Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV**. Court of Justice of the European Union**: PRESS RELEASE No 99/19. Judgment in Case C-40/17. Luxembourg, 29 July 2019. https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf.
- Google LLC, coming to the rights of Google Inc. V, Commission nationale de l'informatique et des libertés (CNIL). (In Case C-507/17). 24 September 2019. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=FR&mode=req&dir=&occ=first&part=1&cid=99559
- Ben Faiza v. France, 08.02.2018. (Application no. 31446/12). 8 February 2020.
- European Court of Human Rights: Dragan Petrović v. Serbia, 14 April 2020. (application no. 75229/10). file:///C:/Users/hp/Downloads/Judgment%20Dragan%20Petrovic%20v.%20Serbia%20%20rights%20violation%20owing%20to%20DNA%20mouth%20swab%20in%20absence%20of%20clear%20law.pdf.

(ISSN: 2537 - 0758)

- CASE OF P.N. v. GERMANY. (Application no. 74440/17), European Court of Human Rights. 11 June 2020. https://hudoc.echr.coe.int/.
- -CASE OF GAUGHRAN v. THE UNITED KINGDOM. (Application no.45245/15). Cour européenne des droits de l'homme. 13 June 2020. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]}
- Privacy International and Others v. the United Kingdom. (Application no. 46259/16), 4 September 2020.
- Orange România SA V, Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP). Court of Justice of the European Union. Case-no: C-61/19. (11 November 2020).
- https://curia.europa.eu/juris/document/document.jsf?text=&docid=233544&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1
- -LAND NORDRHEIN-WESTFALEN V. D.H.T Court of Justice of the European Union (CJE). No: C-620/1.
- 10 December 2020. https://curia.europa.eu/juris/document/document.jsf?text=&docid=235346
- Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others (Case C-623/17; ECLI: EU: C2020: 790) and La Quadrature du Net and Others, French Data Network and Others and Ordre des barreaux francophones et germanophone and Others (Cases C‑511/18, C‑512/18 and C-520/18; ECLI:EU: C:2020:791).
- CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM. (Applications no. 58170/13, 62322/14 and 24960/15). 25 May 2021.
- L.B. v. HUNGARY., European Court of Human Rights. (Application no. 36345/16). 12 Jan 2021.
- https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-207132%22].

- Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA V, Gegevensbeschermingsautoriteit. Court of Justice of the European Union (CJEU).C-645/19). 15 June 2021.
- https://curia.europa.eu/juris/document/document.jsf?text=&docid=242821
- Judgment of the Court (Grand Chamber) (request for a preliminary ruling from the Satversmes tiesa – Latvia) (Constitutional Court, Latvia). (Case C-439/19), 22 June 2021.
- https://curia.europa.eu/juris/document/document.jsf?text=&docid=244575&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=8508699.
- CASE OF LIEBSCHER v. AUSTRIA, European Court of Human Rights, (Application, no. 5434/17). 6 July 2021.
- https://hudoc.echr.coe.int.
- Judgment of 13 May 2014 (Grand Chamber), Google Spain and Google (C-131/12, EU: C 2014:317). Court of justice of the European union, "PROTECTION OF PERSONAL DATA". November 2021.
- Cookies: the CNIL fines GOOGLE €150 million and FACEBOOK €60 million for non-compliance with the law. 06 January 2022.https://www.cnil.fr/fr/cookies-la-cnil-sanctionne-google-hauteur-de-150-millions-deuros-et-facebook-hauteur-de-60-millions
- Human Rights League V Council of Ministers, Case C-817/19. Court of Justice of the European Union (CJE).OPINION OF THE ADVOCATE GENERAL MR GIOVANNI PITRUZZELLA. 27 January 2022. https://curia.europa.eu/juris/document/document.jsf?text=&docid=252841.
- CONCLUSIONS DE L'AVOCAT GÉNÉRAL M. GIOVANNI PITRUZZELLA.Ligue des droits humains v Conseil des ministre (Affaire C‑817/19), 27 janvier 2022.
- Human Rights League V Council of Ministers, Case C-817/19. Court of Justice of the European Union (CJE).OPINION OF THE ADVOCATE GENERAL MR GIOVANNI PITRUZZELLA., 27 January 2022.

(ISSN: 2537 - 0758)

- CASE OF STANDARD VERLAGSGESELLSCHAFT MBH v. AUSTRIA. Application no. 39378/15. European Court of Human Rights, (Fourth Section). 7 March 2022. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-213914%22]}
- La Cour des marchés: Décision quant au fond 46/2022 du 1er avril 2022. Numéro de dossier: DOS-2020-02892. 1 April 2022.https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-46-2022.pdf
- United States of America, Plaintiff, v. Epic Games, Inc. (FTC Matter/File Number 2223087), Civil Action Number 5:22-CV-00518-BO. Enforcement Type Civil Penalties Federal Injunctions. 12 September 2022. https://www.ftc.gov/legal-library
- Facial recognition: €20 million penalty against CLEARVIEW AI. 20 October, 2022.
- https://www.cnil.fr/fr/reconnaissance-faciale-sanction-de-20-millions-deuros-lencontre-de-clearview-ai
- Délibération de la formation restreinte n°SAN-2022-022 du 30 novembre 2022 concernant la société FREE. Délibération SAN-2022-022 du 30 novembre 2022 - Légifrance (legifrance.gouv.fr).
- European Court of Human Rights: (Drelon c. France - 3153/16 et 27758/18 Arrêt 8.9.2022 [Section V]). September 2022. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-13775%22]}
- Austrian Constitutional Court (Verfassungsgerichtshof-VfGH). (G 287/2022-16, G 288/2022-14). 14 Dec 2022.
- https://gdprhub.eu/index.php?title=VfGH_-_G_287/2022-16,_G_288/2022-14
- Deliberation of the restricted formation n ° SAN-2022-025 of December 29, 2022 concerning the company APPLE DISTRIBUTION INTERNATIONAL. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046907077.
- Deliberation of the restricted formation n ° SAN-2022-027 of December 29, 2022 concerning the companies TIKTOK INFORMATION TECHNOLOGIES UK LIMITED and TIKTOK TECHNOLOGY LIMITED. (Commission Nationale de

l'Informatique et des Libertés- Deliberation SAN-2022-027 of December 29, 2022. https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046977994?init=true&page=1&query=SAN-2022 027&searchField=ALL&tab_selection=all.

- European Court of Human Rights: JUDGMENT OF THE COURT (Fifth Chamber). Ministerstvo na vatreshnite raboti, Glavna direktsia za borba s Organiziranata prestapnost, (C-205/21). 26 January 2023. https://curia.europa.eu/juris/document/document.jsf?text=&docid=269704&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1
- Judgment of the Court (First Chamber), (request for a preliminary ruling from the Oberster Gerichtshof – Austria) – RW v Österreichische Post AG, (Case C-154/21). 12 January 2023.
- L.B. v. Hungary, (application no. 36345/16). European Court of Human Right. 9 March 2023. file:///C:/Users/hp/Downloads/Grand%20Chamber%20judgment%20L.B.%20v.%20Hungary%20%20systematic%20publishing%20of%20tax%20debtors%E2%80%99%20personal%20data%20breached%20the%20Convention.pdf

*Codes and laws:

- France Law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data and amending Law No. 78-17 of 6 January 1978 on data processing, files and freedoms.
- Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- Code pénal français. (Amended by Ordinance No. 2018-1125, of 12 December 2018).
- UK Public General Acts 2018.
- Regulation (EU) of the European (GDPR) 2016/679 of 27 April 2016.
- The Act of 1 August 2018 on the organisation of the National Data Protection Commission and the general data protection framework.

(ISSN: 2537 - 0758)

- The Act of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal and national security matters.
- The Act of 30 May 2005 regarding the specific rules for the protection of privacy in the sector of electronic communications.
- Luxembourgian Act Regulating the Use of Nominal Data.
- Swedish Data Act -1988.
- Swedish Bookkeeping Act (SFS 1999).
- Code du patrimoine Dernière modification: 12-3-2023.
- Code du patrimoine 20 février 2004.