تعزيز الحماية القانونية للبيانات الشخصية الحساسة في مجال الاستدلالات

"دراسة مقارنة"

Strengthening the legal protection
of sensitive personal data in the
field of inferences
A comparative study""

إعداد

د / سمير سعد رشاد سلطان

مدرس بقسم القانون المدني

كلية الحقوق – جامعة المنصورة

Dr.Samir Saad Rashad

Lecturer, Department of Civil Law

Faculty of law

Mansoura university

تعزيز الحماية القانونية للبيانات الشخصية الحساسة في مجال الاستدلالات "دراسة مقارنة"

ملخص:

يشير مفهوم البيانات الشخصية الحساسة لمجموعة من البيانات التى قد يترتب على معالجتها آثار قانونية بالغة إذا ما تم مقارنتها بالبيانات الشخصية العادية، وهى أضرار تميزية، ولها تأثيراتها المباشرة على الحقوق الأساسية للأفراد.

وتظهر إشكاليات جمع ومعالجة البيانات الحساسة، بشكل خاص، في مجال عمليات الاستدلالات، وهو ما يشير لقصور التعريف التشريعي للبيانات الحساسة، وكذلك الحماية القانونية لها، خاصة في عصر التكنولوجيا المتطورة والبيانات الضخمة والتى تعتبر آلية أساسية تقوم عليها عمليات الاستدلال.

وتستوجب التكنولوجيا المتقدمة في مجال الاستدلالات إعادة النظر في صياغة مفهوم البيانات الحساسة، بهدف تقرير الحماية الفاعلة لها، وكذلك تقرير حقوق أصحاب تلك البيانات من خلال نصوص قانونية صريحة لا تحتمل الجدل بشأنها.

وتتمتع البيانات الشخصية، سواء المقدمة من الأشخاص المعنيين بالبيانات، أو تلك المستنتجة التي تم التوصل إليها من خلال عمليات الاستدلالات، بأهمية بالغة من الناحية التجارية والاقتصادية حيث تستفيد الغالبية العظمى من الشركات الحديثة من بيانات المستهلك لإنشاء رؤى تجارية، مثل أغراض الإعلانات المستهدفة، وإنشاء ملفات تعريف للعملاء، بل في السنوات الأخيرة، أصبحت هذه الممارسة حاسمة للحفاظ على القدرة التنافسية في العديد من الصناعات.

Abstract

The concept of sensitive personal data refers to a group of data whose processing may have significant legal consequences if compared to regular personal data, which are discriminatory damages, and have direct effects on the basic rights of individuals.

The problems of collecting and processing sensitive data appear, in particular, in the field of inference processes, which indicates a deficiency in the legislative definition of sensitive data, as well as legal protection for it, especially in the era of advanced technology and big data, which is considered a basic mechanism upon which inference processes are based.

Advanced technology in the field of inferences requires reconsidering the formulation of the concept of sensitive data, with the aim of determining effective protection for it, as well as determining the rights of the owners of that data through explicit legal texts that cannot be disputed.

Personal data, whether provided by data subjects, or inferred through inference processes, is of great importance from a commercial and economic perspective, as the vast majority of

modern companies make use of consumer data to create commercial insights, such as for targeted advertising purposes, and to create profiles. Introducing customers, but in recent years, this practice has become crucial to maintaining competitiveness in many industries.

مقدمة عامة

تعتبر البيانات الحساسة إحدى فئات البيانات والتى يترتب على الافصاح عنها بأي صورة من الصور سواء من خلال جمعها أو استخدامها أو معالجتها أو تخزينها أو إتاحتها تشكل خطرًا أكبر مقارنة بأشكال البيانات الأخرى.

وكثيراً ما يُنظر إلى هذه المخاطر من حيث الاحتمال المرتفع للتمييز، أو الأضرار ذات الصلة، التي تتعرض لها الفئات الضعيفة في المجتمع فيما يتعلق بحقوقهم الأساسية، وكذلك إمكانية انتهاك هذه البيانات لأغراض تجارية واقتصادية، وهى جميعها مبررات لحماية البيانات الشخصية بصفة عامة، والحساسة بصفة خاصة.

ونتيجة لذلك، توقعت أطر حماية البيانات تقليديًا وجود عبء أكبر لمعالجة البيانات الحساسة مقارنة بأشكال البيانات الأخرى.

ولا شك أن حماية البيانات الشخصية ترتبط ارتباطاً وثيقاً بالحق في الخصوصية، كما أن الحق في الخصوصية يرتبط كذلك بالشخصية القانونية للإنسان، ولقد أصبح حماية الحق في خصوصية الأفراد يحيطه الكثير من المخاطر، وبصفة خاصة، في عصر ما يسمى بالبيانات الضخمة، وتطور وانتشار تقنيات الذكاء الاصطناعي، بل وكذلك ارتباط العديد من الخدمات التي يتوقف تقديمها للأشخاص على ضرورة تقديم بيانات شخصية أو حساسة.

وستكون المعركة الحقيقية هي تجاوزا الخط الفاصل بين حماية خصوصية المواطنين وتسهيل النمو التكنولوجي للوسائل الحديثة المبتكرة، مما يتطلب معه ضرورة تحقيق قدر من التوازن بينهما.

وإذا كان الوصول للبيانات الشخصية أو الحساسة قد أصبح أمراً معتاداً وبشكل مستمر، بل قد لا يحتاج الأمر لسعي دءوب من قبل المتحكم في البيانات أو المعالج لها، حيث قد يقوم صاحب البيانات بتقديمها بنفسه طواعية واختياراً بهدف الحصول على الخدمات المختلفة، إلا أنه في مجال الاستدلالات على البيانات فإن الأمر جد مختلف، حيث تقوم عملية الاستدلال على نوعين من البيانات، وهما البيانات المدخلة والبيانات المستنتجة أو المشتقة.

وفي هذا الصدد تختلف عمليات المعالجة عن عمليات الاستدلال من حيث جوهر هذه العمليات، وهو ما يؤدي لنتائج خطيرة على حقوق الأفراد، وكذلك قواعد المسئولية المدنية حال الرجوع بالتعويض.

علاوة على ذلك، فإنه في عصر الذكاء الاصطناعي والبيانات الضخمة أصبحت عمليات الاستدلال على البيانات الشخصية، وكذلك الحساسة ميسرة بشكل كبير، وهو ما يمكن أن تكون معه الخطورة أكبر بكثير على التأثير على الحقوق الأساسية للأفراد، وإمكانية التحيز والتمييز، وهو الأمر الذي يستدعى معه إعادة النظر في القواعد التشريعية المنظمة لحماية البيانات، أوروبياً ومصرياً، بهدف التحقق من مدى ملائمتها لتحقيق أغراض في عصر الاستدلالات بشقيها: المعقولة، وعالية المخاطر.

وقد قنن المشرعون للحماية الواجبة للبيانات الشخصية، بل وكذلك للفئات الخاصة المحمية منها وهى ما تعرف بالبيانات الشخصية الحساسة، وتقرير حماية قانونية مشددة بالنسبة للبيانات الشخصية الحساسة.

وعلى الرغم من ذلك، تثير التحديات الكبرى مع انتشار التقنيات العالية والدقيقة لأنظمة الذكاء الاصطناعي، والكم الهائل من البيانات والذي تجاوز ما يمكن تصوره عقلاً، خطورة التوصل ومعالجة البيانات الحساسة، ويظهر ذلك، بشكل جلي، من خلال

عمليات الاستدلالات على البيانات الحساسة، والتي أصبح من اليسير الوصول والتعرف عليها وربطها بأشخاص محددين من خلال بعض البيانات سواء الشخصية، أو غير الشخصية، أو البيانات مجهولة المصدر.

ويشير ذلك بوضوح لضرورة التوسع في مفهوم البيانات الحساسة، بحيث يمكن معها اعتبار البيانات التي يمكن أن تؤدى لاستدلالات حساسة تكون هي الأخرى كذلك، وهو موقف يمكن فهمه، ولو بشكل ضمني، من خلال التشريعات المنظمة لحماية البيانات، سواء على المستوى الأوروبي أو المحلي، كما يمكن اعتبارها كذلك وفق قضاء محكمة العدل الأوروبية بشكل صريح.

وتتمتع البيانات بصفة عامة سواء الشخصية أو الحساسة، والمقدمة من الأشخاص المعنيين بالبيانات، أو تلك المستنتجة التي تم التوصل إليها من خلال عمليات الاستدلالات، بأهمية بالغة من الناحية التجارية والاقتصادية حيث تستفيد الغالبية العظمى من الشركات الحديثة من بيانات المستهلك لإنشاء رؤى تجارية، مثل أغراض الإعلانات المستهدفة، وإنشاء ملفات تعريف للعملاء، بل في السنوات الأخيرة، أصبحت هذه الممارسة حاسمة للحفاظ على القدرة التنافسية في العديد من الصناعات.

ووفقاً لذلك تثار تساؤلات حول مدى الاعتراف لأصحاب البيانات بالحق على بياناتهم، وإن اختلفت الرؤى حول طبيعة هذا الحق بين اعتباره من الحقوق الأساسية للأفراد، أم أنه يمكن تكييفه على أنه حق ملكية فكرية من نوع جديد، ونطاق هذا الحق أي يكون للبيانات ذاتها أم يمتد لأي بيانات يمكن الاستدلال من خلالها على بيانات حساسة.

وإذا كان المشرعين الأوروبي والمصري قد قننا لفكرة المسئولية والتي يمكن اعتبارها إحدى صور حماية البيانات الحساسة، إلا أنها مع ذلك فكرة تقوم في عموميتها على تطبيق القواعد العامة في المسئولية المدنية، وحتى مع ذلك الأمر فإن عملية

الاستدلالات على البيانات الحساسة تثير إشكاليات خاصة في مجال تطبيق هذه المسئولية، ويظهر ذلك جلياً من خلال اختلاف كلاً من المعالجة والاستدلال من حيث جوهرهما كعمليات تتعلق بالبيانات، وكذلك من حيث إقامة هذه المسئولية عن الإخلال بالمتطلبات والقيود والالتزامات القانونية بتشريعات حماية البيانات، أو كذلك بشأن تقنيات الذكاء الاصطناعي التي يتم إجراء عمليات الاستدلال من خلالها.

إشكالية البحث:

نحاول من خلال هذا البحث تسليط الضوء على عملية الاستدلال على البيانات الشخصية الحساسة.

ونعرض للمفهوم الذي قرره المشرع المصري للبيانات الحساسة، وكذلك المفهوم المقنن باللائحة العامة الأوروبية لحماية البيانات الشخصية لعام ٢٠١٦، ومدى توافق النهج التشريعي لتعريف البيانات الحساسة مع التطبيق العملي، خاصة، في مجال عمليات الاستدلالات، حيث أصبح النهج القائم حالياً على فكرة القائمة الحصرية للبيانات الحساسة غير مجد في ظل الاستدلالات المعتمدة على البيانات الضخمة وأنظمة الذكاء الاصطناعي، وهو ما يتطلب ضرورة البحث عن معيار جديد لتحديد البيانات الحساسة وتقرير الحماية المناسبة لها.

ومن إشكاليات هذه الدراسة أيضاً عدم وضع تنظيم قانوني متكامل ودقيق لعمليات الاستدلال على البيانات الحساسة، سواء منها الاستدلالات المعقولة، وكذلك الاستدلالات عالية المخاطر، وتأثيراتها المختلفة على الحقوق الأساسية للأشخاص.

كما تظهر إشكالية مدى تمتع عمليات الاستدلال بالصفة الشخصية للبيانات، بحيث يمكن معها إخضاعها للأحكام القانونية المقررة للحقوق والالتزامات بقانون حماية البيانات الشخصية.

ويظهر ذلك، جلياً، في التفسيرات المختلفة حول الاعتراف بحقوق أصحاب البيانات على البيانات الحساسة التي تم الاستدلال عليها.

كما نبين من خلال هذه الدراسة لمدى كفاية وقابلية القواعد القانونية الواردة بقانون حماية البيانات الشخصية واللائحة العامة الأوروبية لحماية البيانات والمتعلقة بمعالجة البيانات الحساسة، ومدى اختلاف هذه المعالجة عن عمليات الاستدلالات.

وبلاشك أن لكل هذه الاشكاليات تأثيراتها على مجال المسئولية المدنية، وهو ما نحاول بيانه من خلال عرض المسئولية المدنية الناشئة عن معالجة البيانات الحساسة، وإشكاليات هذه المسئولية في مجال الاستدلالات.

منهج الدراسة:

تفرض علينا مقتضيات البحث العلمي ضرورة تحديد منهجاً أو أكثر من مناهج البحث العلمي.

لذا فاني اتبعت في عرض هذه الدراسة منهجا وصفياً تحليلياً مقارناً، حيث قمت بوصف عملية الاستدلالات على البيانات الشخصية الحساسة بنوعيها: الاستدلالات المعقولة، والاستدلالات عالية المخاطر، مع استعراض النصوص التشريعية المنظمة لحماية البيانات الحساسة، وقمت بتحليل هذه النصوص ومدى ملاءمتها وكفايتها للتطبيق، وبطبيعة الحال تم استعراض أكثر من موقف قانوني في الأنظمة المقارنة خاصة بعض نصوص القانون الفرنسي، واللائحة العامة الأوروبية لحماية البيانات الشخصية، إضافة لعرض موقف القانون المصري من الإشكالات المختلفة التي تطرحها عملية الاستدلال على البيانات الحساسة.

خطة البحث:

سوف نقسم هذا البحث لأربعة فصول متتالية، نعرض من خلال الفصل الأول ماهية البيانات الحساسة، مع تقييم نهج المشرع في تحديدها، ومدى ملائمة ذلك النهج في ظل إمكانية الاستدلالات عليها من خلال الوسائل التكنولوجية المتطورة، ونعرض في الفصل الثاني لعملية الاستدلال على البيانات الشخصية الحساسة ومدى تنظيمها من الناحية القانونية والحماية المقررة لأصحاب البيانات بشأنها، ومدى ملائمة قواعد حماية البيانات الحالية لمواجهة عمليات الاستدلالات، ونعرض في الفصل الثالث صور حماية البيانات الحساسة سواء ما تعلق منها بمعالجتها أو الاستدلال عليها، وكذلك الاعتراف بحقوق أصحاب البيانات في مجال الاستدلال، وفي الفصل الرابع نعرض للمسئولية المدنية عن معالجة البيانات الحساسة وإشكاليات المسئولية في مجال الاستدلالات.

الفصل الأول: ماهية البيانات الحساسة.

الفصل الثاني: الاستدلال على البيانات الشخصية الحساسة.

الفصل الثالث: صور الحماية المشددة للبيانات الحساسة.

الفصل الرابع: المسئولية المدنية الناشئة عن معالجة البيانات الحساسة والاستدلال عليها.

الفصل الأول

ماهية البيانات الحساسة

تحدد قوانين حماية البيانات في العديد من البلدان أنواعًا أو فئات معينة من البيانات، والتي تتلقى حماية أكبر من البيانات الشخصية العادية، ويشار إلى هذه الأنواع من البيانات باسم "فئات خاصة من البيانات" أو "بيانات حساسة".

وظهرت أهمية البيانات الشخصية بصفة عامة، والبيانات الحساسة بصفة خاصة، في السنوات القليلة الماضية، خاصة مع تزايد نمو اقتصاديات البيانات والتي تعتمد عليها الشركات التكنولوجية الكبرى، مما استدعى الأمر ضرورة وجود تنظيم تشريعي لحماية البيانات الشخصية والحساسة.

كما تظهر أهمية هذا الأمر من خلال النمو الهائل في مجال التكنولوجيات المتطورة، والتي يمكن من خلالها الاستدلال على البيانات الحساسة، وهو ما يدعو لضرورة النظر في قراءة القواعد التشريعية المنظمة لحماية البيانات في ضوء تلك التطورات، نظراً لما قد يترتب عليها من أضرار يصعب تجاوزها.

ونعرض من خلال هذا الفصل لمبحثين، نعرض من خلال المبحث الأول المقصود بالبيانات الحساسة، والنهج التشريعي في تحديها سواء بالنسبة للقانون المصري، وكذلك الموقف المقارن في ظل اللائحة العامة لحماية البيانات الشخصية الصادرة عن البرلمان الأوروبي، ونبين أيضاً مبررات حمايتها من خلال حماية مشددة عن تلك المقررة للبيانات الشخصية خاصة في مجال الاستدلالات، ونبين كذلك الطبيعة القانونية للبيانات ومدى اعتبارها حقاً لأصحابها.

ونعرض في المبحث الثاني للمعايير التي يمكن الاعتماد عليها في تحديد البيانات الحساسة، ونبين للمعيار الذي اعتنقه المشرع في تحديد البيانات الحساسة، والمعايير الأخرى المقترحة في هذا الشأن خاصة في ظل تطور تحديد البيانات الحساسة في عصر الاستدلالات الحديثة.

ونعرض لذلك فيما يلي:

المبحث الأول: المقصود بالبيانات الحساسة ومبرراتها وطبيعتها القانونية.

المبحث الثاني: معايير تحديد البيانات الحساسة.

المبحث الأول

المقصود بالبيانات الحساسة ومبرراتها وطبيعتها القانونية

لا شك أن القوانين المتعلقة بالخصوصية تبرز بشكل فاعل من خلال الأنشطة التي تتضمن بيانات شخصية، ويظهر من خلال قانون حماية البيانات الشخصية مظاهر الحماية المقررة للبيانات، مما تنعكس بآثارها على تعزيز احترام الحق في الخصوصية(١)، حيث ترتبط البيانات بالحق في الخصوصية ارتباطاً وثيقاً.

وتعزز قوانين حماية البيانات في مختلف التشريعات المقارنة حماية البيانات الحساسة، ويشير المعلقون إلى البيانات الحساسة باعتبارها "الأساس المتين لحماية البيانات الحديثة" (٢).

ومن الجدير بالذكر أن قوانين حماية البيانات لا تغطي جميع البيانات، وإلا فإنها ستكون بلا حدود، لذا فهي تقصر نطاق البيانات محل الحماية على البيانات المتعلقة بالأشخاص، وبالتالي، فإن الحماية المقررة بقانون حماية البيانات تتعلق بما يدخل في نطاق البيانات الشخصية للأشخاص الطبيعين.

وغالباً ما تضع القوانين المقارنة لحماية البيانات مستويين لحماية البيانات، حيث تضع قواعد لحماية البيانات الشخصية، ثم تقرر حماية البيانات الحساسة من خلال

(1) Daniel J. Solove, The Limitations of Privacy Rights, 98 NOTRE DAME L. REV., 2023, p. 975.

(2) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1583.

متطلبات مشددة من خلال القيود المفروضة على الكشف عنها، وجمعها، ومعالجتها، وإتاحتها.

ونعرض من خلال هذا المبحث لتعريف البيانات الشخصية الحساسة، ونهج تحديدها، والتطورات التاريخية لنشأة البيانات الحساسة، ومبررات تعزيز الحماية القانونية للبيانات الحساسة، ونعرض لذلك فيما يلي:

المطلب الأول: تعريف البيانات الحساسة

المطلب الثاني: مبررات حماية البيانات الحساسة في عصر الاستدلالات

المطلب الثالث: الطبيعة القانونية للبيانات الحساسة

المطلب الأول

تعريف البيانات الحساسة

نعرض من خلال هذا المطلب لتعريف البيانات الحساسة، وقد تم تعريفها تشريعياً من قبل المشرع المصري وكذلك المشرع الأوروبي باللائحة العامة لحماية البيانات الشخصية، ثم نعرض لمدى ملائمة هذا التعريف في ظل عصر الاستدلالات على البيانات الحساسة من خلال آليات ووسائل تكنولوجية متطورة.

الفرع الأول

التعريف التشريعي للبيانات الحساسة

عرف المشرع المصري البيانات الشخصية الحساسة[٣] بكونها" 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."

كما عرفتها اللائحة العامة الأوروبية لحماية البيانات الشخصية بكونها البيانات المتعلقة بالبيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني، أو الآراء السياسية، أو المعتقدات الدينية أو الفلسفية، أو عضوية النقابات العمالية، ومعالجة البيانات الجينية، والبيانات البيومترية بغرض تحديد هوية الشخص الطبيعي بشكل فريد، أو البيانات المتعلقة بالصحة أو البيانات المتعلقة بالتوجه الجنسي لشخص طبيعي[٤].

ويأتي هذا التعريف من المشرع للبيانات الحساسة اعترافاً من المشرع بأن البيانات ليست جميعها متماثلة، فقد انتهج المشرع تقسيماً مقنناً للبيانات ويتمثل في

---

(٣) المادة الأولى من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية ، نشر بتاريخ ٢٠٢٠/٧/١٥، الجريدة الرسمية ٢٨، مكرر (ه).

(4) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 9 (1).

وصدرت اللائحة العامة رقم ٦٧٩/٢٠١٦ عن البرلمان الأوروبي والمجلس بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة البيانات، وتم اعتمادها في ٢٧ أبريل ٢٠١٦ ودخلت حيز التنفيذ في ٢٥ مايو ٢٠١٨، ويشار إليها بعد ذلك خلال هذه الدراسة باختصار: (GDPR)

البيانات الشخصية والبيانات الحساسة، ويوفر تصنيف البيانات الحساسة وفقاً لهذا التقسيم المزيد من الحماية، مثل القيود المفروضة على استخدام البيانات، ومتطلبات الموافقة، ومتطلبات تقييم المخاطر.

ولا شك أن تعداد المشرع للبيانات الحساسة يحتاج لتوضيح، خاصة أن التعريف الذي قرره المشرع للبيانات الحساسة قد تضمن العديد من المصطلحات العامة والفضفاضة والتي يجب على الأقل تحديد مضمونها، والتعرف عليها بشكل دقيق، كما أن المشرع بالقانون ذاته ضمن مادة التعريفات به لم يورد تعريفاً لتلك المصطلحات، ومن هذه المصطلحات والتي اعتبرها المشرع من البيانات الحساسة: البيانات الجينية، والبيانات البيومترية والقياسات الحيوية، وهى بيانات غير دارجة بشكل عام مما يتطلب الأمر تحديد مفهومها بشكل دقيق، كما أن اللائحة التنفيذية لقانون حماية البيانات الشخصية المصري لم تصدر بعد، وهي حاجة ملحة لسرعة إصدارها.

وقد حدد المشرع المصري البيانات الحساسة على سبيل الحصر لا المثال، وحددها بكونها البيانات الصحية (خاصة الصحة النفسية أو العقلية أو البدنية أو الجينية)، وبيانات القياسات الحيوية "البيومترية"، والبيانات المالية، والبيانات المتعلقة بالمعتقدات الدينية، والبيانات المتعلقة بالآراء السياسية أو الحالة الأمنية، كما اعتبر بيانات الأطفال من البيانات الشخصية الحساسة.

واتجهت اللائحة العامة الأوروبية لحماية البيانات لوضع تعريفات لتلك المصطلحات، فقد عرفت البيانات المتعلقة بالصحة بأنها البيانات الشخصية المتعلقة بالصحة الجسدية أو العقلية للشخص الطبيعي، بما في ذلك تقديم خدمات الرعاية الصحية، والتي تكشف عن معلومات حول حالته الصحية(٥).

(5) GDPR, art. 4 (15).

كما عرفت البيانات الجينية بكونها البيانات الشخصية المتعلقة بالخصائص الجينية الموروثة أو المكتسبة للشخص الطبيعي والتي تعطي معلومات فريدة عن فسيولوجيا أو صحة ذلك الشخص الطبيعي والتي تنتج، على وجه الخصوص، من تحليل عينة بيولوجية من الشخص المعني(٦)، ولذلك يعتبر البعض أن البيانات الجينية ليست ببيانات شخصية، بل بيانات حساسة يجب أن تتمتع بوضع قانوني خاص ووقائي للغاية(٧).

وتم تعريف البيانات البيومترية بأنها البيانات الشخصية الناتجة عن معالجة تقنية محددة تتعلق بالخصائص الجسدية أو الفسيولوجية أو السلوكية لشخص طبيعي، والتي تسمح أو تؤكد التعرف الفريد لذلك الشخص الطبيعي، مثل صور الوجه أو بيانات تنظير الأصابع(٨).

وحسناً ما فعلته اللائحة العامة لحماية البيانات من وضع تعريفات محددة ودقيقة لفئات البيانات الحساسة، خاصة أنها مصطلحات فنية تتطلب المزيد من التوضيح، ولم يقدم المشرع المصري، على الأقل، تعريفاً واضحاً ومحدداً لبعض الفئات الحساسة من البيانات والتي تعتبر مصطلحات غير دارجة أو شائعة، بل اكتفى بتركها للفهم الدارج بشأنها.

واعترف المشرع المصري بالبيانات المالية على أنها من البيانات الحساسة، وعلى الرغم من اعتبارها بيانات حساسة إلا أنه قد استثنى البيانات الشخصية لدى البنك

(6) GDPR, Art. 4 (13).

(٧) د. طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية، دراسة تحليلية مقارنة، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، العدد ١٢، مجلد ٨، ٢٠٢٠ ص ٣٩١٠.

(8) GDPR, Art. 4 (14).

المركزي والجهات الخاضعة لرقابته وإشرافه من الخضوع لأحكام قانون حماية البيانات الشخصية[٩].

واعتبر المشرع كل البيانات المتعلقة بالأطفال بيانات شخصية حساسة، وتطلب المشرع ضرورة موافقة ولى الأمر في حالة جمع أو نقل أو تخزين أو معالجة البيانات المتعلقة بالأفراد.

وتتميز البيانات الشخصية للإنسان بكونها من الأمور الملازمة لشخصية الإنسان، مما يعنى أنها مرتبطة بصاحبها، وله وحده الحق عليها، وله وحده دون غيره حق استعمالها باعتبار هذا الحق مرتبط بصاحبه وحده[١٠].

ونشير هنا إلى أن البيانات الحساسة التى تم النص عليها سواء باللائحة العامة لحماية البيانات[١١]، أو كذلك القانون المصري قد وردت على سبيل الحصر.

(٩) المادة الثالثة من مواد الاصدار للقانون رقم (١٢١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(١٠) د. بولين أنطونيوس أيوب، الحماية القانونية للحياة الخاصة في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٩، ص ٣٤٠.

(١١) ويعنى ذلك أنه لا يجوز للدول الأعضاء بالاتحاد الأوروبي إضافة بيانات أخرى ضمن نطاق البيانات الحساسة.

(Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1589.)

الفرع الثاني

التوسع في البيانات الحساسة في عصر الاستدلالات

يتضح من النهج التشريعي سواء في القانون المصري، وكذلك القانون المقارن، اعتماد المشرع في تعريفه للبيانات الحساسة بكونها مجموعة من البيانات التى تم تعدادها على سبيل الحصر.

ولا شك أنه في عصر التكنولوجيا المتطورة لم يعد هذا النهج كافياً، خاصة في حالة تطبيق الهدف من الحماية المشددة للبيانات الحساسة، ويظهر ذلك من خلال عمليات الاستدلالات الواسعة، حيث يمكن الوصول للبيانات الحساسة بشكل قد لا يمثل خرقاً لقانون حماية البيانات.

وما يؤكد ذلك، خلال السنوات الماضية، تم استخدام العديد من البرامج والتطبيقات في مجالات مختلفة يمكن من خلالها التوصل لبيانات حساسة من خلال بيانات توصف بكونها عادية، حتى ولو لم تكن بيانات شخصية إلا أنه مع ذلك قد أدت إلى التوصل لبيانات حساسة، وهو ما يستدعى إعادة النظر في المفهوم الذي يجب أن تعرف بمقتضاه البيانات الحساسة، مع ضرورة التوسع في هذا الأمر ليشمل البيانات العادية أو حتى مجهولة المصدر والتي لا تحتوى على عنصر واضح لتحديد الهوية باعتبارها بيانات حساسة إذا أدت عملية الاستدلال من خلالها لبيانات حساسة.

وعلى ذلك يجب إعادة النظر في المفهوم التشريعي للبيانات الحساسة، والابتعاد عن فكرة القوائم الحصرية لهذه البيانات، مع ضرورة التوسع في تحديد البيانات الحساسة باعتبار أي بيانات شخصية أو عادية يمكن الاستدلال من خلالها على بيانات حساسة تعتبر هي الأخرى من قبيل البيانات الحساسة وتخضع لذات الحماية المشددة.

علاوة على ذلك، يمكن أن نقترح ضرورة النص على قاعدة عامة بشأن تحديد البيانات الحساسة، ومؤدى هذه القاعدة أن البيانات الحساسة تكون هى البيانات التى يمكن أن يترتب على معالجتها أو استخدامها ضرراً جسيماً أكثر من غيرها من البيانات وذلك في ضوء سياق وغرض معالجتها أو الاستدلال عليها، على أن يمنح القاضي سلطة تقديرية واسعة في هذا الإطار.

وفي هذا الصدد، نشير إلى أن محكمة العدل الأوروبية قد تبنت تفسيراً موسعاً لمفهوم البيانات الحساسة وفقاً للمادة التاسعة من اللائحة العامة لحماية البيانات، وينبغي الاعتماد على هذا التفسير لمفهوم البيانات الحساسة، حيث أن المادة التاسعة من اللائحة العامة لحماية البيانات لا يمكن تفسيرها على أنها تعني أن معالجة البيانات الشخصية التي من المحتمل أن تكشف، بشكل غير مباشر، عن معلومات حساسة تتعلق بشخص طبيعي معفاة من نظام الحماية المعزز المنصوص عليه في الأحكام المذكورة، ما لم يقوض التأثير المفيد لهذا النظام والحماية للحريات والحقوق الأساسية للأشخاص الطبيعيين التي تهدف إلى ضمانها، مثل الكشف عن بيانات حساسة من خلال استخدام بيانات شخصية عادية[١٢].

ويعنى ذلك أن الحظر يشمل البيانات الشخصية الحساسة لشخص محدد الهوية أو يمكن التعرف عليه بشكل مباشر أو غير مباشر، وكذلك تمتد الحماية المعززة للبيانات الحساسة لتشمل البيانات الشخصية العادية طالما يمكن التوصل والاستدلال من خلالها على بيانات حساسة.

(12) CJUE 1er août 2022, no C-184/20, pt 127.

ويمكن التأكيد على ذلك من خلال الرأي المقدم من مجموعة فريق عمل المادة ٢٩[١٣] فيما يتعلق بمسألة المعلومات الحساسة التي يمكن أن تنشأ من صورة شخص يمكن التعرف عليه وخلصت إلى ما يلي: " في بعض الدول الأعضاء في الاتحاد الأوروبي، تعتبر صور أصحاب البيانات فئة خاصة من البيانات الشخصية، حيث يمكن استخدامها للتمييز بين الأصل العرقي أو الإثني أو لاستنتاج المعتقدات الدينية أو البيانات الشخصية بالنسبة للصحة، ولا يعتبر بشكل عام، الصور الموجودة على الإنترنت بيانات حساسة ما لم يتم استخدامها بشكل واضح للكشف عن بيانات حساسة حول الأفراد"[١٤].

المطلب الثاني

مبررات حماية البيانات الحساسة في عصر الاستدلالات

لا تعد جميع البيانات الشخصية متماثلة، لذا يظهر منها البيانات الحساسة والتي ينبغي توفير حماية مشددة لها، لذا يمكن أن تعتبر بعض البيانات الشخصية غير ضارة تمامًا، بينما يمكن أن تكون البيانات الأخرى كاشفة أو ضارة بسمعة الشخص، مثل البيانات المتعلقة بإصابة الشخص بمرض مميت، ويمكن أن يعاني الشخص أيضًا من

(١٣) تجدر الإشارة إلى أنه اعتبارًا من تطبيق اللائحة العامة لحماية البيانات ("GDPR") في ٢٥ مايو ٢٠١٨، لم يعد فريق عمل المادة ٢٩ موجودًا وخلفه المجلس الأوروبي لحماية البيانات ("EDPB")

European Data Prot. Bd., The European Data Protection Board, Endorsement 1/2018 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_ of_ wp29_documents.pdf [https://perma.cc/8H9A-RQR3]

(14) Groupe 29, Avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne, WP 163.

التمييز، حيث يجد صعوبة في تعيينه في وظيفة أو الحصول على قرض، لذلك يمكن أن يصاب الشخص بضرر بسمعته إذا تم الكشف عن هذه البيانات مما تتطلب معها تقرير حماية مشددة.

ولا تقدم العديد من القوانين أي مبررات محددة لسبب حماية البيانات الحساسة، أو كذلك مبررات لتصنيف بعض البيانات على أنها ذات طبيعة حساسة، ولذلك يعد ما قيل بشأن مبررات حماية البيانات الحساسة يصدق كذلك على جميع البيانات الشخصية.

ونعتقد أن مبررات الحماية الحقيقية للبيانات الحساسة قد تتضح بشكل كبير في مجال الاستدلالات على هذه البيانات، وبصفة خاصة في عصر البيانات الضخمة والذكاء الاصطناعي.

وتظهر مبررات مفهوم البيانات الحساسة – أو الفئات الخاصة للبيانات الشخصية – من خلال الصياغات القانونية الدولية لحماية البيانات، حيث يمكن العثور على مبرر لحماية مشددة للبيانات الحساسة.

ولذلك يمكن أن تستند الحماية المشددة للبيانات الحساسة لمبررات جديرة بالإقناع، كما يمكن تقرير الحماية المشددة لها باعتبار ذلك غاية في حد ذاتها[١٥].

وتكمن ضرورة الحماية المشددة للبيانات الحساسة في عصر الاستدلالات المتطورة لاعتبارات تتمثل في المخاطر الكبرى لاستدلالات البيانات الضخمة والذكاء الاصطناعي، كما تجد الحماية المشددة مبرراً لها في الحماية من المخاطر التي تهدد الحقوق والحريات الأساسية، وكذلك الحماية من التمييز غير القانوني.

ونعرض لهذه المبررات تباعاً.

---

(15) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1587.

أولاً: المخاطر الكبرى لاستدلالات البيانات الضخمة والذكاء الاصطناعي:

تطورت عملية الوصول والاستدلال على البيانات الحساسة بشكل كبير وملفت، في السنوات الأخيرة، في عصر ما يعرف بالبيانات الضخمة والذكاء الاصطناعي، الأمر الذي يؤدي لاستدلالات وتنبؤات غير طبيعية، بل وكثيراً لا يمكن التحقق منها حول سلوكيات الأشخاص مثل خدمات الاعلانات، وحياتهم الخاصة، وبياناتهم الحساسة كالعرق والبيانات الصحية وغيرها، وتتم عمليات الاستدلال من خلال بيانات متنوعة ويترتب عليها خلق فرص جديدة للتوصيف واتخاذ القرارات التميزية والمتحيزة(١٦).

كما تؤدى الاستدلالات على البيانات الحساسة لإنشاء ملفات تعريفية للأشخاص والمجموعات، مما يمكن أن ترتبه من آثار متعددة على حقوقهم وحرياتهم.

ويوضح ذلك من خلال الاتجاه السائد في مجتمعات المعلومات المتقدمة لإنشاء البيانات والملفات الشخصية والمعلومات الأخرى المتعلقة بالأفراد ومشاركتها وبيعها والاحتفاظ بها يمثل تحديات إضافية(١٧).

يمكن إنشاء السجلات الدائمة من خلال التحليلات الاستدلالية، التي تتكون من استنتاجات غير متوقعة وربما مثيرة للقلق، وتكشف عن معلومات وتنبؤات حول الحياة الخاصة والسلوكيات والتفضيلات التي قد تظل خاصة لولا القيام بتلك الاستدلالات.

(16) Tal Z. Zarsky, Understanding Discrimination in the Scored Society, 89 Wash. L. Rev., 2014, p. 1375.

(17) Luciano Floridi, Mature Information Societies - a Matter of Expectations, 29 Phil. & Tech, 2016, p. 1,

كما يمكن استخدام نتائج الاستدلالات بصورة ضارة من خلال دفع الأشخاص والتلاعب بهم لاتخاذ قرارات هامة مثل التوظيف وفرص العمل والحصول على القروض.

وأشار المعلقون، في هذا الصدد، إلى أن عملية صنع القرار الآلي، والتوصيف، وتقنيات التعلم الآلي ذات الصلة تشكل فرصًا جديدة لاتخاذ قرارات تنتهك الخصوصية، وتمييزية، ومتحيزة بناءً على التحليلات الاستدلالية(١٨).

وتكمن الخطورة بشكل واضح هنا في أنه لا يمكن لأي من التطبيقات التى يتم استخدامها في عمليات الاستدلال أن تدعي أنها تولد استنتاجات أو تنبؤات على وجه اليقين المطلق، وفي العديد من الحالات، عانت من إخفاقات واضحة للغاية (مثل Google Flu Trends) (١٩).

ولا شك أن هذه الاستدلالات يتم استخدام العديد منها فقط للإعلانات المستهدفة، بما قد تمثله من مخاطر لا سيما عندما يكون من الصعب التحقق من هذه الاستنتاجات أو عندما لا يحصل الأفراد المتأثرون على أي فائدة، وبالتالي، أصبح من الشائع على نحو متزايد نشر التحليلات الاستدلالية على نطاق واسع، استنادا فقط إلى القدرة على القيام بذلك والدقة المتصورة للطريقة أو الاعتقاد بأن الكفاءة أو الإيرادات سوف تتحسن، وكلها اعتبارات اقتصادية يكون ضحيتها والمضرور منها هو الأفراد وعدم وجود الضمانات القانونية لحمايتهم في مواجهة الاستدلالات الضخمة.

(18) Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev., 2016, p. 671.

(19) David Lazer, Ryan Kennedy, Gary King & Alessandro Vespignani, The Parable of Google Flu: Traps in Big Data Analysis, 343 Science, 2014, p. 1203.

وإذا كانت قوانين حماية البيانات تهدف لحماية خصوصية الأفراد وهويتهم وسمعتهم، إلا أنها حالياً قد أصبحت عاجزة على توفير الحماية اللازمة لحقوق أصحاب البيانات من المخاطر الجديدة للتحليلات الاستدلالية.

ثانياً: الحماية من المخاطر التي تهدد الحقوق والحريات الأساسية:

يقرر القانون العام لحماية البيانات أن البيانات الشخصية التي تعتبر بطبيعتها حساسة، بشكل خاص، فيما يتعلق بالحقوق والحريات الأساسية تستحق حماية خاصة، لأن سياق معالجتها يمكن أن يخلق مخاطر كبيرة على الحقوق والحريات الأساسية(٢٠).

(20) GDPR, recital 51, (51) Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing

=

وتقر اللائحة العامة لحماية البيانات (GDPR) أيضًا مبررًا لزيادة المتطلبات المحيطة بالبيانات الحساسة، وعلى وجه الخصوص، توضح أن هذه البيانات "بطبيعتها حساسة بشكل خاص فيما يتعلق بالحقوق والحريات الأساسية"، وبالتالي، فإنها "تستحق حماية خاصة لأن سياق معالجتها يمكن أن يخلق مخاطر كبيرة على الحقوق والحريات الأساسية"(٢١).

بالإضافة إلى ذلك، توضح حيثيات اللائحة العامة لحماية البيانات عند تناول الحق في عدم الخضوع لقرارات آلية ذات آثار قانونية أو تأثيرات هامة مماثلة على الأفراد، أن أحد المخاوف الهامة هو إمكانية التمييز على أساس البيانات الحساسة، حيث يمكن أن تقوم الآثار التمييزية على الأشخاص الطبيعيين على أساس الأصل العرقي أو الإثني، أو الرأي السياسي، أو الدين أو المعتقدات، أو العضوية النقابية، أو الحالة الجينية أو الصحية أو التوجه الجنسي، أو التي تؤدي إلى تدابير لها مثل هذا التأثير(٢٢).

وعلى ذلك، يوفر القانون العام لحماية البيانات حماية مشددة لبعض أنواع البيانات الشخصية، لأن معالجتها يمكن أن تؤدي إلى مخاطر كبيرة على الحقوق والحريات الأساسية، والتي تشمل - على سبيل المثال لا الحصر - الآثار التمييزية(٢٣).

=

such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

(21) GDPR, art (51).

(22) GDPR, Whereas: (71).

(23) Niels van Dijk, Raphaël Gellert, & Kjetil Rommetveit, A Risk to a Right? Beyond Data Protection Risk Assessments, 32 COMPUT. L. & SEC. REV., 2016, p. 286.

كما يمكن أن تؤسس مبررات حماية البيانات الشخصية الحساسة من خلال الاتفاقية الأوروبية المحدثة رقم ١٠٨ لمجلس أوروبا بشأن المعالجة التلقائية للبيانات الشخصية حيث تشير في تقريرها التوضيحي لضرورة حماية البيانات الحساسة بشكل أكبر، لأن معالجتها قد تؤدي إلى التعدي على المصالح والحقوق والحريات، ويظهر ذلك، بشكل خاص، إذا كان هناك خطر محتمل للتمييز أو الإضرار بكرامة الفرد أو سلامته الجسدية، حيث يكون المجال الأكثر حميمية لصاحب البيانات(٢٤).

ومن الجدير بالملاحظة أن التقرير التوضيحي لاتفاقية مجلس أوروبا قد احتاط بشكل أكبر للأضرار التي يمكن أن ترتب على انتهاك البيانات الشخصية الحساسة، حيث لا يذكر التقرير التمييز فقط، بل يتبنى نهجًا أوسع وهو يقر بأن معالجة البيانات الحساسة من المرجح أن يكون لها آثار سلبية على أصحاب البيانات، ولا سيما التمييز، ولكن أيضًا الإضرار بالكرامة أو السلامة الجسدية، مما يؤثر على مجالهم الأكثر حميمية، وافتراض براءتهم، وما إلى ذلك.

وعلى ذلك، ومن أجل منع التأثيرات الضارة على صاحب البيانات يجب السماح بمعالجة البيانات الحساسة فقط عندما ينص القانون على الضمانات المناسبة والتي تضمن عدم التأثير على حقوق وحريات الأفراد أو يترتب عليها تأثيرات خطيرة.

كما يعتبر احترام البيانات الشخصية شكلاً خاصاً من احترام الخصوصية، خاصة في ظل انتشار الوسائل والتطبيقات التكنولوجية الحديثة، وهو ما يعنى ضرورة الاعتداد

(24) Explanatory Report on No. 223 of the Council of Eur. Treaty Series-- Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, COUNCIL OF EUR., (2018), https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

بالتفسير الموسع للحق في احترام الحياة الخاصة دون الاقتصار فقط على المعنى المنصوص عليه بالقانون المدني(٢٥).

وفي ذات السياق، وبهدف توفير أكبر قدر من الحماية القانونية المشددة لما يعتبر بيانات حساسة تؤكد محكمة العدل الأوروبية هذا الأمر عند شرح سبب حماية البيانات الحساسة بشكل أكثر صرامة، بل وأكدت المحكمة أن الحماية التي تقررها اللائحة العامة الأوروبية للبيانات الحساسة لا تقتصر فقط على حماية البيانات التي تعتبر بطبيعتها حساسة، بل تمتد كذلك للبيانات التي يمكن أن تكشف عن بيانات حساسة مشمولة بالحماية الخاصة والمشددة(٢٦).

كما اعتبرت المحكمة الأوروبية لحقوق الإنسان أن مجرد جمع وتخزين البيانات المتعلقة بالحياة الخاصة للفرد في ملف يشكل تدخلاً في الحياة الخاصة(٢٧).

علاوة على ذلك، فقد اعتبرت المحكمة الأوروبية لحقوق الإنسان أن البيانات ذات الطبيعة العامة يمكن أن تقع ضمن نطاق الحياة الخاصة عندما يتم جمعها وتخزينها، بطريقة منهجية، في ملفات تحتفظ بها السلطات العامة"، وأكثر من ذلك عندما تتعلق هذه البيانات بالماضي البعيد للشخص(٢٨).

---

(٢٥) د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، مجلة كلية الشريعة والقانون، جامعة طنطا، العدد الثالث والثلاثون، الجزء الرابع، ديسمبر ٢٠١٨، ص ١٩٨١.

(26) CJEU, Case 184/20, OT v. Vyriausioji tarnybins etikos komisija, 2022 E.C.R , 51.

(27) Cour européenne des droits de l'homme, 26 mars 1987, n° 9248/81& CEDH 4 mai 2000, Rotaru c/ Roumanie, req. no 28341/95

(28) CEDH 4 mai 2000, Rotaru c/ Roumanie, req. no 28341/95 . – CEDH 16 févr. 2000, Amann c. Suisse, req. no 27798/95 . – CEDH 31 mai 2005, =

وتتبنى هذه المحكمة مفهوماً واسعاً للحياة الخاصة، يشمل السلامة الجسدية والمعنوية للشخص(٢٩).

ثالثاً: الحماية من التمييز غير القانوني:

غالبًا ما تدور المواضيع المشتركة لوجود البيانات الحساسة حول الحاجة إلى منع أشكال التمييز الضارة أو الظواهر ذات الصلة، وعلى سبيل المثال، أصدرت الأمم المتحدة مبادئ توجيهية لتنظيم ملفات البيانات الشخصية المحوسبة في عام ١٩٩٠، مبررة توفير المزيد من الحماية للبيانات الحساسة لأن مثل هذه البيانات "من المرجح أن تؤدي إلى تمييز غير قانوني أو تعسفي"(٣٠).

ويتضح من ذلك أنه ينظر للحماية الواجب توافرها للبيانات الشخصية الحساسة باعتبارها "وسيلة لتحقيق غاية"، أو بعبارة أخرى، مطلوبة للحد من احتمالات وقوع أضرار تميزية(٣١).

وقدم مجلس أوروبا مبررًا للبيانات الحساسة في تقريره التوضيحي حول تحديث الاتفاقية رقم ١٠٨ بشأن المعالجة التلقائية للبيانات الشخصية، حيث أشار إلى أنه يمكن أن

=

Antunes Rocha c/ Portugal, req. no 64330/01 . – CEDH 27 oct. 2009, Haralambie c/ Roumanie, req. no 21737/03 . – CEDH 17 févr. 2011, Wasmuth c/ Allemagne, req. no 12884/03. – CEDH 22 mai 2012, Ovidiu Trailescu c/ Roumanie, req. no 5666/04 et no 14464/05).

(29) CEDH 29 avr. 2002, Pretty c/ Royaume-Uni, req. no 2346/02 . – CEDH 22 juill. 2003, Y.F. c/ Turquie, req. no 24209/94.

(30) G.A. Res. 45/95, para. 5 (Dec. 14, 1990).

(31) Paul Quinn, The Difficulty of Defining Sensitive Data--The Concept of Sensitive Data in the EU Data Protection Framework, 22 German Law Journal, 2021, 1583.

تنطوي البيانات الحساسة على خطر محتمل للتمييز أو الإضرار بكرامة الفرد أو سلامته الجسدية، حيث يتأثر المجال الأكثر حميمية لصاحب البيانات، مثل حياته الجنسية أو توجهه الجنسي، أو حيث يمكن أن تؤثر معالجة البيانات على قرينة البراءة(٣٢).

كما تضمنت مبادئ الأمم المتحدة التوجيهية لتنظيم ملفات البيانات المحوسبة في عام ١٩٩٠ حماية مشددة للبيانات الحساسة لأنها خلقت خطر "التمييز غير القانوني أو التعسفي"(٣٣).

كما يمكن الاستناد في مبررات حماية البيانات الشخصية الحساسة للائحة الخصوصية الإلكترونية المقترحة، حيث يظهر من مقترح هذه اللائحة مبررًا واسعًا لحماية "المعلومات الحساسة"، وتقرر صراحة أنه قد يكشف محتوى الاتصالات الإلكترونية عن معلومات حساسة للغاية حول الأشخاص الطبيعيين المشاركين في الاتصالات، بدءًا من التجارب الشخصية والعواطف، وحتى الحالات الطبية، والتفضيلات الجنسية، والآراء السياسية، والتي يمكن أن يؤدي الكشف عنها إلى أضرار شخصية، وأضرار اجتماعية، وخسارة اقتصادية(٣٤).

(32) Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 6, 55, Oct. 2018, E.T.S. No. 223, https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [https://perma.cc/G5SZ-J77A].

(33) Guidelines for the Regulation of Computerized Personal Data Files, G.A. Res. 45/95, 5 (Dec. 14, 1990).

(34) Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)., & See GDPR, , Recital 2.

ويتضح من هذا المقترح، عدم استخدام مصطلح التمييز، بل تم استخدام مصطلحات أكثر اتساعاً، بحيث تشمل في نطاقها كل المخاطر المتوقعة نتيجة انتهاك البيانات الحساسة، بما يدخل في نطاق الأضرار شخصية سواء المادية أو المعنوية، والأضرار الاجتماعية، والخسارة الاقتصادية.

ومما لا شك فيه أن لهذه المبررات أهميتها البالغة، خاصة، في سياق الطبيعة المتغيرة باستمرار للبيانات الحساسة، وتعني الطبيعة المتطورة أو المتغيرة للطبيعة الحساسة من الناحية الفعلية أن هناك حاجة مستمرة للتساؤل عما إذا كانت البيانات التي تتم معالجتها تتسم بالحساسية أم لا، ويظهر ذلك بشكل جلي في مجال عمليات الاستدلالات على البيانات، حيث يمكن التوصل لبيانات حساسة من خلال استخدام بيانات لا تتسم بالطبيعة الحساسة.

المطلب الثالث

الطبيعة القانونية للبيانات الحساسة

نعرض من خلال الطبيعة القانونية للبيانات الحساسة مدى اعتبارها في ذاتها حقاً لأصحابها، وتكييف هذا الحق من حيث طبيعته.

ويمكن النظر للبيانات الحساسة وفقاً للسياقات المتعددة لأحكام القضاء، والقواعد التشريعية على ارتباط البيانات الشخصية عامة، والحساسة خاصة ارتباطاً وثيقاً بالحقوق الأساسية لأصحاب البيانات.

كما نادي البعض بضرورة الاعتراف للبيانات الشخصية بكونها حق ملكية فكرية من نوع جديد، وما يترتب على ذلك من آثار، حيث لم يعد يقتصر الأمر على النطاق

الأدبي أو المعنوي في ارتباط البيانات بصاحبها، بل يمكن تجاوزه لحد المصلحة المالية لأصحاب البيانات على بياناتهم.

الفرع الأول

مدى الاعتراف بالبيانات الشخصية كحق ملكية فكرية من نوع جديد

يلاحظ من خلال قوانين حماية البيانات الارتباط الوثيق بين البيانات والحقوق الأساسية لأصحابها مثل الحق في الخصوصية، ولا يوجد حتى الآن اعتراف واضح للبيانات بنوعيها الشخصية والحساسة كحق ملكية فكرية ولو من نوع جديد، وذلك في ظل تزايد استخدام المواقع الالكترونية والشبكات الاجتماعية، وشركات الإعلان، وانتشار البيانات الشخصية للمستخدمين وبيعها وتوزعها(٣٥).

وللاعتراف للبيانات بنوع من حقوق الملكية الفكرية من شأنه أن يمنح الفرد العديد من السلطات والحقوق، مثل منحه القدرة على الحصول على المنافع، والاستفادة من حقه، واستخدام عنصر الإجبار لمنع اعتداء الغير(٣٦).

وفي ظل قوانين حماية البيانات الشخصية، وكذلك اللائحة الأوروبية لحماية البيانات، قد يظل هناك عائقاً أمام الاعتراف بالبيانات الشخصية باعتبارها نوعا من الملكية الفكرية، خاصة في ظل متطلبات الموافقة الصريحة التي تتطلبها تلك القوانين حيث عادةً ما يمنح الشخص طرفًا آخر – شخص طبيعي، أو شركة، أو مؤسسة - الحق في الوصول إلى بياناته الشخصية مقابل خدمة معينة.

(35) C. Tucker, The Economic Value of Online Customer Data, OECD (2011).

(36) Harold Demsetz, Toward a Theory of Property Rights, 57(2) THE AMERICAN ECONOMIC REV, 1967, p. 347.

وقد تظهر هنا إشكالية بشأن تحديد البيانات الشخصية والحساسة، على افتراض تم الاعتراف للبيانات بحق ملكلية فكرية من نوع جديد، وتتمثل في تحديد محل هذا الحق، خاصة في عصر الاستدلالات والتى يمكن التوصل من خلالها للبيانات الشخصية والحساسة بواسطة بيانات غير شخصية، وكما يشير البعض، في هذا السياق، فإن الخط الفاصل بين البيانات الشخصية والبيانات غير الشخصية غير واضح، ومع تقدم التكنولوجيا واستخدامها في مجالات الاستدلالات، أصبح من الصعب التمييز بين البيانات الشخصية والبيانات غير الشخصية، لذلك، عندما نقوم بتحليل ملكية البيانات، يجب أن نشير إلى جميع البيانات على أنها بيانات شخصية(٣٧)، خاصة في ظل الاعتراف بأن البيانات التي يمكن أن تؤدى لبيانات شخصية تعد كذلك، والبيانات التى تؤدي لبيانات حساسة تعد كذلك حساسة.

ويمكن تحليل ملكية البيانات من خلال نهجين، وفي كلاهما يمكن الاستناد إلى أن للأشخاص حق ملكية على بياناتهم الشخصية وكذلك الحساسة، ويتمثلان هذين النهجين فيما يلي:

أولاً: النهج التصاعدي: يشير هذا النهج إلى أن الملكية موجودة بالفعل، وأن القانون الوضعي كان يهدف فقط إلى تثبيت الملكية من خلال الأثر الكاشف لها، ويستند ذلك لاعتبار الملكية حقاً طبيعياً يمنح للأشخاص الطبيعيين بمجرد الولادة حياً(٣٨)، وهو ما يعني ارتباطها بالشخصية القانونية للإنسان، كما أن هناك ارتباط وثيق بين شخصية الإنسان والحق في الخصوصية، وتندرج حماية البيانات ضمن الخصوصية.

(37) Vaclav Janecek, Ownership of Personal Data in the Internet of Things, 34 COMPUTER LAW & SECURITY REVIEW, 2018, p. 1039, 1040.

(38) Thomas Mouritz, Comparing the Social Contracts of Hobbes and Locke, 1 THE WEST AUSTRALIAN JURIST, 2010, p. 123.

ثانياً: النهج التنازلي: يشير إلى أن الملكية غير موجودة كحق للإنسان، ويجب أن تنشأ من خلال اعتراف القانون بمنحها للأفراد، أي أن القانون هو من يقررها وينشئها، وهو ما يمكن الاستدلال عليه في قوانين حماية البيانات الشخصية من خلال ضرورة الحصول على موافقة الشخص المعني بالبيانات قبل جمعها وتخزينها ومعالجتها.

وكما يشير البعض إلى أن هناك عدة عناصر أساسية لتقرير ملكية البيانات الشخصية والحساسة وتتمثل في التحكم والحماية والتقييم والتخصيص[٣٩].

وسنعرض لهذه العناصر تباعاً:

العنصر الأول: التحكم:

يسمح التحكم للمالك بتحديد كيفية استخدام البيانات أو بيعها أو تخزينها أو مشاركتها، وهو أمر بالغ الأهمية لمسألة ملكية البيانات.

ويتأكد هذا العنصر من ناحية ضرورة تطلب موافقة صاحب البيانات، فإن حقيقة وجوب منح الموافقة قبل استخدام البيانات الحساسة وجمعها ومعالجتها هي موافقة واضحة على أننا نتحكم في بياناتنا.

ومن ناحية أخري، إذا نظرنا على أساس النهج التنازلي أي بضرورة اعتراف القانون بهذا الحق، فإنه يجب التفكير فيه بشكل جدي نظراً لأن الاعتراف بالمجال الناشئ لاقتصاديات البيانات يمكن أن يكون له تأثير هائل على اقتصاد البيانات، كما أن

(39) Vaclav Janecek, Ownership of Personal Data in the Internet of Things, 34 COMPUTER LAW & SECURITY REVIEW, 2018, p. 1042.

الاعتراف بحق ملكية وسيطرة لصاحب البيانات من خلال إطار تشريعي لا زال أمر غير واضح وغير مؤكد بمقتضي القواعد التشريعية الحالية لحماية البيانات.

ويعد التحكم أحد أهم العناصر التي تم الاسترشاد بها للتأكيد على مدى أهمية السيطرة، وفي هذا السياق يمكن الاسترشاد بقرار المحكمة الأوروبية لحقوق الإنسان لعام ٢٠١٧، التي تجري مقارنة بين المعلومات الشخصية والحمض النووي البشري(٤٠).

ويحتوي الحمض النووي البشري على كميات من البيانات الشخصية الفريدة، وبالتالي فإن أي سيطرة على الحمض النووي البشري تعد انتهاكاً لحق الإنسان الأساسي في الخصوصية بموجب المادة ٨ من الاتفاقية الأوروبية لحقوق الإنسان لعام ١٩٥٠، وأكدت المحكمة أن حماية البيانات الشخصية تلعب دوراً أساسياً في ممارسة الشخص لحقه في احترام حياته الخاصة، ويجب أن تقرر التشريعات المحلية الضمانات المناسبة.

واستنتجت المحكمة أنه في غياب التوازن العادل بين المصالح العامة والخاصة المتنافسة في القضية، فإن الدولة المدعى عليها تكون قد تجاوزت سلطتها التقديرية، وأن التدخل والاعتداء على الحياة الخاصة واحترام حقوق المدعى كان أمراً غير متناسب.

وسلط البعض الضوء على بيان المحكمة، وقال إنه يمكن يتم تفسيره على أنه يعني أن التحكم في البيانات الشخصية الفريدة للفرد يشبه التحكم في الهوية الفردية للشخص(٤١).

(40) Aycaguer v. France, App No. 8806/12 (June 22, 2017) https://hudoc.echr.coe.int /fre# [%22itemid%22:[%22001-174441%22]].

(41) Leon Trakman, Robert Walters & Bruno Zeller, Is Privacy and Personal Data Set to Become the New Intellectual Property?19(70) UNSW LAW RESEARCH PAPER, 2019, p. 937.

ومع ذلك، فإننا قد نفهم من قرار المحكمة الأوروبية لحقوق الإنسان أن البيانات الشخصية هي أمر مرتبط ارتباطاً وثيقاً بالحقوق الأساسية للإنسان، أي يمكن تفسيرها في هذا الإطار دون اعتراف واضح ومحدد بملكية الشخص المعنى لبياناته.

علاوة على ذلك، فإن منح السيطرة والتحكم بالبيانات الشخصية وكذلك البيانات الحساسة للفرد سيكون أداة مفيدة في متابعة مسار البيانات في عصرنا الحديث، ويرجع ذلك للتكنولوجيا الجديدة والتحولات المعقدة التي يتم إجراؤها على البيانات، كما أن منح السيطرة من شأنه أن يخلق إطارًا متماسكًا لإدارة البيانات الشخصية والحساسة(٤٢).

وفي إطار تسويق البيانات، فإن إنشاء حق ملكية للفرد على بياناته الشخصية يمنح السيطرة والتحكم من خلاله لصاحب البيانات، وسيمنع الاستغلال التجاري للبيانات، ويمكن الاعتماد في ذلك على الأساس الأخلاقي لهذا الحق.

ويمكن تشبيه البيانات الشخصية في هذا الشأن بحق المشاهير في الاستفادة من أسمائهم، حيث يمكن للمشاهير تسجيل أسمائهم كعلامة تجارية والتحكم في أي استخدام تجاري للاسم، كمنتج من صنعهم.

ويوضح البعض أنه إذا تم اعتبار حماية المعلومات والبيانات الشخصية بمثابة التزامًا تعاقديًا، فمن المرجح أن يتضرر هذا الالتزام، بينما إذا تم اعتبار المعلومات الشخصية بمثابة ملكية، فإنها تمنح السيطرة للفرد، مما يتطلب معها عدم إمكانية التعامل بشأنها إلا من خلال موافقة الشخص المعني، وكما يشير هذا الرأي أنه لا توجد آلية

(42) Nadezhda Purtova, Do Property Rights in Personal Data Make Sense after the Big Data Turn?, TILBURG LAW SCHOOL, 2017, p. 6.

قانونية تسمح للأفراد بالتعامل مع بياناتهم الشخصية أو كذلك الحساسة باعتبارها حق ملكية فكرية ولو من نوع جديد(٤٣).

العنصر الثاني: الحماية:

يقصد بذلك تقرير المشرع للحماية القانونية للبيانات الحساسة، والتي يمكن تقييم أنظمة هذه الحماية، ومدى كفايتها وفق الأنظمة القانونية المقارنة والتي يمكن أن تؤدى لحماية غير كافية في ظل الأنظمة التكنولوجية الحديثة بل والتي تتطور بشكل أسرع من القانون، وهذا ما تثيره إشكاليات عملية الاستدلال على البيانات الحساسة في عصر البيانات الضخمة والذكاء الاصطناعي.

العنصر الثالث: التقييم:

يجب أن تكون البيانات بشقيها، الشخصية والحساسة، قابلة للتداول والقياس بطريقة تضمن تقييمها وجعلها سلعة ذات قيمة.

وكما هو الحال مع عنصر التحكم، يمكن أن يؤدى تقييم البيانات الشخصية لآثار اقتصادية واسعة النطاق(٤٤)، مما قد يرتب معها منافع اقتصادية ومالية لأصحاب البيانات.

(43) Edward J. Janger, Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy, 44(4) WM. & MARY L. REV., 2003, p. 1801.

(44) Vaclav Janecek, Ownership of Personal Data in the Internet of Things, 34 COMPUTER LAW & SECURITY REVIEW, 2018, p. 1046.

ولا توجد طريقة واضحة اليوم لتحديد سعر لحصة واحدة من البيانات الشخصية والحساسة، ولا لتحديد ما هي تلك الحصة بالضبط، وما الذي يجب أن تتضمنه حصة من هذه البيانات.

وفي الواقع العملي، أصبحت البيانات بالفعل سلعة يتم تقييمها وبيعها والتعامل معها في جميع أنحاء العالم دون إطار قانوني واسع يتبع طريقة تقييمها، بل وأصبحت البيانات الشخصية اليوم سلعة ذات قيمة كبيرة.

العنصر الرابع: الاستئثار:

ويقصد بذلك تحديد مالك البيانات والذي سيتمتع بكافة الحقوق والسلطات عليها، وإذا كان المنطق يقتضي أنه يمكن اعتبار الشخص المعنى بالبيانات هو صاحب البيانات، إلا أنه مع ذلك، يوجد أشخاص آخرون يمكن الاعتراف بحقهم على البيانات مثل مراقبو البيانات والمعالجون والمنتجون وما إلى ذلك.

وهنا قد نجد مصلحتان متعارضتان في تقرير ملكية البيانات لغير الشخص المعنى، وهما: مصلحة مراقبي البيانات ومنحهم ملكيتها، خاصة في ظل استمرار تزايد اقتصاد البيانات، والمصلحة الثانية تتمثل في حماية الحقوق الأساسية لأصحاب البيانات، وخاصة حقهم في الخصوصية(٤٥).

ويلاحظ هنا أن الادعاء بضرورة تقرير حق ملكية البيانات لأصحابها لا يمكن تقريره إلا بتوافر الوسائل المناسبة التي يمكن من خلالها تحديد أصحاب البيانات المالكين

(45) Mai Arlowski, Personal Data as a New Form of Intellectual Property, 102 J. Pat. & Trademark Off. Soc'y, 2022, p. 649.

لها بشكل دقيق، وإلى أن يتم تحقيق التقدم التكنولوجي اللازم، فإن أي محاولة لإنشاء ملكية كاملة للبيانات الشخصية ستظل مجزأة.

وفي هذا الصدد يشير البعض إلى أنه من الضروري تطوير تقنية يمكن من خلالها تحديد أصحاب البيانات باعتبارهم المالكين القانونيين لبياناتهم، ويمكن أن تكتشف ما إذا كان هناك سوء استخدام لبياناتهم(٤٦).

وعلى الرغم من توافر العناصر السابقة لتقرير حق ملكية فكرية من نوع خاص وجديد لحماية البيانات الشخصية والحساسة، إلا أن النظرية والإطار القانوني ليسا متوافقين بالضرورة، حيث لم يتم الاعتراف بشكل صريح ومباشر من قبل التشريعات المختلفة بهذا الحق.

ويشير اصطلاح حق الملكية الفكرية من نوع خاص إلى شكل مختلف من أشكال حماية الملكية الفكرية، وليس إطارًا تقليديًا مثل حق المؤلف وبراءات الاختراع والعلامات التجارية (٤٧).

ولا يعد هذا الأمر مستغرباً أو بعيداً عن الواقع العملي والقانوني، فقد تم إنشاء حقوق فريدة فيما يتعلق بأشكال أخرى من الملكية الفكرية، مثل قواعد البيانات(٤٨)، وتلك

(46) Leon Trakman, Robert Walters & Bruno Zeller, Is Privacy and Personal Data Set to Become the New Intellectual Property?19(70) UNSW LAW RESEARCH PAPER, 2019, p. 937.

(47) Moni Wekesa, What is SUI GENERIS System of Intellectual Property Protection?13 TECHNOLOGY BRIEF, 2006, p. 3.

(٤) المنظمة بالتوجيه EC/٩/٩٦ الصادر عن البرلمان الأوروبي والمجلس بتاريخ ١١ مارس ١٩٩٦ بشأن الحماية القانونية لقواعد البيانات.

=

الاعتراف بالحق الفريد الذي تم منحه بسبب التقدم التكنولوجي الذي تحدى أنظمة الملكية الفكرية التقليدية.

ويفسر ذلك بأن التكنولوجيا التي تسمح بنقل كميات كبيرة من البيانات في شكل قاعدة بيانات تتطور بسرعة، وكان من دواعي القلق الرئيسي أنه بدون حماية كافية لحالة الملكية الفكرية لقواعد البيانات، فإنها ستتعرض للنسخ القانوني بكميات كبيرة قد يؤدي في النهاية إلى تدمير سوق المعلومات بأكمله(٤٩).

كما كانت قواعد البيانات تنتهك بشكل كبير ومستمر، وكان أي مستخدم للإنترنت قادرًا على نسخ وتنزيل قواعد البيانات الموجودة، ومع ذلك، فقد تطورت الوسائل التكنولوجية لحماية قواعد البيانات ومنع الاعتداء عليها.

وتتمثل بعض الأساليب التي أنشأها منشئو قواعد البيانات في تجميع قاعدة البيانات مع مواد محمية بحقوق الطبع والنشر، أو إنشاء طرق جديدة لترخيص استخدام قاعدة البيانات من خلال تعاقدات مع المستخدمين.

كما يمكن توفير هذه الحماية من خلال توفير التحديثات والتحسينات المستمرة لقواعد البيانات للتأكد من أن نسخ البيانات المنسوخة والمخالفة ستكون قديمة، وبالطبع استخدام كلمات المرور وطرق التشفير لحماية قواعد البيانات.

=

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J. (L 77) 20 [hereinafter: Database Directive].

(49) Samuel E. Trosow, Sui Generis Database Legislation: A Critical Analysis, 7 YALE J.L. & TECH., 2004, p. 534.

ولا شك أنه على الرغم من إمكانية توافر الوسائل التكنولوجية التي يمكن أن تتيح حماية قواعد البيانات إلا أنه كانت هناك حاجة ملحة لضرورة وجود حماية تشريعية لها، وبالنسبة للبيانات الشخصية، فإن الوضع مختلف، فعلى الرغم من أن البيانات الشخصية هي بالفعل في صميم الصناعة التكنولوجية، وخاصة شركات التكنولوجيا الكبرى، فإن التكنولوجيا نفسها ليست كافية لحماية أصحاب البيانات، وكما أن التقدم التكنولوجي يعد سببًا حاسمًا لتشجيع التشريع، فهو ليس كافيًا كوسيلة لحماية حقوق الملكية الفكرية ومتغيراتها(٥٠).

الفرع الثاني

مبررات الاعتراف بحق ملكية فكرية من نوع جديد للبيانات الشخصية

توجد مجموعة من المبررات تدعو للاعتراف للبيانات سواء الشخصية أو الحساسة بنوع جديد من الملكية الفكرية يتوائم مع طبيعتها وحقوق أصحابها، ونجمل هذه المبررات فيما يلي:

أولاً: الغموض الذي يكتنف الحق في الخصوصية كوسيلة حماية للبيانات الشخصية والحساسة، حيث قد يكون من الصعب تحقيق التوازن بين حق الملكية الفكرية، الذي تم المناداة به، وما يترتب عليه من منع الآخرين من استخدام البيانات، وبين حق الاستفادة من البيانات وبيعها، مما يجعل حق الملكية الفكرية حقًا اقتصاديًا وليس حقًا معنويًا فقط، وإمكانية تعارض ذلك مع عناصر حقوق الإنسان مثل الخصوصية(٥١).

(50) Kean Birch, DT Cochrane and Callum Ward, Data as an asset? The measurement, governance and valuation of digital personal data by big tech, 1(15) BIG DATA & SOCIETY, 2021, p. 1.

(51) Leon Trakman, Robert Walters & Bruno Zeller, Is Privacy and Personal Data Set to Become the New Intellectual Property?19(70) UNSW LAW RESEARCH PAPER, 2019, p. 944.

ثانياً: هناك مبرر اقتصادي للاعتراف بالملكية الفكرية، وهناك قيمة اقتصادية كبيرة للبيانات الشخصية.

وعند النظر للمبررات الاقتصادية فإن ذلك قد يصطدم بالطريقة الشائعة لتبرير حقوق الملكية والمتمثلة في تخصيص الموارد النادرة، ولا ينطبق ذلك في حالة البيانات الشخصية والحساسة كذلك(٥٢).

وعلى الرغم من أن البيانات ليست سلعة نادرة، إلا أنه قد يساء استخدامها، ويمكن التغلب على ذلك من خلال إنشاء حماية للملكية الفكرية على البيانات، ويترتب على ذلك زيادة مستوى التحكم الذي يتمتع به أصحاب البيانات على تسويق بياناتهم، وتحقيق التوازن بين حقوق أصحاب البيانات والقائمين على جمعها ومعالجتها.

كما أن التجارة في البيانات تشبه التجارة في أي سلعة أخرى، وبالتالي يجب حمايتها، ولكن قد يكون هناك قلق من أن الإفراط القانوني في تنظيم البيانات وحمايتها يمكن أن يؤدي إلى انخفاض حاد في سوق البيانات، كما أن قوانين حماية البيانات أو كذلك قوانين الملكية الفكرية لا تمنح أي نوع من الملكية أو الحماية لأصحاب البيانات فيما يتعلق بالاعتراف بها كحق من نوع جديد، أو الحقوق الاقتصادية لأصحابها.

ويتخوف البعض من أن منح حقوق الملكية الفكرية لأصحاب البيانات يمكن أن يؤدي إلى المزيد من التجارة في البيانات الشخصية والحساسة، مع الإضرار بحقوق الخصوصية(٥٣).

(52) Pamela Samuelson, Privacy as Intellectual Property, 52 STAN. L. REV., 2000, p. 1138.

(53) Julie Cohen, Examined lives: informational privacy and the subject as object, 52 STANF L. REV, 2000, p. 1373.

ويرد على ذلك، بأن حقوق الملكية الفكرية في البيانات الشخصية ليست مطلقة لصاحب البيانات، أو كذلك جامعي البيانات ومعالجيها، بل تعد بمثابة مشروع مشترك بين الطرفين، وينبغي منح حقوق الملكية الفكرية على البيانات الشخصية لأصحاب البيانات وجامعي البيانات معًا(٥٤).

ثالثاً: التطورات التكنولوجية الهائلة، والتي توفر العديد من الوسائل، وبشكل ميسر، للاعتداء على البيانات الشخصية، بل والتوصل من خلالها لبيانات حساسة مما يستدعى معه ضرورة إعادة النظر في الحماية القانونية المقررة حالياً للبيانات الشخصية بصفة عامة، والبيانات الحساسة بصفة خاصة، ويظهر ذلك بشكل واضح في مجال عمليات الاستدلالات على البيانات الشخصية بفئاتها المختلفة في عصر البيانات الضخمة والتقدم التكنولوجي.

رابعاً: عدم وعي الكثير من الأشخاص بما سيحدث لبياناتهم الشخصية والحساسة، أو ما هو وضعها القانوني، وبصفة خاصة في ظل ارتباط العديد من الخدمات بضرورة تقديم بيانات شخصية وأحياناً بيانات حساسة، بل والأكثر من ذلك ضرورة منح الموافقة من صاحب البيانات على معالجتها وفقاً للغرض الذي يقرره المتحكم أو المعالج لها.

خامساً: تشجيع الابتكار والإبداع، وهو هدف مشروع تسعي له الدول وتوفر له البنية التشريعية المشجعة عليه، ومن خلال منح حق الملكية الفكرية للبيانات الشخصية يمكن تشجيع المخترعين والمبدعين والمؤلفين على مواصلة الإبداع وإثراء الثقافة في مجالات مختلفة(٥٥).

(54) Leon Trakman, Robert Walters & Bruno Zeller, Is Privacy and Personal Data Set to Become the New Intellectual Property?19(70) UNSW LAW RESEARCH PAPER, 2019, p. 945.

(55) MARK A. LEMLEY ET. EL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE, 2016, p. 16.

المبحث الثاني
معايير تحديد البيانات الحساسة

يمكن تحديد مفهوم البيانات الحساسة من خلال إتباع معيار معين من مجموعة معايير تتبع في هذا الصدد.

ويمكن النظر لطبيعة البيانات على أنها حساسة بسبب أن جمع واستخدام والكشف عن أنواع معينة من البيانات يمكن أن يكون أكثر ضررًا أو إشكالية من الأنواع الأخرى للبيانات، وهو النهج الذي اعتنقه المشرعين المصري في قانون حماية البيانات الشخصية، والمشرع الأوروبي في اللائحة العامة لحماية البيانات.

كما يمكن الاعتماد على معيار السياق الذي يتم استخدام البيانات فيه، والغرض من معالجتها حتى ولو كانت بيانات لا تحتوى على العنصر الحساس إلا أنه يمكن الاستدلال من خلالها على بيانات حساسة.

بالإضافة إلى ذلك يمكن النظر إلى البيانات الحساسة على أنها البيانات الأكثر عرضة لخطر التسبب في الضرر.

ونعرض فيما يلي للمعايير المختلفة لتحديد مفهوم البيانات الحساسة.

المطلب الأول

معيار طبيعة البيانات

اعتمدت اللائحة العامة لحماية البيانات وكذلك القوانين المختلفة بحماية البيانات الشخصية فئات خاصة من البيانات ضمن قائمة معينة وأطلقت عليها البيانات الشخصية الحساسة.

ويقوم التحديد التشريعي للبيانات الشخصية الحساسة على افتراض أن جمع واستخدام والكشف عن أنواع معينة من البيانات، بشكل عام، يمكن أن يكون أكثر ضررًا أو إشكالية من الأنواع الأخرى للبيانات.

وتم تحديد البيانات الشخصية الحساسة بشكل عام من خلال مصطلحات عامة، ودون الاعتداد بسياقات جمعها والكشف عنها ومعالجتها، ولذلك تظل هذه التعميمات غير دقيقة للغاية بحيث لا تجعل التمييز بينها وبين البيانات العادية جديرًا بالاهتمام.

وكما يشير البعض أنه بالنظر للوضع الحالى لتحديد البيانات الحساسة، فإن فئات البيانات الحساسة "لا يتم إنشاؤها بشكل مدروس أو صارم"(٥٦).

ومع ذلك، يتم اختيار فئات البيانات الحساسة بشكل عشوائي، ويكون نطاقها واسعًا للغاية، فليست كل البيانات التي تندرج ضمن فئة البيانات الحساسة تعد حساسة بنفس القدر، وعلى سبيل المثال، فإن حقيقة أن الشخص يعاني من حالة صحية قد تكون محرجة أو ضارة للغاية، أو قد لا تكون كذلك على الإطلاق، فهناك العديد من الأشخاص

(56) Paul Ohm, Sensitive Information, 88 S. CAL. L. REV., 2015, p. 1125.

الـذين يكشـفون هـذه المعلومـات طوعًـا للجمهـور، ومـن السـهل إخفـاء أنـواع معينـة مـن الحالات أكثر من غيرها(٥٧).

وبنـاء علـى ذلـك، يمكـن القـول بـأن تحديـد البيانـات الحساسـة ضـمن قائمـة محـددة يتميـز بجاذبيـة خاصـة، حيـث إنـه يـؤدي إلـى تجنـب الخطـوط غيـر الواضـحة، والتحليلات المعقدة لكل حالـة علـى حدة، ولكـن مـع ذلـك يظـل الغمـوض قائمـاً حـول حـدود فئـات هـذه البيانات ويظهر ذلك فيما يلي:

أولاً: يعد التعرف على فئات البيانات الحساسة أمر غير متسق تمامًا عبر القوانين المقارنة، حيث يمكن أن تقر بعض القوانين بيانات معينة على أنها ضمن نطاق البيانات الحساسة، في حين لا تعترف قوانين دول أخري بذلك.

ثانيـاً: لـيس مـن الواضـح مـا إذا كانـت قـوائم البيانـات الحساسـة مبنيـة علـى آراء مشتركة، إذ لا يبدو أن واضعي القوانين أجروا أي استطلاع أو حاولوا إجراء أي تحليل لفهم ما يعتبره الناس بيانات حساسة.

علـى سـبيل المثـال، فـي أحـد الدراسـات الاستقصـائية فـي المملكـة المتحـدة فـي عـام ٢٠٠٧، صنف الأشخاص البيانات المالية على أنها أكثر أنواع البيانات حساسية، والتي لـم يـتم تضـمينها حتـى فـي قائمـة البيانـات الحساسـة فـي التوجيـه أو اللائحـة العامـة لحمايـة البيانـات(٥٨)، بينمـا يعتـرف القـانون المصـري بالبيانـات الماليـة ضـمن فئـات البيانـات الحساسة(٥٩).

(57) Daniel J. Solove, Regulating based on harm and risk instead of sensitive data, 118 Nw. U.L. Rev., 2024, p. 1081.

(58) Karen McCullagh, Data Sensitivity: Proposals for Resolving the Conundrum, 2 J. INT'L COM. L. & TECH., 2007, p. 196.

(٥٩) المادة الأولى من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

وهذا يثير التساؤل حول مدى الاعتداد بآراء الأشخاص في تحديد وتصنيف البيانات الحساسة، واختلاف وجهات النظر بشأنها، بل وربما قد تكون آراء الأشخاص غير مدروسة، وقد لا يفهمون بشكل كامل المخاطر المتعلقة بأنواع معينة من البيانات الشخصية، وقد تتغير آرائهم بناءً على الأخبار المتداولة والعقيدة المرتبطة بشأن البيانات.

ولذلك، وعلى الرغم من ضرورة ترجمة القانون لأهداف ومعتقدات الناس المشروعة، وتقرير الحماية اللازمة بشأنها إلا أن النظر إلى المواقف المجتمعية قد لا يكون نهجا مثالياً، ومن الحكمة أن تتجنب القوانين القيام بذلك، أو على الأقل عدم الاعتماد بشكل حصري على هذه المواقف.

ثالثاً: لا يبدو أن هناك أي قاعدة معينة ومحددة للتعرف على البيانات الحساسة، ولا توجد نظريات متفق عليها يمكن الاعتماد عليها، أو مبادئ موحدة يمكن من خلالها تحديد البيانات الحساسة.

ولذلك اتجه البعض، برأي جدير بالتأييد، لاعتبار البيانات بمثابة بيانات حساسة عندما تكون من المرجح أن تسبب الضرر أكثر من البيانات الشخصية العادية(٦٠)، وهو ما يعنى ضرورة الاعتداد بمعيار الضرر الناشئ عن معالجة البيانات الشخصية لاعتبارها ضمن فئة البيانات الحساسة.

ويظهر ذلك، بشكل جلي، في مجال عمليات الاستدلالات على البيانات الشخصية عامة، والبيانات الحساسة بشكل خاص، حيث يمكن اعتبار أي بيانات –سواء شخصية أو عادية أو مجهولة المصدر- يمكن التوصل من خلالها على بيانات شخصية أو حساسة

(60) Daniel J. Solove Regulating based on harm and risk instead of sensitive data, 118 Nw. U.L. Rev., 2024, p. 1081.

تتمتع بذات الطبيعة، ولذلك فإن إحدى إشكاليات الاستدلالات هي أن هذه العملية تنشأ، في كثير من الأحيان، صعوبة بالغة في تحديد مجال منفصل للبيانات الحساسة.

ووفقاً للنهج التشريعي الحالي، سواء باللائحة العامة لحماية البيانات، وكذلك القانون المصري في أنهما قد اعتمدا على نهج طبيعة البيانات وبموجب ذلك تم تحديد فئات البيانات الحساسة ضمن قائمة محددة على سبيل الحصر لتلك البيانات، مما ترتب عليه إنشاء فئات عشوائية للبيانات، حيث تعتبر بعض السيناريوهات أكثر حساسية دون مبرر واضح أو ثابت.

المطلب الثاني

معيار السياق والغرض من المعالجة

يمكن أن يختلف النطاق المحتمل لمفهوم البيانات الحساسة إذا تم الاعتماد على نهج سياق استخدام البيانات وامكانية التوصل لبيانات حساسة من خلالها، أو تحديدها وفقاً للغرض من معالجتها وهو ما يستدعي ضرورة النظر في نية مراقب البيانات أو المتحكم فيها.

ويشير النهج المبني على السياق أو الغرض من المعالجة إلى أن البيانات التي يتم استخدامها ومعالجتها والاستدلال منها على بيانات حساسة، تكون كذلك بيانات حساسة حتى ولو كانت من البداية لا تحتوى على العنصر الحساس، وعلى ذلك ينظر للبيانات في ضوء السياق العام الذي تم استخدامها من خلاله.

ويترتب على تطبيق معيار السياق الذي تم استخدام البيانات فيه إلى التوسع في نطاق البيانات الحساسة، حيث تعتبر أي بيانات حسب سياق استخدامها إذا تم التوصل من خلال لاستدلالات على بيانات حساسة فتعد هى الأخرى ضمن البيانات الحساسة.

ويعتمد معيار سياق استخدام البيانات على الطبيعة الموضوعية للبيانات ذاتها، دون الاعتداد بشكل رئيس على نوايا المراقب أو المتحكم، وهو ما يمكن القول معه بأنه يمكن استنتاج البيانات الحساسة من بيانات قد لا تكون حساسة بطبيعتها.

وينظر النهج السياقي - الذي تم اعتماده في الأصل في ألمانيا والنمسا – إلى مسألة ما إذا كانت البيانات حساسة أم لا من الناحية الموضوعية في المقام الأول، ويمكن لأي بيانات شخصية اعتمادًا على ظروف المعالجة، أن تكون "حساسة"(٦١).

وبناء على ذلك، ينبغي تقييم جميع البيانات الشخصية على خلفية السياق الذي يحدد معالجتها، ووفقاً لعدة عوامل، مثل المصالح المحددة للمراقب أو المتحكم، وكذلك المستلمين المحتملين للبيانات، والأهداف التي يتم جمع البيانات من أجلها، وشروط المعالجة وعواقبها المحتملة على الأشخاص المعنيين، كل هذه العناصر قد تساعد في تحديد مدى حساسية معالجة البيانات.

وعلى ذلك، فإنه لا يمكن الاعتماد في تعريف وتحديد البيانات الحساسة على نهج قائم على الغرض فقط، حيث يعتد النهج القائم على الغرض من المعالجة بنوايا مراقب

(61) Bundesdatenschutzgesetz Federal Data Protection Act, Dec. 20, 1990, BGBL. I S. 2954, § 28, 35 (Ger.)

مشار إليه لدي:

Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1583.

البيانات كعامل أساس في تحديد حساسية البيانات، لأن الاعتداد بالنوايا يمكن أن يخلق مخاطر متعددة، فيمكن أن يزيد من مخاطر سوء التفكير في المعالجة، كما قد لا يكون لدى المراقب أو المتحكم نفسه أي نية لاستخلاص استنتاجات حساسة من البيانات الشخصية، ولكنه مع ذلك قام بمعالجتها بطريقة من شأنها أن تخلق مخاطر تجاه الأطراف الثالثة التي قد يكون لها حق الوصول إلى البيانات وقد تكون قادرة على استخلاصها مثل هذه الاستنتاجات(٦٢).

ومع ذلك، فلا يمكن استبعاد النوايا بشكل مطلق، فمن خلال السياق الذي تم استخدام البيانات من خلاله وغرض المعالجة فيمكن معها أن يؤخذ في الاعتبار النوايا الذاتية لأي مراقب بيانات أو متحكم.

ويظهر من خلال ذلك التفرقة بين النهج السياقي والنهج الهادف والتناقض بينهما، حيث يركز النهج الهادف في المقام الأول على نوايا مراقب البيانات وهدفه من عملية الاستدلال والمعالجة، وينظر بشكل أساس إلى نية مراقب البيانات وما إذا كان ينوي استخلاص استنتاجات من معالجة بيانات معينة يمكن اعتبارها حساسة بطبيعتها.

وعلى ذلك، فإن هذه النوايا ستكون حاسمة بشكل عام في تحديد ما إذا كانت البيانات المستخدمة حساسة أم لا، وبمفهوم المخالفة فإنه عندما لا يكون لدى وحدة التحكم المعنية أي نية للتوصل للبيانات الحساسة، فإن النهج القائم على الغرض سيؤدي إلى أنه لا توجد بيانات حساسة.

(62) Vaclav Janececk & Gianclaudio Malgieri, Commercialization of Data and the Dynamically Limited Alienability Rule, 21 GERMAN L. J., 2020, p. 924.

وعند تحديد ماهية هذا السياق، قد يكون هناك عدد من العوامل الهامة التي يجب أخذها في الاعتبار، منها النظر في البيانات الأخرى التي قد تكون متاحة لمراقب البيانات، وهذا أمر هام لأن الجمع بين مجموعات البيانات المختلفة قد يزيد من احتمال التوصل إلى استنتاجات ذات طبيعة حساسة، حتى عندما لا يكون ذلك واضحا عند النظر في مجموعات بيانات معينة بشكل منفصل(٦٣).

ومن المواقف المؤيدة لذلك اعتماد لجنة حماية الخصوصية البلجيكية، التي أصبحت منذ ٢٥ مايو ٢٠١٨، هيئة حماية البيانات، عدة آراء تعكس هذه الصعوبة، حيث أنه من خلال جلسات الاستماع في مجلس الشيوخ التي سبقت اعتماد التشريع المتعلق بالمراقبة بالفيديو، أكد رئيس اللجنة أن "جميع المعلومات ليست بالضرورة حساسة في حد ذاتها، وقد تنجم هذه الخصائص عن السياق والأغراض التي من أجلها معالجة البيانات"، وبالتالي، فإن لون بشرة الأشخاص الذين تم تصويرهم، سواء كان أبيض أو أسود، لا يمكن اعتباره "حساسا" في حد ذاته، ولكن سيكون الأمر كذلك، على سبيل المثال، إذا كان الهدف من تسجيل الصور هو تحديد وتصنيف الأشخاص الذين تم تصويرهم وفقا للون بشرتهم"(٦٤).

(63) Gianclaudio Malgieri & Giovanni Comandé, Sensitive-by-Distance: Quasi-Health Data in the Alogrithmic Era, 3 INFO., COMMC'N & TECH. L., 2017, p. 1 & See also Bart Custers & Helena Ursic, Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection, INT'L DATA PRIV. L., 2016, p. 8.

(64) Audition de MM. Michel Parisse et Willem De Beuckelaer, président et vice-président de la commission de la protection de la vie privée, Surveillance par caméra, Rapport, Sén., 2005-2006, Document législatif no 3-1413/1.

وفي عدة مناسبات، رأت اللجنة بالفعل أنه إذا كان من الممكن استخلاص معلومات تتعلق بالحالة الصحية لشخص ما من خلال ارتداء نظارات أو ضمادة حول ذراع الشخص، فلا ينبغي استيعاب هذه الصور في البيانات الطبية "الشخصية" في هذه الحالات، حيث لا يجوز استخدام هذه الخصائص لاستنتاج معلومات بشكل منهجي عن الحالة الصحية للأشخاص الذين تم تحديدهم(٦٥).

ومن الجدير بالذكر أنه على الرغم من وضع تنظيم قانوني للبيانات الحساسة، إلا أن طبيعة هذه البيانات نفسها هي في حد ذاتها في حالة تطور كامل ومستمر، ويحدث هذا التغيير في عالم أصبحت فيه مفاهيم مثل إنترنت الأشياء (IoT) و"البيانات الضخمة" شائعة، بل وتستلزم هذه الظواهر الإنشاء المستمر لكميات هائلة من البيانات الشخصية(٦٦).

ومع الزيادات التي لا تنتهي في قوة الحوسبة، وسهولة المشاركة المتزايدة، والجمع بين مجموعات البيانات المتباينة، يمكن القول إن المزيد والمزيد من البيانات أصبحت ذات طبيعة حساسة.

---

(65) CPVP, Avis no 14/95 du 7 juin 1995 sur l'applicabilité de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel à l'enregistrement d'images et ses conséquences ; CPVP, Recommandation no 01/98 du 14 décembre 1998 en matière de Système Informatisé de Réservation ; CPVP, Avis no 17/99 du 10 mai 1999 relatif au projet d'arrêté royal concernant l'installation et le fonctionnement de caméras de surveillance dans les stades de football.

(66) Paul Quinn, The Anonymisation of Research Data-- A Pyric Victory for Privacy That Should Not Be Pushed Too Hard by the EU Data Protection Framework?, 24 EUR. J. HEALTH L., 2017, p.1.

وفي عالم الإنترنت المترابط بشكل متزايد، قد يستلزم ذلك مراعاة النظر للبيانات الشخصية وكذلك الحساسة بشكل واسع، فلا ينظر للبيانات الحساسة فقط بأنها التي قد تكون في حوزة وحدة التحكم فعليًا، ولكن أيضًا البيانات التي قد يكون بإمكانها الوصول إليها من مكان آخر، مثل البيانات التي قد تكون متاحة مجانًا، مع الأخذ في الاعتبار القدرات التقنية لمراقب البيانات، أو غيره من مراقبي البيانات المحتملين، وسيشمل ذلك القدرة الحاسوبية أو التحليلية أو المعرفة التقنية المتاحة لمراقبي البيانات(٦٧).

وبالنظر إلى أن هذه العوامل في حالة تطور مستمر، وأن الوصول إلى مجموعات البيانات التي يحتمل أن تكون مجانية يتزايد باستمرار، فإن السياق المحدد لمعالجة البيانات يتغير دائمًا، ولذلك فإن معالجة البيانات التي ربما لم تكن تعتبر حساسة في الماضي، قد تعتبر حساسة في المستقبل.

ويمكن تصور النهج السياقي الذي تمت معالجة البيانات في سياقه أنه يتناقض مع نهج الغرض من جمع البيانات الحساسة ومعالجتها، ولكن الحقيقة هي أن عناصر أحد النهجين يمكن دمجها مع عناصر نهج آخر، وهنا يمكن أن يكون للقضاء دور إيجابي في تعزيز حماية البيانات الحساسة من خلال الاعتماد على استخدام نهجًا سياقيًا مع بعض العناصر التي قد تكون أيضًا قائمة على الغرض.

ويهدف دمج عناصر أحد الأساليب مع عنصر آخر لتحقيق ميزتين وهما:

أولاً: قد يهدف دمج نهجي: السياق، وغرض المعالجة في التخفيف من تأثير أحد الأساليب، وعلى سبيل المثال، إذا تم استخدام النهج القائم على السياق بالإضافة إلى

(67) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1583.

عناصر الغرض من المعالجة أو النية لاعتبار البيانات ذات طبيعة حساسة، فإن ذلك يوجب على مراقب البيانات أن يكون على دراية بوجود احتمالية لمعالجة البيانات الخاضعة لسيطرته بطريقة تؤدي إلى استنتاجات من شأنها أن تكون ذات طبيعة حساسة، حتى لو لم يكن ينوى القيام بهذه المعالجة(٦٨).

ويمكن استخدام مثل هذا الفهم لتخفيف النمو الهائل المحتمل في حجم البيانات الحساسة التي قد تحدث في المستقبل إذا تم الحفاظ على فهم البيانات الحساسة القائم على السياق بشكل أساسي.

ثانياً: تظهر أهمية ذلك في سد أي فجوة يمكن أن تنشأ نتيجة استخدام نهج واحد بشكل منفصل، وكما يشير البعض(٦٩) إلى أن وحدة تحكم إذا قامت بجمع كميات كبيرة من البيانات الشخصية المتعلقة بخصائص سلوكية معينة بهدف أن يكون هناك شكل من أشكال معالجة البيانات المبتكرة متاحًا في المستقبل، وأن يكون من شأنه أن يسمح باستخلاص استنتاجات بشأن الحالة الصحية لأصحاب البيانات، فيمكن أن يؤدى الاعتماد على النهج السياقي فقط لمفهوم البيانات الحساسة أن مثل هذه المعالجة قد لا يمكن اعتبارها معالجة للبيانات الحساسة، نظرًا لأنه قد لا يكون من الممكن في الوقت الحالي استخلاص مثل هذه الاستنتاجات، لأن العمليات التكنولوجية أو التحليلية المطلوبة قد لا تكون متاحة بعد.

(68) Vaclav Janecek & Gianclaudio Malgieri, Data Extra Commercium, in DATA AS COUNTER-PERFORMANCE--CONTRACT LAW 2.0?, 2019, p. 14-15.

(69) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1583.

ومع ذلك، قد تكون هذه الطريقة في تحديد البيانات الحساسة غير كافية نظرًا لاحتمال أن تجعل التطورات التكنولوجية المستقبلية مثل هذه البيانات حساسة بطبيعتها، على الرغم من أنها قد لا تكون كذلك في الوقت الحاضر، بالإضافة إلى ذلك، قد تصبح هناك أشكال جديدة من البيانات المجانية متاحة، مما يسمح باستخلاص استنتاجات قد تكون حساسة.

ونظرًا لذلك، فإن التعريف الذي يتجاهل الغرض قد لا يكون مناسبًا دائمًا، نظرًا لأن مراقب البيانات يمكنه تجميع البيانات على أمل أن تسمح التطورات المستقبلية غير المعروفة حالياً باستخلاص استنتاجات حساسة، وهو ما لا يمكن تحقيقه في الوقت الحاضر، كما أن إضافة عنصر الغرض إلى تعريف يستند إلى السياق يؤدى إلى توسيع نطاق البيانات الحساسة بطريقة تحمي من عدد من المخاطر المحتملة من حيث الأضرار، مثل التمييز والاعتداء على الحقوق الأساسية، خاصة في ظل الاستدلالات المتطورة وما يترتب عليها من عمليات التصنيف والتوصيف وإنشاء الملفات التعريفية.

المطلب الثالث

معيار الضرر الناشئ عن البيانات

يمكن النظر إلى البيانات الحساسة على أنها البيانات الأكثر عرضة لخطر التسبب في الضرر لأصحاب البيانات.

وبالنظر إلى النهج التشريعي الحالي لمفهوم البيانات الحساسة قد يبدو أنه نهجاً بسيطاً، ولكن عند التدقيق فيها، فإن الحقيقة هي أنها معقدة للغاية ولا يمكن السيطرة

عليها[٧٠]، حيث يمكن استخدام البيانات غير الحساسة بطرق تسبب ضررًا يعادل الضرر الذي تسببه البيانات الحساسة إن لم يكن أكثر.

وهناك العديد من الأمثلة على أنواع البيانات التي لا تعتبر حساسة، ولكن من المحتمل أن تسبب ضررًا جسيمًا، ومنها على سبيل المثال: البيانات الوصفية والعناوين والصور وبيانات الطبقة الاجتماعية.

وبالنسبة لما يعرف بالبيانات الوصفية هو مصطلح يصف نوع من البيانات الشخصية التي يُزعم أنها غير ضارة وتتعلق بالاتصالات واستخدام المنتجات والخدمات الرقمية، مثل البيانات المتعلقة بالتتبع والخصائص والأصل وأحجام الملفات والعناوين والإنشاء، والتاريخ، وغيرها[٧١].

كما أن البيانات الوصفية هي معلومات لا تتعلق بالمحتوى، على سبيل المثال، تعتبر أرقام الهواتف ومدة المكالمة بمثابة بيانات وصفية؛ بينما يعد مضمون المحادثة أثناء المكالمة محتوى، كما تعتبر رؤوس البريد الإلكتروني وعنوانه أيضًا بيانات وصفية لأنها تتكون من معلومات التوجيه؛ بينما رسالة البريد الإلكتروني نفسها محتوى.

وفي هذا الصدد، يحاول القانون التمييز بين أنواع البيانات بناءً على طبيعتها، وهو نفس الشيء المتبع بشأن أحكام البيانات الحساسة، وتتعامل القوانين المختلفة مع أنواع معينة من البيانات على أنها أقل أهمية من الأنواع الأخرى من البيانات. وعلى وجه

(70) Daniel J. Solove, Regulating based on harm and risk instead of sensitive data, 118 Nw. U.L. Rev., 2024, p. 1081.

(71) Chiradeep BasuMallick, What is Metadata? Definition, Types, Uses, and Examples, SPICEWORKS (Oct. 20, 2022), https://www.spiceworks.com/tech /devops/articles/what-is-metadata/ [https://perma.cc/BN9D-8938].

الخصوص، فيما يتعلق بالمكالمة الهاتفية أو البريد الإلكتروني، فإن محتوياتها محمية بشكل أكثر صرامة من البيانات الوصفية المرتبطة بها(٧٢).

وفي سياق متصل، إذا كان منع التمييز يعد أحد الأسباب المنطقية الرئيسية لإدراج فئات البيانات الحساسة في قوانين حماية البيانات؛ إلا أنه مع ذلك لم تدخل في نطاقها البيانات المتعلقة بالطبقة الاجتماعية، ويعد ذلك بمثابة استبعاد تعسفي(٧٣).

وعادة ما ترتبط الطبقة الاجتماعية بفئات معينة من البيانات الحساسة، مثل العرق والأصل، والآراء السياسية وغيرها، وتتشابك البيانات حول الأشخاص بشكل عميق، مما يجعل من الصعب رسم خطوط واضحة ومرتبة حول بيانات معينة و وفصلها عن البيانات الأخرى.

كما تتضمن البيانات المتعلقة بالطبقة الاجتماعية عوامل اجتماعية واقتصادية مختلفة مثل تعليم الشخص وثروته، وعلى الرغم من حظر التمييز على أساس الطبقة الاجتماعية، نادرًا ما تصنف قوانين حماية البيانات بيانات الطبقة الاجتماعية على أنها

(72) Daniel J. Solove, Reconstructing Electronic Surveillance Law, 72 GEO. WASH. L. REV., 2004, p. 1264.

(73) YESHIMABEIT MILNER & AMY TRAUB, DATA FOR BLACK LIVES & DEMOS, DATA CAPITALISM + ALGORITHMIC RACISM 16 (2021), https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf [https://perma.cc/Z4C2-M82F], Malkia Devich -Cyril, Defund Facial Recognition, ATLANTIC (July 5, 2020), https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition/613771/ [https://perma.cc/5B84-AJAD]

حساسة، وإن كان المشرع المصري قد أدرج البيانات المالية ضمن نطاق البيانات الحساسة(٧٤)، وهى نوع فقط من أنواع بيانات الطبقة الاجتماعية.

كما أن هناك نموذجاً آخراً للبيانات الشخصية وهى الصور، حيث يمكن استخدامها بطرق ضارة بشكل كبير، بل وربما بسبب مدى استخدام الصور على نطاق واسع، نادرا ما يتم تضمينها في قوائم البيانات الحساسة.

ومع ذلك فإن الصور يمكن أن تكشف بسهولة عن بيانات حساسة، ولذلك تحاول اللائحة العامة لحماية البيانات التغلب على التحدي الذي تشكله الصور من خلال القول أنه لا ينبغي اعتبار معالجة الصور بشكل منهجي بمثابة معالجة لفئات خاصة من البيانات لأنها مشمولة بتعريف البيانات البيومترية فقط عند معالجتها من خلال وسيلة تقنية محددة تسمح بالتعرف الفريد أو المصادقة على الشخص الطبيعي(٧٥).

يبدو أن اللائحة العامة لحماية البيانات تنظر إلى فئة البيانات الحساسة الوحيدة للصور على أنها بيانات بيومترية، ولكن الصور يمكن أن تؤدي إلى استنتاجات حول

---

(٧٤) المادة الأولى من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(75) GDPR, § 51, "… The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

العرق والانتماء العرقي والدين والصحة وغير ذلك الكثير، وعلى سبيل المثال، يمكن لصور الأشخاص الذين يرتدون ملابس دينية أو بتسريحات شعر معينة أو شعر الوجه أو أغطية الرأس أن تؤدي إلى استنتاجات حول الدين، كما أن بعض الحالات الصحية لها مظاهر جسدية يمكن اكتشافها من خلال الصور، ويمكن أن تكشف الصور عن علامات معينة تدل على الحالة الصحية والنفسية للأشخاص.

وفي إحدى الدراسات، طور الباحثون خوارزمية للتعلم الآلي للتنبؤ بالاكتئاب بناءً على الصور التي نشرها الأشخاص على مواقع التواصل الاجتماعي، حتى قبل تشخيص إصابة هؤلاء الأشخاص بالاكتئاب، وكان أداء الخوارزمية أفضل من الممارسين العامين(٧٦).

كما أنه أحياناً يمكن أن تكون الصور ضارة حتى بدون إجراء أي استنتاجات، فعلى الرغم من عدم إدراج الصور الخاصة في قوائم البيانات الحساسة، إلا أن ممارسة تداول هذه الصور للأشخاص دون موافقتهم تؤدي إلى ضرر كبير يؤثر على حياة ومستقبل الأشخاص بشكل كبير وبأضرار قد لا يمكن أن يكون التعويض مكافئاً لها(٧٧).

وتعد هذه الأضرار أكثر تدميراً بكثير من نشر ملاحظات الطبيب حول بيانات صحية لشخص ما، أو معلومات تفيد بأن الشخص يعتنق معتقدات فلسفية معينة، ويبرز هذا الأمر، بشكل جلي، من خلال وسائل التواصل الاجتماعي المختلفة سهولة توفر

(76) Andrew G. Reece & Christopher M. Danforth, Instagram Photos Reveal Predictive Markers of Depression, 6 EPJ DATA SCI., no. 15, 2017, at 1, 9.

(77) Danielle Keats Citron & Mary Anne Franks, Criminalizing Revenge Porn, 49 WAKE FOREST L. REV., 2014, p. 345; DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE, 2014, p. 5.

الصور على الإنترنت وافتقارها إلى الحماية، يمكن استنتاج الكثير من البيانات حول معتقدات الشخص وسلوكه وشخصيته(٧٨).

وعلى ذلك، فإننا نرى أن نهج البيانات الحساسة المتبع حالياً من قبل التشريعات المختلفة يعد نهجاً قاصراً، حيث لا يشتمل على جميع البيانات الحساسة، كما أنه يقلل من حماية أنواع البيانات المستبعدة، ويرجع ذلك لاعتناق المشرعين لنهج بسيط يتمثل في القائمة الحصرية التي تحدد فئات معينة للبيانات على كونها حساسة.

وبهدف توفير الحماية الفاعلة للبيانات الحساسة، نعتقد أنه يجب إعادة النظر في النهج الواجب اتباعه لتحديد البيانات الحساسة، حيث لم تثبت من الناحية الواقعية فعالية طبيعة البيانات كمعيار لتحديد البيانات الحساسة، ونعتقد بضرورة الاعتداد بأن البيانات الحساسة تتمثل في أي بيانات يمكن أن يترتب عليها ضرراً جسيماً بالشخص حال التوصل إليها، مع الأخذ في الاعتبار سياق معالجتها والغرض منها، وهو ما يترتب عليه التوسع في تحديد مفهوم البيانات الحساسة بحيث يخضع القائمون على المعالجة وعمليات الاستدلال كذلك للقيود والالتزامات القانونية، ويمكن من خلال ذلك تجنب التهرب من القيود والالتزامات من قبل القائمين على عمليات الاستدلالات خاصة حال استخدام بيانات لا تخضع للحماية القانونية بل أمكن من خلال سياق معالجتها ونية الفاعلين من الاستدلال منها على بيانات حساسة.

ويجب الاعتراف لقاضي الموضوع بدور إيجابي فاعل من خلال تقرير سلطته التقديرية الكاملة في مراقبة وتقدير مدى اعتبار البيانات قد تلحق ضرراً أكثر من غيرها بأصحابها، وكذلك سياق استخدامها، ونية القائمين على عمليات الاستدلال.

(78) Mary Anne Franks, "Revenge Porn" Reform: A View from the Front Lines, 69 FLA. L. REV., 2017, p. 1251.

الفصل الثاني
الاستدلال على البيانات الشخصية الحساسة

مقدمة:

تتمتع البيانات الحساسة بحماية قانونية مشددة في القوانين المنظمة لحماية البيانات الشخصية، وعلى الرغم من تقرير الحماية المشددة لهذه الفئة من البيانات، باعتبارها جديرة بحماية أشد من المقررة للبيانات الشخصية العادية، إلا أن الأمر يظل محل شك، خاصة، في ظل التحديد التشريعي للبيانات الحساسة، وإخضاعها لقائمة محددة على سبيل الحصر.

وفي هذا السياق، يظل التساؤل قائماً حول جدوى تحديد البيانات الحساسة من خلال قائمة محددة، وتظهر أهمية الإجابة على ذلك في عصر البيانات الضخمة والذكاء الاصطناعي (AI)، حيث تستخلص تحليلات البيانات الضخمة والذكاء الاصطناعي استنتاجات وتنبؤات غير بديهية وغير قابلة للتحقق حول سلوكيات الأفراد وتفضيلاتهم وحياتهم الخاصة.

وتعتمد هذه الاستنتاجات على بيانات متنوعة للغاية، وغنية بالميزات ذات قيمة لا يمكن التنبؤ بها، وتخلق فرصًا جديدة لاتخاذ قرارات هامة يمكن أن تؤثر على حقوق الأفراد الأساسية.

وإذا كان قانون حماية البيانات يهدف إلى حماية خصوصية الأشخاص وهويتهم وسمعتهم واستقلاليتهم، إلا أنه قد يفشل حاليًا في حماية أصحاب البيانات من المخاطر

الجديدة للتحليلات الاستدلالية، ويظهر ذلك في الدراسات القانونية والفقهية والتي أصبحت محل اختلافات متعددة بشأن الوضع القانوني للاستدلالات.

ونعرض من خلال هذا الفصل لإمكانية الاستدلال على البيانات الحساسة، وهو ما نبينه في المبحث الأول، ثم بين في المبحث الثاني لشروط صحة الاستدلالات وأساسها القانوني، ونبين في المبحث الثالث لخطورة عمليات الاستدلالات في عصر الذكاء الاصطناعي والبيانات الضخمة وتأثيراتها على حقوق الأشخاص، ونعرض لذلك فيما يلي:

المبحث الأول: إمكانية الاستدلال على البيانات الحساسة.

المبحث الثاني: شروط صحة الاستدلالات وأساسها القانوني.

المبحث الثالث: الاستدلال على البيانات الحساسة في عصر البيانات الضخمة وتأثيرها على الحقوق الأساسية للأفراد.

المبحث الأول

إمكانية الاستدلال على البيانات الشخصية الحساسة

يمكن من خلال عمليات الاستدلال الوصول لبيانات حساسة، ويظهر ذلك من خلال التحليلات المتطورة للبيانات لاستنتاج البيانات الحساسة من البيانات غير الحساسة.

وتكمن خطورة الاستدلالات في عدم تطلبها لضرورة الحصول على البيانات المدخلة في عملية الاستدلال من الشخص المعنى بالبيانات، بل يمكن أن تقوم على بيانات عادية، أو كذلك بيانات غير شخصية، بل والأكثر من ذلك يمكنها القيام على بيانات مجهولة المصدر والتي لا تحتوى بشكل واضح على عنصر محدد للهوية.

وعلى ذلك، يثار التساؤل حول مدى تمتع عملية الاستدلالات بالحماية القانونية، وكذلك مدى الحماية القانونية المقررة للبيانات التي تم الاستدلال عليها في ظل القواعد التشريعية المعمول بها حالياً على المستويين الوطني والدولي.

وإذا كان أصحاب البيانات يتمتعون بحقوق على نتائج المعالجة للبيانات الشخصية المتعلقة بهم، فإنه في مجال الاستدلالات، يتوقف مدى الاعتراف لهم بهذه الحقوق على مدى اعتبار الاستدلالات ونتائجها بيانات شخصية.

ونعرض من خلال هذا المبحث للمقصود بعملية الاستدلالات على البيانات الحساسة، والحماية القانونية لها، سواء من حماية عملية الاستدلال ذاتها، وكذلك حماية البيانات المستنتجة منها، ومدى اعتبار الاستدلالات بيانات شخصية.

المطلب الأول: ماهية الاستدلال على البيانات الحساسة.

المطلب الثاني: الحماية القانونية للاستدلالات.

المطلب الثالث: مدى اعتبار الاستدلالات بيانات شخصية.

المطلب الأول

ماهية الاستدلال على البيانات الحساسة

نعرض من خلال هذا المطلب لتعريف عمليات الاستدلالات على البيانات الحساسة، وكذلك لبعض تطبيقات التحليلات الاستدلالية، وهو ما نوضحه في الفرعين التاليين.

الفرع الأول

تعريف الاستدلالات

يقصد بالاستدلال على البيانات الحساسة أنه يمكن من خلال التحليلات المتطورة للبيانات استنتاج البيانات الحساسة من البيانات غير الحساسة.

وبمفهوم آخر تعرف الاستدلالات على أنها معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه، تم إنشاؤها من خلال الاستنباط أو الاستدلال، وليس مجرد الملاحظة أو التجميع من صاحب البيانات(٧٩).

وفي هذا الصدد، تعتمد الاستدلالات على نوعين من البيانات، وهما: أولاً: البيانات المقدمة من صاحب البيانات (البيانات المدخلة) وتتضمن البيانات المقدمة أي بيانات قدمها صاحب البيانات مباشرة إلى مراقب البيانات، على سبيل المثال اسم

(79) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494.

المستخدم أو عنوان البريد الإلكتروني، أو البيانات المرصودة والتي يتم تقديمها أيضًا بواسطة صاحب البيانات ولكن بشكل غير مباشر أو سلبي، بما في ذلك أشياء مثل بيانات الموقع، أو نشاط النقر، أو الجوانب الفريدة لسلوك الشخص مثل الكتابة اليدوية، أو ضغطات المفاتيح، أو أي أمر معين، مثل طريقة المشي أو التحدث(٨٠).

وثانياً: البيانات المستنتجة أو المشتقة التي تم التوصل إليها من خلال عملية الاستدلالات، على سبيل المثال، بلد الإقامة المشتقة من الرمز البريدي للموضوع، والبيانات المستنتجة مثل درجة الائتمان، أو نتائج التقييم الصحي، أو نتائج عملية التخصيص أو التوصية، ولا يتم توفيرها من قبل صاحب البيانات بشكل إيجابي أو سلبي، ولكن يتم إنشاؤها بواسطة مراقب البيانات أو طرف ثالث من البيانات المقدمة من صاحب البيانات وتنتج من معالجة البيانات المدخلة بواسطة عملية الاستدلال.

وبالنظر للقوانين والقواعد المنظمة لحماية البيانات نجد أن اهتمامها البالغ بالنوع الأول من البيانات وهى البيانات المدخلة، دون توفير الحماية المناسبة للبيانات المستنتجة بما قد تشتمل عليه من بيانات حساسة.

ويوجد نوع من الاستدلالات يسمى بالاستدلالات عالية المخاطر وهى الاستدلالات التي يتم إنشاؤها أو استخدامها من قبل مراقبي البيانات أو أطراف ثالثة(٨١)،

(80) Article 29 Data Prot. Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136, at 8 (June 20, 2007) http://ec.europa.eu /justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en .pdf (on file with the Columbia Business Law Review).

(٨١) ويعرف الطرف الثالث بكونه شخصاً طبيعياً أو اعتبارياً أو سلطة عامة أو وكالة أو هيئة بخلاف صاحب البيانات أو المراقب أو المعالج، ويكون له سلطة معالجة البيانات الشخصية من خلال تصريح بذلك من المراقب أو المعالج، في ذلك انظر:

=

ويترتب عليها انتهاك الخصوصية أو الاضرار بالسمعة - أو من المحتمل بشكل كبير أن تكون كذلك في المستقبل - أو تكون إمكانية التحقق منها منخفضة أي تقوم غالباً على التنبؤ أو الاستناد إلى الرأي أثناء استخدامه لاتخاذ القرارات المهمة.

ووفقاً لعملية الاستدلال، فإنه يمكن من خلالها استنتاج العديد من البيانات الحساسة من بيانات شخصية عادية، وإذا تم اعتبار البيانات الشخصية التي يمكن أن تؤدى لبيانات حساسة من خلال عملية الاستدلال أنها حساسة، فإن جميع البيانات الشخصية تقريبًا يمكن أن تكون حساسة، ويمكن لفئات البيانات الحساسة أن تبتلع كل شيء.

ويشبه البعض البيانات الشخصية بالنسيج الكبير، حيث تتشابك أنواع مختلفة من البيانات إلى درجة تجعل من المستحيل فصل الخيوط، ومن خلال استخدام البيانات الضخمة وخوارزميات التعلم الآلي القوية، تؤدي معظم البيانات غير الحساسة إلى استنتاجات حول البيانات الحساسة(٨٢).

وتشير قوانين حماية البيانات المختلفة، وكذلك اللائحة العامة الأوروبية لحماية البيانات، في تعريفها للبيانات الشخصية بأنها أي بيانات متعلقة بشخص طبيعي محدد، أو

=

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) ch. 1, art. 4(10), 'third party' means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data."

(82) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081.

يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق ربطها ببيانات أخري، كالاسم أو الصوت أو الصورة، أو الرقم التعريفي، أو محدد الهوية عبر الانترنت، أو كذلك أي بيانات تحدد الهوية الصحية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية(٨٣).

ويفهم من ذلك أن مصطلح "يمكن تحديده" لا يشير فقط إلى الهوية المدنية أو القانونية للشخص، ولكن أيضًا إلى أي عنصر قادر على "إضفاء طابع فردي" أو تمييز يمكن من خلاله تحديد شخص بعينه.

وقد أورد المشرع البيانات التي يمكن ربطها مع غيرها لتحديد شخص معين على سبيل المثال، وعلى ذلك يمكن إجراء التحديد، أو التفرد، أو التميز من بين أمور متعددة، على سبيل المثال، من رقم تعريف، أو اسم مستعار، أو بيانات بيومترية أو وراثية، أو قاعدة بيانات، أو عنوان IP أو أي معرف آخر، يشير إلى شخص صاحب البيانات، كما يمكن تحديده من خلال جهاز أو مجموعة من الأجهزة مثل كمبيوتر، أو هاتف محمول، أو كاميرا، وما إلى ذلك.

كما لم تعد التعرف أو إمكانية التعرف على عناصر الهوية المدنية لشخص ما ضرورية لإضفاء طابع فردي عليها والتصرف تجاهها، حيث يجب أن يمتد مفهوم "قابلية تحديد الهوية" ليشمل مفهومي "إمكانية التتبع" و"إمكانية الاتصال"، وهذا، على

(٨٣) المادة الأولى من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، وكذلك:
Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) ch. 1, art. 4(1).

وجه الخصوص، يوسع النطاق التعريفي حول طبيعة البيانات الشخصية مثل عنوان IP أو ملفات تعريف الارتباط أو حتى حيازة ساعة مزودة بخصائص معينة(٨٤).

ومن الجدير بالذكر أن الأمر بشأن الاستدلالات على البيانات لا يقتصر فقط على البيانات الحساسة، بل يشمل أيضاً البيانات الشخصية العادية والتي يمكن التوصل إليها والاستدلال عليها من خلال بيانات عادية ليست ذات طبيعة شخصية، وكذلك بالنسبة للبيانات التي توصف بكونها بيانات مجهولة.

ولا تحتوى البيانات مجهولة المصدر على عنصر واضح لتحديد الهوية، وأشار التقرير التوضيحي لمجلس أوروبا إلى أنه في بعض الحالات يمكن استخدام البيانات مجهولة المصدر، والتي لا تتطلب وقتًا أو أنشطة أو موارد غير معقولة، لتحديد هوية الشخص، وهذا هو الحال بشكل خاص، عند الجمع بين أنواع مختلفة من البيانات، مثل البيانات الجسدية أو الفسيولوجية أو الجينية أو الاقتصادية أو الاجتماعية (مزيج من البيانات المتعلقة بالعمر والجنس والنشاط المهني والموقع الجغرافي والحالة العائلية، وما إلى ذلك)، يسمح لمراقب البيانات، أو أي شخص آخر، بتحديد صاحب البيانات، وفي مثل هذه الحالة، لا يمكن اعتبار البيانات مجهولة المصدر ومشمولة بأحكام الاتفاقية(٨٥).

(84) Frédérique CHOPIN, Cybercriminalité – Systèmes et réseaux numériques, objets de l'infraction,Dalloz, Janvier 2020 (actualisation : Décembre 2023)

(85) le rapport explicatif du Conseil de l'Europe (p. 10, no 19) qui note très justement : « Des données en apparence anonymes, car non assorties d'un élément d'identification évident, peuvent néanmoins, dans certains cas (ne nécessitant pas des délais, activités ou ressources déraisonnables) permettre l'identification d'une personne. C'est notamment le cas lorsque la combinaison de différents types de données , telles des données physiques, physiologiques, génétiques, économiques ou sociales (combinaison de données relatives à l'âge, le sexe, l'activité =

ومؤدى ذلك أنه يمكن استخدام البيانات والمعلومات التي قد لا تكون محور اهتمام خاص لدى الأشخاص للاستدلال على بيانات أخرى، ويتم ذلك من خلال تجميع أو رصد البيانات العادية، التي تتيح التكنولوجيا واسعة الانتشار جمعها بشكل خاص لتشكيل ملفات تعريف.

ومنذ عدة سنوات مضت، سارت توصية مجلس أوروبا بشأن التوصيف في هذا الاتجاه، حيث رغبت في عدم استبعاد البيانات المجهولة عندما يهدف استخدامها إلى إنشاء ملف تعريف يكون لتطبيقه تأثير على الشخص(٨٦).

ولذلك، يجب التأكيد صراحة على أن مفهوم "البيانات" تمتد للبيانات ذات الطبيعة الشخصية، وبالتالي، تعد قائمة المشتريات التي تمت في متجر متعدد الأقسام، والتواجد في موقع معين، وزيارة موقع ويب معين، فليست طبيعة البيانات في حد ذاتها هي التي تجعلها شخصية، ولكن المخاطر الناجمة عن إمكانية تجميع البيانات المتعلقة

=

professionnelle, la géolocalisation, la situation de famille, etc.), permet au responsable du traitement, ou à toute autre personne, d'identifier la personne concernée. Dans pareille situation, les données ne sauraient être considérées comme anonymes et sont couvertes par les dispositions de la Convention ».

(86) Recommandation du Conseil de l'Europe en matière de profilage, CM/Rec., 2010. Cf. en particulier le rapport préalable, qui insiste sur la nécessité d'une vue « holistique » du processus et de son résultat final, et non sur une approche a priori qui serait fondé sur la nature des données (Y. Poullet et J.M. Dinant, Rapport à l'attention du Comité des ministres (article 20, paragraphe 3, de la convention STE no 108) : comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel , Strasbourg, Conseil de l'Europe, 2010, disponible à http://www.crid.be/pdf/public/6539.pdf.

بعدد من الأفراد والاستدلال من خلالها على بيانات أخرى أكثر أهمية وحساسية لفرد أو مجموعة من الأفراد، وهو ما يشير لضرورة الاعتداد بمعيار السياق والغرض من جمع ومعالجة البيانات لتحديد الطبيعة الشخصية أو الحساسة بشأنها.

ولا شك أن التمييز بين البيانات ذات الطبيعة الشخصية، والبيانات ذات الطبيعة غير الشخصية، سيختفي عندما يؤدي الاستخدام المشترك لهما لاستدلالات يكون لها تأثير على الشخص المعني وحقوقه.

كما أن الاستدلال المؤدى لنتائج تتعلق بالبيانات الشخصية، أو البيانات الحساسة سوف يفعل معه الحماية المقررة للبيانات بموجب قانون حماية البيانات، وتحظى فئات خاصة من البيانات الشخصية تسمى "البيانات الحساسة" بحماية مشددة، ولكن هذا الأمر في مجال الاستدلالات إنما يتعلق فقط بالبيانات المدخلة (التى تم إجراء الاستدلال من خلالها)، بينما تظل الحماية القانونية للبيانات المستنتجة محل شك واختلاف في تشريعات حماية البيانات.

الفرع الثاني

تطبيقات للتحليلات الاستدلالية

تُستخدم أساليب التحليلات الاستدلالية في العديد من الأعمال والقرارات التي تهم الأشخاص، حيث يمكن من خلالها استنتاج تفضيلات المستخدم، والسمات الحساسة، مثل العرق، والآراء (مثل المواقف السياسية)، كما يمكن استخدام هذه الأساليب لاتخاذ قرارات مهمة، على سبيل المثال، قرارات القروض، والعمل والتوظيف، عمليات التأمين، وحماية المستهلك، وغيرها[٨٧].

(87) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494

وظهرت في السنوات الأخيرة تطبيقات عديدة لتحليلات البيانات الضخمة لاستخلاص استنتاجات مثيرة للقلق بشأن الأفراد والجماعات.

وتقف منصات الإنترنت الرئيسية ومواقع التواصل الاجتماعي وراء العديد من الأمثلة ذات أعلى الملفات الشخصية، حيث قد يكون موقع Facebook قادرًا على استنتاج التوجه الجنسي عبر السلوك عبر الإنترنت(٨٨)، والسمات المحمية الأخرى، على سبيل المثال العرق، والآراء السياسية(٨٩)، بينما استخدمت أطراف أخرى بيانات فيسبوك لاستنتاج الحالة الاجتماعية والاقتصادية للأشخاص(٩٠).

علاوة على ذلك فقد بدأت شركات التأمين في استخدام بيانات وسائل التواصل الاجتماعي لتحديد أقساط التأمين(٩١)، ولا شك أن هذا الأمر يثير القلق لأنه يمكن استخدام

(88) Jose Gonzalez Cabanas, Angel Cuevas & Ruben Cuevas, Facebook Use of Sensitive Data for Advertising in Europe (Feb. 14, 2018) (unpublished manuscript), https://arxiv.org/abs/1802.05030 [https://perma. cc/V2C8-FY3W].

(89) Jeremy B. Merrill, Liberal, Moderate or Conservative? See How Facebook Labels You, N.Y. Times (Aug. 23, 2016), https://www.nytimes.com/2016/08/24/us/politics/facebook-ads-politics.html [https://perma.cc/QNU7-YCBZ].

(90) Astra Taylor & Jathan Sadowski, How Companies Turn Your Facebook Activity into a Credit Score, The Nation (May 27, 2015), https://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/ [https://perma.cc/V4V5-7H55].

(91) Leslie Scism, New York Insurers Can Evaluate Your Social Media Use - If They Can Prove Why It's Needed, Wall St. J. (Jan. 30, 2019), https://www.wsj.com/articles/new-york-insurers-can-evaluate-your-social-media-useif-they-can-prove-why-its-needed-11548856802 (on file with the Columbia Business Law Review).

الشبكة الاجتماعية للشخص لاستخلاص استنتاجات حادة وحميمة عن شخصية المرء حتى بدون علمه.

وفي مجال البيانات الصحية، فإنه في عصر التقدم التكنولوجي الهائل، قد تتعرض البيانات الصحية للأشخاص لمخاطر متعددة، تثار معها إشكاليات تطبيق القيود والحماية المقررة بتشريعات حماية البيانات.

وهناك صور عديدة لإمكانية الاطلاع وجمع البيانات الصحية للأشخاص، بل وكذلك تخزينها وإمكانية معالجتها، واستخدامها في أنشطة متعددة، خاصة التجارية منها، وفي الآونة الأخيرة ظهرت العديد من الوسائل التي يمكن من خلالها جمع البيانات الصحية، مثل تطبيقات الصحة، والأجهزة القابلة للارتداء والتطبيقات المختلفة على الهواتف المحمولة، والتي تعد في ارتفاع مستمر وبشكل كبير سنة بعد أخرى(٩٢).

ويمكن من خلال عمليات الاستدلالات التوصل للبيانات الصحية للأشخاص، حيث يمكن أن تقوم هذه الأجهزة والتطبيقات بجمع بيانات حساسة، بل وإمكانية القيام بذلك دون علم المستخدم، وأحياناً كذلك يتم جمعها من خلال المعلومات التي يُدخلها

(92) Aaron Smith, Record shares of Americans now Own smartphones, have home broadband, PEW RSCH. CTR. (Jan. 12, 2017), https://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/; see also Lionel Sujay Vailshery, Statistical Report, Number of connected wearable devices worldwide by region from 2015 to 2022, STATISTA (Jan. 22, 2021), https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/.

المستخدم في التطبيقات الطبية أو التي يتم جمعها من خلال مستشعرات الأجهزة القابلة للارتداء، أو مشاركتها، أو بيعها، وغالبًا دون علم المستخدم أو موافقته[٩٣].

علاوة على ذلك، تتأثر البيانات الحساسة بالمخاطر التكنولوجية المتطورة، حيث تُظهر العديد من الدراسات كيف يمكن إجراء استنتاجات حول الحالة الصحة للأشخاص بناءً على بيانات وسائل التواصل الاجتماعي[٩٤].

كما طور باحثون آخرون نموذجًا يهدف إلى تحديد الأمراض العقلية والنفسية مثل الاكتئاب، والاضطراب ثنائي القطب، واضطراب الشخصية الحدية، استنادًا إلى منشورات المستخدمين على موقع التواصل الاجتماعي[٩٥].

وبالتالي، بما أن الأجهزة القابلة للارتداء والتطبيقات المتطورة المختلفة تجمع المعلومات الصحية عن مستخدميها، فإنها ستصبح بشكل متزايد مصدرًا لإنشاء البيانات الحساسة[٩٦].

---

(93) Jay Hancock, Workplace wellness programs put employee privacy at risk, CNN HEALTH (Oct. 2, 2015), https://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/index.html

(94) Michal Kosinski, David Stillwell & Thore Graepel, Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, 110 PNAS, 2013, p. 5802.

(95) Jina Kim, Jieon Lee, Eunil Park & Jinyoung Han, A Deep Learning Model for Detecting Mental Illness from User Content on Social Media, 10 SCI. REPS., 2020, p. 11846.

(96) mHealth Market Size, Share & Trends Analysis Report By Component (Wearables, mHealth Apps), By Service (Monitoring, Diagnosis), By Participant (Mobile Operators, Device Vendors), By Region, And Segment Forecasts, 2020 - 2027, GRAND VIEW RSCH. (Feb. 2020), https://www.grandviewresearch.com/industry-analysis/mhealth-market

كما تساهم وسائل التواصل الاجتماعي، بشكل فاعل، في عمليات الاستدلال على البيانات الحساسة، ويؤكد ذلك ما قام به مجموعة من الباحثين بتطوير نموذج للتنبؤ باحتمالية الإصابة باكتئاب ما بعد الولادة بناءً على بيانات المستخدم لفيسبوك قبل الولادة، وركز النموذج على الحد من النشاط الاجتماعي والتفاعل على فيسبوك، حيث اعتبروا أن المعلومات العادية مثل تكرار النشاط على موقع التواصل الاجتماعي هي الجزء المهم من البيانات التي تضيء الخوارزمية[٩٧].

ويلاحظ أن نطاق وطبيعة جمع البيانات بواسطة التطبيقات والأجهزة القابلة للارتداء والجهات الخارجية واسع وهام إلى حد كبير، حيث تجمع التطبيقات الطبية معلومات حول أفكار المستخدم، وأفعاله، وحالته المزاجية، واستجاباته للتدخلات، النظام الغذائي، عادات ممارسة الرياضة، وعمليات الشراء عبر الإنترنت وفي المتجر[٩٨]، وقد توصف كل هذه البيانات باعتبارها بيانات عادية، لكن اليوم يمكن استخدامها في عمليات الاستدلالات، واستنتاج بيانات شخصية منها أو كذلك بيانات حساسة.

وتجدر الإشارة في هذا الصدد أنه على الرغم من مزايا التكنولوجيا المتعددة، وبصفة خاصة هنا في أجهزة وتطبيقات جمع البيانات، والتي يمكن من خلالها تقديم

(97) Munmun De Choudhury, Scott Counts, Eric J. Horvitz & Aaron Hoff, Characterizing and Predicting Postpartum Depression from Shared Facebook Data, in ASS'N FOR COMPUTING MACH., CSCW '14: PROCEEDINGS OF THE 17TH ACM CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK & SOCIAL COMPUTING, 2014, p. 625.

(98) Ashley Hall, 5 Ways to Track Your Personal Health on Your Phone, VERYWELLHEALTH (Mar. 5, 2020), https://www.verywellhealth.com/track-health-information-phone-1739148

إشعار في الوقت المناسب لتفعيل الرعاية الوقائية واستراتيجيات التخفيف والتخطيط الطبي للمستخدمين، بالإضافة إلى ذلك، قد تكون كمية ونوعية البيانات التي تم جمعها مفيدة للأطباء في فهم واكتشاف الحالات الطبية المختلفة بشكل علمي دقيق، مما قد يؤدي إلى تطوير الأدوية، والرعاية الوقائية، والمستحضرات الصيدلانية[٩٩]، فإن استخدام هذه الأدوات قد يصطدم بالقيود المقررة لحماية البيانات الحساسة، وهي إشكالية قانونية قائمة، وبشكل مستمر، تتعلق بكيفية تحقيق التوازن بين تشجيع الابتكار والاستفادة منه لخدمة البشرية وبين حماية الحقوق الأساسية للأشخاص وعدم تعرضها لمخاطر قد يصعب التغلب عليها.

المطلب الثاني

الحماية القانونية للاستدلالات

تحظى الاستدلالات بحماية قانونية أقل بموجب قواعد حماية البيانات الأوروبية مقارنة بالأنواع الأخرى من البيانات الشخصية التي يقدمها صاحب البيانات.

ويكمن السبب الحقيقي في ذلك للاجتهادات القضائية المتواترة لمحكمة العدل الأوروبية والتي تتجه نحو تضييق نطاق تطبيق اللائحة العامة لحماية البيانات في مجال الاستدلالات.

(99) Gunther Eysenbach, The Continued Use of Mobile Health Apps: Insights From a Longitudinal Study, JMIR MHEALTH UHEALTH, Aug. 2019, at 1.

ومع ذلك، وبموجب القواعد الحماية المنظمة للبيانات الشخصية، تعتبر الاستنتاجات التي تؤدى للوصول أو الكشف عن بيانات حساسة بمثابة بيانات حساسة، ومؤدى ذلك أي بيانات شخصية يمكن استنتاج بيانات حساسة منها سيتم اعتبارها أيضًا بيانات حساسة.

ونعرض من خلال هذا المطلب لمدى تمتع الاستدلالات بالحماية القانونية، وهو ما نبينه في الفرع الأول، ونعرض في الفرع الثاني مدى اعتبار الاستدلالات بيانات شخصية.

الفرع الأول

مدى تمتع الاستدلالات بالحماية القانونية

لا تتمتع الاستدلالات وفقاً لقواعد حماية البيانات سواء على المستوى الأوروبي أو المصري بحماية قانونية مماثلة لتلك التي تتمتع بها البيانات المقدمة من أصحاب البيانات.

ويرجع السبب في ذلك للقيود المفروضة على اختصاص قانون حماية البيانات من قبل محكمة العدل الأوروبية والتي تلعب دورًا رئيسيًا في تحديد اختصاص قانون حماية البيانات، حيث أدي ذلك لتضييق نطاق تطبيق قانون حماية البيانات الشخصية في مجال عملية الاستدلالات.

واتخذ قضاء محكمة العدل الأوروبية موقفاً بشأن اختصاص قانون حماية البيانات، حيث قررت محكمة العدل الأوروبية إن الغرض من قانون حماية البيانات هو حماية البيانات الشخصية المقدمة من صاحب البيانات، وليس تقييم دقة عمليات صنع القرار المتعلقة بالبيانات الشخصية.

وعلى هذا الأساس، تم رفض طلبات المتقدمين للحق في الوصول للمعلومات المستنتجة، لأن نيتهم كانت تقييم دقة تقييم البيانات الشخصية.

ولا يخضع هذا الأمر لقانون حماية البيانات، وقررت محكمة العدل الأوروبية إنه ينبغي الرجوع للقوانين الأخرى المطبقة على الحالة المحددة لتقييم ما إذا كانت إجراءات اتخاذ القرار دقيقة.

وعلى وجه التحديد، ذكرت محكمة العدل الأوروبية ما يلي:

"على النقيض من البيانات المتعلقة بطالب تصريح الإقامة الواردة في المحضر والتي قد تشكل الأساس الواقعي للتحليل القانوني الوارد فيها، فإن مثل هذا التحليل ليس في حد ذاته عرضة لأن يكون موضوع فحص وتقييم من حيث الدقة من قبل مقدم الطلب والتصحيح بموجب المادة ١٢(ب) من التوجيه ٤٦/٩٥ ، واستندت المحكمة إلى أن التوسع في حق الوصول لمقدم الطلب للحصول على تصريح إقامة استناداً إلى هذا التحليل القانوني لن يخدم في الواقع غرض التوجيه المتمثل في ضمان حماية حق مقدم الطلب في الخصوصية فيما يتعلق بمعالجة البيانات المتعلقة به، ولكنه يخدم غرض آخر وهو ضمان حق الوصول إلى الوثائق الإدارية، وهو ما لا يغطيه التوجيه ٤٦/٩٥"[1].

ولم تكن القيود المقررة على حق الوصول هي المرة الوحيدة التي أكدت عليها المحكمة، ففي دعوى أخري قضت محكمة العدل الأوروبية بأن حق الوصول يقتصر على توفير المعلومات المتعلقة بنطاق البيانات قيد المعالجة (وهو أمر ضروري لتصحيح

(1) Cases C-141/12 & 372/12, YS v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, PP 45-46.

هذه البيانات أو محوها)، للتحقق من مشروعية المعالجة، أو الاعتراض على المعالجة[١].

بالإضافة إلى ذلك فقد اكتفت محكمة العدل الأوروبية بأن يكون مقدم الطلب في حوزته ملخصًا كاملاً لتلك البيانات في شكل واضح، أي في شكل يسمح أن يصبح مقدم الطلب على علم بتلك البيانات والتحقق من دقتها ومعالجتها وفقًا لهذا التوجيه" [٢].

ويثير قضاء محكمة العدل الأوروبية بشأن حق الوصول للبيانات انتقادات، خاصة فيما يتعلق بمعايير اتخاذ القرار، وذلك للأسباب الآتية:

أولاً: يقوم التحليل القانوني للبيانات المقدمة على استنتاجات أو افتراضات أو آراء قد تكون استنتاجات مؤقتة، إلا أنها مع ذلك تقوم عليها الاستنتاجات النهائية والقرارات اللاحقة.

ويعد استبعاد الوصول إلى هذا التحليل ومراجعته من نطاق قانون حماية البيانات يعني أن أصحاب البيانات غير قادرين على تقييم كيفية اتخاذ الاستنتاجات والقرارات ذات التأثير الكبير على حقوقهم[٣].

(1) Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 2009 E.C.R. I-3889, PP 51-52.

(2) Cases C-141/12 & 372/12, YS v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, P 44.

(3) Douwe Korff, The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data, EU Law Analysis (Oct. 15, 2014), http://eulawanalysis.blogspot.com/2014/10/the-proposed-general-data-protection.html [https://perma.cc/SRY9-JDW8]; Robert Madge, Five Loopholes in the GDPR, Medium (Aug. 27, 2017), https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b [https://perma.cc/L8EM-8YPM]

ثانيًا: بشأن ما قررته المحكمة من الاكتفاء بمشاركة ملخص البيانات الشخصية التي تخضع للمعالجة فقط، فإن ذلك يحد بشدة من قدرة صاحب البيانات على حق الوصول، وكذلك على تقييم مشروعية معالجة البيانات ودقة بياناته المستخدمة لإجراء قرار معين.

ثالثاً: يعد تضييق نطاق اختصاص قانون حماية البيانات أمر يثير القلق، حيث أن معايير صنع القرار القابلة للتطبيق بشكل عام موجودة في القطاع العام على أساس الشرعية وتخضع لعمليات الرقابة والمسئولية، ولكن من غير المرجح أن تحكم معايير مماثلة قابلة للتطبيق على نطاق واسع القطاع الخاص(١).

رابعاً: على مستوى الأفراد، غالبًا ما تكون القيمة المحتملة والبصيرة للبيانات الناتجة أثناء استخدام التقنيات الرقمية في مجال الاستدلالات غامضة، حيث يمكن لمراقبي البيانات استخلاص استنتاجات غير بديهية وغير متوقعة، دون علم الأفراد على الإطلاق(٢)، مما يشكل مخاطر على الخصوصية والهوية، وحماية البيانات والسمعة، وتقرير المصير المعلوماتي.

وعلى الرغم من أن استقلالية صنع القرار للكيانات الخاصة مقيدة بقوانين معينة، القواعد القانونية والدستورية التي تحظر التمييز، فإن الشركات الخاصة أقل احتمالا من القطاع العام أن يكون لديها إجراءات أو قواعد ملزمة قانونا يتعين عليها إتباعها عند اتخاذ القرارات.

---

(1) Serge Gutwirth & Paul De Hert, Regulating Profiling in a Democratic Constitutional State, in Profiling the European Citizen, 2008, p. 275.

(2) Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev., 2018, p. 1085.

وبالتالي، وفقًا لقضاء محكمة العدل الأوروبية، عندما تستخلص شركة خاصة استنتاجات من البيانات المجمعة أو تتخذ قرارات بناءً عليها، حتى لو تم النظر إلى الاستنتاجات أو القرارات النهائية على أنها بيانات شخصية أو حساسة، فإن أصحاب البيانات غير قادرين على تصحيحها بموجب قانون حماية البيانات.

كما يفتقر أصحاب البيانات أيضًا إلى إمكانية الوصول إلى الأسباب الكامنة وراء القرارات، والتي لا تعتبر بيانات شخصية، فضلاً عن وسائل تصحيح الاستدلالات بموجب قانون حماية البيانات.

ولا شك أن المخاطر الجديدة التي أدخلتها تحليلات البيانات الضخمة واتخاذ القرارات الآلية، خاصة في ظل تقنيات الذكاء الاصطناعي، تشير إلى أن الاختصاص المنصوص عليه لقانون حماية البيانات قد يكون ضيقًا للغاية بحيث لا يمكن تطبيقه لتحقيق الأهداف الأصلية للقانون.

كما أن انتشار تحليلات البيانات الضخمة والزيادة الناتجة في قدرة مراقبي البيانات على استنتاج معلومات حول الحياة الخاصة للأفراد، وتعديل وترسيخ هويتهم، والتأثير على سمعتهم، والتأثير على حقوقهم المختلفة يشير إلى أن هناك حاجة إلى مستوى أعلى من الحماية مما كان عليه الوضع في القواعد المنظمة لحماية البيانات.

وعلى ذلك، وبهدف تقرير حماية اكبر وأوسع نطاقاً لأصحاب البيانات يجب التركيز على إدارة بيانات المخرجات، أو الاستدلالات والقرارات، لإعادة تشكيل الخصوصية كمفهوم شمولي، دون الاعتداد والاكتفاء فقط بحساسية البيانات وقابليتها للتعرف والتحديد والتي أصبحت لا تجدي في عصر البيانات الضخمة وإلا تصبح الحماية القانونية بموجب قانون حماية البيانات فارغة من مضمونها.

ويؤيد ذلك ما اتجه إليه البعض[1] بأنه "في عالم البيانات الضخمة، ما يستدعي التدقيق غالبًا ليس دقة البيانات الأولية بل دقة الاستدلالات المستمدة من البيانات."

كما أنه من خلال العديد من الفروق بين أنواع البيانات (الشخصية، والحساسة) فسيؤثر ذلك على الوضع القانوني للاستدلالات في مجال تطبيق اللائحة العامة الأوروبية لحماية البيانات، وكذلك القوانين الوطنية المنظمة لحماية البيانات الشخصية.

الفرع الثاني

مدى اعتبار الاستدلالات بيانات شخصية

يترتب على الاعتراف بالاستدلالات أنها بيانات شخصية أو كذلك حساسة إذا تم التوصل من خلالها لبيانات حساسة حقوقاً لأصحاب البيانات على نتائج الاستدلالات مثل حقوق الوصول، والتصحيح، والاعتراض، والطعن على نتائجها.

وعلى الرغم من الاتجاه الموسع لتعريف البيانات الشخصية الذي تبنته محكمة العدل الأوروبية، إلا أن ذات المحكمة قد تبنت نهجاً أكثر تقييدًا لنطاق البيانات الشخصية والحقوق المعمول بها.

أولاً: الاتجاه المؤيد لاعتبار الاستدلالات بيانات شخصية:

بموجب قانون حماية البيانات الشخصية يتمتع أصحاب البيانات حقوقاً على نتائج المعالجة للبيانات الشخصية، مثل حق الاعتراض على معالجة البيانات الشخصية، أو

(1) Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop., 2013, p. 239.

نتائجها، خاصة إذا تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات(٢).

ويتم منح أصحاب البيانات حقوقًا قابلة للتطبيق على نطاق واسع بشأن نتائج معالجة بياناتهم بموجب قانون حماية البيانات، ولذلك يجب اعتبار الاستنتاجات أو الاستدلالات بمثابة بيانات شخصية(٣).

ويترتب على اعتبار الاستدلالات بيانات شخصية أن الأثر التمييزي لأنواع البيانات المقرر بقوانين حماية البيانات سيكون محلاً للتطبيق على عملية الاستدلال، أي تخضع عمليات الاستدلال على البيانات الحساسة للقيود المقررة قانوناً، ويتمتع أصحاب البيانات بالحقوق كذلك المقررة.

كما أن للتمييز بين نوعى البيانات أثر بالغ، حيث إن البيانات الحساسة تفرض قيودًا إضافية على عملية المعالجة(٤)، ويترتب على ذلك أنه إذا كانت الاستدلالات بيانات شخصية، فإن هذا التمييز بين الأنواع الحساسة وغير الحساسة، والمعيار الأعلى للحماية الممنوحة للأولى، سينطبق أيضًا.

---

(٢) المادة (٦/٢) من القانون المصري رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(3) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494.

(٤) المادة (١٢) من القانون المصري رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، وكذلك:

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) ch. 1, art. 9(2-4).

وتـوفر المبـادئ التوجيهيـة الصـادرة عـن فرقـة العمـل المعنيـة بالمـادة ٢٩[٥] إرشـادات بشـأن التوصـيف (Profiling)[٦]، واتخـاذ القـرار الآلـي، وتشـير إلـى أن التوصـيف حيـث يعمـل عـن طريـق إنشـاء بيانـات مشـتقة أو مسـتنبطة عـن الأفـراد تعتبـر بمثابـة بيانـات شخصـية جديـدة لـم يـتم تقـديمها مباشـرة مـن قبـل أصـحاب البيانـات أنفسهم.

وفـي مبـدأ تـوجيهي آخـر أقـرت فرقـة العمـل أنـه فـي أغلـب الأحيـان، ليسـت المعلومات التي تم جمعها في حد ذاتها هي الحساسة، بل الاستدلالات المستخلصة منها و

(5) Article 29 Data Prot. Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP136, at 8 (June 20, 2007) http://ec.europa.eu/ justice/article-29/documentation/opinion-recommendation /files/2007/wp136_en.pdf (on file with the Columbia Business Law Review).

ونشير هنا إلى أنه اعتبارًا من تطبيق اللائحة العامة لحماية البيانات ("GDPR") في ٢٥ مايو ٢٠١٨، لم يعد فريق عمل المادة ٢٩ موجودًا، وخلفه المجلس الأوروبي لحماية البيانات ("EDPB")

European Data Prot. Bd., The European Data Protection Board, Endorsement 1/2018 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/news /endorsement_of_ wp29_documents.pdf [https://perma.cc/8H9A-RQR3]

(٦) يقصد بالتوصيف أنه أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتكون من استخدام البيانات الشخصية لتقييم بعض الجوانب الشخصية المتعلقة بشخص طبيعي، ولا سيما لتحليل أو التنبؤ بالجوانب المتعلقة بأداء ذلك الشخص الطبيعي في العمل، والوضع الاقتصادي، والصحة، والشخصية، والتفضيلات أو الاهتمامات أو الموثوقية أو السلوك أو الموقع أو الحركات.

Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) ch. 1, art. 4(4).

الطريقة التي يتم بها استخلاص هذه الاستنتاجات يمكن أن تكون هى الحساسة وتثير القلق[٧].

ويتضح من ذلك أنه إذا كان من الممكن اعتبار الاستدلالات بيانات شخصية أو حساسة حسب ما تسفر عنه من نتائج، فيقصد بذلك البيانات المشتقة أو المستنتجة، وهى البيانات التي تم التوصل إليها من خلال عملية الاستدلالات، والتي لم يتم توفيرها من قبل صاحب البيانات بشكل إيجابي أو سلبي، ولكن يتم إنشاؤها بواسطة مراقب البيانات أو طرف ثالث من البيانات المقدمة من صاحب البيانات[٨].

وعلى الرغم من أن المبادئ التوجيهية غير ملزمة قانونًا، إلا أنها تؤيد بوضوح وجهة النظر القائلة باعتبار أن الاستدلالات هي بمثابة بيانات.

ومع ذلك فإن مدى اعتبار الاستدلالات بمثابة بيانات شخصية محل شك، خاصة في ظل القضاء الملزم قانوناً لمحكمة العدل الأوروبية (ECJ).

(7) Article 29 Data Prot. Working Party, Opinion 03/2013 on Purpose Limitation, at 47, 00569/13/EN, WP203 (Apr. 2, 2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/X6PC-825X].

(8) Martin Abrams, The Origins of Personal Data and its Implications for Governance (Nov. 24, 2014) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510927[https://perma.cc/9YZ5-FT96]

ثانياً: الاتجاه المعارض لاعتبار الاستدلالات بيانات شخصية:

تشير الاجتهادات القضائية لمحكمة العدل الأوروبية للتفسير الموسع لمفهوم البيانات الشخصية، ومع ذلك فقد كان للمحكمة تاريخيًا وجهة نظر أكثر تقييدًا لنطاق البيانات الشخصية والحقوق المعمول بها(٩).

واتجه قضاء محكمة العدل الأوروبية إلى أن "البيانات المتعلقة بطالب تصريح الإقامة الواردة في المحضر، وحيثما كان ذلك مناسبًا، وكذلك البيانات الواردة في التحليل القانوني الوارد في المحضر هي "بيانات شخصية" وفقاً للمعنى المقصود في هذا الحكم، في حين أنه على النقيض من ذلك، لا يمكن تصنيف هذا التحليل في حد ذاته على هذا النحو"(١٠).

ويشير هذا الحكم بشكل واضح إلى أن نطاق البيانات الشخصية يشتمل على البيانات الواردة أو المستخدمة في التحليل القانوني فقط، وليس التحليل نفسه، وتخضع فقط البيانات الواردة والمستخدمة في التحليل لتوصيف البيانات الشخصية، وتخضع للحماية بموجب توجيه حماية البيانات لعام ١٩٩٥ المعمول به وقتها.

(9) Case C-101/01 Lindqvist [2003] E.C.R. I-12971, P 24; Joined Cases C-465/00, C-138/01 and C-139/01 Osterreichischer Rundfunk and Others [2003] E.C.R. I-4989, P 64; Case C-73/07 Satakunnan Markkinaporssi and Satamedia [2008] E.C.R. I-9831, PP 35, 37; Case C-524/06 Huber [2008] E.C.R. I-9705, P 43; and Case C-553/07 Rijkeboer [2009] E.C.R. I-3889, P 62.

(10) Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, P 48.

كما أشارت محكمة العدل الأوروبية إلى تعريف واسع للبيانات الشخصية، والذي يتضمن البيانات الواردة في شكل آراء وتقييمات، بشرط أن تكون متعلقة بموضوع البيانات، وقررت المحكمة أن الرأي أو التقييم المرتبط بشخص معين بسبب محتواه أو غرضه أو تأثيره يعتبر بيانات شخصية(١١)، واستندت محكمة العدل الأوروبية إلى أن تقييم الشخص يمكن أن يكون لها تأثير عليه وعلى حياته الخاصة، وهي وبالتالي بياناته الشخصية، ولكن تجدر الإشارة إلى أن أسئلة الاختبار أو التقييم في ذاتها لا تعتبر بيانات شخصية للمرشح.

وعلى الرغم من توسيع المحكمة لنطاق البيانات الشخصية إلا أنها قررت أن القدرة على ممارسة حقوق حماية البيانات الفردية ذات الصلة بشكل كامل لا تنبع تلقائيًا من هذا التصنيف، بل إن نطاق الحقوق المرتبطة بالبيانات الشخصية يجب تفسيره على حسب الغاية من جمع البيانات ومعالجتها، مع الإشارة إلى أهداف قانون حماية البيانات، والغرض الذي تم من أجله جمع البيانات ومعالجتها(١٢).

وبمعنى آخر، يجب تفسير نطاق حقوق حماية البيانات في هذا الإطار، من خلال الإشارة إلى الأغراض المحددة التي تم جمع البيانات من أجلها، والأهداف الأوسع لقانون حماية البيانات، وهذا يعني أن سبب جمع هذه البيانات يحدد حقوق حماية البيانات.

(11) Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994, P 60

(12) Cases C-141/12 & 372/12, YS v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, P 44.

وعلى وجه التحديد، أشارت محكمة العدل الأوروبية إلى أن "الاسم وتاريخ الميلاد والجنسية والجنس والانتماء العرقي والدين واللغة لمقدم الطلب" فقط، أو أن البيانات التي "تتعلق" بموضوع البيانات فقط هي بيانات شخصية(١٣).

وما يثير الاهتمام بشأن قضاء محكمة العدل الأوروبية هو أن سابقاً كان يطلب من المحكمة في الغالب أن تبت في الوضع القانوني للبيانات التي يمكن التحقق منها مثل البيانات المتعلقة بشخص محدد، وليس التقييمات أو البيانات غير القابلة للتحقق، من أمثلة البيانات الشخصية المذكورة في الأحكام السابقة مثل أرقام الهاتف، ومعلومات عن ظروف العمل والهوية(١٤)، أو كذلك "اللقب والمسمى" واسم بعض الأشخاص الطبيعيين الذين يتجاوز دخلهم حدودًا معينة (١٥)، وكذلك "بصمات الأصابع"(١٦)، وكذلك صورة شخص مسجلة بالكاميرا(١٧)، و"البيانات الضريبية(١٨).

(13) Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 Law Innovation & Tech, 2018, p. 28.

(14) Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.C.R. I-12992.

(15) Case C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinaporssi Oy & Satamedia Oy, 2008 E.C.R. I-09831.

(16) Case C-291/12, Michael Schwarz v. Stadt Bochum, 2013 E.C.R. I-670.

(17) Case C-212/13, Franti hac sek Rynehac s v. Urad pro Ochranu Osobnich udaju, 2014 E.C.R. I-2428, P 22.

(18) Case C-201/14, Smaranda Bara and Others v. Preedintele Casei Naionale de Asigurari de Sanatate, 2015 E.C.R. I-638, P 29.

وفي قضية أخرى، تناولت محكمة العدل الأوروبية ما إذا كان التحليل القانوني يمكن اعتباره بيانات شخصية، وهذا التحديد وثيق الصلة بشكل كبير بالوضع القانوني للاستدلالات.

ويمكن مقارنة التحليل القانوني بتحليل البيانات الشخصية حيث يتم استخلاص بيانات جديدة أو الاستدلال عليها.

ويمكن أن يتكون هذا التحليل من استنتاجات متعددة مرتبطة بفرد محدد أو يمكن التعرف عليه، مما يؤدي إلى رأي نهائي أو نتيجة أو استنتاج.

واعتبرت محكمة العدل الأوروبية أن التحليل القانوني، والاستدلالات المستخلصة فيه لا تعد بيانات شخصية[١٩].

ولا تميز محكمة العدل الأوروبية بين التحليل القانوني والآراء أو النتائج أو الاستدلالات الناتجة التي تم إنشاؤها أثناء المعالجة[٢٠].

ويلاحظ على قضاء محكمة العدل الأوروبية أنها قد وسعت نطاق البيانات الشخصية ليشمل الآراء والتقييمات، لكنها مع ذلك اتبعت رأيها السابق حيث يتم منح حقوق محدودة فقط فيما يتعلق بالتقييمات والآراء الناتجة عن الاستدلالات.

علاوة على ذلك، لم يكن هدف قانون حماية البيانات هو تقييم مدى دقة هذه التحليلات والاستدلالات، ولا يحق لأصحاب البيانات تصحيح نتائج الاستدلالات المؤقتة، أو نتائج الاستدلالات النهائية[٢١].

(19) Cases C-141/12 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, P 39, 48.

(20) Cases C-141/12 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2013 E.C.R. I-838, at P 49 n.40.

(21) Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994, P 55.

أخيرًا، اقتصر اختصاص قانون حماية البيانات مرة أخرى على اكتشاف نطاق البيانات التي تتم معالجتها، وتقييم ما إذا كانت المعالجة قانونية، ويبقى تقييم دقة التحليلات الاستدلالية وعمليات صنع القرار خارج نطاقه(٢٢).

وكما يشير البعض إلى أنه نظرًا لحقيقة أن الحقوق الواردة في اللائحة العامة لحماية البيانات يجب تفسيرها حسب الغاية من جمعها وغرض معالجتها، فليس من المستبعد أن تمنح السوابق القضائية المستقبلية الحق في التصحيح فيما يتعلق بمحتوى التقييمات والاستدلالات(٢٣).

ومع ذلك، في كثير من الحالات، سيطلب الأشخاص تقييمًا لعملية الاستدلال لما قد يترتب عليها من تأثيرات بالغة قد تلحق بهم أضراراً مادية وأدبية، وعلى سبيل المثال للحصول على عمل أو تأمين أو قرض، وغيرها.

ثالثاً: رأي الباحث:

يؤيد الباحث من جانبه الاتجاه الأول، حيث يجب اعتبار الاستدلالات التى تؤدي للتوصل لاستنتاجات عن البيانات الحساسة بمثابة بيانات حساسة، مما مؤداه خضوع الاستدلالات لقيود قانونية حماية لحقوق أصحاب البيانات على بياناتهم الحساسة.

(22) Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 2009 E.C.R. I-03889, P 49.

(23) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494

ويمكن تأييد رأينا بما يلي:

١- في حالة عدم القدرة على التنبؤ بالتحليلات الكامنة وراء اتخاذ القرار الآلي والتوصيف، يمكن أن يكون ذلك في حد ذاته ضارًا للأفراد، وهذا ما أكدته السوابق القضائية للمحكمة الأوروبية لحقوق الإنسان ("ECHR")[٢٤].

٢- كما أن استخدام مصادر البيانات غير التقليدية للتوصل إلى استنتاجات غير متوقعة وغير بديهية حول الأشخاص يمكن أن يؤثر على حرية التعبير، الحق في الخصوصية والهوية وغيرها للأفراد، مما يوجب الاعتراف بحقوق أصحاب البيانات على الاستدلالات ونتائجها وهو ما يؤدي للقول بضرورة الاعتراف بالاستدلالات كبيانات تثبت حقوقاً لأصحابها.

٣- يمكن تأييد رأينا أيضاً بربط الحق في الشخصية بالحق في الخصوصية[٢٥]، ويشير هذا الرابط إلى أنه، لكي يظل أصحاب البيانات متحكمين في هويتهم في مواجهة عدم اليقين الذي يمكن أن تمثله عمليات الاستدلال، فإنهم قد يغيرون سلوكهم (مثل الرقابة الذاتية) عند استخدام التقنيات الرقمية.

(24) Council of Europe, Case Law of the European Court of Human Rights Concerning the Protection of Personal Data, T-PD(2017)23 (2017), https://rm.coe.int/case-law-on-data-protection/1680766992 [https://perma.cc/H4F2-9WVZ].

(25) Alessandro Mantelero, Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework, 33 Comp. L. & Security Rev., 2017, p. 584.

المبحث الثاني

شروط صحة الاستدلالات وأساسها القانوني

تنتج عن عمليات الاستدلال الوصول لبيانات حساسة تم استنتاجها والاستدلال عليها من بيانات أخري قد تكون شخصية، أو غير شخصية، أو مجهولة المصدر.

وهنا يثار التساؤل حول مدى اعتبار البيانات غير الحساسة التي تم استخدامها كبيانات مدخلات في عمليات الاستدلال أنها بيانات حساسة إذا كانت البيانات التي تم الاستدلال عليها ذات طبيعة حساسة.

ونعرض من خلال هذا المبحث لأمرين هامين، نبين في أولهما شروط اعتبار البيانات المدخلة في عملية الاستدلال بيانات حساسة وهو ما نعرض له في المطلب الأول، ونعرض في المطلب الثاني الأساس القانوني لعملية الاستدلال على البيانات الحساسة.

ونبين ذلك فيما يلي:

المطلب الأول: شروط اعتبار البيانات المدخلة في عملية الاستدلال بيانات حساسة.

المطلب الثاني: الأساس القانوني للاستدلالات على البيانات الحساسة.

المطلب الأول

شروط اعتبار البيانات المدخلة في عملية الاستدلال بيانات حساسة

يمكن لعملية الاستدلال أن تؤدى للكشف عن معلومات حول سمات الفئة الحساسة للبيانات من خلال الربط والاستدلال عليها من بيانات أخري ليست حساسة في ذاتها.

وتطرح هذه الحقيقة تساؤلاً حول الشروط الواجب توافرها لإعادة تصنيف البيانات الشخصية غير الحساسة على أنها بيانات حساسة من خلال الاستدلالات.

ويجب لاعتبار البيانات غير الحساسة أنها بيانات حساسة وتصنفيها على هذا الأساس ضرورة توافر عدة شروط تتمثل فيما يلي: ضرورة توافر النية أو القصد لاستنتاج البيانات الحساسة، وتوافر شرط موثوقية البيانات التي يتم من خلالها استنتاج البيانات الحساسة، كما يجب التحقق من تقليل الأضرار المحتملة، بالإضافة لضرورة تحقق شرط التناسب.

ونعرض لتلك الشروط تباعاً.

أولاً: نية استنتاج البيانات الحساسة:

وفيما يتعلق بالنية أو القصد، فقد اتجه العديد من المعلقين القانونيين(٢٦) بأن تصنيف البيانات على أنها بيانات حساسة يجب أن يعتمد على الغرض المعلن من المعالجة.

(26) Alexander Nguyen, Videouberwachung Insensitiven Bereichen, 35 Datenschutz und Datensicherheit,2011, p. 715; Alexander Schiff, =

ويجب أن يكون لدى مراقبي البيانات نية استنتاج معلومات وبيانات حساسة من مجموعة مختارة من البيانات حتى يتم تصنيفها على أنها حساسة.

وعلى سبيل المثال إذا كان هناك مطعم يقوم بتوصيل الطعام للعملاء في مركز صحي، فلن تعتبر سجلات المعاملات التي يحتفظ بها المطعم أنها بيانات حساسة إلا إذا كان هذا المطعم ينوي استنتاج معلومات حول الحالة الصحية لعملائه من خلال استخدام الاستدلالات للوصول للبيانات الحساسة.

كما أنه يمكن من خلال الأسماء الأخيرة والموقع الجغرافي للميلاد - على الرغم من إمكانية الاعتماد عليها لاستنتاج العرق - لا تكون حساسة إلا إذا كان مراقب البيانات ينوي استنتاج العرق(٢٧).

وعلى ذلك فإن شرط توافر النية لدى مراقب البيانات هو أمر أساس لتصنيف البيانات على كونها حساسة، وإذا لم يتوافر النية أو القصد للاستدلال على البيانات الحساسة فلا يمكن تصنيفها على أنها حساسة.

وفي هذا السياق، اتجه البعض إلى حد القول بأن السمات الحساسة التي تم الكشف عنها بالصدفة بواسطة بيانات غير حساسة لا تتطلب إعادة تصنيف بيانات المصدر على

=

Besonderer Kategorien personenbezogener Daten, in Datenschutz-Grundverordnung, 2017, p. 20-21.

(27) Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a "Right to an Explanation' Is Probably Not the Remedy You Are Looking For, 16 Duke L. & Tech. Rev., 2017- 2018, p. 68.

أنها حساسة، مثل صورة دائرة تلفزيونية مغلقة تصور شخصًا يرتدي الملابس الدينية، والتي لم يتم التقاطها لتقييم المعتقدات الدينية للفرد[٢٨].

وينطبق الشيء نفسه على الصور التي تكشف عن الإعاقات أو الصور والتي يمكن استنتاج التوجهات الدينية وغيرها من البيانات الحساسة، ما لم يتم وضع الكاميرا عن قصد لاستخلاص بيانات حساسة على سبيل المثال، عند نقطة التقاء معروفة لمجموعة محمية معينة من البيانات[٢٩].

وفي المقابل، على الرغم من أن فرقة العمل المعنية بالمادة ٢٩من اللائحة الأوروبية لحماية البيانات لم تتناول القصد بشكل مباشر، فقد قدمت بعض المؤشرات على أن أنواعًا معينة من البيانات يمكن أن تكون حساسة دون معرفة كيفية معالجتها، حيث يُنظر إلى الصور وكاميرات المرور وأجهزة المراقبة الأخرى على أنها تثير مخاوف خاصة بشأن قدرتها على الكشف، عن طريق الصدفة أو غير ذلك، عن سمات حساسة مثل الأصل العرقي أو الحالة الصحية[٣٠].

(28) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494

(29) Alexander Nguyen, Videouberwachung Insensitiven Bereichen, 35 Datenschutz und Datensicherheit, 2011, p. 715.

(30) Article 29 Data Prot. Working Party, Advice Paper on Special Categories of Data ("Sensitive Data"), at 10, Ares (2011) 444105-20/04/2011 (2011), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011 /2011_04_20_letter_ artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [https://perma.cc/FV7G-VVS4].

وإذا لم تتوافر النية لاستخلاص البيانات الحساسة من البيانات الشخصية العادية أو أي بيانات أخرى، فلا يمكن تصنيف الأخيرة على أنها بيانات حساسة، بل يخضع التصنيف في هذه الحالة للبيانات الحساسة وفق القائمة المغلقة التي قرر المشرع فيها فئات البيانات الحساسة(٣١).

ثانياً: موثوقية الوسائل المستخدمة لاستنتاج البيانات الحساسة:

يشترط، كذلك، لإعادة تصنيف البيانات غير الحساسة على أنها بيانات حساسة أن تكون عملية الاستدلال عليها توفر أساسًا موثوقًا أو ذا دلالة إحصائية لاستنتاج معلومات حساسة(٣٢).

ويجب على مراقبي البيانات إثبات أن الأساليب التحليلية، والبيانات المستخدمة لاستخلاص الاستدلالات، بما في ذلك اتخاذ القرارات الآلية، أنها موثوقة، ويمكن التحقق من ذلك، على سبيل المثال، من خلال تقنيات التحقق الإحصائي(٣٣).

(31) Douwe Korff, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments 41 (European Comm'n Directorate-General Justice, Freedom and Security, Working Paper No. 2, 2010).

(32) Alexander Nguyen, Videouberwachung Insensitiven Bereichen, 35 Datenschutz und Datensicherheit, 2011, p.715.

(33) Wim Schreurs. Mireille Hildebrandt, Els Kindt & Michael Vanfleteren, Cogitas, Ergo Sum., The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector, in Profiling the European Citizen, 2008, p. 253.

وعلى سبيل المثال، لا يمكن اعتبار سجلات الحضور في الأحداث النقابية أن يكشف عن عضوية النقابات العمالية أو الآراء السياسية لأصحاب هذه البيانات على وجه اليقين، وبالتالي لا يجب تصنيفها على أنها بيانات حساسة في حد ذاتها.

ويتجه البعض إلى أن شرط الموثوقية الواجب توافره في عملية الاستدلالات على البيانات الحساسة لا يعنى أن تكون البيانات المستنتجة حساسة على وجه اليقين، بل يكفي أن تكون الاستدلالات من خلال الوسائل والأساليب المستخدمة فيها ذات دلالة كافية ومؤشر جيد على استنتاج البيانات الحساسة(٣٤).

ويؤكد ذلك أنه لا يمكن لأي من التطبيقات التي تستخدم في عمليات الاستدلالات أن تدعي أنها تولد استنتاجات أو تنبؤات على وجه اليقين المطلق، وفي العديد من الحالات، عانت من إخفاقات واضحة للغاية، حيث يتم أيضًا استخدام العديد منها فقط للإعلانات المستهدفة(٣٥).

ويعد تبرير هذه الاستخدامات المنتهكة للبيانات الشخصية أمرًا بالغ الأهمية من الناحيتين الأخلاقية والقانونية، لا سيما عندما يكون من الصعب التحقق من هذه الاستنتاجات، أو عندما لا يحصل الأفراد المتأثرون (أصحاب البيانات) على أي فائدة، وبالتالي، أصبح من الشائع على نحو متزايد نشر التحليلات الاستدلالية على نطاق واسع،

(34) Alexander Schiff, Besonderer Kategorien personenbezogener Daten, in Datenschutz-Grundverordnung, 2017, p. 20-21.

(35) David Lazer, Ryan Kennedy, Gary King & Alessandro Vespignani, The Parable of Google Flu: Traps in Big Data Analysis, 343 Science, 2014, p. 1203.

استنادا فقط إلى القدرة على القيام بذلك والدقة المتصورة للطريقة أو الاعتقاد بأن الكفاءة أو الإيرادات سوف تتحسن(٣٦).

وعلى ذلك، فإن الأساليب المستخدمة في الاستدلالات يجب أن تكشف بشكل موثوق عن معلومات حساسة حتى تعتبر بيانات حساسة، وذلك من خلال عملية استدلال تتمتع بالموثوقية والمصداقية حتى ولو لم تصل إلى حد عتبة اليقين.

وتتوافق الحاجة إلى إثبات الموثوقية مع حيثيات اللائحة العامة لحماية البيانات، والتي تقترح أنه من أجل ضمان معالجة عادلة وشفافة، يتم توجيه مراقبي البيانات للتحقق من الدقة الإحصائية لأنظمتهم، والتأكد من عدم الدقة في البيانات الشخصية، وإمكانية تصحيحها، ومنع الآثار التمييزية لعملية صنع القرار الآلي(٣٧).

(36) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494.

(37) Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 14,"In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade

=

وبالمثل، تدعو فرقة العمل المعنية بالمادة ٢٩ صراحةً إلى تنفيذ "المراجعة الخوارزمية" لتقييم "دقة وأهمية اتخاذ القرار الآلي بما في ذلك التوصيف "[٣٨].

ويتحمل مراقبو االبيانات، المسئولية القانونية الكاملة عن بيانات الإدخال، والتي يجب لتقرير هذه المسئولية إثبات أن البيانات المدخلة كانت "غير دقيقة أو غير ذات صلة، أو مأخوذة من سياقها"، أو تنتهك "التوقعات المعقولة لأصحاب البيانات " فيما يتعلق بالغرض الذي تم جمع البيانات من أجله[٣٩].

ثالثاً: التقليل من الأضرار المحتملة:

تظهر أهمية هذا الشرط ، بوجه خاص، في نطاق عمليات الاستدلالات عالية المخاطر، حيث يجب تقليل الأضرار المحتملة الناشئة عن عملية الاستدلالات عالية المخاطر.

ويقصد بالاستدلالات عالية المخاطر هي تلك الاستدلالات التي يتم استخلاصها من خلال تحليلات البيانات الضخمة، والتي يترتب عليها انتهاك الحق في الخصوصية، أو الإضرار بالسمعة، أو لديها احتمال كبير أن تكون كذلك في المستقبل، وكذلك

=

union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.".

(38) Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN, WP251rev.01, at 19 (Feb. 6, 2018), http://ec.europa.eu/newsroom/article29/ document.cfm?doc_id=49826

(39) Bart Custers, Simone van der Hof, Bart Schermer, Sandra Appleby-Arnold & Noellie Brockdorff, Informed Consent in Social Media Use - The Gap Between User Expectations and EU Personal Data Protection Law, 10 SCRIPTed 435, 2013, p. 445.

الاستدلالات التي تتمتع بإمكانية تحقق منخفضة بمعنى كونها تنبؤية أو مبنية على الرأي أثناء استخدامها لاتخاذ قرارات مهمة.

ونظراً لخطورة الاستدلالات عالية المخاطر بما لها من تأثير كبير على حقوق الأشخاص، فيمكن هنا الاستناد لمفهوم الآثار القانونية التي تؤثر على الأشخاص بشكل كبير، حيث يحق لصاحب البيانات عدم الموافقة على الخضوع لقرار يعتمد فقط على المعالجة الآلية، بما في ذلك التوصيف، مما ينتج عنه آثار قانونية تتعلق به أو تؤثر عليه بشكل كبير وفقاً لما قررته اللائحة العامة لحماية البيانات(٤٠).

وينطبق ذلك على القرارات المهمة وهي تلك التي لها مثل هذه "الآثار القانونية أو آثار ذات أهمية مماثلة" على الأشخاص، ومع ذلك، فإن هذه التأثيرات لا تقتصر على القرارات "الآلية فقط" كما هو الحال في اللائحة العامة لحماية البيانات، لأن المخاطر على الحياة الخاصة الناجمة عن استخدام استنتاجات غير طبيعية لا تعتمد فقط على مدى الأتمتة في عملية صنع القرار(٤١).

ويستثنى من ذلك كون القرار الآلي المستند للمعالجة يتخذ بسبب كونه (أ) ضروريًا لإبرام عقد أو تنفيذه بين صاحب البيانات ومراقب البيانات؛ (ب) مصرح به بموجب قانون الاتحاد أو قانون الدول الأعضاء الذي يخضع له المراقب والذي يضع

(40) GDPR, art. 22(1). Specifically, "automated decision-making" is defined as "a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

(41) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081.

أيضًا التدابير المناسبة لحماية حقوق وحريات صاحب البيانات ومصالحه المشروعة؛ أو (ج) يعتمد على موافقة صريحة من صاحب البيانات(٤٢).

كما تظهر أهمية هذا الشرط بالنظر لخصوصية الأضرار التي يمكن أن تحدث نتيجة هذه الاستدلالات، خاصة أنها تتعلق بإمكانية انتهاك الحق في الخصوصية أو الإضرار بالسمعة، أو أن هناك احتمال كبير أن تكون كذلك في المستقبل.

كما يمكن أن تقع هذه الأضرار بسبب كون هذه الاستدلالات تتمتع بإمكانية تحقق منخفضة بمعنى كونها تنبؤية أو مبنية على الرأي أثناء استخدامها لاتخاذ قرارات مهمة تؤثر على الأشخاص.

رابعاً: شرط التناسب:

يجب أن يكون هناك تناسباً بين المنفعة المتوقعة من عملية الاستدلال، والضرر الذي يلحق بالخصوصية أو السمعة أو الحقوق الأساسية لأصحاب البيانات المتأثرين بعمليات الاستدلالات.

ووفقاً لذلك، يجب أن تخضع عملية الاستدلال لاختبار فعال بشأن التناسب للمقبولية المعيارية، والذي بموجبه يجب أن يكون الضرر الذي يلحق بالخصوصية أو السمعة الناجم عن استخدام مصدر بيانات معين لاستخلاص الاستدلال متناسبا مع المنفعة أو المنفعة المتوقعة.

ولا يجب انفراد مراقبي البيانات بإجراء تقييمات التناسب والانتهاك المحتمل لمصدر البيانات وغرض المعالجة.

---

(42) GDPR, art. 22(2).

ولا شك أن شرط التناسب يتعلق بشكل أكثر دقة بتقييم تأثير حماية البيانات، المقررة بموجب اللائحة العامة لحماية البيانات، وذلك بهدف ضمان مستوى كافٍ من المراجعة الخارجية أو الحوكمة(٤٣).

وتقرر اللائحة العامة لحماية البيانات بالمادة (٣٥) أنه عندما تتم المعالجة من خلال استخدام التقنيات الجديدة، مثل البيانات الضخمة وتقنيات الذكاء الاصطناعي، ومع الأخذ في الاعتبار طبيعة ونطاق وسياق وأغراض المعالجة، وكان من المرجح أن يؤدي ذلك إلى خطر كبير على حقوق وحريات الأشخاص الطبيعيين، فيجب على المراقب، قبل المعالجة، إجراء تقييم لتأثير عمليات المعالجة المتوخاة على حماية البيانات الشخصية.

وفي هذا السياق يجب على المراقب طلب مشورة مسئول حماية البيانات، حيثما تم تعيينه، عند إجراء تقييم تأثير حماية البيانات.

ويجب إجراء تقييم تأثير حماية البيانات في حالة: (أ) تقييم منهجي وشامل للجوانب الشخصية المتعلقة بالأشخاص الطبيعيين يعتمد على المعالجة الآلية، بما في ذلك التوصيف، والذي يعتمد عليه أن تكون القرارات مبنية على آثار قانونية تتعلق بالشخص الطبيعي أو تؤثر بشكل كبير على الشخص الطبيعي.

(ب) المعالجة على نطاق واسع للفئات الخاصة من البيانات مثل البيانات الحساسة، وكذلك البيانات الشخصية المتعلقة بالإدانات الجنائية والجرائم.

وعلى ذلك، يجب هذه الشروط كنقطة انطلاق لتطبيق الحق في التوصل إلى استنتاجات واستدلالات معقولة، وهى شروط ضرورية لا غنى عنها، ويجب تحققها جميعاً.

---

(43) GDPR, art. 35.

وتعتبر الاستدلالات التي تستوفي الشروط السابقة مستوفية للحد الأدنى لممارسة "الحق في الاستدلالات المعقولة".

المطلب الثاني

الأساس القانوني للاستدلالات على البيانات الحساسة

بداية لا يستند الأساس القانوني بالضرورة لنص تشريعي صادر عن البرلمان، ولكن يمكن أن يكون من خلال السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي والمحكمة الأوروبية لحقوق الإنسان(٤٤)، والتي تشير هذه السوابق دائماً إلى أنه يجب أن يكون واضحًا ويمكن التنبؤ به ويمكن الوصول إليه.

ومع ذلك، يجب أن تشير التشريعات المنظمة لحماية البيانات على الأقل إلى الأهداف المتوخاة، وأغراض المعالجة، والبيانات ذات الطبيعة الشخصية التي تخضع للمعالجة، وإجراءات ضمان سلامة وسرية البيانات ذات الطابع الشخصي، والإجراءات المنصوص عليها لإتلافها، مما يوفر الضمانات الكافية ضد مخاطر الاستخدام التعسفي.

ويمكن أن نرجع عمليات الاستدلال على البيانات الحساسة من حيث أساسها القانوني الذي تقوم عليه للقواعد التشريعية المنظمة لحماية البيانات، وكذلك المبادئ القانونية والمشروعية لمعالجتها، بالإضافة للمصالح المشروعة للمتحكمين والتوقعات المعقولة لأصحاب البيانات، ونعرض لهذه الأمور تباعاً فيما يلي:

(44) Cour eur. D.H., 2 août 1984, Malone c. Royaume-Uni, série A, no 82, § 67 ; CJUE, 17 décembre 2015, WebMindLicenses, C-419/14, § 81.

أولاً: القواعد التشريعية المنظمة لحماية البيانات:

تقرر القواعد التشريعية المنظمة لحماية البيانات، أوروبياً ومصرياً، قيوداً على معالجة البيانات الحساسة بهدف توفير الحماية الملائمة لها.

حيث حظر المشرعين من حيث المبدأ جمع ونقل وتخزين ومعالجة وإتاحة البيانات الشخصية الحساسة إلا بتوافر الأمور الآتية: (١) الحصول أولاً على ترخيص من مركز حماية البيانات الشخصية على ذلك، (٢) الحصول مسبقاً على موافقة كتابية من الشخص المعنى بتلك البيانات، (٣) توافر حالة من الحالات المرخص فيها بمعالجة البيانات الحساسة وحينئذ لا تتطلب موافقة الشخص المعني[٤٥].

ويلاحظ على ذلك أن كل العمليات المتعلقة بالبيانات الشخصية الحساسة بما فيها عمليات الاستدلال عليها إنما تستند للقواعد التشريعية المنظمة لحماية البيانات، وإن كان الأمر في هذا الصدد فيما يتعلق بضرورة استيفاء القيود القانونية إنما يتعلق بكون البيانات المدخلة في عمليات الاستدلال بأنها بيانات شخصية حساسة، دون أن يتطرق المشرع لامكانية استخدام عمليات الاستدلالات بيانات شخصية عادية، أو كذلك بيانات عادية وليست من طبيعة شخصية، أو كذلك البيانات مجهولة المصدر، والتي يمكن أن يترتب عليها جميعاً استنتاجات بشأن البيانات ذات الطبيعة الحساسة.

ونوصي في هذا الصدد، وبهدف تقرير وتفعيل الحماية الهادفة للبيانات الحساسة، أن ينص المشرع المصري على ضرورة خضوع كل البيانات (الشخصية، الحساسة، العادية، ومجهولة المصدر) للقيود المقررة لعمليات جمع ونقل وتخزين ومعالجة وإتاحة

(٤٥)المادة (١٢) من القانون المصري رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

البيانات الحساسة، طالما كانت عمليات الاستدلال منها تؤدى لاستنتاجات بشأن البيانات ذات الطبيعة الحساسة، مما مؤداه-وقتها- بتمتعها بذات الطبيعة.

أولاً: احترام المبادئ الأساسية لحماية البيانات:

تحدد المادة الخامسة من اللائحة العامة لحماية البيانات جميع المبادئ الأساسية لحماية البيانات، وتتمثل فيما يلي: مبادئ الشرعية والولاء والشفافية الذي سيتخذ شكل التزامات على عاتق الأشخاص المعنيين؛ تقييد الأغراض؛ التقليل من البيانات؛ الدقة ; الحد من الاحتفاظ بالبيانات، النزاهة والسرية؛ والمسئولية(٤٦).

لذلك، لكي تكون المعالجة قانونية ومقبولة بموجب اللائحة العامة لحماية البيانات، يجب أن تحترم معالجة البيانات التي يتم إجراؤها هذه المبادئ الأساسية ، كما يجب أن تكون معالجة البيانات ذات الطبيعة الشخصية قانونية وعادلة وشفافة، ويجب أن تسعى إلى تحقيق غرض محدد وصريح وشرعي، ويجب أن تضمن أمان البيانات.

بالإضافة إلى ذلك، يجب أن تقتصر المعالجة فقط على البيانات ذات الصلة بالغرض المقصود، وعلى ما هو ضروري، والتي تقدم صفات الدقة والتحديث، ويتم الاحتفاظ بها لمدة لا تتجاوز ما هو ضروري لتحقيق الغرض.

ويكمن حجر الزاوية في نظام حماية البيانات الشخصية في مبدأ تحديد الغرض من جمع البيانات الشخصية بصفة عامة، والبيانات الحساسة بصفة خاصة، والاحتفاظ بها ومعالجتها(٤٧).

(46) GDPR, art. 5.

(47) Groupe 29, Avis 03/2013 sur la limitation des finalités, 3 avril 2013.

وتبدو القواعد الحالية في المادة الخامسة من اللائحة العامة الأوروبية حول العدالة، وتحديد الغرض، والدقة، وتقليل البيانات (بما في ذلك مدى ملامتها للغرض المنشود) مناسبة للوهلة الأولى، ولكنها تبدو غير كافية[٤٨].

(48) GDPR,, Article 5, "1.Personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation'); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation'); (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy'); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation'); (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). 2.The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

ووفقاً لهذه المادة يجب أن تتم معالجة البيانات الشخصية بشكل قانوني وعادل، وبطريقة شفافة فيما يتعلق بصاحب البيانات (الشرعية والإنصاف والشفافية)؛ كما يجب أن يتم جمعها لأغراض محددة وصريحة ومشروعة، ولم يتم معالجتها بطريقة لا تتوافق مع تلك الأغراض.

كما تؤكد على مبدأ تقليل البيانات بضرورة الاقتصار على البيانات الكافية، وذات صلة ومحدودة بما هو ضروري فيما يتعلق بالأغراض التي تتم معالجتها من أجلها.

كما يجب أن تكون البيانات دقيقة وحديثة عند الضرورة؛ ويجب اتخاذ كل خطوة معقولة لضمان مسح أو تصحيح البيانات الشخصية غير الدقيقة، مع مراعاة الأغراض التي تتم معالجتها من أجلها، ودون تأخير وهو ما يعرف بمبدأ الدقة.

كما يتم الاحتفاظ بها في نموذج يسمح بتحديد أصحاب البيانات لمدة لا تزيد عن ما هو ضروري للأغراض التي تتم معالجة البيانات الشخصية من أجلها.

كما يجب تنفيذ الإجراءات الفنية والتنظيمية المناسبة واتخاذ التدابير التي تتطلبها اللائحة العامة من أجل حماية حقوق وحريات صاحب البيانات ("قيود التخزين")؛ وأن تتم معالجتها بطريقة تضمن الأمان المناسب للبيانات الشخصية، بما في ذلك الحماية من المعالجة غير المصرح بها أو غير القانونية وضد الفقدان العرضي أو التدمير أو الضرر، وذلك من خلال استخدام التدابير الفنية أو التنظيمية المناسبة (النزاهة والسرية).

كما تقرر الفقرة الثانية من المادة الخامسة مبدأ مسئولية مراقب البيانات ومدى امتثاله والتزامه بما ورد بها من أحكام، ويقع عليه عبء إثبات قيامه بتنفيذ الشروط والضوابط والإجراءات.

كما يرتبط بذلك أيضاً واجب الولاء والشفافية والذي يقتضي ضرورة جمع البيانات مباشرة من الأشخاص المعنيين، وليس بشكل غير مباشر من مصادر خارجية(٤٩).

وهذا هو الحال في سياق علاقات قانون العمل، خاصة أثناء إجراءات تعيين العمال(٥٠).

وفي مجال البيانات الصحية والطبية يجب –من حيث المبدأ- جمعها من الشخص المعني، ولا يجوز جمعها من مصادر أخري إلا في حالة الضرورة لتحقيق غرض المعالجة أو أن صاحب البيانات غير قادر على تقديم البيانات(٥١).

وكما يشير البعض أن هناك عنصراً مسبقاً يجب على مراقبي البيانات استيفائه قبل الشروع في عملية الاستدلالات، ويتمثل في بيان مدى معقولية عملية الاستدلالات من خلال بيان ما يلي(٥٢):

١- سبب اعتبار بعض البيانات أساسًا مقبولًا من الناحية المعيارية لاستخلاص الاستنتاجات.

(49) V. Verbruggen, Les Codes commentés. La protection des données, Bruxelles, Larcier, 2011, p. 55 et 56.

(50) Recommandation no CM/Rec(2015)5 du 1er avril 2015 du Comité des ministres du Conseil de l'Europe sur le traitement des données à caractère personnel dans le cadre de l'emploi, pt 5.1.

(51) V. Verbruggen, Les Codes commentés. La protection des données, Bruxelles, Larcier, 2011, p. 55.

(52) Janneke Gerards, The Discrimination Grounds of Article 14 of the European Convention on Human Rights, 13 Hum. Rts. L. Rev. 99, 2013, p. 114-115.

٢- سبب كون هذه الاستنتاجات مقبولة من الناحية المعيارية، وذات صلة لغرض المعالجة المختار أو نوع القرار الآلي.

٣- بيان ما إذا كانت البيانات والأساليب المستخدمة لاستخلاص الاستدلالات دقيقة وموثوقة إحصائياً.

ينبغي سن هذه المتطلبات من خلال تقديم متطلبات التحقق والإخطار الملزمة قانونًا والتي يجب أن يستوفيها مراقبو البيانات قبل نشر التحليلات الاستدلالية عالية المخاطر على نطاق واسع.

وكما يشير البعض إلى أنه سيتم تعزيز التبرير المسبق من خلال آلية لاحقة إضافية تمكن من تحدي الاستنتاجات غير المعقولة، مع الأخذ في الاعتبار التوفيق بين الحق في الحصول على استنتاجات معقولة وموازنته مع قانون الملكية الفكرية والحقوق الأساسية للأفراد(٥٣).

ثانياً: المصالح المشروعة والتوقعات المعقولة:

تقرر حيثيات اللائحة العامة لحماية البيانات(٥٤) معيار المصالح المشروعة لمعالجة البيانات كأساس قانوني للمعالجة، بشرط ألا تؤثر على مصالح وحقوق وحريات صاحب البيانات الأساسية.

كما يجب أن يؤخذ في الاعتبار التوقعات المعقولة لأصحاب البيانات بناءً على علاقتهم مع المراقب أو المتحكم في البيانات.

(53) Joris van Hoboken, Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines, 2012, p. 316-332.

(54) GDPR ,Whereas (47).

وتبين حيثيات اللائحة العامة أنه قد توجد مثل هذه المصلحة المشروعة، على سبيل المثال، عندما تكون هناك علاقة ذات صلة ومناسبة بين صاحب البيانات ووحدة التحكم في حالات معينة، مثل عندما يكون صاحب البيانات عميلاً لدى وحدة التحكم.

وعلى أية حال، فإن وجود مصلحة مشروعة سيحتاج إلى تقييم دقيق بما في ذلك ما إذا كان صاحب البيانات يمكن أن يتوقع بشكل معقول في ذلك الوقت وفي سياق جمع البيانات الشخصية التي قد تتم معالجتها لهذا الغرض، وهذا ما أكد عليه المجلس الأوروبي لحماية البيانات (EDPB) أن العدالة تتعلق بالتوقعات المعقولة لأصحاب البيانات فيما يتعلق بالأضرار والعواقب المحتملة(٥٥).

ويمكن أن تتجاوز المصالح والحقوق الأساسية لصاحب البيانات مصلحة مراقب البيانات، حيث تتم معالجة البيانات الحساسة في ظروف لا يتوقع فيها أصحاب البيانات بشكل معقول مزيدًا من المعالجة.

كما يمكن اعتبار معالجة البيانات لأغراض التسويق المباشر على أنها تتم لمصلحة مشروعة.

ومع ذلك، حتى لو تم إتباع معيار التوقعات المعقولة لصاحب البيانات، فإن هذه التوقعات ليست مبررًا كافيًا أو معياريًا، فحقيقة أن شيئًا ما أصبح طبيعيًا أو شائعًا لا تعني بالضرورة أنه أصبح أمراً مبرراً أو مرغوب فيه اجتماعيًا(٥٦).

(55) European Data Prot. Bd., The European Data Protection Board, Endorsement 1/2018 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files /files/news /endorsement_of_ wp29_documents.pdf [https://perma.cc/8H9A-RQR3].

(56) Daniel J. Solove, The Limitations of Privacy Rights, 98 NOTRE DAME L. REV., 2023, p. 975 .

ومن الجدير بالذكر أن هذه الأحكام لم تثبت فعاليتها نظرًا لوجود أغراض غامضة وواسعة يتم ذكرها في الشروط والأحكام التي تحكم جمع البيانات ومعالجتها.

ومن الأمثلة على ذلك الشكاوى المقدمة المتعلقة بالموافقة القسرية، حيث توضح اللائحة العامة لحماية البيانات أنه لا يمكن اعتبار الموافقة مقدمة بحرية إلا إذا كانت البيانات المطلوبة تقتصر على ما هو ضروري لتقديم الخدمة[٥٧].

فإذا كان يجب إعطاء الموافقة لجمع ومعالجة البيانات بما يتجاوز ما هو ضروري تمامًا لتقديم الخدمة كشرط أساسي لاستخدام الخدمة، فلا يمكن اعتبار الموافقة في هذه الحالة ممنوحة بحرية.

ويلاحظ هنا أن تحديد الغرض من المعالجة ومبدأ الدقة، وتقليل البيانات (بما في ذلك مدى ملاءمتها للغرض المنشود) يبدو أنها تنطبق فقط على البيانات المدخلة، دون الإشارة لنتائج المعالجة والاستدلالات بما قد تسفر عنه من نتائج بالغة الخطورة على حقوق أصحاب البيانات.

وعلى ذلك، فإن التفسير الواقعي للمبادئ التي قررتها اللائحة العامة لحماية البيانات وكذلك قانون حماية البيانات الشخصية المصري إنما يُنظر إليها على أنها أداة شفافية للمعالجة، وليست آلية تبرير كأساس للاستدلالات المعقولة، وينتج عن ذلك[٥٨]:

(57) GDPR , Article 7, "4-When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

(58) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081.

١- يترك لمراقبي البيانات أو المتحكمين سلطة تقرير وتحديد غرض البيانات المجمعة وأهميتها بشأن عمليات المعالجة والاستدلالات.

٢- فتح مجال الاجتهاد بشأن الحق في الحصول على استنتاجات معقولة، ومدى اعتبار ما إذا كانت ممارسات المعالجة مقبولة من الناحية المعيارية.

٣- تقرير المساواة بين الحق في الحصول على استنتاجات معقولة مع الاستنتاجات التي يستخلصها مراقب البيانات، وكذلك الاستنتاجات الواردة من طرف ثالث والتي يمكن إعادة توظيفها لاحقًا.

ومن الجدير بالذكر هنا أن معيار المصالح المشروعة لمراقب البيانات أو المتحكم لم يعد من الأغراض القانونية والمشروعة لمعالجة البيانات الحساسة، وعلى ذلك، فإن الفارق الرئيس بين إمكانية معالجة كلاً من البيانات الشخصية والبيانات الحساسة- وفقاً للائحة العامة الأوروبية لحماية البيانات الشخصية- هو أنه لا يمكن استخدام أساس المصالح المشروعة كأساس قانوني لمعالجة البيانات الحساسة وفقاً للائحة الأوروبية العامة لحماية البيانات.

ويبرر ذلك بهدف تقرير حماية فاعلة وموسعة للبيانات الحساسة، حيث أنه في حالة تقرير غرض المصالح المشروعة لمعالجة البيانات الحساسة فانه يمكن استخدامه بشكل متكرر لمعالجة البيانات دون موافقة صاحب البيانات، مما يقوض معه حماية هذا النوع من البيانات.

المبحث الثالث

الاستدلال على البيانات الحساسة في عصر البيانات الضخمة وتأثيرها على الحقوق الأساسية للأفراد

بموجب التمييز القائم في تشريعات حماية البيانات بين البيانات الشخصية والحساسة والانتقادات التي وجهت إلى هذا التمييز من حيث المعيار الذي تم الاعتماد عليه، إلا أن مستوى الحماية المقرر للبيانات الحساسة وهي حماية مشددة يجب أن يكون محل اعتبار واهتمام بالغين في ظل عمليات الاستدلالات على هذا النوع تحديداً من البيانات في عصر تكنولوجيا الذكاء الاصطناعي والبيانات الضخمة.

ولا شك أن عمليات الاستدلال على البيانات الحساسة في ظل التقنيات التكنولوجية المتطورة وعالية الخطورة لها تأثيراتها البالغة على الحقوق الأساسية للأفراد.

ونعرض من خلال هذا المبحث لعمليات الاستدلال على البيانات الحساسة في عصر البيانات الضخمة وهو ما نوضحه في المطلب الأول، ثم نبين لتأثير هذه الاستدلالات على الحقوق الأساسية للأفراد وهو ما نعرض له في المطلب الثاني، ومدى ملائمة القواعد التشريعية الحالية لحماية البيانات لتحقيق أهدافها في ضوء التكنولوجيا المتطورة.

المطلب الأول: دور الاستدلالات في عصر البيانات الضخمة

المطلب الثاني: تأثير الاستدلالات على الحقوق الأساسية

المطلب الثالث: مدى ملائمة قواعد حماية البيانات لتحقيق أهدافها في عصر البيانات الضخمة

المطلب الأول

دور الاستدلالات في عصر البيانات الضخمة

تكمن الخطورة في عصر الذكاء الاصطناعي واستخدام تقنياته المتعددة في الاستدلال على البيانات الشخصية والحساسة أنه من المؤكد أن حماية البيانات الحساسة، واحترام الحق في الخصوصية، وعدم الكشف عن الهوية، لا يمكن أن يصمد أمام التحليل الضخم والمتقاطع لكميات البيانات الضخمة، وهى أمور تم طرحها من قبل المتخصصون في مجال التكنولوجيا(٥٩).

وتستخدم البيانات الضخمة مجموعة كبيرة من الخوارزميات المعقدة لتحليل البيانات، والتي يعتمد الكثير منها على التعلم الآلي، حيث تتطور مع تغذيتها بكميات متزايدة من البيانات(٦٠)، حيث يمكن بسهولة استخلاص استنتاجات حول البيانات الحساسة من بيانات غير حساسة(٦١).

(59) S. Mascetti, A. Montreale, A. Ricci et A. Gerino, « Anonymity : a comparison between the legal and computer science perspective », in S. Gutwirth et al. (eds), European Data Protection Coming of Age, Springer, 2013, pp. 85

(60) CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY, 2016, p. 75-77.

(61) Hideyuki Matsumi, Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?, 48 CUMB. L. REV., 2017, p. 149, 150.

وتستخلص تحليلات البيانات الضخمة والذكاء الاصطناعي ("AI") استنتاجات وتنبؤات غير بديهية وغير قابلة للتحقق حول سلوكيات الأفراد وتفضيلاتهم وحياتهم الخاصة، وتعتمد هذه الاستنتاجات على بيانات متنوعة للغاية، وغنية بالميزات ذات قيمة لا يمكن التنبؤ بها، بل تخلق فرصًا جديدة لعمليات التوصيف واتخاذ القرارات التمييزية والمتحيزة والمتعدية على الحق في الخصوصية(٦٢).

وعلى ذلك، وبفضل عمليات الاستدلالات في عصر البيانات الضخمة يمكن الاستدلال على العديد من البيانات الشخصية الحساسة من خلال بيانات عادية للغاية، فيمكن استنتاج العرق من المكان الذي يعيش فيه الشخص، ويمكن استنتاج الدين من الموقع أو أنماط الأكل، ويمكن استنتاج المعتقدات الفلسفية من عادات القراءة، ويمكن استنتاج المعتقدات السياسية من أي شيء تقريبًا، حيث يتم تسييس مجموعة متزايدة من القضايا والسلوكيات في ظل ما يعرف "اقتصاد الاستدلال"(٦٣).

كما يمكن استنتاج العرق والانتماء العرقي من العديد من أنواع البيانات الشخصية الأخرى، مثل الموقع والصور، وعلى سبيل المثال، تمكن مكتب الحماية المالية للمستهلك

(62) Brent Daniel Mittelstadt, Patrick Allo, Mariarosaria Taddeo, Sandra Wachter & Luciano Floridi, The Ethics of Algorithms: Mapping the Debate, Big Data & Soc'y, July-Dec. 2016, at 1-2.

(63) يعرف "اقتصاد الاستدلال" بأنه "اقتصاد تستخدم فيه المؤسسات البيانات المتاحة التي تم جمعها من الأفراد لتوليد مزيد من المعلومات حول هؤلاء الأفراد والأشخاص الآخرين". (Alicia Solow-Niederman, Information Privacy and the Inference Economy, 117 NW. U. L. REV., 2022, p. 357, 361.)

في أمريكا (CFPB) من استنتاج العرق والانتماء العرقي من خلال مجموعة من المعلومات الجغرافية واللقب في طلبات الرهن العقاري[٦٤].

وتشير العديد من الدراسات إلى أن البشر أقل قدرة من أجهزة الكمبيوتر على التوصل إلى استنتاجات من البيانات غير الحساسة، وهذا يكشف عن مشكلة مثيرة للقلق لدى البشر، حيث لا يمكنهم رؤية ما يمكن أن تستنتجه الخوارزميات، وقامت العديد من الدراسات التي تتضمن الخوارزميات بفحص مدى قدرة البشر على التوصل إلى استنتاجات بناءً على نفس البيانات التي يتم تغذيتها للآلات، وكشفت الدراسات أن أجهزة الكمبيوتر أكثر دقة وغالباً بفارق كبير[٦٥].

كما كشفت دراسة أخرى أن أجهزة الكمبيوتر كانت أكثر قدرة من البشر على إجراء تقييمات لشخصيات الأفراد، كما أن الأحكام الشخصية المستندة إلى الكمبيوتر أفضل في التنبؤ بنتائج الحياة والسمات السلوكية الأخرى ذات الصلة من الأحكام البشرية[٦٦].

(64) CONSUMER FIN PROT. BUREAU, USING PUBLICLY AVAILABLE INFORMATION TO PROXY FOR UNIDENTIFIED RACE & ETHNICITY: A METHODOLOGY & ASSESSMENT 3 (2014), https://files.consumerfinance.gov/f/ 201409 _cfpb_report_proxy-methodology.pdf [https://perma.cc/5CY4-NK3L].

(65) Hammaad Adam, Ming Ying Yang, Kenrick Cato, Ioana Baldini, Charles Santeio, Leo Anthony Celi, Jiaming Zeng, Moninder Singh & Marzyeh Ghassemi, Write It Like You See It: Detectable Differences in Clinical Notes by Race Lead to Differential Model Recommendations, PROC. AAAI/ACM CONF. ON AI, ETHICS, & SOC., 2022, p. 14.

(66) Wu Youyou, Michal Kosinski & David Stillwell, Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans, 112 PNAS, 2015, p. 1036.

وأظهرت تطبيقات عديدة لتحليلات البيانات الضخمة لاستخلاص استنتاجات مثيرة للقلق بشأن الأفراد والجماعات[٦٧]، وعلى سبيل المثال تقف منصات الإنترنت الرئيسية وراء العديد من الأمثلة ذات أعلى الملفات الشخصية، وقد يكون Face book قادرًا على استنتاج العديد من البيانات الشخصية الحساسة من خلال نمط السلوك عبر الإنترنت[٦٨].

ولا شك أن هذه الاستدلالات تثير العديد من المخاوف بشأن المساءلة الخوارزمية، وغالباً ما تكون في الواقع مخاوف بشأن الطريقة التي ترسم بها هذه التقنيات استنتاجات تنتهك الخصوصية ولا يمكن التحقق منها والتي لا يمكن التنبؤ بها أو فهمها أو دحضها.

وفي عصر ما يسمى " بالبيانات الضخمة" وتكنولوجيات الذكاء الاصطناعي يمكن أن تقوض البيانات الضخمة التمييز الكامل بين فئات البيانات المختلفة: الشخصية والحساسة[٦٩].

(67) Christopher Kuner, Fred H. Cate, Christopher Millard & Dan Jerker B. Svantesson, The Challenge of "Big Data" for Data Protection, 2 Int'l Data Privacy L., 2012, p. 47.

(68) Jose Gonzalez Cabanas, Angel Cuevas & Ruben Cuevas, Facebook Use of Sensitive Data for Advertising in Europe (Feb. 14, 2018) (unpublished manuscript), https://arxiv.org/abs/1802.05030 [https://perma. cc/V2C8-FY3W].

(69) Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV., 2017, p. 995, 1013.

كما أنه مع الزيادات التي لا تنتهي في قوة الحوسبة والسهولة المتزايدة للمشاركة، والجمع بين مجموعات البيانات المتباينة، يمكن القول إن المزيد والمزيد من البيانات أصبحت ذات طبيعة حساسة(٧٠).

ويلاحظ هنا أن العديد من تقنيات البيانات الضخمة تركز على استخلاص استنتاجات دقيقة حول الأشخاص من البيانات، ومع تزايد هذه التقنيات، قد تتمكن من توسيع نطاق استخدام واتساع فئات المعلومات الحساسة الاستدلالية(٧١).

وتظهر العديد من الأبحاث مدى سهولة ودقة الخوارزميات في التوصل إلى استنتاجات حول البيانات الحساسة من البيانات غير الحساسة، وفي دراسات كثيرة حول الاستدلالات وجد أن السمات القابلة للاستدلال تشمل الجنس، والعمر، والسياسة، والموقع، والمهنة، والعرق، والأسرة والعلاقات، والتعليم، والدخل، والصحة، والدين، والطبقة الاجتماعية(٧٢).

كما أن عمليات الاستدلالات لم تعد قاصرة –كما سبق ذكره- على البيانات الشخصية والاستدلال من خلالها على بيانات حساسة، بل اتسع الأمر ليشمل كذلك البيانات مجهولة المصدر والتي لا تحتوى على عنصر واضح ومحدد للهوية الشخصية.

(70) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1591.

(71) Paul Ohm, Sensitive Information, 88 S. CAL. L. REV., 2015, p. 1125, 1170.

(72) Joanne Hinds & Adam N. Joinson, What Demographic Attributes Do Our Digital Footprints Reveal? A Systematic Review, 13 PLOS ONE, 28 Nov.,2018, at 1, 5.

ويشير المتخصصون في مجال التكنولوجيا أن التقاطع اللانهائي لعدد متزايد من البيانات "المجهولة"، وهو التقاطع الذي أصبح ممكنًا بفضل القدرات الأساسية لأنظمة المعلومات، يجعل من الممكن إزالة إخفاء هوية البيانات.

كما تعمل البيانات المجهولة، جنبًا إلى جنب، مع البيانات ذات الطبيعة الشخصية، ويمكن أن تؤدي، في عمليات التوصيف، ليس فقط إلى التمييز والتحديد الفردي، بل إلى التمييز الجماعي أيضاً.

وبالتالي، إذا تم استخدام بيانات مجهولة المصدر، مثل متوسط دخل سكان منطقة جغرافية معينة، أو متوسط مستوى تعليمهم في الخوارزميات المستخدمة في الاستدلالات، فيمكن من خلال عملية الاستدلال تحديد ملف تعريف المشترين المحتملين لمثل هذه البيانات أو مثل هذه العلامة التجارية أو نوع السيارة، ولا يمكننا أن نعتبر أن هذه البيانات، مجهولة المصدر بطبيعتها، حيث تصبح "ذات طابع شخصي" من خلال الاستخدام، أي من خلال دمجها في تعريف الملف الشخصي، ويجب أن تكون خاضعة لتنظيم حماية البيانات.

وهذا ما وضحه وأكد عليه التقرير التوضيحي لمجلس أوروبا، حيث يشير هذا التقرير إلى أن البيانات مجهولة المصدر لا تكون مصحوبة بعنصر واضح لتحديد الهوية، ولكن مع ذلك في بعض الحالات (لا تتطلب وقتًا أو أنشطة أو موارد غير معقولة) تسمح بتحديد هوية الشخص، وهذا هو الحال بشكل خاص عند الجمع بين أنواع مختلفة من البيانات، مثل البيانات الجسدية أو الفسيولوجية أو الجينية أو الاقتصادية أو الاجتماعية (مزيج من البيانات المتعلقة بالعمر والجنس والنشاط المهني والموقع الجغرافي والحالة العائلية، وما إلى ذلك)، يسمح لمراقب البيانات، بتحديد صاحب

البيانات، وفي مثل هذه الحالة، لا يمكن اعتبار البيانات مجهولة المصدر ويجب مشمولة بأحكام الاتفاقية(٧٣).

وفي هذا الصدد، فإنه يجب إعادة النظر في المعيار المحدد لطبيعة البيانات، حيث يجب الابتعاد والتخلي عن فكرة قوائم البيانات الحساسة بشكل حصري، والاعتماد بدلاً من ذلك على النهج القائم على اعتبار البيانات الشخصية هي أي بيانات يمكن بطبيعتها أو عن طريق الاستخدام بشكل أو بآخر مثل الاستدلالات تشير إلى تحديد شخص ما من خلال إضفاء طابع فردي عليها، كما يجب اعتبار أي بيانات تؤدى من خلال الاستدلالات إلى التوصل لبيانات حساسة اعتبارها كذلك حساسة في سياق الغرض الذي تم استخدامها من خلاله.

وعلى ذلك، تم انتقاد تحديد فئات البيانات الشخصية الحساسة في لائحة الاتحاد الأوروبي وكذلك التشريعات المختلفة، من خلال مصطلحات عامة وواسعة ومرتبطة دائماً بطبيعة البيانات ذات الطبيعة الشخصية.

(73) le rapport explicatif du Conseil de l'Europe (p. 10, no 19) qui note très justement : « Des données en apparence anonymes, car non assorties d'un élément d'identification évident, peuvent néanmoins, dans certains cas (ne nécessitant pas des délais, activités ou ressources déraisonnables) permettre l'identification d'une personne. C'est notamment le cas lorsque la combinaison de différents types de données, telles des données physiques, physiologiques, génétiques, économiques ou sociales (combinaison de données relatives à l'âge, le sexe, l'activité professionnelle, la géolocalisation, la situation de famille, etc.), permet au responsable du traitement, ou à toute autre personne, d'identifier la personne concernée. Dans pareille situation, les données ne sauraient être considérées comme anonymes et sont couvertes par les dispositions de la Convention ».

وفي ظل عصر البيانات الضخمة وما يعرف بالتعلم العميق وأنظمة الذكاء الاصطناعي سيصبح، وبلا شك، التمييز الذي تقوم عليه تشريعات حماية البيانات بشأن حماية البيانات ذات الطبيعة الشخصية في مقابل البيانات ذات الطبيعة غير الشخصية لن يكون له معنى مستقبلاً(٧٤).

كما تكمن خطورة الأمر في أنه من خلال عملية الاستدلال يمكن لجميع البيانات الشخصية العادية تقريبًا، سواء منفردة أو مجتمعة، أن تؤدي إلى استنتاجات حول البيانات الحساسة، توضح الأبحاث بشكل مستمر، وبشكل قاطع، مدى سهولة التوصل إلى استنتاجات حول البيانات الحساسة.

ومع تطور الخوارزميات واستهلاكها لكميات أكبر من البيانات، ستكون قادرة على التوصل إلى المزيد من الاستدلالات حول استنتاجات البيانات الحساسة التي تكون غير متوقعة تمامًا ويصعب توقعها.

وغالبًا ما تتغاضى القوانين المتعلقة بحماية البيانات عن هذه المشكلة، لكن هذا ليس خللًا بسيطًا يجب تعديله، بل هي صعوبة تجعل نهج البيانات الحساسة معقدًا للغاية وغير قابل للتطبيق بشكل أساسي(٧٥).

(74) A. Rouvroy, L'homo juridicus est-il soluble dans les données ? », D.,2019, p. 428.

(75) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081.

المطلب الثاني

تأثير الاستدلالات على الحقوق الأساسية

تظهر عمليات الاستدلال على البيانات الشخصية، وما يمكن أن تتوصل إليه من بيانات حساسة تأثير بالغ الخطورة على الحقوق الأساسية للأفراد، يستوي في ذلك تأثيرها على الحقوق المدنية المتعلقة بنتائج الاستدلالات (البيانات المستنتجة)، أو كذلك تأثيرها على حقوق الأشخاص من حيث القرارات التي يتم اتخاذها استناداً لنتائج الاستدلالات، مثل الحق في العمل، أو الحصول على قرض، أو الاشتراك في عملية تأمين، وغيرها.

وتم الاعتراف منذ فترة طويلة بالإشكالات بين التوصيف والتمييز والخصوصية وقانون حماية البيانات(٧٦)، ومع ذلك تظهر خطورة الأمر بالنسبة للاستدلالات خاصة في عصر البيانات الضخمة واستخدام التقنيات التكنولوجية الحديثة في هذه العمليات.

وفي هذا الصدد، وكما يشير البعض أن مصطلح "حماية البيانات" مضلل، لأنه يوحي بأن القوانين تهدف إلى حماية البيانات، في حين أن المقصود في الواقع هو حماية الأشخاص أصحاب تلك البيانات(٧٧).

(76) Viktor Mayer-Schonberger, Delete: The Virtue of Forgetting in the Digital Age, 2009.& Brent Daniel Mittelstadt & Luciano Floridi, The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, 22 Sci. & Engineering Ethics, 2016, p. 303.

(77) Mireille Hildebrandt, Profiling: From Data to Knowledge, 30 Datenschutz und Datensicherheit, 2006, p. 548.

ومما يؤكد هذا الأمر، أن حماية الخصوصية والبيانات يُنظر إليها تقليديًا على أنها حقوق فردية في الاتحاد الأوروبي(٧٨).

وانطلاقًا من الحق في الخصوصية والذي يقوم على فكرة أنه يجب أن يكون للفرد الحق في أن تتركه الدولة بمفرده، فقد تم اقتراح الحق في الخصوصية في الأصل كآلية دفاع ضد المراقبة الحكومية(٧٩).

وتشكل عملية صنع القرار الآلي، والتوصيف، وتقنيات التعلم الآلي ذات الصلة فرصًا جديدة لاتخاذ قرارات تنتهك الحق في الخصوصية، والقيام بممارسات تمييزية ومتحيزة بناءً على التحليلات الاستدلالية(٨٠).

وفي مجال عمليات الاستدلال، يأخذ القرار الآلي صدى مختلفًا تمامًا في سياق البيانات الضخمة والتوصيف لأسباب تجارية أو أمنية، بالإضافة إلى ذلك، يتم اتخاذ احتياطات جديدة من خلال منح صاحب البيانات الحق في الحصول على تدخل بشري من جانب المراقب، وكذلك الحق في التعبير عن وجهة نظره والاعتراض على القرار، وهذا

(78) Alessandro Mantelero & Giuseppe Vaciago, Data Protection in a Big Data Society. Ideas for a Future Regulation, 15 Digital Investigation, 2015, p. 104.

(79) Alessandro Mantelero, Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection, 32 Computer L. & Security Rev., 2016, p. 238.

(80) Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev., 2016, p. 671.

هو في الواقع الحد الأدنى المطلوب للأمل في مكافحة الاستخدام المفرط، وحتى المنحرف، للخوارزميات التنبؤية(٨١).

وتتمتع تحليلات البيانات الحديثة بإمكانية الوصول إلى كميات غير مسبوقة وأنواع مختلفة من البيانات المرتبطة بتقييم سلوكيات الأفراد وتفضيلاتهم وحياتهم الخاصة(٨٢).

ويتنوع نطاق الضحايا المحتملين لهذه الأضرار من خلال التركيز في تحليلات البيانات الحديثة على إيجاد روابط صغيرة ولكن ذات معنى بين الأفراد(٨٣)، بل قد يتسع الأمر لإنشاء ملفات تعريف جماعية لمجموعة من الأشخاص من البيانات الشخصية وبيانات الأطراف الأخرى، وكذلك البيانات مجهولة المصدر(٨٤).

كما يمكن لعمليات الاستدلال أن تكشف بشكل مباشر أوغير مباشر عن جوانب من الحياة الخاصة للفرد، الأمر الذي يوفر، من بين أمور أخرى، أسبابًا للتمييز.

(81) Céline Castets-Renard , Brève analyse du règlement général relatif à la protection des données personnelles, Dalloz, IP/IT, 2016, p. 331.

(82) Brent Daniel Mittelstadt & Luciano Floridi, The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, 22 Sci. & Engineering Ethics, 2016, p. 304; Tal Z. Zarsky, Understanding Discrimination in the Scored Society, 89 Wash. L. Rev., 2014, p. 1375.

(83) Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev., 2014, p. 4; Peter Grindrod, Beyond Privacy and Exposure: Ethical Issues Within Citizen-Facing Analytics, Phil. Transactions Royal Soc'y A, Dec. 28, 2016, at 10-12.

(84) Brent Mittelstadt, From Individual to Group Privacy in Big Data Analytics, 30 Phil. & Tech., 2017, p. 475, 476.

ويمكن من خلال عملية الاستدلالات الوصول للبيانات والملفات الشخصية والمعلومات الأخرى المتعلقة بالأفراد ومشاركتها وبيعها والاحتفاظ بها.

كما يمكن إنشاء السجلات الدائمة للبيانات الشخصية من خلال التحليلات الاستدلالية، التي تتكون من استنتاجات غير متوقعة وربما مثيرة للقلق، وتكشف عن معلومات وتنبؤات حول الحياة الخاصة والسلوكيات والتفضيلات التي قد تظل خاصة لولا القيام بعمليات الاستدلال(٨٥).

وقد يوفر الحق في الخصوصية الحماية ضد مثل هذه الإفصاحات التي يمكن أن تؤدي إلى التمييز وإلى أضرار لا يمكن إصلاحها، ولها عواقب طويلة المدى على الفرد وعلى بيئته الاجتماعية، وإن كان الأمر مع ذلك يصبح محلاً للشك في ظل الاستدلالات القائمة على البيانات الضخمة التي تتيحها الوسائل التكنولوجية الحديثة.

ويمكن تفسير ذلك في مجال عملية الاستدلال على البيانات بأنه بالنسبة للأشخاص غالبًا ما تكون القيمة المحتملة والبصيرة للبيانات الناتجة أثناء استخدام التقنيات الرقمية غامضة.

كما يمكن لمراقبي البيانات استخلاص استنتاجات غير بديهية وغير متوقعة، دون علم الأفراد على الإطلاق(٨٦).

(85) Brent Daniel Mittelstadt & Luciano Floridi, The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, 22 Sci. & Engineering Ethics, 2016, p. 306.

(86) Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev., 2018, p. 1085.

ويشكل ذلك، بلا شك، مخاطر على الخصوصية[٨٧]، والهوية[٨٨]، وحماية البيانات والسمعة، وتقرير المصير المعلوماتي.

ويكمن التحدي والخطورة في ذلك أن التغيير المثير للقلق الذي يفرضه النشر الواسع النطاق لتحليلات البيانات الضخمة هو أن الملف الشخصي أو المعلومات المتعلقة بالأفراد قد لا تكون قابلة للتعديل، ويتم الاحتفاظ بها واستخدامها من قبل أطراف أخري لغرض محدد، ولكنها "تستمر بمرور الوقت، وتنتقل مع الشخص بين الأنظمة وتؤثر على الفرص المستقبلية والمعاملة على أيدي الآخرين"[٨٩].

ولا شك أن لذلك تأثيره البالغ على حقوق الأفراد الأساسية، خاصة ما يتعلق منها بالهوية والسمعة، وتقويض حق الفرد "في السماح له بتجربة حياته الخاصة، والبدء من جديد، دون أن يكون لديه سجلات ثابتة عن هويته الشخصية إلى الأبد"[٩٠].

وبالتالي فإن التحليلات الاستدلالية تشكل مخاطر كبيرة وجديدة ليس فقط على الهوية، ولكن أيضًا على السمعة، والخيارات المقدمة للفرد من خلال الخدمات المستندة إلى نتائج الاستدلالات مثل التوظيف والحصول على فرص العمل المناسبة وكذلك القروض وغيرها.

(87) Paul Ohm, The Fourth Amendment in a World Without Privacy, 81 Miss. L.J., 2012, p. 1316-18;& see also Pauline T. Kim, Data-Driven Discrimination at Work, 58 Wm. & Mary L. Rev., 2017, p. 857.

(88) Luciano Floridi, The Informational Nature of Personal Identity, 21 Minds & Machines, 2011, p. 549, 550.

(89) Brent Mittelstadt, From Individual to Group Privacy in Big Data Analytics, 30 Phil. & Tech., 2017, p. 482.

(90) Luciano Floridi, Four Challenges for a Theory of Informational Privacy, 8 Ethics & Info. Tech., 2006, p. 109.

وكما يشير البعض أنه في عالم البيانات الضخمة، هناك ضرورة للتدقيق غالبًا ليس دقة البيانات الأولية بل دقة الاستدلالات المستمدة من البيانات(١).

وقد أقرت فرقة العمل العاملة بموجب المادة ٢٩ بتحدي مماثل، بحجة أنه "في أغلب الأحيان، ليست المعلومات التي تم جمعها في حد ذاتها هي الحساسة، بل الاستدلالات المستخلصة منها، والطريقة التي يتم بها استخلاص هذه الاستنتاجات يمكن أن تثير القلق"(٢).

وأعرب المشرف الأوروبي على حماية البيانات (EDPS) أيضًا عن قلقه بشأن مخاطر الخصوصية الناجمة عن الاستدلالات والحاجة إلى الحوكمة(٣).

وبالمثل، تدرك المنظمات غير الحكومية والمجموعات الناشطة هذه المخاوف وقد قدمت مؤخرًا العديد من الشكاوى للنضال من أجل مزيد من الوضوح بشأن المقبولية القانونية والأخلاقية للتحليلات الاستدلالية(٤).

(1) Omer Tene & Jules Polonetsky, Big Data for All: Privacy and User Control Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop., 2013, p. 239.

(2) Article 29 Data Prot. Working Party, Opinion 03/2013 on Purpose Limitation, at 47, 00569/13/EN, WP203 (Apr. 2, 2013), https://ec.europa.eu/justice/article-29/ documentation/opinion-recommendation/files/2013/wp203_ en.pdf [https://perma.cc/X6PC-825X].

(3) European Data Prot. Supervisor, EDPS Opinion on Online Manipulation and Personal Data at 5, 8-16, Opinion 3/2018 (Mar. 19, 2018), https://edps.europa .eu /sites /edp /files/publication/18-03-19_online_manipulation_en.pdf [https://perma .cc/ 3KJ6-VSUD].

(4) Johnny Ryan, Regulatory Complaint Concerning Massive, Web-Wide Data Breach by Google and Other "Ad Tech" Companies Under Europe's =

كما يمكن أن تتشكل الخطورة والإضرار بحقوق الأفراد من خلال عدم القدرة على التنبؤ بالتحليلات الكامنة وراء اتخاذ القرار الآلي، والتوصيف فيمكن أن يكون ذلك في حد ذاته ضارًا للأفراد، كما أن استخدام مصادر البيانات غير التقليدية للتوصل إلى استنتاجات غير متوقعة وغير بديهية حول الأشخاص يمكن أن يؤثر على حرية التعبير، والحق في الخصوصية والهوية(١).

واستقرت المحكمة الأوروبية لحقوق الإنسان منذ أمد طويل على ربط الحق في الشخصية بالحق في الخصوصية للإنسان(٢)،كما أن الخصوصية تتعلق بالفردية والاستقلالية والنزاهة والكرامة(٣).

ويتناول الحق الأوسع في الخصوصية الحياة الشخصية والعائلية، والعلاقات الاقتصادية، كما يمتد ليشمل، بشكل أوسع، قدرة الفرد على التعبير عن شخصيته بحرية دون خوف من العواقب(٤).

=

GDPR, Brave (Sept. 12, 2018), https://www.brave.com/blog/adtech-data-breach-complaint/ [https ://perma.cc/3DFW-JZTX]

(1) Antoinette Rouvroy, Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence, 2 Stud. Ethics, L., & Tech. 2008, p. 3-4.

(2) Alessandro Mantelero, Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework, 33 Comp. L. & Security Rev., 2017, p. 584.

(3) A Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, 2002, p. 128-129.

(4) Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev., 2007, p. 745.

وهو ما يشير للحاجة الملحة للغاية لحماية الحق في الخصوصية، بل يمكن اعتبار ذلك أيضاً مصلحة عامة وجماعية [١].

ويمكن القول أنه في ظل القيود الحالية المفروضة على اختصاص قانون حماية البيانات والتضييق من نطاق تطبيقه أن تضر بهدفه الأوسع المتمثل في حماية الخصوصية من المخاطر التي تشكلها التقنيات الجديدة.

وتعد حماية الحق في الخصوصية الهدف الأسمى والأساسي لقانون حماية البيانات، وتم الاعتراف بذلك من قبل الاجتهادات والسوابق القضائية لمحكمة العدل الأوروبية، وكذلك للمحكمة الأوروبية لحقوق الإنسان حيث تم الاعتراف بأن الهدف من قانون حماية البيانات هو حماية هذه الجوانب الأوسع من الخصوصية، أو بعبارة أخرى، تقييد معالجة بيانات التعريف الشخصية التي تؤثر على هذه المناطق من الحق في الخصوصية، وبالتالي، فإن حماية البيانات ليست سوى جزء واحد من الخصوصية[٢].

(1) Priscilla M. Regan, Privacy as a Common Good in the Digital World, 5 Info., Comm'n. & Soc'y , 2002, p.382.

(2) Case C-101/01, Criminal Proceedings Against Bodil Lindqvist, 2003 E.R.C. I-12971; Case C434/16 Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994; Case C582/14, Patrick Breyer v. Bundesrepublik Deutschlan, 2016 E.C.R. I-779.

see also Council of Europe, Case Law of the European Court of Human Rights Concerning the Protection of Personal Data (2017), https://rm.coe.int/case-law-on-data-protection/1680766992 [https://perma. cc/MP7S-2DKP].

المطلب الثالث

مدى ملائمة قواعد حماية البيانات

لتحقيق أهدافها في عصر البيانات الضخمة

يهدف قانون حماية البيانات إلى حماية خصوصية الأشخاص وهويتهم وسمعتهم واستقلاليتهم، لكنه يفشل حاليًا في حماية أصحاب البيانات من المخاطر الجديدة للتحليلات الاستدلالية.

ويظهر ذلك، بشكل واضح، من خلال طبيعة البيانات محل الحماية، وكذلك حقوق الأفراد الفردية في مجال الاستدلالات، فعالية التمييز بين أنواع البيانات في مجال الاستدلالات، تأثير تحديد هوية الأشخاص على عملية الاستدلالات، ونعرض مدى ملائمة القواعد التشريعية الحالية لتحقيق أهدافها بالنسبة لهذه الأمور في الفروع التالية:

الفرع الأول

طبيعة البيانات محل الحماية

يمكن تفسير المفهوم الواسع للبيانات الشخصية ليشمل الاستنتاجات والتنبؤات والافتراضات التي تشير إلى الفرد أو تؤثر عليه، خاصة، إذا تم النظر إليها على أنها بيانات شخصية، فسيتم منح الأفراد حقوقًا عديدة بموجب قانون حماية البيانات(١).

(1) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494

ومع ذلك، فإن الوضع القانوني للاستدلالات محل نزاع كبير في الدراسات القانونية، ويتميز بالتناقضات داخل وفيما بين آراء فرقة العمل المعنية بالمادة ٢٩[١]، ومحكمة العدل الأوروبية.

وقامت محكمة العدل الأوروبية[٢] بتقييد اختصاص قانون حماية البيانات بشكل ثابت لتقييم الشرعية فقط في مرحلة الإدخال لمعالجة البيانات الشخصية، بما في ذلك تصحيح المدخلات ومحوها، والاعتراض على المعالجة غير المرغوب فيها.

كما أنه من المثير للاهتمام، في هذا الصدد، أن محكمة العدل الأوروبية أوضحت أن قانون حماية البيانات ليس المقصود منه ضمان دقة القرارات وعمليات صنع القرار التي تتضمن البيانات الشخصية، أو جعل هذه العمليات شفافة تمامًا[٣].

ومؤدى ذلك أنه يتمتع أصحاب البيانات بالتحكم في كيفية جمع بياناتهم الشخصية ومعالجتها، ولكن لديهم سيطرة قليلة للغاية على كيفية تقييمها.

---

(١) تجدر الإشارة إلى أنه اعتبارًا من تطبيق اللائحة العامة لحماية البيانات ("GDPR") في ٢٥ مايو ٢٠١٨، لم يعد فريق عمل المادة ٢٩ موجودًا وخلفه المجلس الأوروبي لحماية البيانات ("EDPB")

European Data Prot. Bd., The European Data Protection Board, Endorsement 1/2018 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_ wp29_documents.pdf [https://perma.cc/8H9A-RQR3]

(2) Case C-28/08 P, European Comm'n v. Bavarian Lager Co., 2010 E.C.R. I-6055, PP 49-50; Case C-434/16, Peter Nowak v. Data Prot. Comm'r, 2017 E.C.R. I-994, PP 54-55; Joined Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, PP 45-47.

(3) Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 2009 E.C.R. I-293, PP 48-52.

وتوضح محكمة العدل الأوروبية أنه إذا كان صاحب البيانات يرغب في الطعن في نتائج تقييمه التي تمت من خلال عملية الاستدلالات، فيجب اللجوء إلى ذلك من خلال القوانين المعنية بذلك، وليس قانون حماية البيانات.

ووفقاً للائحة الأوروبية لحماية البيانات، وكذلك القانون المصري لحماية البيانات الشخصية إنما يتعلق بمنح الرقابة والتحكم في كيفية جمع البيانات الشخصية ومعالجتها، ويركز قانون حماية البيانات في المقام الأول على آليات إدارة جانب المدخلات من المعالجة.

وبالنسبة لمخرجات المعالجة، والبيانات المستنتجة، والمشتقة والملفات الشخصية والقرارات، التي تم الاستدلال عليها فتحظى بآليات قليلة في قوانين حماية البيانات.

وفي عصر تحليلات البيانات الضخمة، لم يعد التركيز على البيانات المدخلة في قانون حماية البيانات أمرًا مجدياً، حيث تشكل مخرجات المعالجة مخاطر على الأفراد بشكل أكبر وأوسع نطاقاً، ومع ذلك يتم منح أصحاب البيانات سيطرة أقل بكثير على كيفية إنتاج هذه المخرجات واستخدامها.

كما تكمن إحدى الإشكاليات الحالية في عدم وعي الأفراد بعملية صنع القرار، بل والافتقار للأساس القانوني الملزم لفحص عملية صنع القرار.

وكما يوضح البعض أن تلك الإشكاليات تعد نتيجة للوضع القانوني غير المؤكد للاستدلالات ونطاق آليات الرقابة المعمول بها في قوانين حماية البيانات، ولم تعد آليات الشفافية والموافقة المصممة لإدارة بيانات المدخلات كافية؛ وبدلاً من ذلك، يتطلب انتشار تحليلات البيانات الضخمة الاستدلالية رد فعل في قانون حماية البيانات، والذي يتم من

خلاله منح التحكم والاختيار الهادفين للاستدلالات والملفات الشخصية لأصحاب البيانات[١].

الفرع الثاني

حقوق الأفراد الفردية في مجال الاستدلالات

لا يتمتع – غالباً- أصحاب البيانات بالقدرة على الوصول إلى الاستدلالات المستخلصة عنهم أو تقييمها، وكذلك العمليات التي أدت إلى هذه الاستدلالات.

ومن الجدير بالذكر أن منح الأفراد حقوقاً على الاستدلالات ونتائجها تحتاج لاعتراف تشريعي ذلك، ولا يقتصر الأمر فقط على مجرد الاجتهادات القضائية.

وعلى الرغم من أن حماية الخصوصية والبيانات، دائماً ما ينظر إليها على أنها حقوقاً فردية للأشخاص، بل والأكثر من ذلك توسع تفسير الحق في الخصوصية، بل وربطه بالحق في شخصية الإنسان[٢]، وتعلق ذلك بالعديد من الحقوق مثل الاستقلالية والكرامة وكذلك شموله للحياة الشخصية والعائلية، والعلاقات الاقتصادية، كما يمتد ليشمل، بشكل أوسع، قدرة الفرد على التعبير عن شخصيته بحرية دون خوف من العواقب[٣].

(1) Serge Gutwirth & Paul De Hert, Regulating Profiling in a Democratic Constitutional State, in Profiling the European Citizen, 2008, p. 271.

(2) Alessandro Mantelero, Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework, 33 Comp. L. & Security Rev., 2017, p. 584.

(3) Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev., 2007, p. 745.

وعلى ذلك، تظهر ضرورة تقرير حماية أكثر للحق في الخصوصية من خلال قانون حماية البيانات، خاصة في ظل عمليات الاستدلالات في عصر البيانات الضخمة واستخدام التقنيات الجديدة.

وما يدعو لذلك هو أن عملية الاستدلالات -في ذاتها- تتمتع بحماية أقل بموجب قوانين حماية البيانات بسبب ضرورة الموازنة بين طلبات الوصول أو المحو أو الحقوق الأخرى مع مصالح مراقبي البيانات (مثل الأسرار التجارية والملكية الفكرية) وحقوق الآخرين وحرياتهم.

ومن المثير للاهتمام أن الاستدلالات تحظى بأقل قدر من الحماية من بين جميع أنواع البيانات التي تتناولها قوانين حماية البيانات، ومع ذلك فإنها ربما تشكل الآن أكبر المخاطر فيما يتعلق بالخصوصية والتمييز والإضرار بحقوق الأشخاص.

الفرع الثالث

فعالية التمييز بين أنواع البيانات في مجال الاستدلالات

يتمتع التمييز بين أنواع البيانات، بصرف النظر عن النهج التشريعي لهذا التمييز، بأهمية قصوى في مجال حماية البيانات المختلفة، ومدى ضرورة توافر قدر أكبر من الحماية لبعض فئات البيانات الشخصية.

كما يشمل التمييز بين أنواع البيانات التمييز القائم على بيانات الإدخال والتي يمكن الحصول عليها من الأشخاص أصحاب البيانات، وبيانات مخرجات عملية الاستدلال وهى البيانات المستنتجة.

وينبغي أن يشمل أثر هذا التمييز في التطبيق على عملية الاستدلال، وبمفهوم المخالفة، إذا لم يتم تطبيق التمييز بين أنواع البيانات في عمليات الاستدلالات فسيؤدى

ذلك للإضرار بالحقوق الأساسية للأفراد مثل الاعتداء على الحق في الخصوصية وأضرار التمييز وغيرها.

ويؤكد ذلك أنه يمكن استخلاص العديد من الاستنتاجات من البيانات الشخصية للفرد، ولكن هذا ليس المصدر الوحيد الممكن، بل يمكن أيضًا استخدام البيانات مجهولة المصدر، والأشكال الأخرى من البيانات غير الشخصية لتطوير الاستدلالات والملفات الشخصية.

ويمكن بعد ذلك تطبيق هذه المعرفة الأساسية، المبنية من بيانات مجهولة المصدر أو غير شخصية على موضوعات البيانات الفردية، ويمكن بهذه الطريقة فصل عملية استخلاص الاستدلالات وإنشاء الملفات الشخصية عن تطبيقها النهائي على شخص يمكن التعرف عليه[٤].

ونتيجة لذلك، توجد فجوة بين قدرة وحدات التحكم على جمع البيانات واستخلاص استنتاجات حول الأشخاص منها، وقدرة قانون حماية البيانات على التحكم في التحليلات الاستدلالية التي لا تتناول فردًا محددًا[٥].

كما يترتب على ذلك أن يصبح الأفراد المتأثرون غير قادرين بشكل كامل على ممارسة حقوق حماية البيانات الخاصة بهم مثل حق الوصول إليها أو تعديلها أو محوها[٦].

---

(4) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081.

(5) Mireille Hildebrandt, Profiling: From Data to Knowledge, 30 Datenschutz und Datensicherheit, 2006, p. 548.

(6) Rubinstein, for example, doubts that the right to be forgotten would apply to to profiles built from anonymised or aggregated data. Ira S. Rubinstein, =

الفرع الرابع

تأثير تحديد هوية الأشخاص على عملية الاستدلالات

تشكل إمكانية تحديد هوية الشخص المعني بالبيانات عائقًا أمام المساءلة الهادفة للتحليلات الاستدلالية، حيث يمكن أن يتأثر الأفراد بنتائج الاستدلالات المستقلة والتي تعتمد على تطبيق بيانات مجهولة المصدر أو بيانات غير شخصية أو بيانات أطراف أخري على المستوى الفردي(٧).

بل ويمكن لمراقبي البيانات تجنب العديد من القيود القانونية من خلال استخدام بيانات غير مرتبطة بشخص معين، أو عن طريق إخفاء هوية أصحاب البيانات بشكل مقصود قبل القيام بعملية الاستدلالات وإنشاء الملفات الشخصية(٨).

ولا يقصد من ذلك أن الأفراد يجب أن يكون لديهم حقوق على بيانات الآخرين، أو البيانات التي لم يتم تطبيقها عليهم، بل تكمن الصعوبة في افتقار الأفراد إلى سبل الانتصاف ضد البيانات والمعالجة المجهولة التي أدت إلى الاستنتاجات أو تكوين الملفات

=

Big Data: The End of Privacy or a New Beginning?, 3 Int'l Data Privacy L., 2013, p. 74.

(7) Mireille Hildebrandt, Profiling: From Data to Knowledge, 30 Datenschutz und Datensicherheit, 2006, p. 548

(8) Wim Schreurs. Mireille Hildebrandt, Els Kindt & Michael Vanfleteren, Cogitas, Ergo Sum. The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector, in Profiling the European Citizen, 2008, p. 241, 246.

الشخصية المطبقة عليهم، ما لم يتم تطبيق معايير صنع القرار والتي تقررها القوانين المعنية بذلك مثل قانون مكافحة التمييز[٩].

وعلى سبيل المثال، أثيرت مخاوف بشأن تصنيف البيانات التي تجمعها السيارات ذاتية القيادة، حيث يمكن لأجهزة الاستشعار مسح الطريق أمام السيارة، والكشف عن الأشياء التي يجب تجنبها، والتي قد تشمل المشاة.

ولا شك أن مثل هذه البيانات التي تصف محيط السيارة لا تقع بوضوح ضمن نطاق "البيانات الشخصية" في قانون حماية البيانات، على الرغم من كونها قد تحتوى على بيانات حول الأشخاص ، إلا أن هذه الصور لا تسمح عادةً بتحديد هوية الأفراد المسجلين بشكل لا لبس فيه[١٠].

ويجب لخضوع البيانات لنطاق البيانات الشخصية، وبالتالي للحماية المقررة بالقوانين المتعلقة بحماية البيانات أن تكون البيانات متعلقة بشخص محدد أو يمكن تحديده، ومع ذلك فإن قابلية التحديد، لا تحتاج إلى تحديد هوية الفرد على وجه اليقين المطلق، بل يكفي أن يمكن تمييز الشخص من بين مجموعة من الأشخاص، حتى لو كان اسمه غير معروف ، ولكن هناك خصائص أخرى تصف الشخص بشكل كاف[١١].

(9) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494

(10) Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Transparent, Explainable, and Accountable AI for Robotics, Sci. Robotics, May 31, 2017, at 1

(11) Ira S. Rubinstein & Woodrow Hartzog, Anonymization and Risk, 91 Wash. L. Rev., 2016, p. 703.

ويجب تقييم إمكانية تحديد هوية الشخص بشكل معقول، مع الأخذ في الاعتبار جميع الوسائل التي من المحتمل بشكل معقول استخدامها، مثل التفرد، إما من قبل المراقب أو من قبل شخص آخر لتحديد هوية الشخص الطبيعي بشكل مباشر أو غير مباشر(١٢).

وعلى الرغم من وصف هذه البيانات، في كثير من الأحيان، بكونها بيانات مجهولة المصدر، إلا أن الباحثون قد أظهروا أن البيانات مجهولة المصدر يمكن ربطها بالأفراد(١٣).

وفي ذات السياق قد يكون للسائق والمشاة وشركات التأمين والمنظمين وغيرهم مصلحة في الوصول إلى بيانات الاستشعار غير الشخصية، ومع ذلك فإن مسألة الوصول، هذه، قد تقع خارج نطاق قانون حماية البيانات.

(12) Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 5.

(13) Nadezhda Purtova, Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency, 10 J.L. & Econ. Reg., 2017, p. 64; Latanya Sweeney, Only You, Your Doctor, and Many Others May Know, Tech. Sci. (Sept. 29, 2015), https://techscience.org/a/2015092903 [https://perma.cc/38L5-ATQ8]; Vijay Pandurangan, On Taxis and Rainbows, Medium (June 21, 2014), https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1 [https://perma.cc/HW7B-C6UW].

وللتغلب على هذه الإشكاليات، ومنعاً للإضرار بالبيانات الشخصية، وتأثيرات عمليات الاستدلالات على الحقوق الأساسية للأشخاص فقد اقترح البعض[١٤] ضرورة الابتعاد عن التصنيفات القائمة للبيانات الشخصية الواردة بقوانين حماية البيانات، وتعطيلها، وضرورة التخلي عنها.

ولا شك أن التخلي عن هذا التمييز من شأنه، بطبيعة الحال، أن يترك فجوة في قانون حماية البيانات تتطلب إدخال تصنيف آخر للبيانات لتحديد نطاق تطبيق القانون، وبدون تصنيف جديد، ستصبح جميع البيانات المتعلقة بالأشخاص بيانات شخصية بشكل فعال، مما يوسع بشكل كبير نطاق تغطية قانون حماية البيانات[١٥].

وبالنظر إلى هذا الاقتراح، وعلى الرغم من وجاهته ومنطقيته في إزالة الحدود المتداخلة بين البيانات الشخصية وغير الشخصية، إلا أنه قد لا تقضي على الإشكاليات المتعددة لعمليات الاستدلالات، كما يصطدم هذا الاقتراح بالطبيعة الخاصة لبعض فئات البيانات الشخصية والمتمثلة في البيانات الحساسة حيث لا يجوز –بسبب خصوصيتها- جمعها أو معالجتها، بأي شكل من الأشكال، دون موافقة صريحة من المعني بها، وضرورة حصول مراقب البيانات أو المتحكم على ترخيص بذلك من الجهة المختصة.

ومما سبق يتضح بشكل لا لبس فيه ولا غموض أن الاستمرار في الاعتماد على معايير الحساسية وإمكانية تحديد الهوية، أو على التمييز غير الواضح بين البيانات الشخصية والبيانات الحساسة، وكذلك البيانات غير الشخصية والمجهولة، كمقاييس لمستوى الحماية الممنوحة للبيانات هو أمر لم تثبت فعاليته في تظل التطورات المتلاحقة

(14) Sandra Wachter, Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, 34 Computer L. & Security Rev., 2018, p. 436.

(15) Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 Law Innovation & Tech, 2018, p. 58.

فـي عمليـات المعالجـات الالكترونيـة والاسـتدلالات مـن خـلال اسـتخدام تقنيـات الـذكاء الاصطناعي والبيانات الضخمة.

كما يترتب على الاستمرار في الاعتماد على هذا النهج الإخلال الكبير في حماية الخصوصـية بـالمعنى الأوسـع، خاصـة، فـي ظـل المخـاطر الجديـدة لتحلـيلات البيانـات الضـخمة واتخـاذ القرارات الآليـة، بـل وينبغـي التركيـز بشكل أكبـر علـى إدارة مخرجـات معالجة البيانات، والتي تُفهم هنا على أنها استنتاجات أو قرارات، بغض النظر عن نـوع البيانات التي استندت عليها.

كما أن تأثير البيانات غير الشخصية على الحق في الخصوصية أصبح أمراً بلا منازع في ظل التطور التكنولوجي الهائل في شتى المجالات، ومع ذلك يظل حالياً دون سند قانوني للتنظيم والحماية، مما يمكن معه الاقتراح بضرورة الاعتماد على الاجتهادات القضائية بهدف توسيع نطاق قانون حماية البيانات لضمان اتخاذ قرارات دقيقة وعادلة حين تعتمد على هذا النوع من البيانات.

كما يجب ربط الحق في الاستدلالات، سواء المعقولة أو عالية المخاطر، بالحق فـي الخصوصـية، والنظـر إلـى الاسـتدلالات علـى كونهـا آليـة تهـدف إلـى حمايـة الهويـة والسمعة، ويوفر ذلك لأصحاب البيانات حماية إضافية ضد الاستنتاجات المستخلصة من خـلال تحلـيلات البيانـات الضـخمة والتـي يُتوقـع أن تسـبب ضـررًا بالسـمعة أو تنتهـك خصوصـية الشـخص، وكـذلك إذا هـذه الاسـتدلالات ذات إمكانيـة تحقـق منخفضـة بمعنـى كونها تنبؤية أو قائمة على الرأي بينما استخدامها لاتخاذ قرارات مهمة.

ويحتـاج ذلـك فـي تنفيـذه لضـرورة التوسـع فـي تفسـير قـانون حمايـة البيانـات فيمـا يتعلق بحقوق الفرد في البيانات المستنتجة والمشتقة، والتوصيف، واتخاذ القرارات الآلية التي تنطوي على مثل هذه المعلومات.

الفصل الثالث

صور حماية البيانات الشخصية الحساسة

لا شك أن النهج التشريعي الحالي ينظر للبيانات الحساسة على كونها مجموعة من فئات البيانات الشخصية والتي تتطلب حماية خاصة، وأوردها غالبية المشرعين ضمن قائمة مغلقة أي أن تعدادها كان وارداً على سبيل الحصر، ومقرراً لها حماية قانونية مشددة، وغالبًا ما تتضمن قوانين حماية البيانات التي تتضمن أحكامًا خاصة بالبيانات الحساسة مستويين من الحماية: أحدهما للبيانات الشخصية العادية، والآخر للبيانات الحساسة.

وتظهر الحاجة ضرورة تقرير حماية فاعلة ومشددة للبيانات الحساسة بصفة عامة، وفي مجال الاستدلالات عليها بصفة خاصة.

وإذا كانت القواعد التشريعية الحالية، على المستويين الوطني والدولي، تشير لصور هذه الحماية، وتظهر، بشكل جلي، من خلال تقرير مبدأ حظر من حيث الأصل على معالجة البيانات الحساسة، مع تقرير بعض الاستثناءات المقيدة بنطاقها وحدودها لإمكانية القيام بتلك المعالجة، وتقرير حقوق أصحاب البيانات في حالة معالجة بياناتهم الحساسة، إلا أن هذه القواعد إنما تشير لحالة البيانات التى يتم الحصول عليها من الأشخاص المعنيين دون الإشارة لحالة امكانية التوصل لتلك البيانات من خلال عمليات الاستدلال.

ولذلك، وفي ضوء القواعد التشريعية المعمول بها حالياً، أوروبياً ومصرياً، فإن هذه الحماية قد لا تتسم بالفاعلية في حماية أصحاب البيانات في مواجهة الاستدلالات على

البيانات الحساسة، وهو ما يستدعى وجوب الاعتراف بحقوق أصحاب البيانات في مواجهة عمليات الاستدلالات، وكذلك تقرير الحماية الكافية للبيانات المستنتجة.

ونعرض من خلال هذا الفصل لأمرين جوهريين، نبين أولا حظر معالجة البيانات الحساسة، وهو ما نعرض له من خلال المبحث الأول، ثم نبين لضرورة تقرير الحماية القانونية في مجال لاستدلالات، وهو ما نوضحه في المبحث الثاني.

المبحث الأول: حظر معالجة البيانات الحساسة

المبحث الثاني: تقرير الحماية القانونية في مجال الاستدلالات

المبحث الأول

حظر معالجة البيانات الحساسة

تقر التشريعات المنظمة لحماية البيانات الشخصية، من حيث الأصل، حظراً عاماً على جمع واستخدام ونقل وتخزين ومعالجة وإتاحة البيانات الحساسة، ويعتبر حظر معالجة البيانات الشخصية الحساسة هو نظام حظر عام تمليه حقيقة أن البيانات المعنية من المحتمل في حد ذاتها أن تنتهك الحريات الأساسية أو الخصوصية.

كما تتشدد هذه التشريعات في القيود المفروضة على إمكانية معالجة البيانات الحساسة حيث يجب أن يتوافر استيفاء المتحكم أو المعالج لقيد إجرائي في البداية وهو ضرورة الحصول على ترخيص بذلك من قبل مركز حماية البيانات الشخصية، وبعد ذلك ضرورة الحصول على موافقة الشخص المعني بالبيانات، ما لم يتوافر أساس قانوني لمعالجتها من الأسس المقررة قانوناً.

كما يمكن أن تتم معالجة البيانات الشخصية الحساسة من قبل معالج من الباطن حصل على تعاقد كتابي من قبل المتحكم للقيام بعملية المعالجة بالمشاركة معه، أو المعالجة لحساب المتحكم، وهو ما يفرض على المعالج من الباطن الخضوع لذات القيود والالتزامات المقررة بموجب قانون حماية البيانات.

ونعرض من خلال هذا المبحث لمطالب ثلاثة، نعرض في أولها لتطبيق مبدأ حظر معالجة البيانات الحساسة ومدى امكانية تطبيقه على حالات الاستدلالات، ونعرض في المطلب الثاني لغرض المعالجة، ونعرض في المطلب الثالث متطلبات الموافقة في مجال الاستدلال على البيانات الحساسة، وذلك على النحو التالي:

المطلب الأول: تطبيق مبدأ حظر معالجة البيانات الحساسة.

المطلب الثاني: غرض المعالجة

المطلب الثالث: متطلبات الموافقة في مجال الاستدلال على البيانات الحساسة

المطلب الأول

تطبيق مبدأ حظر معالجة البيانات الحساسة

يعد الأصل في نطاق البيانات الحساسة هو حظر معالجتها، وفي حالة المعالجة لها استناداً لأي أساس قانوني فإنها تخضع للعديد من القيود، ونعرض من خلال هذا المطلب لنطاق مبدأ الحظر، ومدى امكانية تطبيق مبدأ الحظر على الاستدلالات.

الفرع الأول

نطاق مبدأ الحظر

تفرض القواعد التشريعية من حيث الأصل مبدأ عاماً يحظر معالجة البيانات الحساسة، ومن ذلك ما نص عليه المشرع المصري حيث قرر " يحظر على المتحكم أو المعالج سواء كان شخصاً طبيعياً أو اعتبارياً جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز. وفيما عدا الأحوال المصرح بها قانوناً، يلزم الحصول على موافقة كتابية وصريحة من الشخص المعني. وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر. ويجب ألا تكون مشاركة الطفل في لعبة، أو مسابقة، أو أي نشاط آخر، مشروطة بتقديم

بيانات شخصية للطفل تزيد على ما هو ضروري للمشاركة في ذلك. وذلك كله وفقا للمعايير والضوابط التي تحددها اللائحة التنفيذية لهذا القانون"(١٦).

كما قرر المشرع الفرنسي بالمادة الثامنة من قانون حماية البيانات الشخصية بأنه يُحظر معالجة البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني المزعوم أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو العضوية النقابية لشخص طبيعي أو معالجة البيانات الجينية والبيانات البيومترية لأغراض تحديد الهوية بشكل فريد شخص طبيعي، بيانات تتعلق بالصحة أو بيانات تتعلق بالحياة الجنسية أو التوجه الجنسي لشخص طبيعي(١٧).

وتقرر المادة التاسعة من اللائحة العامة لحماية البيانات، التي تحكم البيانات الحساسة، حظر عام على معالجة البيانات الحساسة، حيث تحظر معالجة البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني، أو الآراء السياسية، أو المعتقدات الدينية أو الفلسفية، أو عضوية النقابات العمالية، ومعالجة البيانات الجينية، والبيانات البيومترية بغرض تحديد هوية الشخص الطبيعي بشكل فريد، أو البيانات المتعلقة بالصحة أو البيانات المتعلقة بالحياة الجنسية للشخص أو توجهه الجنسي(١٨).

ويستفاد من ذلك أن نطاق الحماية القانونية المقررة للبيانات الحساسة إنما هى قاصرة على البيانات الحساسة والتى يتم جمعها أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها من قبل المتحكم في البيانات أو المعالج لها، ويعد مبدأ حظر معالجة البيانات

---

(١٦) المادة (١٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(17) Loi n° 2018 493 du 20 juin 2018, relative à la protection des données personnelles NOR : JUSC1732261L) JO , 21 juin 2018)

(18) GDPR, art. 9(1).

الحساسة مبدأ واسع للغاية حيث يتم تطبيقه منذ لحظة معالجة البيانات مروراً بجميع مراحلها.

ومؤدى ذلك أن نطاق هذا الحظر ينطبق فقط – وفق صريح هذا النص- على حالات يمكن الحصول من خلالها على بيانات حساسة لشخص معين سواء بطريقة الجمع أو النقل أو التخزين أو الحفظ أو المعالجة أو حتى إتاحتها.

وما يؤكد ذلك أن المشرع المصري قد تطلب ضرورة الحصول مسبقاً على موافقة صاحب البيانات قبل الشروع في جمعها ومعالجتها بأي صورة من الصور.

ويتضح من ذلك أننا أمام أمرين محققين بالفعل وهما: أولاً: وجود صاحب البيانات (الشخص المعني بالبيانات)، وثانياً: وجود البيانات الحساسة بالفعل.

ولذلك لا تظهر اشكاليات أو عقبات في سبيل تطبيق مبدأ حظر معالجة البيانات الحساسة، أو كذلك الاستثناءات الواردة عليه.

وإذا كانت البيانات الحساسة جديرة بالحماية المشددة، وهى بالفعل كذلك، فإن الأمر جد مختلف في حال التوصل للبيانات الحساسة من خلال عمليات الاستدلالات.

وهكذا يبدو أن حماية البيانات الحساسة منصوص عليه في مختلف التشريعات الأوروبية بطريقة متماسكة، وكذلك بالقانون المصري لحماية البيانات، مما يؤدي إلى إنشاء شبكة من معايير الحماية.

الفرع الثاني

مدى امكانية تطبيق مبدأ الحظر على الاستدلالات

تعد البيانات هى جوهر عملية الاستدلالات، وتعتمد الاستدلالات على نوعين من البيانات وهما: أولاً: البيانات المدخلة، ولهذه البيانات صور متعددة، منها: البيانات

المقدمة من أصحاب البيانات أياً كان وصفها أي سواء بيانات شخصية أو بيانات حساسة، كما يدخل في نطاق البيانات المدخلة البيانات العادية، وكذلك البيانات مجهولة المصدر.

ثانياً: البيانات المستنتجة: وهى البيانات التى تم استنتاجها والتوصل إليها من خلال عمليات الاستدلالات، ويستوى أن تكون البيانات المستنتجة ذات طبيعة شخصية، أو كذلك ذات طبيعة حساسة.

ووفقاً للقواعد القانونية المقررة لحماية البيانات الحساسة وتقرير مبدأ حظر عام على معالجتها، فإن هذه القواعد إنما تتعلق بالنوع الأول من بيانات عمليات الاستدلال وهى البيانات المدخلة، دون توفير الحماية الكافية بالمماثلة للبيانات المستنتجة حتى ولو تم التوصل لبيانات حساسة.

ويعني ذلك أن تطبيق مبدأ حظر معالجة البيانات الحساسة يمكن تطبيقه فقط على البيانات المدخلة في عملية الاستدلال وبشرط أن تكون هذه البيانات ذات طبيعة حساسة.

وعلى ذلك، فإن الحظر يشمل البيانات الحساسة لشخص محدد الهوية أو يمكن التعرف عليه بشكل مباشر أو غير مباشر.

وبمفهوم آخر إذا كانت البيانات المدخلة لا تتضمن بيانات ذات طبيعة حساسة فلا تخضع عمليات الاستدلال للقيود المقررة بشأن معالجة البيانات الحساسة، حتى ولو تم التوصل من خلال الاستدلالات لبيانات حساسة.

علاوة على ذلك، يمكن للقائمين على عمليات الاستدلالات، سواء المتحكمين أو المعالجين للبيانات، التهرب من القيود القانونية، وبصفة خاصة المقررة على البيانات الحساسة من خلال استخدام بيانات عادية أو حتى بيانات مجهولة يمكن من خلال ربطها ببيانات أخري في مجموعات متباينة الاستدلال على بيانات حساسة.

ويظهر من ذلك مدى الاهتمام التشريعي على المستويين الأوروبي والوطنى بالبيانات المدخلة دون الاهتمام بشكل مماثل بمخرجات عمليات الاستدلالات، على الرغم من كون هذه المخرجات لها تأثيرها البالغ على حقوق الأفراد في المجالات الحياتية المختلفة.

ونعتقد أن هذا الأمر يتعلق بقصور تشريعي، يجب النص عليه صراحة بقانون حماية البيانات، بضرورة امتداد الحماية القانونية والمعززة للبيانات الحساسة سواء تعلقت ببيانات مدخلات أو بيانات مستنتجة من عمليات الاستدلالات، مع ضرورة النص صراحة على ضوابط عمليات الاستدلال لتعلقها بالحقوق الأساسية للأشخاص.

وإذا كان المشرعيين، الأوروبي والمصري، قد أدركا عند إعداد تشريعات حماية البيانات اعتبارات التقدم العلمى، وبصفة خاصة في مجال الصحة، فيجب كذلك الاعتداد بهذه الاعتبارات في عصر التقدم التكنولوجى والذكاء الاصطناعي وامكانية القيام باستدلالات متقدمة للغاية على البيانات الحساسة.

ويظهر ذلك من خلال ما تضمنته اللائحة العامة الأوروبية لحماية البيانات لعام ٢٠١٦ فئتين جديدتين من البيانات في قائمة البيانات التي تُحظر معالجتها من حيث المبدأ وهما: البيانات البيومترية، والبيانات الجينية.

ويعد هذا امتدادًا رئيسيًا لحماية البيانات الحساسة، والتي تأخذ في الاعتبار التقدم العلمي في هذا المجال، حيث تشكل القياسات الحيوية صورة جزء من الجسم البشري للشخص، والتي يسمح قياسها بمستوى عالٍ جدًا من المصداقية؛ كما يمكن الآن استغلال البيانات الجينية بسهولة، من الحمض النووي المشفر أو غير المشفر، لتحديد الأشخاص على وجه اليقين ومعرفة بعض خصائصهم الجسدية أو أمراضهم، وتم تعزيز حماية هذه البيانات بالحظر من حيث المبدأ.

علاوة على ذلك، نظرت مجموعة فريق عمل المادة ٢٩[١٩] في مسألة البيانات الحساسة التي يمكن أن تنشأ من صورة شخص يمكن التعرف عليه وخلصت إلى ما يلي:

"في بعض الدول الأعضاء في الاتحاد الأوروبي، تعتبر صور أصحاب البيانات فئة خاصة من البيانات الشخصية حيث يمكن استخدامها للتمييز بين الأصل العرقي أو الإثني أو لاستنتاج المعتقدات الدينية أو البيانات الشخصية بالنسبة للصحة، ولا يعتبر بشكل عام، الصور الموجودة على الإنترنت بيانات حساسة ما لم يتم استخدامها بشكل واضح للكشف عن بيانات حساسة حول الأفراد"[٢٠].

ويمكن تطبيق نفس الأمر بالنسبة للبيانات الأخرى التي تغطيها المادة التاسعة من اللائحة العامة لحماية البيانات حيث يمكن تطبيق ذلك على البيانات الشخصية التي تكشف عن الأصل العرقي أو الإثني أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو عضوية النقابات العمالية، فضلاً عن معالجة البيانات الجينية، بدءًا من البيانات البيومترية وحتى أغراض تحديد هوية الشخص الطبيعي بشكل فريد.

(١٩) تجدر الإشارة إلى أنه اعتبارًا من تطبيق اللائحة العامة لحماية البيانات ("GDPR") في ٢٥ مايو ٢٠١٨، لم يعد فريق عمل المادة ٢٩ موجودًا وخلفه المجلس الأوروبي لحماية البيانات ("EDPB")

European Data Prot. Bd., The European Data Protection Board, Endorsement 1/2018 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents.pdf [https://perma.cc/8H9A-RQR3]

(20) Groupe 29, Avis 5/2009 du 12 juin 2009 sur les réseaux sociaux en ligne, WP 163.

المطلب الثاني

غرض المعالجة

يعد الغرض من معالجة البيانات الحساسة إحدى المسائل الجوهرية التى تم الاهتمام بها في تشريعات حماية البيانات، ونعرض من خلال هذا المطلب لإمكانية تطبيق غرض المعالجة في مجال الاستدلالات، ومدى اعتبار المصالح المشروعة أساساً للمعالجة وكذلك للاستدلالات.

الفرع الأول

تطبيق غرض المعالجة في مجال الاستدلالات

يجب أن تخضع معالجة البيانات الحساسة لغرض محدد أو أكثر، ويتضمن ذلك معرفة الهدف أو الأهداف التي تهدف هذه المعالجة إلى تحقيقها منذ البداية لمعالجة البيانات، ولا يمكن أن يكون الغرض معدومًا[٢١].

وعلى ذلك، يجب أن يكون لمعالجة البيانات الحساسة غرضاً محدداً، ويقع كذلك ضمن نطاق الاستثناءات التي قررتها اللائحة العامة لحماية البيانات والقوانين الوطنية المنظمة لحماية البيانات، فيعد تحديد الغرض أمرًا أساسيًا، لأنه هو الذي سيحدد معالجة البيانات الشخصية مثل معالجة إدارة العملاء، الرقابة في مكان العمل، مكافحة الاحتيال،

(21) Le Groupe 29 (Opinion 03/2013 on purpose limitation, WP 203, 2 avril 2013, p. 15.

العلاقات العامة، أمن الممتلكات والأشخاص، الرعاية الصحية، وغيرها، والسماح للشخص المعني بالتحكم في مصير البيانات المتعلقة به(٢٢).

وإذا كان وجوب تحديد غرض معالجة البيانات الحساسة يمثل إحدى القيود القانونية بهدف توفير الحماية لهذه البيانات، إلا أنه في مجال الاستدلالات تظهر الاشكالية بشكل مختلف، فدائماً ما تستند عمليات الاستدلالات لأغراض مشروعة، خاصة في ظل ما يعرف باقتصادات البيانات، وظهور الشركات التكنولوجية الكبري، وما تضيفه من قيمة كبري للاقتصاد القومي، بل وتحول الأمر عالمياً إلى حد اعتبار البيانات بمثابة سلعة يمكن الاتجار فيها.

ومن الجدير بالذكر أن عمليات معالجة البيانات لم تعد تتسم بالشكل التقليدى والذي تم تنظيمه بقوانين حماية البيانات، عالمياً ومحلياً، بل أصبح الحصول على البيانات (مدخلات عملية الاستدلال) يتسم بالسهولة واليسر خاصة في ظل انتشار وسائل التواصل الاجتماعي، وتقنيات الذكاء الاصطناعي، وكاميرات المراقبة، بل وأصبح الحديث كذلك عن أجهزة وتقنيات السيارات ذاتية القيادة، وجميعها تمثل وسائل متقدمة يمكن من خلالها الحصول على العديد من البيانات والمعلومات بل وبعضها لا يخضع للحماية القانونية.

كما يتم استخدام التكنولوجيا المتطورة في عمليات الاستدلال للوصول للبيانات المستنتجة الحساسة، بل وكذلك لانشاء ملفات تعريف شخصية وجماعية.

---

(22) M.-H. Boulanger et al., « La protection des données à caractère personnel en droit communautaire », J.D.E., 1997, p. 377 ;& M. Van Overstraeten et S. Depré, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », Rev. trim. dr. h., 2003, p. 685 et 686.

وكما أشرنا في أكثر من موضع إلى أن الاهتمام القانوني كان دائماً ببيانات المدخلات دون إعطاء المخرجات والبيانات المستنتجة لذات الأهمية.

وإذا كان يتطلب في غرض المعالجة أن يكون دقيقًا بحيث يسمح لصاحب البيانات بممارسة الحقوق التي يمنحها له القانون، كما سيسمح ذلك أيضًا لمراقب البيانات بتحديد البيانات التي يجب جمعها ومعالجتها، كما يجب أن تكون البيانات التي تتم معالجتها ذات صلة بالغرض، إلا أن ذلك يرتبط ارتباطاً وثيقاً بالبيانات الحساسة التى يتم جمعها من صاحب البيانات شخصياً، ولا يمتد نطاقه للبيانات المرصودة أو البيانات التى يمكن الوصول إليها بشكل مباشر أو غير مباشر من قبل القائمين على عمليات الاستدلالات.

وفي هذا السياق، فإن الالتزامات المقررة بقانون حماية البيانات المصري على عاتق كلاً من المتحكم والمعالج، ينظم فيها المشرع العلاقة بين صاحب البيانات والمتحكم والمعالج لها حين يتم تلقي المتحكم للبيانات من قبل الشخص المعني بها، حيث يلتزم المتحكم[٢٣] التأكد من صحة البيانات ومدى اتفاقها وكفايتها للغرض المحدد لجمعها، وفي إطار الغرض المحدد للمعالجة يلتزم بوضع طريقة وأسلوب ومعايير المعالجة، مع ضرورة التأكد من انطباق غرض المعالجة مع البيانات التي تم جمعها، وعدم القيام بأي عمل إيجابي أو سلبي من شأنه إتاحة البيانات في غير الأحوال المصرح بها قانوناً[٢٤].

(٢٣) يعرف المتحكم بكونه أي شخص طبيعي أو اعتباري، يكون له بحكم أو طبيعة عمله الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها ، أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه. (المادة (١) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية).

(٢٤) المادة (٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

كما يلتزم معالج البيانات[٢٥] في إجراء المعالجة وتنفيذها بالتقيد التام بالقواعد القانونية المنظمة لذلك[٢٦]، كما يتم التقيد بالحالات القانونية لإجراء المعالجة، وخاصة ما يتعلق بنطاق العملية وموضوعها وطبيعتها ونوع البيانات واتفاقها وكفايتها مع غرض المعالجة، ويجب أن تكون أغراض المعالجة وممارستها مشروعة ولا تخالف النظام العام والآداب، وعدم تجاوز حدود غرض المعالجة ومدته، كما لا يجوز أن يكون غرض المعالجة متعارضاً مع غرض المتحكم أو نشاطه ويستثنى من ذلك الغرض الإحصائي والتعليمي الذي لا يهدف لتحقيق الربح وبشرط عدم الإخلال بحرمة الحياة الخاصة.

علاوة على ذلك، يجب تقديم هذه المعلومات بلغة يفهمها المستخدم، ومع ذلك، فإن قراءة العديد من "سياسات الخصوصية" توضح أن اللغة المستخدمة في العديد من الدول هي اللغة الإنجليزية على الرغم من أن المعالجة تتعلق ببيانات من أشخاص ليس لديهم معرفة جيدة بهذه اللغة، وبالتالي فإن العملاء الذين لا يجيدون اللغة الإنجليزية سوف يفوتون بعض المعلومات التي تعتبر مع ذلك ضرورية لإعطاء الموافقة المستنيرة[٢٧].

لذلك من الضروري يجب أن يكون مراقب البيانات منتبهًا للجمهور الذي يستهدفه من أجل تكييف اللغة المستخدمة من حيث المعلومات.

---

(٢٥) يعرف معالج البيانات بأنه أي شخص طبيعي أو اعتباري مختص، بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه، أو لصالح المتحكم بالاتفاق معه ووفقاً لتعليماته. (المادة (١) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية).

(٢٦) المادة (٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(27) J.-M. Van Gyseghem, « L'économie collaborative et la protection des données : quel partage de données ? », Aspects juridiques de l'économie collaborative, Limal, Anthemis, 2017, p. 251-275

ويجب أن يكون الغرض أيضًا صريحًا، أي أنه يجب الإعلان عنه بشكل لا لبس فيه، وعدم إبقائه سريًا أو غامضاً[٢٨].

ويمكن النظر في غرض المعالجة في مجال الاستدلالات من منظرو آخر، وهو نية القائمين على الاستدلالات، وكما أشرنا من قبل، فإنه يجب لإصباغ الصفة الحساسة على بيانات المدخلات –إذا تم الاستدلال منها على بيانات حساسة- أن تتجه نية مراقبو البيانات أو المتحكمين فيها لغرض استنتاج بيانات حساسة، وهو الأمر الذي يستلزم معه ضرورة إعلام أصحاب البيانات به، وبشكل صريح لا لبس فيه ولا غموض.

وعلى الرغم من وجاهة السمات التى يجب أن يتسم بها غرض معالجة البيانات الحساسة، إلا أنه في ظل عدم التنظيم التشريعي الواضح والصريح لعمليات الاستدلالات ستظل هناك الكثير من العقبات والتى ينبغي على المشرع ضرورة مواجهتها والتغلب عليها بنصوص واضحة تحقق التوازن بين حقوق أصحاب البيانات، وتشجيع الابتكارات في عالم التكنولوجيا المتطورة والاستدلالات.

الفرع الثاني

مدى جواز قيام معالجة البيانات الحساسة والاستدلال عليها لغرض المصالح المشروعة

يجب أن تستند معالجة البيانات الحساسة لأساس قانوني، ومع ذلك يوجد إغفال ملحوظ من القواعد المتعلقة بمعالجة البيانات الحساسة وهو المعالجة بغرض المصالح

(28) C. de Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », Cabinet d'avocats et technologies de l'information : balises et enjeux, coll. Cahiers du CRID, no 26, Bruxelles, Bruylant, 2005, p. 157.

المشروعة، وبالتالي، من الناحية العملية، فإن الفرق الرئيسي بين البيانات الشخصية والبيانات الحساسة- وفقاً للائحة العامة الأوروبية لحماية البيانات الشخصية- هو أنه لا يمكن استخدام أساس المصالح المشروعة كأساس قانوني لمعالجة البيانات الحساسة وفقاً للائحة الأوروبية العامة لحماية البيانات.

وتعد عدم القدرة على معالجة البيانات الحساسة للمصالح المشروعة قيدًا كبيرًا، لأن المصالح المشروعة هي مبرر يستخدم بشكل متكرر لمعالجة البيانات دون موافقة صاحب البيانات.

بينما تعد الأسس القانونية الأخرى لمعالجة البيانات دون موافقة ضيقة إلى حد ما، مما يجعل المصالح المشروعة هي الأساس المفضل للاستخدام، وبشكل عملي ترغب العديد من الشركات في استخدام البيانات الشخصية للتسويق أو تحقيق الدخل أو التأثير أو الإقناع، وهذه الأسباب لا تتناسب مع الأسس القانونية الأخرى لمعالجة البيانات الحساسة(٢٩).

وبخلاف الحصول على موافقة صريحة، وهو الأمر الذي قد يكون صعبًا للغاية، فإن الطريقة الرئيسية للمعالجة هي من خلال الأساس القانوني للمصالح المشروعة والذي لم يتم النص عليه بموجب اللائحة العامة لحماية البيانات.

وحسناً ما فعله المشرع الأوروبي من عدم تقرير استثناء معالجة البيانات الحساسة لغرض المصالح المشروعة، نظراً لحساسية هذا النوع من البيانات والتي توصف بفئات خاصة من البيانات، ولما يمكن أن يسفر عنه معالجة البيانات الحساسة من تعارض مع استخدام معيار المصالح المشروعة.

(29) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081.

كما أن معيار المصالح المشروعة معياراً مرناً وواسعاً، وقد يهدف بشكل رئيس لاستخدامه في الممارسات التجارية والمالية والتي تتعارض بشكل جوهري مع طبيعة البيانات الحساسة وكذلك الحقوق الأساسية للأفراد، وما يمكن أن تشكل معه انتهاكاً للحياة الخاصة للأفراد.

ولم يكن المشرع المصري ببعيد عن هذا النهج، فلم يقرر المشرع ضمن نطاق حالات المعالجة الالكترونية المشروعة حالة المعالجة لمصالح مشروعة[٣٠]، وهو اتجاه حسن للقانون المصري بعدم تقريره، لما قد يمثله من فتح الاجتهاد بشأنه وإمكانية التوسع في مفهوم المصالح المشروعة بما قد يتعارض مع الحقوق الأساسية للأشخاص.

وعلى الرغم من وجاهة كل الأسانيد التى تدعم عدم اعتبار المصالح المشروعة أساساً لمعالجة البيانات الحساسة، إلا أن معيار المصالح المشروعة قد يكون المعيار الأساس في عمليات الاستدلال، وهو ما يظهر التناقض الكبير بين المعالجة التقليدية للبيانات الحساسة، والاستدلالات على هذه البيانات، وكما ذكرنا من قبل، فإن القائمين على عمليات الاستدلال يمكنهم التغلب على العديد من القيود القانونية المقررة على معالجة البيانات الحساسة، خاصة إذا لم تكن البيانات الحساسة هى المحل المعتمد عليه في بيانات المدخلات، بل تم الاعتماد على بيانات شخصية، أو عادية، أو مجهولة المصدر، وغالباً ما تكون البيانات الحساسة هى النتيجة التى يتم التوصل إليها من خلال الاستنتاجات والاستدلالات خاصة في عصر البيانات الضخمة، وهو ما لا يتوافر معها تقرير الحماية الفاعلة لهذه البيانات باعتبارها بيانات مستنتجة في ظل عمليات الاستدلال.

(٣٠) المادة (٦) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

وسيواجه المشرع صعوبات في ضرورة التوفيق بين المصالح المتعارضة بين حقوق أصحاب البيانات، وحقوق القائمين على الاستدلالات سواء من الناحية الاقتصادية أو كذلك من ناحية تشجيع الابتكار والتقدم.

وعلى ذلك، فإن معيار المصالح المشروعة لا يعد أساساً مقبولاً بغرض معالجة البيانات الحساسة، وإن كان مع ذلك، واقعياً، يعد معياراً أساساً تقوم عليه عمليات الاستدلالات.

المطلب الثالث

متطلبات الموافقة في مجال الاستدلال على البيانات الحساسة

بموجب القواعد العامة لحماية البيانات، لا يمكن جمع البيانات الحساسة أو معالجتها دون أساس قانوني، أي سبب مسموح به ومحدد في القانون.

وتعتبر الموافقة إحدى المتطلبات الأساسية لامكانية جمع ومعالجة البيانات الحساسة، وتبدأ الحماية القانونية المشددة للبيانات الحساسة منذ لحظة جمعها ووصولاً لمعالجتها وإتاحتها، حتى لو كانت المعالجة لا تستهدف البيانات الشخصية للعنصر الحساس الذي تحتوي عليه.

وتظهر الموافقة لإمكانية جمع ومعالجة البيانات الحساسة من خلال توافرين أمرين مجتمعين، وهما: أولاً: ضرورة الحصول على ترخيص من مركز حماية البيانات الشخصية، وثانياً: موافقة الشخص المعني بالبيانات.

ونعرض للأمرين فيما يلي، مع بيان تطلب خضوع عمليات الاستدلال على البيانات الحساسة لمتطلبات الموافقة.

الفرع الأول

ضرورة حصول المتحكم أو المعالج على

ترخيص من مركز حماية البيانات الشخصية

بالنظر للطبيعة الخاصة للبيانات الحساسة، فقد أورد المشرع قيوداً متعددة لإمكانية جمع وتخزين ونقل ومعالجة وإتاحة هذا النوع من البيانات.

ويعد أول هذه القيود، متمثلاً في أنه قيد إجرائي، بل وكذلك التزام على عاتق كلاً من المتحكم أو المعالج للبيانات، سواء أكان شخصاً طبيعياً أو اعتبارياً، ويتمثل في ضرورة حصول المتحكم أو المعالج على ترخيص أو تصريح من مركز حماية البيانات الشخصية للتعامل مع هذه البيانات(٣١).

كما أورده المشرع كالتزام قانوني ضمن التزامات المتحكم، وعلى ذلك، يقع على عاتق المتحكم في البيانات عبء إثبات استيفائه للقيد الإجرائي، فيجب عليه إثبات حصوله على ترخيص أو تصريح من مركز حماية البيانات قبل القيام بأي عمل يتعلق بالبيانات الحساسة(٣٢).

كما أن عبء الإثبات هنا أعم وأشمل، حيث يمتد كذلك لإثباته تنفيذ كافة الالتزامات المقررة قانوناً عليه بموجب قانون حماية البيانات الشخصية، وبما يمكن معها مركز حماية البيانات من اتخاذ إجراءات الرقابة والتفتيش(٣٣).

---

(٣١) المادة (١٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.
(٣٢) المادة (١٠/٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.
(٣٣) المادة (١٢/٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

كما يمتد هذا الالتزام ليقع على عاتق كل متحكم، وذلك في حالة التعدد، حيث يلتزم كل منهم بجميع الالتزامات القانونية المقررة، ويحق للشخص المعنى بالبيانات ممارسة حقوقه تجاه كل متحكم على حدة.

كما يقع على عاتق معالج البيانات –إذا كان شخص آخر غير المتحكم- الالتزام بضرورة الحصول على ترخيص أو تصريح من مركز حماية البيانات قبل القيام بأي عمل يتعلق بالبيانات الشخصية الحساسة[٣٤].

كما قرر المشرع جزاءاً جنائياً يتمثل في عقوبة الغرامة، يتم توقيعه على كلاً من المتحكم والمعالج، إذا قام أياً منهما بمخالفة القيد الإجرائي في الحصول على ترخيص أو تصريح من مركز حماية البيانات قبل التعامل بأي شكل مع البيانات الحساسة[٣٥]، وبطبيعة الحال عدم الإخلال بحق صاحب البيانات المضرور من الرجوع بأحكام المسئولية المدنية.

ونشير هنا إلى أن هذا القيد الإجرائي بضرورة الحصول على موافقة مسبقة من مركز حماية البيانات الشخصية إنما يتعلق بحالات التعامل مع البيانات الحساسة، وهو مجال لا يتوافر بشكل كبير في مجال عمليات الاستدلالات.

ونوضح ذلك بأن ضرورة استيفاء القيد الإجرائي إنما يتعلق ببيانات المدخلات إذا كانت تتضمن بيانات ذات طبيعة حساسة (وفق تعداد البيانات الحساسة المقررة على سبيل الحصر)، بينما لا يمتد نطاق هذا القيد للبيانات التى لا تحوى عنصراً حساساً، أو التى يمكن التوصل من خلالها لبيانات حساسة، وهو ما يتضح من صريح نص المادة

(٣٤) المادة (١١/٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.
(٣٥) المادة (٣٨) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(١٢) من قانون حماية البيانات الشخصية المصري حيث قرر " يحظر على المتحكم أو المعالج ... جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز".

ويفهم من ذلك أن محور الحماية –المتطلب له القيد الإجرائي- هو كل العمليات القائمة على البيانات الحساسة، أي باعتبارها بيانات حساسة من البداية، وعلى العكس من ذلك، فإن عمليات الاستدلالات –محور حديثنا- يتم من خلالها التوصل لبيانات حساسة كبيانات مستخرجة أو مستنتجة تم الاستدلال عليها، وهو ما يمثل معه ظهور خلل تشريعي في تقرير حماية البيانات المستنتجة وخاصة منها البيانات الحساسة.

الفرع الثاني

موافقة الشخص المعني بالبيانات

يستوجب القانون العام لحماية البيانات (GDPR) بشكل جوهري ضرورة وجود أساس قانوني سواء لمعالجة البيانات الشخصية أو كذلك لمعالجة البيانات الحساسة.

وتعد موافقة الشخص المعني هي الأساس القانوني لمعالجة البيانات الشخصية والبيانات الحساسة، وهي مظهر من مظاهر التعبير عن إرادة الشخص المعنى بالبيانات، وكما يشير البعض –بحق- أن رضاء صاحب البيانات يعد حجر الأساس في حماية البيانات الشخصية، حيث يعد أهم الأدوات التشريعية للتيقن من صحة ومشروعية عمليات جمع ومعالجة البيانات، ولا يمكن الاستعاضة عن موافقة المعنى بالبيانات إلا في حالات استثنائية مقررة على سبيل الحصر[٣٦].

(٣٦) د. تامر محمد الدمياطي، الرضا الرقمي بمعالجة البيانات الشخصية دراسة مقارنة، مجلة القانون والتكنولوجيا، الجامعة البريطانية، كلية القانون، عدد (١)، مجلد (٢)، ٢٠٢٢، ص ١٨.

وبموجب اللائحة العامة لحماية البيانات، يجب أن تكون الموافقة مؤشرًا محددًا ومستنيرًا لا لبس فيه لرغبات صاحب البيانات، والذي يشير من خلال بيان أو عمل إيجابي واضح، إلى الموافقة على معالجة البيانات المتعلقة به(٣٧).

وتقرر الفقرة الثانية من المادة التاسعة من اللائحة الأوروبية العامة لحماية البيانات أنه يجوز معالجة بيانات محددة إذا أعطى صاحب البيانات موافقة صريحة على معالجة هذه البيانات الشخصية لواحد أو أكثر من الأغراض المحددة(٣٨).

ومع ذلك، فإن اللائحة العامة لحماية البيانات أزالت بشكل أساس أي اختلاف ذي معنى بين طبيعة الموافقة المطلوبة بالنسبة للبيانات الشخصية مقابل البيانات الحساسة(٣٩).

بالإضافة إلى ذلك، لا يسمح القانون العام لحماية البيانات (GDPR) للدول الأعضاء بإضافة المزيد من الحماية للبيانات الحساسة باستثناء البيانات الجينية والبيولوجية والصحية(٤٠).

(37) GDPR, art. 4(11).'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

(38) GDPR, art. 9(2- a), " the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject".

(39) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1601.

(40) GDPR, art 9(4).

كما قرر المشرع المصري صراحة ضرورة الحصول على موافقة كتابية وصريحة من الشخص المعني بالبيانات، وهى شرط متطلب ولازم قبل إجراء جمع وتخزين ونقل ومعالجة وإتاحة البيانات الشخصية الحساسة، وإذا كانت أي عملية من هذه العمليات تتعلق ببيانات الأطفال فيلزم موافقة ولي الأمر(٤١).

كما اعتبر المشرع المصري أن المعالجة الالكترونية تكون مشروعة وقانونية(٤٢) في عدة حالات، منها: موافقة الشخص المعنى بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر(٤٣).

وتجدر الملاحظة في هذا الشأن أن المشرع حين تطلب الموافقة لجواز معالجة البيانات الشخصية قد وصفها بضرورة الموافقة الصريحة، بينما تشدد، بعض الشيء، في مجال الموافقة المتطلبة لأي عمل يتعلق بالبيانات الحساسة حيث تطلب أن تكون موافقة صريحة وكتابية(٤٤).

وبهدف تحقيق تنظيم أكثر دقة في ضرورة استيفاء متطلب الموافقة على معالجة البيانات الشخصية الحساسة جعل المشرع المصري الموافقة أمر لازم لتحقق مشروعية عملية المعالجة، ويعد التحقق من موافقة الشخص المعنى بالبيانات التزام على عاتق معالج البيانات(٤٥)، كما تعد التزام على عاتق المتحكم في البيانات حيث لا يجوز للمتحكم

(٤١) المادة (١٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(٤٢) ويمكن انتقاد صياغة المشرع المصري بصدد المادة (٦) من قانون حماية البيانات حيث تنص على" تعد المعالجة الالكترونية مشروعة وقانونية في حال توافر إحدى الحالات الآتية ..."، حيث يمكن اعتبار كل معالجة قانونية هي معالجة مشروعة، وهو ما يمكن اعتباره تكراراً لا معنى له.

(٤٣) المادة (١/٦) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(٤٤) المادتين (٢، ١٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(٤٥) المادة (١/٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

الحصول على البيانات الشخصية الحساسة أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها إلا بعد الحصول على موافقة الشخص المعنى أو في الأحوال المصرح بها قانوناً[٤٦].

ولكي تكون الموافقة صالحة، يجب أن يتم منحها بحرية كاملة وإرادة واعية دون أي ضغط وهى ما تعرف بالموافقة الحرة، مع ضرورة المعرفة الكاملة بالحقائق فيما توصف الموافقة بكونها مستنيرة، وأن تتم الموافقة بطريقة محددة وليست عامة (الموافقة المحددة).

وكما يشير البعض[٤٧] إلى أنه إذا كان التعريف الوارد باللائحة العامة لحماية البيانات أكثر دقة، ومع ذلك يظل من غير المؤكد أنه يجلب مستوى إضافيًا حقيقيًا من المتطلبات، حيث يصعب إثبات مفاهيم مثل: "مستنيرة وغير غامضة"، حتى لو كان عبء الإثبات يقع على عاتق الشخص المسئول عن العلاج، فإن الحاجة إلى "إعلان أو عمل إيجابي واضح" ينبغي أن تجعل من الممكن ضمان حقيقة حدوث الرضا بشكل أفضل.

ويلاحظ هنا أنه إذا تم إعطاء موافقة صاحب البيانات في سياق إعلان مكتوب يتعلق أيضًا بمسائل أخرى بجانب الموافقة، أي أن بند الموافقة كان وارداً ضمن بنود أخري، فيجب تقديم بند الموافقة بطريقة يمكن تمييزها بوضوح عن الأمور الأخرى، وفي شكل واضح وسهل الوصول إليه، باستخدام لغة بسيطة وواضحة، وأي إخلال بذلك

(٤٦) المادة (١/٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(47) Céline Castets-Renard , Brève analyse du règlement général relatif à la protection des données personnelles, Dalloz, IP/IT, 2016, p. 331.

الأمر، أو كانت الموافقة بغير هذه الطريقة، فلا يعتد بها، ولا تكون ملزمة لصاحب البيانات من الناحية القانونية[٤٨].

وعند تقييم ما إذا كانت الموافقة تم منحها بحرية من قبل صاحب البيانات، يجب الأخذ في الاعتبار ما إذا كان تنفيذ العقد، بما في ذلك تقديم الخدمة، مشروطًا بالموافقة على معالجة البيانات الشخصية التي ليست ضرورية لتنفيذ ذلك العقد[٤٩].

كما يقرر القانون العام لحماية البيانات جواز سحب الموافقة المقدمة من صاحب البيانات في أي وقت، ولا يؤثر سحب الموافقة على مشروعية المعالجة التي تمت بناءً على الموافقة قبل سحبها، ويجب إبلاغ صاحب البيانات بذلك، كما يجب أن تكون عملية سحب الموافقة سهلة مثل إعطاء الموافقة[٥٠].

ويقع التزام على عاتق مراقب البيانات بإثبات قيام الشخص المعنى بإعطاء موافقته على معالجة البيانات الشخصية[٥١]، ويجب أن يكون لدى وحدة التحكم في عملية المعالجة إعلان صريح من صاحب البيانات بالموافقة، قد يأخذ ذلك شكل مربع لجمع الموافقة تم إعداده خصيصًا لمعالجة البيانات الحساسة، أو إعلان كتابي موقع من الشخص المعني أو إرسال بريد إلكتروني، مغطى على سبيل المثال بتوقيع إلكتروني أو مصحوبة برسالة تأكيد بالبريد الإلكتروني أو حتى جهاز تحقق آمن (رابط التحقق أو

(48) GDPR, art. 7(2).
(49) GDPR, art. 7(4).
(50) GDPR, art. 7(3).
(51) GDPR, art. 7(1).

رسالة نصية قصيرة تحتوي على رمز التحقق لتأكيد الموافقة)، كما يمكن أيضًا قبول مستند ممسوح ضوئيًا يحمل توقيع الشخص المعني(٥٢).

كما يلتزم معالج البيانات، وفقاً لأحكام القانون المصري، بتوفير الإمكانيات اللازمة لإثبات التزامه بتنفيذ المتطلبات القانونية في معالجة البيانات، كما يخضع لتفتيش ورقابة من قبل مركز حماية البيانات الشخصية للتأكد من تنفيذ التزاماته(٥٣).

وتعتبر هذه الشكلية المتطلبة للحصول على موافقة الشخص المعني مطلوبة في مواقف معينة حيث ينشأ خطر جسيم مرتبط بحماية البيانات الحساسة، وحيث يوجد مستوى عالٍ من التحكم في البيانات من قبل صاحب البيانات.

ومع ذلك، لم يعد هذا الاستثناء قادراً على الوفاء بالغرض من تقريره، وذلك عندما يكون مراقب البيانات هو صاحب العمل الحالي أو المحتمل لصاحب البيانات، أو عندما يكون صاحب البيانات في حالة اعتماد على مراقب البيانات مما يمنعه من رفض الموافقة الحرة.

وفي حالة إخلال المتحكم أو المعالج للبيانات الحساسة بالحصول على موافقة كتابية وصريحة من الشخص المعني بالبيانات، فقد قرر المشرع المصري جزاءاً جنائياً يتمثل في عقوبتي الحبس والغرامة أو أياً منهما يتم توقيعها على المخالف(٥٤)، مع عدم الإخلال بحق المضرور بالرجوع بالمسئولية المدنية، وكذلك حق مركز حماية المعلومات في تطبيق الجزاءات الإدارية.

---

(52) Christiane Féral-Schuhl, Les données à caractère personnel, Livre 1, Dalloz, 2020-2021.

(٥٣) المادة (١٠/٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(٥٤) المادة (٤١) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

وعلى الرغم من التشدد التشريعي في ضرورة استيفاء موافقة الشخص المعني بالبيانات، إلا أنه في مجال الاستدلالات على البيانات الحساسة قد لا يتطلب هذا الأمر من الناحية القانونية، وفق القواعد المعمول بها حالياً.

وتوضيح ذلك أنه غالباً ما تخضع عمليات جمع ومعالجة البيانات الحساسة لعلاقات عقدية، وهو ما يستوجب ضرورة توافر الرضا والموافقة بشكل واضح وصريح من قبل الشخص المعني بالبيانات، وتحظى المصادر التعاقدية بمكانة مرموقة، حيث يتطلب التنظيم إبرام عقد أو اعتماد بنود تعاقدية موحدة في حالة التعاقد من الباطن، ومع ذلك فإن هذا العقد يخضع لقواعد تنظيمية صارمة(٥٥)، مما يزيد من تقليص دور الإرادة في الحرية التعاقدية(٥٦).

بينما قد تقوم عمليات الاستدلالات على بيانات غير خاضعة للحماية القانونية المقررة بتشريعات حماية البيانات، مثل البيانات العادية أو مجهولة المصدر، مما يتطلب معها ضرورة استيفاء قيد الموافقة بشكل مسبق، كما قد يرجع السبب في عدم معرفة نتيجة الاستدلالات وما تسفر عنه من نتائج بشكل مسبق، حتى ولو تم التوصل بعد ذلك لبيانات حساسة من خلال تلك الاستدلالات.

(55) GDPR, art. 28.

(56) Céline Castets-Renard , Brève analyse du règlement général relatif à la protection des données personnelles, Dalloz, IP/IT, 2016, p. 331.

المبحث الثاني

تقرير الحماية القانونية في مجال الاستدلالات

يوجد اختلافات كبيرة في الأطر القانونية المنظمة لحماية البيانات الشخصية حول حقوق أصحاب البيانات التي تنطبق على الاستدلالات.

ويظهر ذلك من خلال اللائحة العامة لحماية البيانات[٥٧]، والمبادئ التوجيهية بشأن توفير المحتوى الرقمي[٥٨]، وقانون حماية البيانات الشخصية المصري[٥٩]، ولا توفر هذه الأطر حماية كافية لأصحاب البيانات ضد الاستدلالات.

ونعرض من خلال هذا المبحث للحماية القانونية لبيانات عملية الاستدلال وهو ما سنوضحه في المطلب الأول، ثم نعرض في المطلب الثاني لحقوق أصحاب البيانات في مواجهة عمليات الاستدلالات على البيانات الحساسة.

---

(57) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119).

(58) Report on the Proposal for a Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content, Nov. 27, 2017, Eur. Parl. Doc. A8-0375/2017, http://www.europarl.europa. eu/ sides /getDoc.do?pubRef=-//EP//NONSGML+REPORT+A8-2017-0375+0+DOC+PDF+V0//EN [https://perma.cc/DL8P-TBEN].

(٥٩) القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

المطلب الأول

الحماية القانونية لبيانات عملية الاستدلال

تعتمد عمليات الاستدلالات على نوعين من البيانات وهما البيانات المدخلة، والبيانات المستنتجة، وغالباً ما يتم التركيز في قوانين حماية البيانات على البيانات المدخلة من خلال تقرير الحماية القانونية، على الرغم من الخطورة البالغة للبيانات المستنتجة خاصة إذا تم التوصل لبيانات حساسة.

ومن الجدير بالملاحظة، في هذا الصدد، أن الحماية الخاصة للبيانات الحساسة واضحة في اللائحة العامة لحماية البيانات والتشريعات المقارنة في العديد من الدول، إلا أن المدى الذي يمكن عنده تصنيف الاستنتاجات على هذا النحو ليست كذلك.

وبموجب القوانين المنظمة لحماية البيانات الشخصية، تعتبر الاستنتاجات التي تؤدى للوصول أو الكشف عن بيانات حساسة بمثابة بيانات حساسة، ومؤدى ذلك أن أي بيانات شخصية يمكن استنتاج بيانات حساسة منها سيتم اعتبارها أيضًا بيانات حساسة.

ويمكن الاعتداد بمعياري الغرض من المعالجة، وكذلك سياق المعالجة في مجالات الاستدلال على البيانات الحساسة، مما مؤداه ضرورة اعتبار الاستدلالات على البيانات الحساسة وكأنها بيانات حساسة، وتكون حمايتها مرتبطة بالسياق والغرض من معالجتها، حيث إنه عادة ما تكون أقل من حيث الحماية من البيانات الحساسة المقدمة من صاحب البيانات.

وبالنظر إلى التعريف الوارد للبيانات الحساسة سواء باللائحة العامة أو التشريعات المقارنة فإن الجنس والعمر والمعلومات المتعلقة بالوضع المالي للشخص

والموقع الجغرافي والملفات الشخصية لا تعتبر بيانات حساسة، على الرغم من أنها غالبًا ما تكون أساسًا للتمييز[٦٠]، أي يمكن أن يتوافر بشأنها العنصر الحساس للبيانات في إطار غرض وسياق المعالجة.

كما تعتبر البيانات القابلة للتعريف بشخص ما بمثابة بيانات شخصية بموجب تعريفات العديد من قوانين حماية البيانات، وبشكل أساسي، يمكن التعرف على البيانات غير المحددة عندما يمكن إجراء استنتاجات حولها من خلال ربطها ببيانات أخري يمكن من خلالها التعرف على شخص معين، وينطبق نفس المبدأ على البيانات الحساسة.

ويشير البعض إلى أن الاستدلالات على البيانات الحساسة يمكن فهمها من خلال تعريف "الفئات الخاصة أو الحساسة من البيانات الشخصية"، حيث تشير عبارة "الكشف عن البيانات الشخصية" إلى أن التعريف يهدف إلى تغطية البيانات التي تكشف بشكل مباشر أو غير مباشر عن السمات المحمية[٦١].

(60) Article 29 Data Prot. Working Party, Advice Paper on Special Categories of Data ("Sensitive Data"), at 10, Ares(2011)444105-20/04/2011 (2011), https://ec. europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_mme_le_bail_directive _9546ec_annex1_en.pdf [https://perma.cc/FV7G-VVS4].

(61) Sebastian Schulz, Verarbeitung besonderer Kategorien personenbezogener Daten, in Datenschutz-Grundverordnung VO (EU) 2016/679, 2017, p. 11-12

كما أن تعريف الفئات الخاصة (الحساسة) لا يشمل "فقط البيانات التي تحتوي بطبيعتها على معلومات حساسة ولكن أيضًا البيانات التي تحتوي على معلومات حساسة فيما يتعلق بالفرد الذي يمكن التوصل إليه"(٦٢).

وبالتمييز القائم نوعياً بين البيانات الشخصية والحساسة، فإن عتبة جمع ومعالجة البيانات الحساسة مرتفعة نسبيًا بالمقارنة بالبيانات الشخصية العادية.

ولا شك أن طلبات معرفة الاستدلالات ونقلها وتصحيحها وحذفها تتطلب تحقيق توازن بين مصالح أصحاب البيانات ووحدات التحكم.

وبموجب اللائحة العامة لحماية البيانات والتشريعات الوطنية، تعتبر البيانات التي يمكن أن تؤدي إلى استنتاجات حول البيانات الحساسة بيانات حساسة أيضًا(٦٣).

(62) Article 29 Data Prot. Working Party, Advice Paper on Special Categories of Data ("Sensitive Data"), at 10, Ares(2011)444105-20/04/2011 (2011), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [https://perma.cc/FV7G-VVS4].

(63) Article 29 Data Protection Working Party, Advice Paper on Special Categories of Data ("Sensitive Data"), at art. 8(1) (2011), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf [https://perma.cc/R53R-NXVK] (noting that sensitive data includes "not only data which by its nature contains sensitive information . . . but also data from which sensitive information with regard to an individual can be concluded").

كما يمكن من خلال عمليات المعالجة الالكترونية لمجموعة من البيانات، حتى ولو كانت لا تحتوى على عنصر حساس، أن تؤدى للوصول لبيانات حساسة.

ومن الممكن اليوم التوصل إلى استنتاجات حول البيانات الحساسة من العديد من الأنواع المختلفة من البيانات غير الحساسة التي تهدد البيانات الحساسة بتوسيعها، بل سيمكن مستقبلاً تحقيق المزيد، وكما يشير البعض[٦٤] أي أنه "بمرور الوقت ونظرًا لتحليل البيانات الضخمة، يتزايد حجم "الفئات الخاصة".

وذكر المجلس الأوروبي لحماية البيانات (EDPB) أنه يمكن أن يؤدي التوصيف إلى إنشاء بيانات فئة خاصة عن طريق الاستدلال من البيانات التي ليست بيانات فئة خاصة في حد ذاتها، ولكنها تصبح كذلك عند دمجها مع بيانات أخرى[٦٥].

وفي هذا الصدد، يمكن اعتبار أي بيانات طبية يمكن أن تؤدي إلى استنتاج "حول الحالة الصحية الفعلية أو المخاطر الصحية لشخص ما" تشكل بيانات صحية[٦٦].

(64) Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV., 2017, p. 1013.

(65) Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, at art. 9, 17/EN WP251rev.01 (2018), https://ec.europa.eu/newsroom/article29/items/612053/ en [https://perma.cc/YW6D-87ED].

(66) Annex Health Data in Apps and Devices, at 1, 2, Article 29 Data Protection Working Party, (2015), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_ letter_art29wp_ec_health_data_after_ plenary_annex_en.pdf [https://perma.cc/FZ4M-ULRE].

ويترتب على هذه النتيجة أن كل شيء تقريبًا يمكن أن يشكل بيانات صحية، حيث يمكن بسهولة استنتاج البيانات الصحية من أنواع أخرى لا حصر لها من البيانات غير الحساسة، وهو ما يشير له البعض من أن كل ما يفعله الناس ويشترونه ويأكلونه يمكن أن يؤثر على الصحة، وكذلك الجنس والعمر والانتماء العرقي والموقع(٦٧).

وفي ذات السياق، وباعتبار أن البيانات الصحية تعد بمثابة بيانات حساسة، وتخضع لقواعد مشددة بشأن حمايتها، فإنه وفقًا لتوجيهات الاتحاد الأوروبي، تتضمن البيانات الصحية بيانات "يمكن استخدامها بحد ذاتها، أو بالاشتراك مع بيانات أخرى، لاستخلاص استنتاج حول الحالة الصحية الفعلية أو المخاطر الصحية للشخص"(٦٨).

كما يمكن أن تتضمن كذلك بيانات حول شراء المنتجات، والأجهزة والخدمات الطبية، عندما يمكن استنتاج الحالة الصحية من خلال هذه البيانات.

وعلى الرغم من أن بعض البيانات، مثل الرمز البريدي، ليست حساسة بطبيعتها، فإنه يجب معاملتها على هذا النحو إذا كانت "تكشف بشكل غير مباشر" أو يمكن استخدامها لاستنتاج سمات حساسة(٦٩).

---

(67) Daniel J. Solove, REGULATING BASED ON HARM AND RISK INSTEAD OF SENSITIVE DATA, 118 Nw. U.L. Rev., 2024, p. 1081

(68) Annex Health Data in Apps and Devices, at 1, 2, Article 29 Data Protection Working Party, (2015), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_ letter_art29wp_ec_health_data_after_ plenary_annex_en.pdf [https://perma.cc/FZ4M-ULRE].

(69) Article 29 Data Prot. Working Party, Advice Paper on Special Categories of Data ("Sensitive Data"), at 6, Ares(2011)444105-20/04/2011 (2011), =

وبناء على ذلك، يجب أن يمتد نطاق الحماية المعززة للبيانات الحساسة لتشمل البيانات الحساسة بطبيعتها، وكذلك البيانات التى يمكن استخدامها بذاتها للتوصل لبيانات حساسة، أو البيانات التى يمكن ربطها من خلال بيانات أخري لاستنتاج بيانات حساسة.

وتأكيداً على ذلك، وفي مبدأ توجيهي آخر، أشارت فرقة عمل المادة ٢٩، التي سبقت EDPB أنه "قد يكون من الممكن استنتاج الحالة الصحية لشخص ما من سجلات تسوقه للأغذية، بالإضافة إلى البيانات المتعلقة بجودة الأطعمة ومحتوى الطاقة فيها"(٧٠).

وفي عام ٢٠٢٢، أقرت محكمة العدل الأوروبية (CJEU) أن البيانات التي تؤدي إلى استنتاجات حول البيانات الحساسة هي أيضًا بيانات حساسة بموجب اللائحة العامة لحماية البيانات GDPR (٧١).

كما أوضحت المحكمة أن نشر البيانات التي من شأنها الكشف ولو بشكل غير مباشر عن بيانات حساسة لشخص طبيعي يشكل معالجة فئات خاصة من البيانات الشخصية، لغرض تلك الأحكام.

=

https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_ artwp_mme_le_bail_directive _9546ec_annex1_en.pdf [https://perma.cc/FV7G-VVS4].

(70) Article 29 Data Protection Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, at art. 9, 17/EN WP251rev.01 (2018), https://ec.europa.eu/newsroom/article29/items /612053/en [https://perma.cc/YW6D-87ED].

(71) CJEU - C-184/20 - Vyriausioji Tarnybinės Etikos Komisija, 2022 E.C.R 117.

وعللت المحكمة ذلك بأن فعالية الحماية المشددة للبيانات الحساسة سوف يتم تقويضها إذا لم يتم تضمين البيانات التي تؤدي إلى استنتاجات حول البيانات الحساسة على أنها بيانات حساسة.

وتكمن الإشكالية هنا بشأن ما إذا كان ينبغي النظر إلى حساسية البيانات المستنتجة من عملية الاستدلال بشكل موضوعي بناءً على إمكانية عمل استنتاجات، أو بشكل شخصي بناءً على النوايا المعلنة لوحدة التحكم في البيانات.

ويشير البعض هنا إلى أن قانون الاتحاد الأوروبي غير متسق بشأن هذه المسألة، بل وأن كلا النهجين يحيطهما العديد من الصعوبات(٧٢).

وأشار البعض أن فريق عمل المادة ٢٩ لم يتناول المسألة بشكل مباشر، لكنها أدركت أن بعض أنواع البيانات يمكن تصنيفها بشكل موضوعي على أنها حساسة، بغض النظر عن نوايا أولئك الذين يسعون إلى معالجة البيانات(٧٣).

ونعتقد بأنه يمكن دمج المعيارين معاً، بهدف توسيع الحماية للبيانات الحساسة، أي أنه يستوى أن يتم الاستدلال على البيانات الحساسة بشكل موضوعي من خلال عمليات الاستدلال حتى ولو لم تكن نية المتحكم في البيانات قد اتجهت لذلك ومع ذلك تم التوصل إليها، ومن باب أولى كذلك إذا اتجهت نية المراقب أو المتحكم لاستنتاج بيانات حساسة بواسطة الاستدلالات.

(72) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p. 1591.

(73) Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, COLUM. BUS. L. REV., 2019, p. 494.

كما يجب أن تستند عملية الاستدلال لغرض محدد ومشروع، ويجب النص صراحة على الحالات التى يجوز من خلالها الاستدلال على البيانات الحساسة.

ويمكن تأكيد ذلك، وعلى سبيل المثال، المتطلبات المتعلقة بالاعتراض على المعالجة، قد يتم التغلب على الاعتراض استناداً لفكرة "المصالح المشروعة" لوحدة التحكم في البيانات من خلال الأسباب المشروعة المقنعة لوحدة التحكم(٧٤).

ولكن هذا ليس هو الحال بالنسبة للبيانات الحساسة، حيث لا يمكن أن تكون "المصالح المشروعة" لمراقب البيانات أو المتحكم بمثابة أساس قانوني لمعالجة البيانات(٧٥)، كما أن المشرعين لم يقرروا أساس المصالح المشروعة ضمن الأسس المقررة على سبيل الاستثناء لمعالجة البيانات الحساسة.

ولا تزال هناك استثناءات محتملة لمعالجة البيانات الحساسة مثل الموافقة الصريحة أو جعل صاحب البيانات بياناته عامة بشكل واضح لمعالجة البيانات الحساسة أو استخلاص استنتاجات حساسة بالطبع، ولكن بالمقارنة مع البيانات غير الحساسة، يتوفر طريق أقل لوحدات التحكم في الاعتماد على أساس قانوني لمعالجة البيانات الحساسة.

(74) Article 29 Data Prot. Working Party, Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller Under Article 7 of Directive 95/46/EC, 844/14/EN WP 217 (Apr. 9, 2014), https://ec.europa.eu/justice/article-29/ documentation /opinion-recommendation/files/2014/wp217_en.pdf [https://perma .cc/J3P5 -GUL2].

(75) Norbert Nolte & Christoph Werkmeister, Recht auf Loschung ("Recht auf Vergessenwerden"), in Datenschutz-Grundverordnung VO (EU) 2016/679, 2017, at 47-48

ويمكن تأييد ذلك ببيان مجلس حماية البيانات الأوروبي الذي أوضح فيه أن البيانات التي تكشف عن آراء سياسية يجب أن ينظر إليها على أنها بيانات فئة خاصة(٧٦).

كما شدد هذا البيان على أن حقيقة أن صاحب البيانات ربما جعل هذه البيانات متاحة للجمهور، والتي عادة ما تكون استثناء من المادة التاسعة من اللائحة العامة لحماية البيانات، لا يمكن استخدامها كمبرر لمعالجة البيانات على أساس "المصلحة المشروعة"، وبالتالي لا تجوز معالجتها دون موافقة صريحة، وشدد البيان أيضًا على ضرورة احترام مبادئ الشرعية والعدالة والشفافية.

ويمكن أن يجد هذا البيان أساساً قانونياً له من خلال القيود الواردة باللائحة العامة لحماية البيانات، وبصفة خاصة، إذا كانت عملية المعالجة تتم بصورة آلية(٧٧)، ولكن يظل هذا الأساس محدوداً بالقيود المتعلقة فقط بالمعالجة الآلية دون أن يمتد لما سواها.

وبناء على ذلك، ومن أجل تقرير حماية أكبر للبيانات الحساسة نوصي بتطبيق الحماية المعززة للبيانات الحساسة على الاستدلالات على أن تشمل هذه الحماية كلاً من:

أولاً: البيانات المستنتجة أو المشتقة بشكل مباشر والتي تكشف عن السمات المحمية -على سبيل المثال عندما يستنتج المعالج العرق لشخص ما من تاريخه التعليمي- فيجب التعامل معها على أنها بيانات حساسة.

(76) European Data Prot. Bd., Statement 2/2019 on the Use of Personal Data in the Course of Political Campaigns (Mar. 13, 2019), https://edpb.europa.eu/sites /edpb /files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf [https://perma.cc/5BS2-4VJE].

(77) GDPR, art art. 22.

هذا هو شكل مباشر من أشكال التطبيق حيث يتم التعامل مع الاستنتاجات بشكل لا يختلف عن البيانات الحساسة المقدمة من صاحب البيانات.

ثانيًا: البيانات الحساسة التي يمكن استنتاجها من البيانات الشخصية للسمات التي تم الكشف عنها بشكل غير مباشر، يمكن أيضًا التعامل مع بيانات المصدر التي يمكن استخلاص الاستدلالات الحساسة منها على أنها بيانات حساسة، على سبيل المثال الاسم الأخير أو مكان الميلاد لاستنتاج العرق أو الأصل.

ومن الجدير بالذكر أن التمييز بين نوعي البيانات الشخصية والحساسة أصبح متزايداً بشكل ملحوظ في عصر تحليلات البيانات الضخمة، حيث يبدو أن أي بيانات يمكن أن تصبح بيانات حساسة إذا أمكن العثور على طريقة لاستنتاج معلومات حول السمات المحمية منها(٧٨).

وبناء على ذلك، نستطيع القول أن تصنيف البيانات التي تؤدي إلى استنتاجات حول البيانات الحساسة على أنها حساسة هو النهج المتماسك، والمنطقي الذي يمكن لقوانين الخصوصية وحماية البيانات الشخصية إتباعه، وبخلاف ذلك، فإن حماية البيانات الحساسة لن يكون لها أي معنى، لأن الاستدلالات من البيانات غير الحساسة يمكن استخدامها بسهولة، مما يسمح بالابتعاد القيود المقررة بشكل مشدد لحماية البيانات الحساسة.

(78) Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 Seton Hall L. Rev, 2017, p. 995.

المطلب الثاني

تعزيز حقوق أصحاب البيانات في مجال الاستدلالات

بينا من قبل أن الاهتمام القانوني دائماً ما يتجه نحو بيانات المدخلات في عمليات الاستدلال، دون أن تحظى البيانات المستنتجة بذات الحماية، خاصة فيما يتعلق بالاعتراف بحقوق أصحاب البيانات على نتائج الاستدلالات.

ولذا فإننا نعرض من خلال هذا المطلب لضرورة تعزيز حقوق أصحاب البيانات، وبصفة خاصة حقوقهم على نتائج عمليات الاستدلال، بداية من الحق في معرفة الاستنتاجات، والحق في تصحيحها، والحق في المحو، وحق الطعن في القرارات المبنية على الاستدلالات.

الفرع الأول

الحق في معرفة الاستنتاجات

يتقرر حق الأفراد في معرفة الاستدلالات الناتجة عن استخدام بياناتهم الشخصية وما توصلت إليه نتائج هذه الاستدلالات من بيانات حساسة، ويمكن الاستناد في ذلك للشفافية الواجب توافرها في شأن عملية الاستدلالات.

ووفقاً للائحة العامة لحماية البيانات يجب على مراقب البيانات عندما يتم جمع البيانات الشخصية المتعلقة بصاحب البيانات أن يزود الأخير بالمعلومات المتعلقة بهوية مراقب البيانات، وتفاصيل الاتصال بمسئول حماية البيانات، والأغراض المستهدفة

لمعالجة البيانات الشخصية، وإذا كانت المعالجة بغرض المصالح المشروعة فيجب تزويد صاحب البيانات بهذه المصالح التي يسعى المراقب أو الطرف الثالث لتحقيقها[٧٩].

وبتطبيق ذلك على عملية الاستدلالات، فإن حقوق الشفافية ستُعلم أصحاب البيانات بوجود ومعالجة البيانات الشخصية المستنتجة والمشتقة، أو البيانات التي لم يقدمها صاحب البيانات بشكل مباشر[٨٠]، ويعد هذا النوع من الرقابة شرطًا أساسيًا لممارسة الحقوق الأخرى التي تمنحها القواعد العامة لحماية البيانات.

ومع ذلك فإنه من غير المرجح أن تحقق واجبات الإخطار الخاصة باللائحة العامة لحماية البيانات هذا الهدف[٨١].

وتحدد اللائحة العامة العديد من متطلبات الإخطار لمراقبي البيانات عندما يقومون بجمع البيانات الشخصية مباشرة من صاحب البيانات، في الوقت الذي يتم فيه جمع البيانات، حيث يجب على المراقب تزويد صاحب البيانات بمعلومات حول الأغراض التي ستتم معالجة البيانات من أجلها، وأي مستلمين محتملين من جهات خارجية أو فئة من المستلمين.

ولا شك أن هذا الأمر إنما يتعلق بالبيانات فقط المقدمة من صاحب البيانات، بما في ذلك البيانات المرصودة، بينما يمكن لعمليات الاستدلالات الاعتماد على بيانات غير مقدمة من ذوي الشأن، مثل البيانات العادية والبيانات مجهولة المصدر، كما أنه لا يمكن

(79) GDPR, art. 13(1).

(80)Article 29 Data Prot. Working Party, Guidelines on the Right to Data Portability, 16/EN, WP242rev.01, at 10 (Dec. 13, 2016), https://ec.europa.eu/newsroom /document.cfm?doc_id=44099

(81) GDPR, art.(13- 14).

تضمين البيانات المستنتجة أو المشتقة لاحقًا في الكشف عن موضوع البيانات لأنه لم يتم إنشاؤها بعد.

وبالنسبة للمعلومات التي يجب على مراقب البيانات تقديمها عندما لا يتم الحصول على البيانات الشخصية من صاحب البيانات فتتمثل في المعلومات المتعلقة بالهوية وتفاصيل الاتصال بوحدة التحكم، وممثل وحدة التحكم، تفاصيل الاتصال بمسئول حماية البيانات، أغراض المعالجة التي تهدف البيانات الشخصية إلى تحقيقها، بالإضافة إلى الأساس القانوني للمعالجة، وفئات البيانات الشخصية المعنية؛ والمستلمون أو فئات مستلمي البيانات الشخصية(٨٢).

ولضمان معالجة عادلة وشفافة فيما يتعلق بموضوع البيانات، يجب على مراقب البيانات تزويد صاحب البيانات –بالإضافة للمعلومات السابقة- بالمعلومات الآتية: الفترة التي سيتم تخزين البيانات الشخصية لها، أو إذا لم يكن ذلك ممكنا، المعايير المستخدمة لتحديد تلك الفترة؛ وتحديد المصالح المشروعة عندما تستند المعالجة إلى المصالح المشروعة التي يسعى إليها المراقب أو طرف ثالث مثل عملية التسويق المباشر؛ وجود الحق في طلب الوصول إلى البيانات الشخصية وتصحيحها أو محوها أو تقييد المعالجة المتعلقة بصاحب البيانات والاعتراض على المعالجة وكذلك الحق في إمكانية نقل البيانات(٨٣).

كما يحق لصاحب البيانات الحصول على تأكيد من وحدة التحكم بشأن ما إذا كانت البيانات الشخصية المتعلقة به تتم معالجتها أم لا، وفي هذه الحالة، حقه في الوصول إلى البيانات الشخصية والمعلومات التالية:أغراض المعالجة؛ وفئات البيانات الشخصية

(82) GDPR, art. 14(1).
(83) GDPR, art 14 (2).

المعنية؛ والمستلمون أو فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم أو سيتم الكشف عنها، ولا سيما المستلمون في بلدان ثالثة أو منظمات دولية؛ والفترة المتوقعة التي سيتم تخزين البيانات الشخصية لها، أو، إذا لم يكن ذلك ممكنًا، المعايير المستخدمة لتحديد تلك الفترة(٨٤).

ويستفاد من ذلك أن الالتزامات المتعلقة بقيام مراقب البيانات بتقديم المعلومات عن البيانات الشخصية وغرض معالجتها لصاحب البيانات إنما يتعلق بالبيانات الشخصية التي تم الحصول عليها بشكل مباشر أو غير مباشر، دون الإشارة لعملية الاستدلالات، وما تسفر عنه من استنتاجات حول بيانات لم يتم الإفصاح عنها.

كما اعترف المشرع المصري صراحة بحق صاحب البيانات في العلم بالبيانات الشخصية الخاصة به الموجودة لدى حائز أو متحكم أو معالج، كما يتقرر حقه في الاطلاع عليها والوصول إليها والحصول عليها(٨٥).

ويمكن تفسير هذا النص من جانبين، وهما: **أولاً:** باعتباره حقاً لصاحب البيانات، وهو حق واسع يشمل نطاقه العلم بالبيانات، والاطلاع عليها والوصول إليها والحصول عليها.

كما أن هذا الحق إنما يتعلق بالبيانات الشخصية التي يمكن نسبتها لشخص معين وهو ما يسمى بصاحب البيانات أو الشخص المعني بالبيانات، والتي قد يتم جمعها بشكل مباشر من قبل صاحب البيانات والذي قام بتقديمها طواعية للحائز أو المتحكم أو المعالج،

(84) GDPR, art. 15(1).

(٨٥) المادة (٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

وتشمل كذلك البيانات التي يحصل عليها أي شخص معنى بعمليات المعالجة أو الاستدلال والتي تشير من خلالها لشخص معين وترتبط به ويمكن من خلالها التعرف عليه.

ثانياً: يعتبر ما قرره المشرع من حق للشخص المعنى بالبيانات بالوصول والعلم والاطلاع على البيانات الشخصية المتعلقة به التزاماً على عاتق أي شخص معنى بعمليات المعالجة أو الاستدلال.

وما يجب أن نشير إليه هنا أنه بالنظر لخطورة عمليات الاستدلالات فيجب تقسيم البيانات التي تقوم عليها هذه العمليات، فهناك بيانات إدخال (مدخلات) وهى البيانات التي يتم تغذية عملية الاستدلال بها سواء تم تقديمها من جانب الشخص المعنى بالبيانات أو من خلال وصول الأشخاص المعنيين بالمعالجة والاستدلال بأنفسهم، وبيانات المخرجات (البيانات المستنتجة أو المستدل عليها) وهى بيانات لم يشر النص صراحة لحق صاحب البيانات في العلم والوصول إليها والاعتراض عليها إلا في حالة تعارضها مع الحقوق والحريات الأساسية للشخص المعنى بالبيانات دون النص على حق صاحب البيانات في معرفة كيفية إجراء وإتمام عملية الاستدلال ومبررات التوصل لنتائج الاستدلالات وهو ما يقف عائقاً أمام ممارسة صاحب البيانات لحقوقه المشروعة.

كما لم يتعرض النص لتنظيم عمليات الاستدلالات بما يمكن أن تمثله من خطورة بالغة، في حالة كون بيانات المدخلات لا تتعلق بشخص محدد أو يمكن تحديده مثل البيانات غير الشخصية، والبيانات مجهولة المصدر والتي قد تعتمد عليها عمليات الاستدلالات ويمكن من خلالها التوصل لبيانات شخصية، وكذلك لبيانات حساسة، حيث في ظل الوضع القانوني القائم لا يمكن أن يخضع هذا النوع من البيانات ضمن نطاق حق صاحب البيانات في العلم والوصول والاطلاع عليها، حيث لا تعتبر بيانات شخصية، ولا

تدخل ضمن نطاق الحماية، مما يمكن معها للمعنيين بمعالجة والاستدلال على البيانات الاعتماد عليها هروباً من القيود المقررة بقوانين حماية البيانات الشخصية.

لذلك يجب النص صراحة على حق الشخص المعنى بالبيانات بالوصول للبيانات المستنتجة والاطلاع عليها، كما يجب تقرير حق صاحب البيانات في معرفة البيانات التي تم من خلالها الاستدلال على بياناته بعد إجراء الاستدلالات حتى ولو كانت بيانات غير شخصية أو مجهولة المصدر طالما تم التوصل من خلالها لبيانات شخصية أو حساسة تتعلق بصاحب البيانات، وتقرير حقه في الاعتراض عليها، لما قد يكون لها بالغ الأثر على حقوقه، وتمهيداً لممارسة سائر حقوقه اللاحقة على ذلك، مثل تصحيح البيانات الناشئة عن الاستدلالات، والطعن عليها، والحق في محوها.

الفرع الثاني

الحق في تصحيح الاستدلالات

نشير بداية إلى أن اللائحة العامة لحماية البيانات تقرر لأصحاب البيانات الحق في تصحيح البيانات الشخصية غير الدقيقة أو استكمال البيانات غير المكتملة "عن طريق تقديم بيان تكميلي"، يأخذ نطاقه في الاعتبار الغرض من المعالجة(٨٦).

كما قرر المشرع المصري بحق صاحب البيانات في التصحيح، أو التعديل، أو المحو، أو الإضافة، أو التحديث في البيانات الشخصية(٨٧).

(86) GDPR, art. 16, " The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

(٨٧) المادة (٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

ونعتقد بأن هذين النصين إنما يتعلقان بالبيانات الشخصية التى يمكن استخدامها في عمليات المعالجة باعتبارها بيانات مدخلة، دون الاشارة لعمليات الاستدلالات، ولا كون التصحيح يتعلق بالبيانات المستنتجة من عملية الاستدلال.

ويتضح من ذلك، أن نطاق الحق في تصحيح البيانات أو تعديلها أو تحديثها إنما يتعلق بالبيانات الشخصية المقدمة من الشخص المعنى بالبيانات للأشخاص المعنيين بجمع البيانات ومعالجتها، والتي تقوم عليها المعالجة، بينما لم تتم الإشارة في هذا النص على إمكانية الاستدلالات من خلال بيانات غير شخصية ويمكن من خلالها التوصل لبيانات شخصية أو حساسة تتعلق بشخص محدد أو يمكن تحديده.

ويعتمد التصحيح ضمنيًا على مفهوم التحقق، مما يعني أنه يمكن إثبات أن سجل البيانات الذي تم استخدامه في عملية المعالجة أو الاستدلال غير دقيق أو غير كامل، وبالتالي تم تصحيحه من قبل صاحب البيانات.

ويكون الحق في التصحيح سهل التطبيق عندما تكون البيانات المستخدمة أو الاستدلالات التي يتم استخلاصها ذات أساس واقعي، أو بمعنى آخر قابلة للتحقق، مثل: الاسم، تاريخ الميلاد، الحالة الاجتماعية، الدخل، وغيرها.

وبالنسبة للبيانات المقدمة من صاحب البيانات، يمكن التحقق منها والاستناد إليها لبيان الأسباب التي توضح الخلل في البيانات الموجودة أو التي تم الاستدلال عليها.

ومع ذلك، ليست كل عمليات الاستدلالات تستند لحقائق يمكن التأكد منها وتصحيحها إذا لزم الأمر، فيمكن أن تكون الاستدلالات أيضًا افتراضات احتمالية لا يمكن التحقق منها في الوقت الحالي لتعلقها بأمور مستقبلية.

وبالنسبة للبيانات المتعلقة باستدلالات عالية المخاطر أو تنبؤية في المستقبل فلا يمكن التحقق منها وطلب تصحيحها.

وقد تم ربط هذا التمييز بين الاستدلالات التي يمكن التحقق منها، وتلك التي لا يمكن التحقق منها، بانطباق الحق في التصحيح على البيانات المستنتجة والمشتقة، وتعريف البيانات الشخصية والحساسة على نطاق أوسع.

ويرى البعض أن البيانات التي يمكن التحقق منها فقط هي التي تعتبر بيانات شخصية، وبالتالي تقع ضمن نطاق الحق في التصحيح، باستثناء البيانات المستنتجة التي لا يمكن التحقق منها(٨٨).

بينما يذهب البعض إلى أن الحق في التصحيح لا ينبغي أن يستبعد الاستدلالات التي لا يمكن التحقق منها، لأن إمكانية التحقق من الاستدلال لا تحدد آثاره على صاحب البيانات(٨٩).

ونعتقد بأنه يجب الاعتراف قانوناً بحق صاحب البيانات في معرفة البيانات المستنتجة، وحقه كذلك في طلب تصحيها يستوي في ذلك الاستدلالات التى يمكن التحقق منها، أو تلك التى لا يمكن التحقق منها، لأنه، بالقطع، في كلتا الحالتين سترتب آثاراً بالغة على حقوق الأشخاص.

وهنا تظهر إشكالية الاستدلالات في ظل التطورات التكنولوجية والتي يمكن أن تعتمد على بيانات غير شخصية، أو كذلك مجهولة المصدر ولا تحتوى على عنصر محدد وواضح لتحديد الهوية، ويمكن من خلالها الوصول لاستدلالات تفصح عن بيانات

(88) Gianclaudio Malgieri, Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, 4 PinG Privacy in Ger., 2016, p. 133.

(89)Hans-Georg Kamann and Martin Braun, Recht auf Berichtigung, in Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2017, p. 20-21

شخصية أو حساسة أو كلاهما لشخص محدد أو يمكن تحديده، ولا تخضع هذه البيانات لنطاق الحماية القانونية الحالية للبيانات الشخصية، ولا تكون كذلك محلاً لممارسة صاحب البيانات حقوقه عليها.

الفرع الثالث

الحق في المحو

يعد الحق في المحو أيضًا بمثابة علاج ضد الاستنتاجات التي لا يتفق معها صاحب البيانات(٩٠).

ويحق لصاحب البيانات أن يطلب من المراقب أو المتحكم أو المعالج محو البيانات الشخصية المتعلقة به، ودون تأخير لا مبرر له، ويكون المراقب ملزمًا بمحو البيانات الشخصية دون تأخير لا مبرر له، إذا توافر أحد الأسباب التالية: (أ) لم تعد البيانات الشخصية ضرورية فيما يتعلق بالأغراض التي تم جمعها من أجلها أو معالجتها بطريقة أخرى غير التي تم جمعها من أجلها؛ (ب) سحب صاحب البيانات الموافقة التي تستند إليها المعالجة، ولا يوجد أي أساس قانوني آخر للمعالجة; (ج) اعتراض صاحب البيانات على المعالجة ولا توجد أسباب مشروعة ومبررة للمعالجة من قبل وحدة التحكم؛ (د) تمت معالجة البيانات الشخصية بشكل غير قانوني؛ (هـ) يجب محو البيانات الشخصية للامتثال لالتزام قانوني مقرر في قوانين الدول الخاضع لها المراقب(٩١).

(90) Joris van Hoboken, Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines, 2012, p. 316.

(91) GDPR, art. 17 (1).

وفيما يتعلق بالسبب الثاني للحق في محو البيانات، قد يوجد لدي مراقب البيانات سبباً أو وجهة نظر تتعلق بالمصالح المشروعة مثل حرية ممارسة الأعمال التجارية[٩٢].

ونعتقد أن حق صاحب البيانات في طلب محو البيانات يثير أمراً هاماً يتعلق بضرورة التوازن بين حقين –قد يبدو متعارضين- وهما حق صاحب البيانات في المحو والمصلحة المشروعة لوحدات التحكم، وهو ما لم يتم النص عليه في تشريعات حماية البيانات.

كما يفسر تقديم صاحب البيانات لطلب بالمحو إنما يقصد به أنه لم يعد يوافق على المعالجة التي يقوم بها المتحكم أو المعالج، وفي حالة كون البيانات تم إتاحتها من خلال المواقع الالكترونية، فيجب على المتحكم أو المعالج –حسب من قام منهما بعملية المعالجة- بإبلاغ موفري محرك البحث الالكتروني بسحب الشخص المعنى بالبيانات موافقته[٩٣].

وفيما يتعلق بالاستدلالات على وجه التحديد، شكك البعض في إمكانية تطبيق الحق في المحو على الاستدلالات، ويستند في ذلك إلى أن المادة ١٧ من اللائحة العامة الأوروبية-التى تحدد حالات طلب المحو- لن تنطبق على الاستدلالات تمامًا[٩٤].

---

(92) Norbert Nolte & Christoph Werkmeister, Recht auf Loschung ("Recht auf Vergessenwerden"), in Datenschutz-Grundverordnung VO (EU) 2016/679, 2017, at 47-48.

(٩٣) د. مشعل محمد أحمد سلامة، الحق في محو البيانات الشخصية، دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي وأحكام المحاكم الأوروبية، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة مدينة السادات، مجلد ٣، عدد ٢، ٢٠١٧، ص ١١٢.

(94) Norbert Nolte & Christoph Werkmeister, Recht auf Loschung ("Recht auf Vergessenwerden"), in Datenschutz-Grundverordnung VO (EU) 2016/679, 2017, p.48.

بينما أيد البعض الرأي السابق لكن يضيف أن النفقات المالية لمراقب البيانات لإنشاء استنتاجات سوف تتفوق على طلب صاحب البيانات بالحذف[٩٥]، وهو ما أشرنا له بعدم وجود نص يحكم عملية تحقيق التوازن بين المصالح المتعارضة، ومع ذلك يمكن أن يستفاد ضمنياً من خلال اللائحة العامة لحماية البيانات حين قررت أنه عندما يقوم المراقب بنشر البيانات الشخصية ويكون ملزمًا بموجب الفقرة ١ بمحو البيانات الشخصية، يجب على المراقب، مع الأخذ في الاعتبار التكنولوجيا المتاحة، وتكلفة التنفيذ، اتخاذ خطوات معقولة، بما في ذلك التدابير الفنية، لإبلاغ المراقبين لأي روابط لتلك البيانات الشخصية أو نسخها أو تكرارها[٩٦].

وهو ما يعني أن تنفيذ مراقب البيانات أو المتحكم لطلب المحو يتقيد بعدة أمور منها الوسائل التكنولوجية المتاحة، وتكلفة التنفيذ، كما لم يلزم نص اللائحة المراقبين إلا باتخاذ خطوات معقولة لتنفيذ طلب المحو من خلال التدابير الفنية.

ويقر القانون المصري بحق صاحب البيانات الشخصية في محو البيانات الشخصية، وحقه كذلك في سحب موافقته المسبقة على جمع البيانات ومعالجتها[٩٧]، كما اعتبر المشرع المصري من شروط جمع ومعالجة البيانات الشخصية والاحتفاظ بها شرط عدم الاحتفاظ بها مدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها[٩٨].

(95) Gianclaudio Malgieri, Trade Secrets v. Personal Data: A Possible Solution for Balancing Rights, 6 Int'l Data Privacy L., 2016, p. 102.

(96) GDPR, art. 17 (2).

(٩٧) المادة (٢) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(٩٨) المادة (٣) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

كما يعد محو البيانات الشخصية التزاماً قانونياً على عاتق كلاً من المتحكم والمعالج للبيانات، حيث يلتزم المتحكم في البيانات بمحوها فور انقضاء الغرض المحدد منها وفي حالة الاحتفاظ بها لسبب مشروع بعد ذلك فيجب إخفاء هوية الشخص المعنى بالبيانات[٩٩]، كما يقع التزام قانوني على عاتق معالج البيانات بمحوها بانقضاء مدة المعالجة أو تسليمها للمتحكم[١٠٠].

ونعتقد كذلك بأن ما أشار إليه المشرع المصري يتعلق بالبيانات الشخصية المستخدمة في عمليات المعالجة، وحتى في مجال الاستدلالات فتدخل في نطاق البيانات المدخلة، دون الاشارة إلى حقه في طلب محو البيانات الحساسة التى يمكن استنتاجها أو الاستدلال عليها.

كما أن التزام كلاً من المتحكم والمعالج بمحو البيانات فور انقضاء الغرض المحدد منها إنما يتعلق بالبيانات المقدمة لاستخدامها في عملية المعالجة دون التطرق لتقرير الحماية للبيانات المستنتجة من عملية الاستدلال والتى قد تكون أكثر خطورة على حقوق الأفراد ولم يتم النص على حمايتها.

(٩٩) المادة (٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.
(١٠٠) المادة (٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

الفرع الرابع

ضرورة منح أصحاب البيانات حق الطعن

في القرارات المبنية على الاستدلالات

تظهر إشكالية حق الطعن على القرارات المبنية على الاستدلالات في أمرين وهما: أولاً: الاعتراض على نتائج الاستدلالات والبيانات المستنتجة، ثانياً: عدم وضوح المعايير التى قامت عليها الاستدلالات بل وصعوبة إثباتها.

ولا يوجد إجماع حول الحقوق القانونية لأصحاب البيانات على الاستدلالات، ومع ذلك، فإن هناك رأي يتجه إلى أن اللائحة العامة لحماية البيانات تتجاوز التحكم في البيانات الإجرائية وإدارتها (تقرير المصير المعلوماتي)، وتوفر ضمانات مثل حق الطعن ضد الاستدلالات والقرارات المستندة إلى الاستدلالات في نطاق المادة ٣/٢٢ من اللائحة العامة لحماية البيانات(١٠١).

ومع ذلك يظل التشكيك قائماً في إمكانية تنفيذ الحق في الطعن بشكل هادف دون وجود معايير أساسية لصنع القرار المستند لهذه الاستدلالات.

وتصف المادة ٣/٢٢ من اللائحة العامة لحماية البيانات الضمانات ضد القرارات التي تعتمد فقط على المعالجة الآلية، بما في ذلك التوصيف، والتي تنتج آثارًا قانونية أو تأثيرات مهمة مماثلة لأصحاب البيانات(١٠٢).

---

(101) Isak Mendoza & Lee A Bygrave, The Right Not to Be Subject to Automated Decisions Based on Profiling (Mar. 9, 2018), https://papers. ssrn.com/abstract= 2964855 [https://perma.cc/NPK5-MGE2].

(102) GDPR, art. 22.

ووفقاً لذلك يُمنح أصحاب البيانات حقوق التعبير عن آرائهم، والطعن في القرارات، والحصول على التدخل البشري.

وتشير هذه الضمانات إلى أن اللائحة العامة لحماية البيانات تنتقل إلى ما هو أبعد من مجرد التحكم في البيانات الإجرائية وإدارتها أو تقرير المصير المعلوماتي للسماح لأصحاب البيانات بتقييم وتحدي القرارات الآلية والتوصيف التي يمكن أن تستند إلى استنتاجات.

وعلى الرغم من أن للأشخاص الحق في التعبير عن آرائهم ووجهة نظرهم فيما يتعلق ببياناتهم وهو أمر معترف به، إلا أن اللائحة العامة لحماية البيانات تشيران إلى اهتمامات أصحاب البيانات بكيفية التعامل مع بياناتهم، حيث تحظى العمليات التي يتم تقييمها بأهمية متزايدة، على الأقل في الحالات التي تكون فيها المعالجة مؤتمتة بالكامل، على الرغم من إمكانية التشكيك في مدى إلزامية هذا الأمر من الناحية القانونية(١٠٣).

ووفقاً للائحة العامة يحق لصاحب البيانات عدم الخضوع لقرار يعتمد فقط على المعالجة الآلية، بما في ذلك التوصيف، مما ينتج عنه آثار قانونية تتعلق به أو تؤثر عليه بشكل كبير، خاصة إذا كانت البيانات ضرورية لإبرام عقد أو تنفيذه بين صاحب البيانات ومراقب البيانات؛ أو كذلك حالة الموافقة الصريحة من صاحب البيانات، ويجب على مراقب البيانات تنفيذ التدابير المناسبة لحماية حقوق وحريات صاحب البيانات ومصالحه المشروعة، على الأقل الحق في الحصول على تدخل بشري من جانب المراقب، للتعبير عن وجهة نظره والطعن في القرار.

(103) Brent Mittelstadt, Chris Russell & Sandra Wachter, Explaining Explanations in AI, in FAT "19: Conference on Fairness, Accountability, and Transparency (FAT '19), January 29-31, 2019

وعلى ذلك، وحماية لأصحاب البيانات، يتمتع صاحب البيانات بالحق في عدم الخضوع لقرار قد يتضمن إجراءً وتقييم الجوانب الشخصية المتعلقة به، والذي يعتمد فقط على المعالجة الآلية والذي ينتج عنه آثار قانونية تتعلق به أو تؤثر عليه بشكل كبير ، مثل الرفض التلقائي لطلب الائتمان عبر الإنترنت أو ممارسات التوظيف الإلكتروني دون أي تدخل بشري(١٠٤).

وتتضمن هذه المعالجة "التوصيف" الذي يتكون من أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تقيم الجوانب الشخصية المتعلقة بالشخص الطبيعي، ولا سيما التحليل أو التنبؤ بالجوانب المتعلقة بأداء صاحب البيانات في العمل، أو الوضع الاقتصادي، أو الصحة، أو التفضيلات الشخصية أو المصالح أو الموثوقية أو السلوك أو الموقع أو التحركات، حيث ينتج عنها آثار قانونية عليه أو تؤثر عليه بشكل كبير.

ومع ذلك، ينبغي السماح باتخاذ القرارات بناءً على هذه المعالجة، بما في ذلك التوصيف، حيثما يسمح بذلك صراحةً القانون الذي يخضع له المراقب، بما في ذلك لأغراض مراقبة الاحتيال والتهرب الضريبي ومنعه وفقًا للقانون، كما يسمح بذلك في الأحوال اللازمة لإبرام أو تنفيذ عقد بين صاحب البيانات ووحدة التحكم، أو عندما يعطى صاحب البيانات موافقته الصريحة.

وعلى أية حال، يجب أن تخضع هذه المعالجة للضمانات المناسبة، والتي يجب أن تتضمن معلومات محددة عن صاحب البيانات والحق في الحصول على تدخل بشري، للتعبير عن وجهة نظره، والحصول على تفسير للقرار الذي تم التوصل إليه بعد هذا التقييم، وإمكانية الطعن في القرار.

---

(104) GDPR, art Whereas : 71.

ولا شك أن هذا الاعتراف بالمصالح المشروعة لأصحاب البيانات فيما يتعلق بمخرجات معالجة البيانات يتميز عن غالبية الآليات الأخرى في اللائحة العامة لحماية البيانات، والتي تركز بدلاً من ذلك على إدارة بيانات الإدخال بدلاً من التركيز على المخرجات.

ويوفر الحق في الاعتراض بشكل فعال لأصحاب البيانات القدرة على الاعتراض على القرارات الآلية في القطاعات التي قد لا تكون فيها القرارات المتخذة على أساس بشري قابلة للاعتراض عليها، أو حيث قد لا توجد معايير قانونية أو أخلاقية ذات صلة لصنع القرار.

كما يجب تبرير الحماية الأكبر التي يوفرها القانون العام لحماية البيانات من خلال المخاطر المتزايدة والجديدة التي يتم تقديمها من خلال استخدام اتخاذ القرار الآلي في مجالات مثل فرص العمل، أو الائتمان أو التأمين، أو الاستهداف (موضوعات البيانات) مع منتجات مالية شديدة الخطورة أو مكلفة[١٠٥].

ويبدو أن الحق في الاعتراض يعزز الحماية الممنوحة لأصحاب البيانات ضد جميع أنواع اتخاذ القرارات الآلية ذات الأهمية القانونية.

ووفقاً لذلك يحق لأصحاب البيانات الآن الاعتراض على القرارات المؤتمتة بالكامل بغض النظر عن القطاع الذي تم فيه اتخاذ القرار ودون الرجوع إلى اللوائح السائدة ومعايير اتخاذ القرار.

(105) Article 29 Data Prot. Working Party, Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679, 17/EN, WP251rev.01, at 10 (Feb. 6, 2018), http://ec.europa.eu/ newsroom /article 29/ document.cfm?doc_id=49826

ومع ذلك، فإن نجاح الاعتراض المقدم من صاحب البيانات يعتمد على قدرته على الطعن في معايير اتخاذ القرار القانونية أو الأخلاقية القابلة للتطبيق والتي تم انتهاكها.

ويجب الأخذ في الاعتبار أن الحق في الاعتراض وحده لا يوفر سوى القليل من الحماية ضد القرارات الآلية والاستدلالات الأساسية في حالة عدم وجود معايير واضحة يمكن الطعن عليها، وهو ما يظهر بشكل جلي في العصر الحالي القائم على التكنولوجيا المتطورة والذكاء الاصطناعي.

وقد يستند الضعف في حق الطعن للتضييق الوارد على نطاق اختصاص قانون حماية البيانات، أو على الأقل كما فسرته محكمة العدل الأوروبية في أحكام سابقة.

ومن ذلك ما قررته محكمة العدل الأوروبية أن اختصاص قانون حماية البيانات لا يشمل تقييم دقة ومحتوى عملية صنع القرار، وتم اتخاذ هذا الموقف من المحكمة في إشارة إلى كلاً من توجيه حماية البيانات واللائحة العامة لحماية البيانات (التي كانت وشيكة في وقت صدور الحكم).

ورفضت المحكمة حق أصحاب البيانات في الطعن وتقييم نتائج اتخاذ القرار بأنفسهم، موضحة أن هذا التقييم يقع على عاتق السلطات الوطنية المختصة التي تتعامل مع الشكاوى أو القوانين المعنية بذلك وليست قوانين حماية البيانات(١٠٦).

وعلى ذلك فإن المستقر عليه أن تفسير حقي حماية البيانات وهما حق الوصول للبيانات، وحق تصحيحها في هذه الحالات يقتصر على تقييم دقة واكتمال بيانات الإدخال دون أن يمتدا لعملية التقييم والاستدلال.

(106) Cases C-141 & 372/12, YS, M and S v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, PP 45-47.

وبتطبيق ذلك على ما قررته اللائحة العامة لحماية البيانات من حق الاعتراض (أي طلب إلغاء أو تعديل قرار آلي)، فإن هذا التفسير يشير إلى أن الاعتراض لن يكون ناجحًا إلا في حالات محددة، نذكر منها على سبيل المثال: (١) إذا كانت البيانات المدخلة غير صحيحة أو غير كاملة، (٢) إذا تم انتهاك مبادئ حماية البيانات الأخرى كفشل مراقب البيانات في إثبات الأساس القانوني للمعالجة.

كما أنه لا يمكن الاعتراض على الأسباب أو العوامل الكامنة وراء القرارات إلا في حالة وجود معايير لصنع القرار، مثل الإخلال بقانون مكافحة التمييز، خارج قانون حماية البيانات، الذي لا يضع في حد ذاته معايير تتعلق بمحتوى أو نتائج عمليات صنع القرار.

ويترتب على ذلك أن الحق في الطعن يصبح مجرد حق إجرائي لإلغاء القرارات أو التصنيف المؤثر الذي تم إجراؤه باستخدام بيانات مدخلة غير دقيقة أو غير كاملة.

ومن غير المحتمل إلزام مراقبي البيانات على مراجعة القرارات الآلية بناءً على الاستنتاجات ما لم يتم انتهاك معايير صنع القرار الخاصة بقطاع معين أو أحكام أخرى في قانون حماية البيانات، كما أنه إذا لم تكن هناك معايير لاتخاذ القرارات، فلن يكون صناع القرار مخالفين للقانون.

ويترتب على ذلك، أنه في إطار الوضع القانوني الحالي للاستدلالات وعمليات صنع القرار الآلية فإن الحماية القانونية مجرد حماية فارغة من مضمونها.

ويحتاج الأمر، وبلا شك، لاجتهادات عديدة لتبنى النهج القائم على الغاية لتوسيع حقوق الطعن وتصحيح محتوى التقييمات والاستدلالات.

كما يجب وضع معايير تقييم معقولة، لأن الطعن في القرارات أو الاستنتاجات لن ينجح إلا في حالة انتهاك معيار أو قاعدة محددة.

الفصل الرابع

المسئولية المدنية عن معالجة البيانات الحساسةوالاستدلال عليها

نظمت اللائحة العامة لحماية البيانات الأوروبية المسئولية المدنية الناشئة عن معالجة البيانات الشخصية بالمادة (٨٢) من اللائحة، حيث تقرر أن الفعل الموجب للمسئولية هو أي معالجة يتم إجراؤها بشكل مخالف لما قررته اللائحة العامة لحماية البيانات (GDPR)[١٠٧].

وعلى الرغم من أن هذا النص يشير صراحة للبيانات الشخصية بصفة عامة، إلا أنه مع ذلك يطبق على البيانات الحساسة.

وتظهر عمليات الاستدلالات على البيانات الحساسة إشكاليات متعددة في مجال إعمال أحكام المسئولية المدنية، ومن هذه الاشكالات عدم التنظيم القانوني الواضح للاستدلالات ومدى تمتعها بالحماية القانونية وبصفة خاصة البيانات الناتجة عنها، كما أنه في حالة الاعتراف بالحماية تظل إشكالية الاستدلالات قائمة بسبب استخدام الوسائل التكنولوجية المتطورة وبصفة خاصة تحديد معايير الاستدلالات والتى لا يجوز الطعن على نتائج الاستدلالات إلا من خلال معرفة تلك المعايير، كما تعتبر الاتجاهات المضيقة لتطبيق قانون حماية البيانات إحدى الاشكاليات أمام تطبيق أحكام المسئولية المدنية.

ونعرض من خلال هذا الفصل لمبحثين:

المبحث الأول: إشكاليات المسئولية المدنية في مجال الاستدلال على البيانات الحساسة.

المبحث الثاني: تطبيق قواعد المسئولية المقررة علي معالجة البيانات الحساسة.

---

(107) GDPR, art. 82.

المبحث الأول

إشكاليات المسئولية المدنية عن الاستدلالات على البيانات الحساسة

تواجه المسئولية المدنية الناشئة عن الاستدلال على البيانات الحساسة إشكاليات متعددة، خاصة في عصر التقدم التكنولوجي والمتطور بشكل سريع وهائل.

وتتجسد الإشكاليات في عدة صور، نذكر منها: مدى الاعتراف القانوني للاستدلالات بالحماية خاصة في ظل الفروق الجوهرية بين الاستدلالات والمعالجة، وحتى مع الاعتراف بالحماية تظل إشكالية الاستدلالات قائمة بسبب استخدام الوسائل التكنولوجية المتطورة، وكذلك تحديد نطاق البيانات محل الحماية وفق القواعد التشريعية المنظمة لحماية البيانات، والاتجاهات المضيقة لتطبيق قانون حماية البيانات.

ونعرض بشيء من التفصيل لهذه الإشكاليات فيما يلي:

المطلب الأول

عدم المساواة بين المعالجة والاستدلالات على البيانات الحساسة

نشير بداية إلى أنه يوجد اختلاف كبير بين كلاً من الاستدلالات وعملية معالجة البيانات، وأن ما قامت به التشريعات المقارنة من تقرير الحماية القانونية إنما كانت واضحاً ومباشراً لعمليات المعالجة دون التطرق بشكل واضح وصريح لعمليات الاستدلال على البيانات الحساسة بشكل عام، وما يحيطها من مخاطر متعددة في عصر البيانات الضخمة والذكاء الاصطناعي بشكل خاص.

وتظهر الاختلافات بين عمليات المعالجة والاستدلالات من خلال جوهر كل عملية منهما، فالمعالجة تتطلب ضرورة الوصول للبيانات، سواء الشخصية أو الحساسة، من خلال جمعها وتخزينها واستخدامها ومعالجتها وامكانية اتاحتها، وهي ما تخضع معها للحماية والقيود المقررة قانوناً بنصوص صريحة لا خلاف ولا اجتهاد بشأنها.

وبالنسبة لقواعد المسئولية المدنية، فإن محور تطبيق نص المادة (٨٢) من اللائحة العامة الأوروبية لحماية البيانات الشخصية تتعلق بمعالجة البيانات الشخصية، ومن باب أولى تطبيقها على البيانات الحساسة.

ومع ذلك، فإن الأمر يختلف بشكل جوهري وموضوعي في مجال عمليات الاستدلال على البيانات الحساسة، وكما ذكرنا من قبل في مواضع متعددة، أن الاستدلالات على البيانات الحساسة وفق التنظيم القانوني الحالى لحماية البيانات لا تخضع للعديد من القيود المقررة لحماية البيانات الحساسة.

وإذا كانت المسئولية المدنية عن معالجة البيانات بشقيها الشخصية، والحساسة، تخضع في مضمونها الأعم لتطبيق القواعد العامة، مما يستلزم وجود فعل ضار يرتكبه الشخص إخلالاً بالقواعد القانونية في هذا الصدد، وهو ما يمكن قيامه وإثباته من خلال عمليات معالجة البيانات، بينما قد يصعب أو يتعذر ذلك في مجال الاستدلالات مما يصعب معه في كثير من الحالات تطبيق نصوص قواعد المسئولية المدنية على عمليات الاستدلالات.

علاوة على ذلك، يمكن تقويض قواعد الحماية المقررة للبيانات الحساسة خاصة في عصر الاستدلالات القائمة على ما يسمى " بالبيانات الضخمة" وتكنولوجيات الذكاء

الاصطناعي، حيث يمكن أن تزيل البيانات الضخمة التمييز الكامل بين فئات البيانات المختلفة[١٠٨]، سواء البيانات الشخصية أو الفئات المحمية مثل البيانات الحساسة.

كما أصبحت العديد من البيانات ذات طبيعة حساسة، ويظهر ذلك نتيجة الزيادات الهائلة، والتي تفوق العقل البشري، في قوة الحوسبة والسهولة المتزايدة للمشاركة، والجمع بين مجموعات البيانات المختلفة[١٠٩]، ويعني ذلك أن التوصل للبيانات الحساسة قد تم بشكل غير مخالف للقواعد القانونية، كما تم التوصل إليها مع تجنب القيود القانونية المقررة للبيانات الحساسة.

ويترتب على ذلك أنه إذا كانت حماية البيانات الحساسة هدفاً في ذاتها فقد تم انتهاك هذا الهدف بالوصول إليها مع عدم الإخلال بالأحكام القانونية المقررة، وإذا كانت حمايتها بهدف عدم التأثير أو المساس بالحقوق الأساسية للأفراد فيمكن القول أيضاً بعدم تحقق هذا الهدف نظراً لقدرة عمليات الاستدلال على إنشاء الملفات التعريفية والتى يتعذر الوصول لمعاييرها المستندة إليها في ظل تقنيات الذكاء الاصطناعي.

وبالإضافة إلى ذلك يمكن القول أن الأمر بشأن الاستدلالات على البيانات لا يقتصر فقط على البيانات الحساسة، بل يشمل أيضاً البيانات الشخصية العادية والتي يمكن التوصل إليها والاستدلال عليها من خلال بيانات عادية ليست ذات طبيعة شخصية، وكذلك بالنسبة للبيانات التي توصف بكونها بيانات مجهولة.

---

(108) Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 SETON HALL L. REV., 2017, p. 995, 1013.

(109) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021, p.1591.

وبهدف تعزيز الحماية القانونية للبيانات الحساسة فإنه يجب التوسع في تقرير الحماية المشددة لهذه البيانات، ويمكن أن يكون ذلك من خلال دور القاضي في تقريره لاعتبار أي بيانات سواء شخصية أو عادية، أو مجهولة يمكن أن يترتب على جمعها وتصنيفها وتوصيفها ومعالجتها الاستدلال على بيانات حساسة تتعلق بفرد محدد الهوية أو يمكن تحديده أن تكون حساسة كذلك وتخضع للقيود والحماية المشددة، ووقتئذ يمكن إعمال أحكام المسئولية المدنية بشأنها.

ومؤدى ذلك أنه يجب تقرير المسئولية المدنية على عاتق الحائز لتلك البيانات (الشخصية، العادية، المجهولة المصدر)، والمتحكم فيها، والمعالج لها، شأنها في ذلك شأن الحماية المشددة للبيانات الحساسة.

كما يمكن الاستعانة بالتفسير الموسع للبيانات الحساسة في مجال الاستدلالات، حيث يمكن اعتبار أي بيانات يمكن الاستدلال من خلالها على بيانات حساسةتعتبر بمثابة بيانات حساسة، وأي بيانات شخصية يمكن استنتاج بيانات حساسة منها سيتم اعتبارها أيضًا بيانات حساسة، لكن المشكلة هي أن العواقب أعظم بكثير مما هو معترف به حالياً.

ويترتب على الاعتراف بالحماية القانونية، وبصفة خاصة، الحماية المشددة للبيانات العادية، وكذلك البيانات مجهولة المصدر والتي يمكن أن يترتب عليها استدلالات بشأن البيانات الشخصية الحساسة، ما يلي:

١- حظر معالجتها من حيث المبدأ وفقاً للقاعدة المقررة بشأن حماية البيانات الحساسة، مع جواز معالجتها وفق الحالات الاستثنائية المصرح فيها لمعالجة البيانات الشخصية الحساسة.

٢- ضرورة الحصول على موافقة الشخص المعني بالبيانات قبل معالجتها والاستدلال منها على بيانات حساسة.

٣- ضرورة استيفاء القيود المقررة على ذلك، مثل الحصول مسبقاً على ترخيص من مركز حماية البيانات الشخصية قبل الشروع في عمليات الاستدلالات.

٤- يجب الكشف عن استخدام هذه البيانات، وإخضاعها للتصحيح من قبل صاحب البيانات، والاعتراف بسائر الحقوق الأخرى لصاحب البيانات، مثل معرفة نتيجة الاستدلالات لما قد يكون لها من تأثير على حقوقه الأساسية، وتقرير حقه في الطعن عليها.

٥- تحديد معايير وأسس عمليات الاستدلالات بشكل واضح وعادل وشفاف.

وعلى الرغم من كون هذه التوصيات لها أهميتها البالغة سواء لحماية البيانات الحساسة أو كذلك لحقوق أصحاب البيانات إلا أنها مع ذلك قد تصطدم بصعوبة بالغة بل وربما مشروعة تتعلق بتحقيق التوازن مع المصالح الاقتصادية الكبرى للشركات التكنولوجيا وتأثيرها على الابتكار والتقدم حالة الغلو في القيود على عمليات الاستدلالات.

المطلب الثاني

إشكالية المساءلة بسبب وسائل الاستدلالات المتطورة

وفي ظل التقدم التكنولوجي الهائل، تركز العديد من تقنيات البيانات الضخمة على استخلاص استنتاجات دقيقة حول الأشخاص من البيانات، ومع تزايد هذه التقنيات، قد يصل الأمر لتوسيع نطاق استخدام واتساع فئات المعلومات الحساسة الاستدلالية(١١٠).

ومن خلال البيانات الضخمة يتم استخدام مجموعة كبيرة من الخوارزميات المعقدة لتحليل البيانات، والتي يعتمد الكثير منها على التعلم الآلي، حيث تتطور مع تغذيتها بكميات متزايدة من البيانات(١١١)، حيث يمكن بسهولة استخلاص استنتاجات حول البيانات الحساسة من بيانات غير حساسة(١١٢).

وعلى ذلك، فإن اعتماد عمليات الاستدلالات على البيانات الضخمة والتي تتيحها تقنيات الذكاء الاصطناعي ويتم التوصل من خلالها لبيانات مستنتجة وقد تكون هذه البيانات حساسة، تثير إشكالية كبري في نطاق المسئولية المدنية وتوضح محكمة العدل

(110) Paul Ohm, Sensitive Information, 88 S. CAL. L. REV., 2015, p.1125.

(111) CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 75-77 (2016).

(112) Hideyuki Matsumi, Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?, 48 CUMB. L. REV. 149, 150 (2017).

الأوروبية أنه إذا كان صاحب البيانات يرغب في الطعن في نتائج تقييمه التي تمت من خلال عملية الاستدلالات، فيجب اللجوء إلى ذلك من خلال القوانين المعنية بذلك، وليس قانون حماية البيانات(١١٣).

وتظهر العديد من الأبحاث مدى سهولة ودقة الخوارزميات في التوصل إلى استنتاجات حول البيانات الحساسة من البيانات غير الحساسة، وفي دراسات كثيرة حول الاستدلالات وجد أن السمات القابلة للاستدلال تشمل الجنس، والعمر، والسياسة، والموقع، والمهنة، والعرق ، والأسرة والعلاقات، والتعليم، والدخل، والصحة، والدين، والطبقة الاجتماعية(١١٤).

وكان للعمل الأكاديمي باع كبير خلال السنوات الماضية لمعالجة وتفسير عمليات صنع القرارات والمبررات التي تستند إليها بهدف تحقيق المساءلة في أنظمة صنع القرار من خلال الخوارزميات(١١٥).

---

(113) Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 2009 E.C.R. I-293, PP 48-52.

(114) Joanne Hinds & Adam N. Joinson, What Demographic Attributes Do Our Digital Footprints Reveal? A Systematic Review, 13 PLOS ONE, Nov., 2018, p. 28, at 1, 5.

(115) Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (2015); Joshua A. Kroll et al., Accountable Algorithms, 165 U. Pa. L. Rev., 2017, p. 633; Tim Miller, Explanation in Artificial Intelligence: Insights from the Social Sciences, Artificial Intelligence, Feb. 2019, at 1; Brent Mittelstadt, Chris Russell & Sandra Wachter, Explaining Explanations in AI, in FAT "19: Conference on Fairness, Accountability, and Transparency (FAT '19), January 29-31, 2019, Atlanta, GA, USA, 2019, p. 279; S. C. Olhede & P.J. Wolfe, The Growing Ubiquity of Algorithms in Society: Implications, Impacts and

=

واتخذ هذا العمل أشكالا عديدة، منها دعوات التنظيم[١١٦]، كما تمت المناداة بضرورة تطوير الطرق التقنية للشرح والتفسير[١١٧]، وآليات التدقيق[١١٨]، ووضع معايير للمساءلة الخوارزمية في المؤسسات العامة والخاصة[١١٩].

وتعتبر مسارات العمل المتنوعة هذه ضرورية في السعي إلى زيادة مساءلة الذكاء الاصطناعي، ولحسن الحظ فقد حققت تقدمًا كبيرًا على المستوى القانوني والأخلاقي والسياسي والتقني.

=

Innovations, Phil. Transactions Royal Soc'y A, Aug. 6, 2018, at 8; Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L., 2017, p. 76; Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 Harv. J.L. & Tech., 2018, p. 841.

(116) Marion Oswald, Algorithm-Assisted Decision-Making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power, Phil. Transactions Royal Soc'y A, Aug. 6, 2018, at 1, 3; Andrew Tutt, An FDA for Algorithms, 69 Admin. L. Rev., 2017, p. 83.

(117) Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L., 2017, p. 76.

(118) Pauline T. Kim, Essay, Auditing Algorithms for Discrimination, 166 U. Pa. L. Rev. Online, 2017, p. 189.

(119) European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2013(INL)), Eur. Parl. Doc. P8_TA(2017)0051, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP// NONSGML+TA+P8-TA-2017-0051+0+DOC+PDF+V0 //EN [https:// perma. cc/ 9H5H-W2UE]

ومع ذلك، لا تزال هناك نقطة غائبة تستند إليها كل المطالبات، وتتمثل في ضرورة وجود أساس قانوني أو أخلاقي لتبرير المطالبة بالتفسيرات وتحديد محتواها المطلوب(١٢٠).

ونتيجة لذلك، فإن الكثير من العمل السابق بشأن الأساليب والمعايير والأبحاث الأخرى حول التفسيرات سيكون ذا قيمة بالمعنى الأكاديمي أو التنموي، لكنه سيفشل في مساعدة المستفيدين المستهدفين من المساءلة الخوارزمية وهم الأشخاص الذين تتأثر حقوقهم بالقرارات الخوارزمية.

ولا يوجد سبب مقنع لافتراض أن المؤسسات وأصحاب الأعمال سيقدمون بشكل إرادي وطوعي تفسيرات كاملة تغطي عملية الاستدلال، ومبررات، ودقة اتخاذ القرار الخوارزمي ما لم تكن ملزمة بذلك، بل وغالبًا ما تكون هذه الأنظمة معقدة للغاية، وتتضمن بيانات شخصية (حساسة)، وتستخدم أساليب ونماذج تعتبر أسرارًا تجارية، بلاضافة إلى أن تقديم التوضيحات يفرض تكاليف ومخاطر إضافية على الشركات والأشخاص(١٢١).

(120) Doshi-Velez & Mason Kortz, Accountability of AI Under the Law: The Role of Explanation (Berkman Klein Ctr. Working Grp. on Explanation and the Law Working Paper, 2017).

(121) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494.

ومن الجدير بالذكر في هذا السياق أن معايير صنع القرار لا تكون عادة جزءا لا يتجزأ من الحق المطلق الذي يتطلب الكشف عن إجراءات اتخاذ القرار الكاملة؛ ويبقى، على سبيل المثال، صاحب العمل حراً ومستقلاً في اتخاذ قرارات التوظيف.

وبدلاً من ذلك، توفر معايير صنع القرار أسبابا للمطالبة بتفسيرات محدودة توضح بالتفصيل خطوات عملية صنع القرار اللازمة لتحديد ما إذا كانت الإجراءات المعنية قد تم إتباعها، ولذلك، على سبيل المثال، قد يكون لمقدم الطلب الحق في إتباع معايير معينة ضمن هذا الإجراء، مثل عدم استناد قرار التوظيف إلى سمة محمية (على سبيل المثال، العرق أو الدين) لأن القيام بذلك يشكل تمييزًا.

ومع ذلك، فإن منح التفسيرات ليس سوى وسيلة واحدة ممكنة للمضي قدما في جعل عملية صنع القرار الخوارزمي خاضعة للمساءلة، ويمكن أن توفر هذه التفسيرات والتوضيحات علاجًا لاحقًا فعالاً، ولكن لا يمكن تقديم التفسير إلا بعد اتخاذ قرار(١٢٢).

وكما يشير البعض إلى أن التفسير قد يُعلم الفرد بالنتيجة أو القرار حول الافتراضات أو التنبؤات أو الاستدلالات الأساسية التي أدت إليه، ومع ذلك، فإنه لا يضمن أن القرار أو الافتراض أو التنبؤ أو الاستدلال له ما يبرره(١٢٣).

وفي هذا الصدد يجب الاعتراف والتأكيد على الحقوق على المستوى الفردي والتي من شأنها أن تمنح أصحاب البيانات القدرة على إدارة كيفية رسم الاستدلالات التي

(122) Brent Mittelstadt, Chris Russell & Sandra Wachter, Explaining Explanations in AI, in FAT "19: Conference on Fairness, Accountability, and Transparency (FAT '19), January 2019, p. 29-31.

(123) Mireille Hildebrandt, Primitives of Legal Protection in the Era of Data-Driven Platforms, 2 Geo. L. Tech. Rev., 2018, p. 252, 271.

تنتهك الخصوصية، والسعي للتعويض ضد الاستدلالات غير المعقولة عندما يتم إنشاؤها أو استخدامها لاتخاذ قرارات مهمة.

وأصبح الاعتراف بالأضرار المحتملة للاستدلالات من قبل الباحثين القانونيين وصانعي السياسات الأوروبيين ليس محلاً للشك، ومع ذلك فإن قانون حماية البيانات لم يوفر الحماية المناسبة لذلك، بل ويتلقى أصحاب البيانات القليل من المساعدة في التعامل مع معلوماتية البيانات التي يقدمونها للمراقبين، الذين ليسوا ملزمين قانونًا بالكشف عن معاييرهم أو تبريرها وطرقهم المستخدمة لاستخلاص الاستنتاجات واتخاذ القرارات بناءً عليها(١٢٤).

المطلب الثالث

التضييق من نطاق تطبيق قانون حماية البيانات الشخصية

يهدف قانون حماية البيانات الشخصية لتقرير حماية فاعلة لأصحاب البيانات فيما يتعلق ببياناتهم الشخصية، وتقرير حماية مشددة بشأن بياناتهم الشخصية الحساسة.

لذلك، فإن الاتجاه نحو تضييق نطاق تطبيق قانون حماية البيانات الشخصية، وبصفة خاصة، في مجال الاستدلال على البيانات الحساسة يؤدى لنتائج سلبية، ولا يعكس حقيقة الحماية المشددة المشروعة للفئات الخاصة المحمية من البيانات.

(124) Sandra Wachter & Brent Mittelstadt, A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI, 2019 COLUM. BUS. L. REV., 2019, p. 494

ومن الإشكالات القانونية، في هذا الصدد، هو الاتجاه الذي اتخذته محكمة العدل الأوروبية بشأن الاستدلالات على البيانات الشخصية، واعتبرت المحكمة أن الغرض من قانون حماية البيانات ليس تقييم دقة عمليات صنع القرار المتعلقة بالبيانات الشخصية، وعلى هذا الأساس، رفضت طلبات المتقدمين للحق في الوصول للمعلومات المستنتجة، لأن نيتهم كانت تقييم دقة تقييم البيانات الشخصية(١٢٥).

ولا يخضع هذا الأمر لقانون حماية البيانات، وقررت محكمة العدل الأوروبية أنه ينبغي الرجوع للقوانين الأخرى المطبقة على الحالة المحددة لتقييم ما إذا كانت إجراءات اتخاذ القرار دقيقة وليس على أساس قانون حماية البيانات الشخصية.

كما أنه في محاولة تضييق نطاق تطبيق قانون حماية البيانات الشخصية، فسرت محكمة العدل الأوروبية حق الوصول للمعلومات والبيانات من قبل صاحب البيانات يقتصر على توفير المعلومات المتعلقة بنطاق البيانات قيد المعالجة (وهو أمر ضروري لتصحيح هذه البيانات أو محوها)، للتحقق من مشروعية المعالجة، أو الاعتراض على المعالجة(١٢٦).

ويترتب على الاعتداد بقضاء المحكمة تأثير بالغ الخطورة حيث أن الاستدلالات على البيانات الشخصية، بل وكذلك البيانات الشخصية الحساسة تمثل خطورة كبيرة على حقوق أصحاب البيانات لما قد يكون لها تأثير بالغ على الحقوق المختلفة.

(125) Cases C-141/12 & 372/12, YS v. Minister voor Immigratie, Integratie en Asiel, 2014 E.C.R. I-2081, PP 45-46.

(126) Case C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, 2009 E.C.R. I-3889, PP 51-52.

كما تستخدم الاستدلالات المؤقتة كوسيلة يتم الاعتماد عليها في الاستنتاجات النهائية والقرارات اللاحقة.

ويؤدي استبعاد الوصول إلى نتائج الاستدلالات ومراجعتها من نطاق قانون حماية البيانات أن أصحاب البيانات لن يكونوا قادرين على تقييم كيفية اتخاذ الاستنتاجات والقرارات ذات التأثير الكبير بشأنهم(١٢٧).

كما يترتب على ذلك إهدار العديد من المبادئ التي تقوم عليها معالجة البيانات الشخصية، وخاصة الحساسة منها، مثل مبادئ المشروعية والدقة والعدالة، حيث أن الاكتفاء بمشاركة ملخص البيانات الشخصية – وفقاً لما قضت به المحكمة- التي تخضع للمعالجة فقط مع صاحب البيانات عبر حق الوصول يحد بشدة من قدرة صاحب البيانات على تقييم مشروعية معالجة البيانات ودقة بياناته الشخصية المستخدمة لإجراء قرار معين.

وعلى ذلك، لا تتوافر الضمانات الكافية لحماية أصحاب البيانات الشخصية الحساسة، خاصة في ظل علاقات القانون الخاص على الرغم من أن استقلالية صنع القرار للكيانات الخاصة مقيدة بقوانين معينة (مثل قانون مكافحة التمييز)، فإن الشركات الخاصة أقل احتمالا من القطاع العام أن يكون لديها إجراءات أو قواعد ملزمة قانونا يتعين عليها إتباعها عند اتخاذ القرارات(١٢٨).

(127) Douwe Korff, The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data, EU Law Analysis (Oct. 15, 2014), http://eulawanalysis.blogspot.com/2014/10/the-proposed-general-data-protection.html [https://perma.cc/SRY9-JDW8]; Robert Madge, Five Loopholes in the GDPR, Medium (Aug. 27, 2017), https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b [https://perma.cc/L8EM-8YPM]

(128) Serge Gutwirth & Paul De Hert, Regulating Profiling in a Democratic Constitutional State, in Profiling the European Citizen, 2008, 275.

كما يظهر تأثير ذلك على التزامات الفاعلين في قانون حماية البيانات الشخصية، مثل حائز البيانات، والمتحكم فيها، والمعالج لها، مما يؤدى تضييق نطاق قانون حماية البيانات الشخصية عدم مسئوليتهم في حالات الاستدلالات على البيانات الشخصية بفئاتها المختلفة، وذلك في وقت انتشار تحليلات البيانات الضخمة والزيادة الناتجة في قدرة مراقبي البيانات على استنتاج معلومات حول الحياة الخاصة للأفراد، وتعديل وترسيخ هويتهم، والتأثير على سمعتهم، يشير إلى أن هناك حاجة إلى مستوى أعلى من الحماية مما كان عليه في السابق.

وبالتالي، وفقًا لمحكمة العدل الأوروبية، عندما تستخلص شركة خاصة استنتاجات من البيانات المجمعة أو تتخذ قرارات بناءً عليها، حتى لو تم النظر إلى الاستنتاجات أو القرارات النهائية على أنها بيانات شخصية، فإن أصحاب البيانات غير قادرين على تصحيحها بموجب قانون حماية البيانات، مما يعطل معها فعالية قانون حماية البيانات في تقرير حماية وحقوق أصحاب البيانات.

كما يفتقر أصحاب البيانات أيضًا إلى إمكانية الوصول إلى الأسباب الكامنة وراء القرارات، والتي لا تعتبر بيانات شخصية، فضلاً عن وسائل تصحيح الاستدلالات بموجب قانون حماية البيانات.

وبالإضافة إلى ذلك وجود صعوبات عديدة ستواجه أصحاب البيانات –حتى مع الاعتراف بعملية الاستدلال كبيانات شخصية- في ظل استخدام البيانات الضخمة وتقنيات الذكاء الاصطناعي والتي يصعب معها الوصول لكيفية إجراء الاستدلالات والتقييمات، بل وإشكالاتها العديدة التي شغلت الفقه الأكاديمي في مجال المسئولية المدنية.

المبحث الثاني

تطبيق قواعد المسئولية المقررة

علي المعالجة والاستدلال على البيانات الحساسة

توضح حيثيات اللائحة العامة لحماية البيانات[١٢٩] مسئولية المعالج ووحدة التحكم في البيانات، حيث تقرر أنه يجب على وحدة التحكم أو المعالج تعويض أي ضرر قد يتعرض له الشخص نتيجة للمعالجة التي تنتهك هذه اللائحة.

(129) GDPR,Whereas (146)," The controller or processor should compensate any damage which a person may suffer as a result of processing that infringes this Regulation. The controller or processor should be exempt from liability if it proves that it is not in any way responsible for the damage. The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law. Processing that infringes this Regulation also includes processing that infringes delegated and implementing acts adopted in accordance with this Regulation and Member State law specifying rules of this Regulation. Data subjects should receive full and effective compensation for the damage they have suffered. Where controllers or processors are involved in the same processing, each controller or processor should be held liable for the entire damage. However, where they are joined to the same judicial proceedings, in accordance with Member State law, compensation may be apportioned according to the responsibility of each controller or processor for the damage caused by the processing, provided that full and effective compensation of the data subject who suffered the damage is ensured. Any controller or processor which has paid full compensation may subsequently institute recourse proceedings against other controllers or processors involved in the same processing."

ووفقاً للقواعد التشريعية لحماية البيانات فإن البيانات الحساسة ليست محلاً للحماية في مجال الاستدلالات إلا إذا تم الاعتماد على البيانات الحساسة من البداية في عملية الاستدلالات كبيانات مدخلات، أو كذلك البيانات الشخصية التى يمكن الاستدلال منها على بيانات حساسة، وكل ذلك سواء أكانت بيانات شخصية أو حساسة كبيانات مدخلات تكون محلاً للحماية وتخضع للقيود القانونية المقررة في شأن جمعها ومعالجتها وتخزينها وإتاحتها.

وما نود الإشارة إليه أن مخرجات عمليات الاستدلال خاصة إذا نتج عنها الوصول لبيانات حساسة يجب أن تكون لها ذات القدر من الحماية القانونية، حتى ولو تم التوصل إليها من خلال بيانات أو أنشطة ليست خاضعة لنطاق قانون حماية البيانات.

وتخضع قواعد المسئولية عن الإخلال بحماية البيانات الحساسة للقواعد العامة في القانون المدني.

لذا، يجب عرض أركان هذه المسئولية من حيث الخطأ والضرر وعلاقة السببية بينهما، كما سنبين دفع هذه المسئولية من خلال السبب الأجنبي، ونبين كذلك طبيعة هذه المسئولية سواء أكانت عقدية أم تقصيرية، ومدى إمكانية تفسير نص اللائحة العامة لحماية البيانات الشخصية المتعلق بالمسئولية على تقريره للمسئولية المفترضة.

ونبين كذلك لأحكام المسئولية وآثارها من حيث قواعد التضامن، والتعويض، وأحكام توزيع المسئولية في حالة تعدد المسئولون.

ونعرض في المطلب الأول لأركان المسئولية المدنية، ونعرض في المطلب الثاني لدفع المسئولية والإعفاء منها، ثم نعرض في المطلب الثالث لطبيعة المسئولية وأحكامها.

المطلب الأول

أركان المسئولية

تقنن اللائحة العامة لحماية البيانات الأوروبية للمسئولية المدنية الناشئة عن معالجة البيانات الشخصية بالمادة (٨٢) من اللائحة، حيث تقرر أن الفعل الموجب للمسئولية هو أي معالجة يتم إجراؤها بشكل مخالف لما قررته اللائحة العامة لحماية البيانات (GDPR)(١٣٠).

(130) GDPR, art. 82, "1.Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. 2.Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. 3.A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage. 4.Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject. 5.Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance

=

ويتطلب تطبيق قواعد المسئولية المدنية ضرورة توافر أركان هذه المسئولية وهى الخطأ والضرر وعلاقة السببية بينهما.

ونعرض لأركان المسئولية المدنية في ضوء القواعد المقررة لحماية البيانات الشخصية بصفة عامة، والبيانات الحساسة بصفة خاصة.

الفرع الأول

الخطأ

وفقاً للقواعد العامة في المسئولية المدنية فإن كل خطأ سبب ضرراً للغير يلزم من ارتكبه بالتعويض(١٣١)، وعلى ذلك يجب لقيام المسئولية المدنية تحقق أركان ثلاثة وهي: الخطأ والضرر وعلاقة السببية بينهما.

وتم الاستقرار بشكل متكرر على تعريف الخطأ بكونه إخلال بالتزام قانوني بما يمثل معه انحراف أو تعدى عن السلوك المألوف للشخص المعتاد، كما يقترب من ذلك الخطأ في المسئولية العقدية باعتباره إخلال بالتزام عقدي، حيث أن التزام المدين بعقد معين يوجب عليه تنفيذ التزامه.

ومناط التعدي هو تجاوز الحدود التي يجب على الشخص الالتزام بها، مع توافر عنصري الإدراك والتمييز من جانب المتعدى، إدراك بأن الفعل يشكل تعدى على حق

=

with the conditions set out in paragraph 2. 4.5.2016 L 119/81 Official Journal of the European Union EN 6.Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2)."

(١٣١) المادة (١٦٣) من القانون المدني المصري.

الغير، والتمييز من خلال توافر الأهلية القانونية والتي تعد من الشروط اللازمة لقيام المسئولية المدنية(١٣٢).

ويتنوع الالتزام العقدي الذي يعد الإخلال به خطأ يوجب المسئولية العقدية إلى التزام بتحقيق نتيجة، والتزام ببذل عناية، بينما يعد الالتزام القانوني الذي يكون الإخلال به موجباً للمسئولية التقصيرية هو دائماً التزام ببذل عناية ومؤداه توافر درجة من اليقظة والبصر في سلوك الشخص كي لا يضر بالغير(١٣٣).

ويظهر دور الخطأ بشكل جلي في مجال معالجة البيانات الشخصية الحساسة، حيث أخضعها المشرع من حيث المبدأ لحظر المعالجة ما لم تتوافر حالة من الحالات الاستثنائية المقررة لجواز معالجتها.

ويشترط بشأن هذه الحالات الاستثنائية التقيد بنطاقها وعدم تجاوز حدود الاستثناء ولا يجوز التوسع فيه أو القياس عليه، وعلى ذلك فإن قيام معالج البيانات بمعالجة بيانات حساسة دون توافر حالة من حالات الاستثناءات المقررة، أو كذلك حالة تجاوز حدود الاستثناء من خلال مثلاً تجاوز حدود المعالجة المسموح بها أو الغرض منها، كان ذلك بمثابة خطأ يوجب مسئولية فاعله تجاه صاحب البيانات(١٣٤).

---

(١٣٢) د. نبيل إبراهيم سعد، مصادر وأحكام الالتزام، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣، ص ٣٨٤.

(١٣٣) د. عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الأول، مصادر الالتزام، منشأة المعارف، الاسكندرية، طبعة ٢٠٠٤، ص ٦٤٤.

(١٣٤) وقضت محكمة النقض المصرية بأنه "قد يقع خطأ الشخص وهو يستعمل حقاً، فإذا جاوز الحدود المرسومة والمشروعة للحق الذي يستعمله، كان هذا أيضاً خطأ موجب للمسئولية." (نقض مدني، جلسة ٢٠١٣/٣/١٣، الطعن رقم ١٥٢٦٠، لسنة ٧٩ ق، مكتب فني ٦٣، ص ٤٢٩)

كما يمكن أن يشكل التعرض للبيانات الحساسة دون سند قانوني خطراً يتعلق بالتدخل في الحياة الخاصة مما يوجب مسئولية فاعله، حيث يجب أن يخضع التدخل في الحياة الخاصة للأشخاص لضوابط مشروعية يقرها القانون.

وتؤكد المحكمة الأوروبية لحقوق الإنسان بشكل متكرر أن "حماية البيانات الشخصية تلعب دورًا أساسيًا في ممارسة الحق في احترام الحياة الخاصة والعائلية[١٣٥].

وبمفهوم المخالفة، إذا كان وصول المتحكم في البيانات الحساسة، وكذلك المعالج لها وصولاً مشروعاً أي كان هذا الأمر يستند لمبرر قانوني، فلا تتحقق مسئوليتهما حتى ولو أصيب صاحب البيانات بضرر بسبب هذا الوصول[١٣٦]، كما يمكن أن يتأسس ذلك، وفقاً للقواعد العامة، بأن من استعمل حقه استعمالاً مشروعاً لا يسأل عما يصيب الغير من ضرر[١٣٧].

ويمكن تقرير معالجة البيانات الحساسة من خلال ارتباط صاحب البيانات بالمتحكم فيها أو المعالج بعقد، وتكون المسئولية في هذه الحالة ضمن نطاق قواعد المسئولية العقدية، كما أن العلاقة بين المتحكم في البيانات والمعالج لها -إذا كان شخص غير المتحكم- تكون دائماً علاقة عقدية[١٣٨].

---

(135) CEDH 4 déc. 2008, S. et Marper c/ Royaume-Uni, req. nos 30562/04 et 30566/04, § 103. – CEDH 18 sept. 2014, Brunet c/ France, req. no 21010/10 , § 35).

(١٣٦) د. عبد العزيز اللصاصمة، المسئولية المدنية التقصيرية عن الفعل الضار، الدار العلمية الدولية ودار الثقافة للنشر، عمان، ٢٠٠٢، ص ١٩٢.

(١٣٧) المادة (٤) من القانون المدني المصري.

(١٣٨) المادة (٣/٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

ويتحقق الخطأ العقدي نتيجة عدم قيام المدين بتنفيذ التزامه الناشئ عن العقد أياً كان السبب في ذلك، ويعد استخلاص الخطأ الموجب للمسئولية العقدية من سلطة محكمة الموضوع التقديرية، ولا رقابة عليه لمحكمة النقض فيه إلا بالقدر الذي يكون استخلاصه غير سائغ(١٣٩).

وإذا كان صاحب البيانات غير مرتبط بعقد في مواجهة المتسبب في الضرر سواء أكان المتحكم أو المعالج أو المعالج من الباطن تطبق في هذه الحالة قواعد المسئولية التقصيرية.

وفي مجال البيانات الحساسة يمكن تقرير مسئولية معالج هذه البيانات حال إخلاله بأي التزام قانوني فرضه المشرع عليه، ويمكن تقرير مسئوليته، على سبيل المثال، في إحدى الحالات الآتية:

أولاً: المعالجة غير القانونية:

ويقصد بذلك ضرورة أن تتم معالجة البيانات بشكل قانوني، ويعني ذلك أن معالجة البيانات الشخصية وكذلك الحساسة يجب أن تتم وفقًا لجميع القواعد القانونية المعمول بها، وهذا يعني الامتثال لقواعد حماية البيانات، ليس هذا فحسب، ولكن أيضًا مع أي قاعدة قانونية أخرى قد تنطبق على حالة معالجة البيانات، مثل الالتزامات المتعلقة بقانون العمل أو قانون العقود أو حماية المستهلك، أو الالتزام بالسرية المهنية في الحالة التي تتطلب ذلك حيث ينطبق ذلك مثلاً على الطبيب الذي يكشف عن اسم أحد مرضاه في منشور على الإنترنت يرتكب معالجة غير قانونية.

(١٣٩) نقض مدني مصري، جلسة ٢٠١٣/١/٢، الطعن رقم ١٦٤٠٣، لسنة ٧٩ ق، مكتب فني ٦٤، ص ٨٣.

وكما يشير البعض[١٤٠] أنه في حالة قيام معالج البيانات بمخالفة أحد الشروط العامة لمعالجة البيانات الشخصية، أو مخالفة أحد الشروط الخاصة بمعالجة بعض الفئات الخاصة من البيانات (الحساسة) فانه يكون مرتكباً لخطأ تقصيري، ويلتزم بتعويض صاحب البيانات عما أصابه من ضرر.

كما يدخل في نطاق مشروعية معالجة البيانات الشخصية الحساسة عدم محو البيانات التي لم تعد ضرورية لأغراض المعالجة أو التي يجب محوها من أجل الامتثال لالتزام قانوني، كما يدخل في نطاق المعالجة غير القانونية سحب الشخص المعني بالبيانات لموافقته على المعالجة[١٤١].

كما يدخل في نطاق ذلك قيام عمليات الاستدلال على البيانات الحساسة من خلال استخدام بيانات شخصية دون موافقة صاحب البيانات، وتكمن خطورة الأمر هنا في كيفية إثباته، حيث يتم استخدام البيانات المستنتجة في إنشاء ملفات تعريف شخصية وجماعية من خلال الأنظمة المتطورة، والتى قد يفاجأ الشخص بنتائجها بعد فترات زمنية طويلة ولا يستطيع التعرف أو إثبات كيفية إنشائها، بل ويمكن استخدامها بشكل يؤثر على حقوقه المشروعة.

(١٤٠) د. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، مجلة الحقوق، جامعة الكويت، مجلد ٣٥، عدد ٣، ٢٠١١، ص ٤٣٤.

(141) Céline Castets-Renard , Brève analyse du règlement général relatif à la protection des données personnelles, Dalloz, IP/IT, 2016, p. 331.

ثانياً: المعالجة بشكل غير عادل وشفاف:

يجب معالجة البيانات ليس بشكل قانوني فحسب، بل أيضًا "بشكل عادل وشفاف(١٤٢).

ويعد خطأ الإخلال بمباديء العدالة والشفافية، ويتحقق ذلك في حالة الحصول على البيانات أو معالجتها بطرق أو وسائل غير عادلة، عن طريق الخداع، وفي إحدى الوقائع تم قيادة مستخدمي فيسبوك الذين استجابوا لاختبار الشخصية المعنية للاعتقاد بأنهم كانوا يعملون في إطار دراسة جامعية وأن الهدف المنشود كان أكاديميًا، بينما في الواقع كان الهدف من جمع البيانات هو التنقيب التجاري والسياسي(١٤٣).

ولا يجوز أن تتم معالجة البيانات دون معرفة الأشخاص الذين تتعلق بهم البيانات، بطريقة قد تكون غير متوقعة أو لا يمكن التنبؤ بها تمامًا بالنسبة لهم، ويجب أن يكون أصحاب البيانات، مع المعرفة الكاملة بالحقائق، قادرين على إقامة علاقة ثقة مع أولئك الذين يعالجون بياناتهم الشخصية(١٤٤).

---

(142)GDPR, Art. 5, § 1er, a.

(143) C. Cadwalladr et E. Graham-Harrison, « Revealed : 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », The Guardian, 17 mars 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook- influence-us-election ; M. Rosenberg, N. Confessore et C. Cadwalladr, « How Trump Consultants Exploited the Facebook Data of Millions », The New York Times, 17 mars 2018, https://www.cnil.fr/fr/affaire-cambridge-analytica-facebook ; CNIL, « Affaire Cambridge Analytica/Facebook », 12 avril 2018, https://www.cnil.fr/fr/affaire- cambridge-analytica-facebook.

(144) E. Degrave, « Le Règlement général sur la protection des données et le secteur public », Rev. Droit communal, 2018, p. 4-5. Égal. Groupe 29, =

وعلى الرغم من تأييدنا الكامل لحقوق أصحاب البيانات المشروعة في حقهم بمعرفة المعالجة، مع الأخذ في الاعتبار توقعاتهم المعقولة، وكذلك المصالح المشروعة للمعالجين أو القائمين على عمليات الاستدلال إلا أن ذلك جد مختلف في مجال عمليات الاستدلال في عصر البيانات الضخمة والذكاء الاصطناعي، حيث لم يعد الأمر يحتاج للقيود القانونية المقررة حالياً بصورة مشددة للبيانات الحساسة حيث أصبح بإمكانهم التوصل للبيانات الحساسة من خلال بيانات عادية وبيانات مجهولة لا تخضعان للحماية القانونية، ويمكن استخدامهما من خلال ربطهما بمجموعات متباينة من البيانات الأخرى والوصول لاستنتاجات عالية الدقة بشأن البيانات الحساسة، الأمر الذي دعانا مراراً وتكراراً من خلال هذه الدراسة لضرورة توفير الحماية التشريعية المناسبة للبيانات الحساسة على المستويين المحلي والعالمي.

ثالثاً: الإخلال بغرض المعالجة:

يعد مبدأ تحديد الغرض أو "مبدأ الغرض"، كما يطلق عليه عادة، حجر الزاوية الحقيقي لحماية البيانات، وهو يتطلب جمع البيانات لأغراض محددة وصريحة ومشروعة، ولا تتم معالجتها لاحقًا بطريقة تتعارض مع هذه الأغراض.

ولذلك يجب أن تكون أغراض معالجة البيانات محددة وواضحة منذ البداية، ويمكن تنفيذ جميع العمليات على هذه البيانات التي سيتم اعتبارها متوافقة مع هذه الأغراض الأصلية(١٤٥).

=

Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018, WP 260 rev.01, § 2

(145) Groupe 29, Opinion 03/2013 on purpose limitation, WP 203, 2 avril 2013, p. 11-12.

وفي مجال إثبات الخطأ، فإن الدائن بالالتزام العقدي يقع عليه عبء إثبات عدم قيام المدين بتنفيذه، مما يحق للأول أن يطالب بتعويض عن الضرر الذي لحق به جراء عدم تنفيذ المدين لالتزامه.

وعلى ذلك إذا لم يقم المتحكم أو المعالج للبيانات بتنفيذ الالتزامات المقررة عليه بمقتضي القانون والرابطة العقدية بينه وبين الشخص المعنى بالبيانات فيكون ذلك بمثابة خطأ عقدي يرتب مسئوليته بالتعويض بشرط إثبات صاحب البيانات الضرر المادي أو المعنوي الذي لحق به جراء خطأ المتحكم أو المعالج.

وفي حالة عدم توافر الرابطة العقدية يمكن الرجوع بأحكام المسئولية التقصيرية حال إخلال المتحكم في البيانات بأي التزام فرضه القانون عليه، وبشرط ثبوت الضرر المادي أو الأدبي جراء خطأ المتحكم أو المعالج.

وإذا تعدد المتحكمون في البيانات الشخصية، فإن كل منهم يلتزم بما قرره المشرع من التزامات، ويحق لصاحب البيانات ممارسة حقوقه تجاه كل منهم على حدة(١٤٦).

وفي حالة وجود أكثر من معالج للبيانات، فالأصل هو الرجوع للعقود المنظمة لعمل هؤلاء المعالجين لتحديد التزاماتهم ومسئوليتهم، وفي حالة عدم وجود عقد فإن كل معالج منهم يلتزم بكافة الالتزامات المقررة بقانون حماية البيانات الشخصية(١٤٧).

(١٤٦) المادة (٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.
(١٤٧) المادة (٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

الفرع الثاني

الضرر

يعد الضرر ركناً جوهرياً في المسئولية المدنية، ويعد ثبوت الضرر شرط لازم لقيام المسئولية، ويستوي في إيجاب التعويض عن الضرر أن يكون الضرر مادياً أو أدبياً.

ويمكن تعريف الضرر بكونه إخلال بمصلحة للمضرور، وهى مصلحة معتبرة، سواء أكانت مصلحة مادية أي ذات قيمة مالية فيكون الضرر مادياً، أو كانت مصلحة غير مالية وهو الضرر الأدبي.

ويجب لتحقق المسئولية المدنية قيام المضرور بإثبات الضرر الواقع عليه سواء أكان ضرراً مادياً أم ضرراً أدبياً، ويؤكد القضاء بشكل مستقر على ضرورة إثبات الضرر في دعوى المسئولية المدنية(١٤٨).

ويشترط في الضرر المادي الذي يجوز التعويض عنه أن يكون ضرراً حالاً، وأن يكون محقق الوقوع سواء بوقوعه فعلاً أو بحتمية وقوعه، بينما لا يجوز التعويض عن الضرر الاحتمالي غير محقق الوقوع ولا يستحق التعويض عنه إلا بوقوعه بالفعل.

وتجدر الإشارة هنا إلى أنه يمكن أن يترتب على معالجة البيانات الشخصية الحساسة مثل البيانات المالية أو البيانات الصحية حدوث خطأ في المعالجة مما ترتب

(148) Cour d'appel de Pau, Chambre sociale, 1 juin 2023 / n° 21/02773.

على ذلك ضرراً للمعنى بالبيانات مما يجيز له الرجوع بالمسئولية المدنية والمطالبة بالتعويض عن الضرر الواقع فعلياً عليه.

كما أن الضرر هنا نتيجة المعالجة الخطأ للبيانات الحساسة يمكن أن يترتب عليها تفويت فرصة محققة على الشخص المعني بالبيانات، ووفقاً للقواعد العامة يجوز التعويض عن تفويت الفرصة باعتبار أن تفويتها يعد أمراً محققاً حتى ولو كانت الفرصة في ذاتها أمراً احتمالياً، ولا يمنع القانون من أن يدخل في عناصر التعويض ما كان المضرور يأمل الحصول عليه من كسب من وراء تحقق الفرصة بشرط أن يكون ذلك قائماً على أسباب مقبولة من شأنها –وفقاً للمجرى العادي للأمور- ترجيح كسب فوته عليه العمل الضار غير المشروع(١٤٩).

وقد أوضحت محكمة العدل الأوروبية هذا الحق في التعويض واعتبرت أن مجرد المخالفة لأحكام اللائحة العامة لحماية البيانات لا تكفي لمنح الحق في التعويض، بل يجب أن يحصل مفهوم "الضرر"، وبشكل أكثر تحديدًا في هذه الحالة، مفهوم "الضرر المعنوي"، على تعريف مستقل وموحد خاص بقانون الاتحاد؛ وبالتالي لا يمكن جعل التعويض عن الضرر المعنوي مشروطاً بأن يصل الضرر الذي لحق بالشخص المعني إلى درجة معينة من الخطورة(١٥٠).

كما تؤكد حيثيات اللائحة العامة لحماية البيانات(١٥١)، أنه يجب على وحدة التحكم أو المعالج تعويض أي ضرر قد يتعرض له الشخص نتيجة للمعالجة التي تنتهك هذه

(١٤٩) نقض مدنى، جلسة ١٠/ ١٩٩٤/١١، الطعن رقم ٤٣٠٠، لسنة ٦٣ ق، مكتب فني ٤٥، ج ٢، ص ١٣٦٣.

(150) (CJUE 4 mai 2023, no C-300/21).

(151) Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing =

اللائحة، وينبغي تفسير مفهوم الضرر على نطاق واسع، في ضوء السوابق القضائية لمحكمة العدل التابعة للاتحاد الأوروبي (CJEU)، بطريقة تأخذ في الاعتبار الكامل أهداف اللائحة، والمتمثلة في ضمان الإنصاف الفعال للشخص المعني، وضرورة إصلاح الخسارة الناتجة عن الضرر بالكامل.

ولا شك أن جمع البيانات الشخصية الحساسة مثل البيانات الصحية والمالية، وكذلك تخزينها دون إذن أو موافقة صاحب البيانات، وكذلك معالجتها دون سند قانوني قد يصيب الشخص المعني بالبيانات بضرر مادي أو ضرر معنوي، نتيجة شعوره بانتهاك حرمة حياته الخاصة، وحقه في الخصوصية من خلال الاطلاع على بياناته الحساسة، بل وإمكانية إفشائها للغير(١٥٢).

كما ترتبط البيانات الشخصية الحساسة بالحق في الخصوصية ارتباطاً وثيقاً، فأي اعتداء على البيانات الحساسة يمكن معه أن يمثل اعتداء على الحياة الخاصة والحق في الخصوصية، مما يعتبر معه، وبلا شك، ضرراً يصيب الشخص المعني بالبيانات، حتى ولو كان فقط ضرراً أدبياً أو معنوياً، ويكفي وحده لقيام المسئولية والحكم بالتعويض أياً كان حجم الضرر ومقداره.

=

of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119)Whereas (146).

(١٥٢) د. سامح عبد الواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسئولية التقصيرية عن معالجتها: دراسة في القانون الإماراتي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، عدد ٦٧، ٢٠١٨، ص ٦٥٤.

وعلى ذلك يعد إفشاء البيانات المالية وكذلك البيانات الصحية، أو المعتقدات الدينية، أو الآراء السياسية يمكن أن يصيب صاحب البيانات بأضرار مادية وأدبية تستحق معها ضرورة التعويض.

كما يمكن تحقق الضرر الأدبي الذي يصيب الشخص من مجرد الاعتداء على حق ثابت له، فأي اعتداء على حق ثابت لشخص معين يجيز له المطالبة بالتعويض عن الضرر الأدبي الذي لحق به سواء تمثل في إيذاء الشخص في شرفه أو اعتباره أو عاطفته واحساسه ومشاعره مما يلحق بالشخص حزناً وغماً وأسى مما يعتبر ذلك معه ضرراً أدبياً.

وتعتبر محكمة النقض المصرية أن الضرر الأدبي يجد محله في وجدان الإنسان وهو مستودع فكره ومشاعره وأحاسيسه وسبب تكريمه على ما عداه من المخلوقات باعتبارها مجرد موجودات مالية مسخرة له، ذلك أن قدرة الإنسان على الكسب منوطة باستقراره، بل إن كل ما سبق له كسبه يغدو عديم القيمة إذا لم يستقر وجدانه وإن تفاوت الضرر الناشئ عن الاعتداء عليه من شخص لآخر طبقاً لاعتبارات عدة ترجع لشخص المضرور والظروف الملابسة، وهو على هذا النحو – وبحسبانه خسارة غير مالية – لا يمكن محوه وإزالته بالتعويض النقدي، ولكن قصارى ما قصده المشرع من النص عليه أن يوجد لهذا الضرر معادلاً موضوعياً يرمز له ويتكافأ معه يحمل عنه أو معه نير الألم والحزن والأسى فيخفف عنه ذلك(١٥٣).

ولا يوجد معياراً لحصر أحوال التعويض عن الضرر الأدبي، وعلى ذلك، يمكن اعتبار كل ضرر يصيب الشخص في شرفه أو اعتباره أو عاطفته واحساسه ومشاعره

(١٥٣) في هذا المعني: نقض مدني، جلسة ٢٠٠٨/١/٢٨، الطعن رقم ٩٢٧٤، لسنة ٦٥ ق، مكتب فنى ٥٩، ص ١٦٠.

ممـا يلحـق بالشـخص حزنـاً وغمـاً وأسـى بمثابـة ضـرر أدبـي يجيـز المطالبـة عنـه بالتعويض[١٥٤].

الفرع الثالث

علاقة السببية

يتبين من القواعد العامة في المسئولية المدنية أن علاقة السببية هي أحد أركان المسئولية المدنية، ويشترط أن يكون هناك سببية بين الخطأ والضرر الذي يجوز التعويض عنه.

ومؤدى ذلك أنه يجب أن يكون للانتهاك أو المخالفة المشكلة لخطأ مدني علاقة سببية بضرر مادي أو معنوي حتى يتم تقرير المسئولية المدنية عنه، يستوي في ذلك المسئولية العقدية والمسئولية التقصيرية.

كما أن السببية كفكرة قانونية تعد عنصراً لازماً ليس فقط لانعقاد المسئولية المدنية، بل أيضاً لتحديد مدى التعويض كأثر قانوني يترتب على انعقادها[١٥٥].

ومن الجدير بالذكر أن علاقة السببية قد تظهر بشكل مستقل عن الخطأ، ويظهر هذا الاستقلال بشكل واضح في حالة كون المسئولية المدنية قائمة على خطأ مفترض، بينما لا يظهر هذا الاستقلال بوضوح في حالة الخطأ واجب الإثبات[١٥٦].

---

(١٥٤) وقرر المشرع المصري التعويض عن الضرر الأدبي بموجب المادة (١/٢٢٢) من القانون المدني والتى تقرر" يشمل التعويض الضرر الأدبي أيضاً، ولكن لا يجوز في هذه الحالة أن ينتقل إلى الغير إلا إذا تحدد بمقتضي اتفاق، أو طلب الدائن به أمام القضاء".

(١٥٥) د. ثروت عبد الحميد، النظرية العامة للالتزامات في القانون المدني المصري، الجزء الأول، مصادر الالتزام، بدون دار نشر، بدون سنة نشر، ص ٤٣٣.

(١٥٦) د. عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الأول، مصادر الالتزام، مرجع سابق، ص ٧٣٣.

ويتبين ذلك في حالة كون الخطأ واجب الإثبات حيث يجب على المضرور إثبات الخطأ، وفي الغالب يكون إثبات المضرور للخطأ هو السبب في إحداث الضرر، وهو ما يعني أن إثبات الخطأ يؤدى لإثبات علاقة السببية، فتستتر السببية وراء الخطأ ولا يظهر بوضوح كونها ركن مستقل.

وفي مجال المسئولية المدنية عن الإخلال بالقواعد المنظمة للبيانات الحساسة، يجب أن يكون الإخلال من قبل المتحكم في البيانات أو من قبل معالج البيانات هو السبب وراء حدوث الضرر للشخص المعني بالبيانات.

وعلى ذلك، وعلى سبيل المثال، يمكن تحقق الضرر الموجب للمسئولية بسبب إخلال معالج البيانات أو المتحكم بالشروط الواجب توافرها لجمع ومعالجة وتخزين ونقل وإتاحة البيانات الحساسة، مثل كون الضرر قد تحقق بسبب جمع البيانات لأغراض غير مشروعة، أو تم جمعها ومعالجتها لأغراض غير المعلن عنها للشخص المعني بالبيانات، أو أن البيانات المجمعة كانت غير صحيحة وغير سليمة ومؤمنة وترتب على ذلك ضرر للشخص المعني بالبيانات، أو كذلك تم إتاحتها ونشرها مما أصيب معها الشخص المعنى بالبيانات بضرر سواء مادي أو أدبي.

المطلب الثاني

دفع المسئولية والإعفاء منها

نعرض من خلال هذا المطلب لحالتي دفع المسئولية، والإعفاء منها، حيث يمكن دفع المسئولية بتوافر حالة من اثنين وهما: إثبات أن الضرر كان غير مباشر ولم يكن نتيجة طبيعية للخطأ، أو كذلك بإثبات السبب الأجنبي.

كما يمكن الإعفاء من المسئولية، ويتوقف ذلك على تحديد طبيعة المسئولية ومدى كونها عقدية أو تقصيرية.

الفرع الأول

دفع المسئولية

يجب لانتفاء المسئولية المدنية أن يثبت الشخص- المدعى عليه في دعوى التعويض- أن الضرر الذي وقع بالمضرور لا يد له فيها، ويمكن تحقق ذلك بإحدى صورتين، وهما: (١) إثبات أن الضرر الواقع على المضرور كان ضرراً غير مباشر، أي أنه لم ينتج عن الخطأ بشكل مباشر(١٥٧)، (٢) أو إثبات أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه(١٥٨)، وهو ما ينتفي من خلاله علاقة السببية بين الخطأ والضرر.

ويُعفى المتحكم أو المعالج من المسئولية إذا أثبت أنه ليس مسئولاً بأي شكل من الأشكال عن الفعل الذي أدى إلى حدوث الضرر(١٥٩).

(١٥٧) تنص الفقرة الأولى من المادة (٢٢١) من القانون المدني المصري على أنه " إذا لم يكن التعويض التعويض مقدراً في العقد أو بنص في القانون، فالقاضي هو الذي يقدره، ويشمل التعويض ما لحق الدائن من خسارة وما فاته من كسب، بشرط أن يكون هذا نتيجة طبيعية لعدم الوفاء بالالتزام أو للتاخير في الوفاء به، ويعتبر الضرر نتيجة طبيعية إذا لم يكن في استطاعة الدائن أن يتوقاه ببذل جهد معقول".

(١٥٨) تنص المادة (١٦٥) من القانون المدني المصري على " إذا أثبت الشخص أن الضرر قد نشأ عن سبب أجنبي لا يد له فيه، كحادث مفاجيء أو قوة قاهرة أو خطأ من المضرور أو خطأ من الغير، كان غير ملزم بتعويض هذا الضرر، ما لم يوجد نص أو اتفاق على غير ذلك".

(159) GDPR,art. 82 (3), " A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage."

كما أن مسئولية معالج البيانات إنما تتقرر عن الضرر الناجم عن المعالجة بسبب عدم امتثاله للالتزامات القانونية المفروضة عليه، كما تتقرر مسئولية حال خروجه عن التعليمات القانونية المقررة على وحدة التحكم في البيانات.

وعلى ذلك، تتقرر مسئولية المتحكم في البيانات الحساسة بحكم كونه المسئول قانوناً عن وضع طريقة وأسلوب ومعايير المعالجة طبقاً للغرض المحدد للمعالجة، وفي هذا الصدد، قرر المشرع المصري جواز تفويض المعالج في ذلك بموجب تعاقد مكتوب(١٦٠).

ووفقاً للقواعد العامة، يمكن دفع المسئولية المدنية بانعدام السببية لقيام السبب الأجنبي(١٦١)، والمتمثل في قوة قاهرة أو حادث مفاجئ أو خطأ من المضرور، أو خطأ الغير(١٦٢).

ومؤدى ذلك أنه إذا كان الضرر الواقع على الشخص المعني بالبيانات لم يكن نتيجة إخلال المتحكم أو المعالج لالتزاماته القانونية فتنتفي في هذه الحالة مسئوليته المدنية.

(١٦٠) المادة (٣/٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(١٦١) المادة (١٦٥) من القانون المدني المصري.

(١٦٢) وبينت المذكرة الايضاحية للمشروع التمهيدى للقانون المدني المصري أنه يكون السبب الأجنبي بوجه عام حادثاً فجائياً أو قوة قاهرة –وليس ثمة محل للتفريق بينهما- أو خطأ وقع من المضرور أو من الغير، وهذا البيان غير وارد على سبيل الحصر، فقد يكون السبب الأجنبي عيباً لاصقاً بالشيء، أو مرضاً بالمضرور". (مجموعة الأعمال التحضيرية، ج ٢، ص ٣٧٨)

الفرع الثاني

الإعفاء من المسئولية

يمكن للشخص المعني بالبيانات (المضرور) الرجوع على المتسبب في الضرر سواء أكان المتحكم أم المعالج للبيانات الشخصية الحساسة بموجب قواعد المسئولية العقدية أو التقصيرية على حسب الأحوال.

ويكمن تميز المسئولية العقدية عن المسئولية التقصيرية في وجود الإرادة الحرة التي تنشأ العلاقة العقدية، والذي يعتبر العقد معها وليد إرادة المتعاقدين، وعلى ذلك تعتبر الإرادة الحرة هي أساس المسئولية العقدية، وبناء عليه تنشأ المسئولية العقدية من خلال الإرادة الحرة، ويجوز كذلك تعديل أحكامها بالإرادة الحرة طالما تم هذا التعديل في إطار القانون واحترام قواعد النظام العام والآداب.

ولا يتحقق وجود الإرادة الحرة بشكل مسبق في مجال المسئولية التقصيرية، بل أنها تتقرر بحكم القانون، مما لا يجوز معها تعديل قواعدها بالاتفاق، كما قرر المشرع المصري ببطلان كل شرط يقضي بالإعفاء من المسئولية المترتبة على العمل غير المشروع(١٦٣).

ويجوز الاتفاق في حالة المسئولية العقدية على تعديل قواعد المسئولية تشديداً مثل تحمل المدين المسئولية حتى في حالة وجود السبب الأجنبي، كما يجوز الاتفاق على تعديلها تخفيفاً.

(١٦٣) المادة (٣/٢١٧) من القانون المدني المصري.

وتقيداً بحدود النظام العام والذي يقيد من حرية المتعاقدين، فلا يجوز الاتفاق على تعديل قواعد المسئولية العقدية التي تنشأ عن الفعل العمدى أو الخطأ الجسيم للمدين، وإن كان يجوز الاتفاق على إعفاء المدين من الخطأ العمدى أو الخطأ الجسيم الصادر عن أشخاص يستخدمهم المدين في تنفيذ التزاماته(١٦٤).

ومن خلال العقود المنظمة لعلاقات المتحكمين بعضهم ببعض، وكذلك العقد المنظم لعلاقة المتحكم بالمعالج، وعلاقة المعالج الأصلي بالمعالج من الباطن يمكن من خلال بنود هذه التعاقدات أن تنظم تقاسم المسئولية مسبقًا، عن طريق بنود تحديد المسئولية، وكذلك الإعفاء منها.

وفي نطاق المسئولية العقدية يقع باطلاً كل شرط يؤدى لإفراغ الالتزام الأساسي للمدين من جوهره(١٦٥)، وكما يشير البعض إلى أن الالتزام الأساسي أو الجوهري إنما يكيف وفقاً لطبيعة الجزاء على مخالفته(١٦٦).

كما أنه، على سبيل المثال، إذا تم الاتفاق بمقتضى العقد على حد أقصي لمبلغ التعويض وكان هذا الحد منخفضًا بشكل غير طبيعي، فيجوز في هذه الحالة إعادة النظر في مقدار التعويض المستحق(١٦٧)، كما يجوز ذلك حالة ثبوت إهمال جسيم والذي يتصف

(١٦٤) المادة (٢/٢١٧) من القانون المدني المصري.

(165) Art. 1170 (Ord. no 2016-131 du 10 févr. 2016, art. 2, en vigueur le 1er oct. 2016) Toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite.

(166) Ph. Jestaz, L'obligation et la sanction: A la recherche de l'obligation fondamentale: in Ph. Jestaz, Autour du droit civil. Écrits dispersés, idées convergentes, Dalloz, 2005, p. 325.

(167) Cour de cassation, Troisième chambre civile, 23 mai 2013, n° 12-11.652. & Cour de cassation, Chambre commerciale, 13 février 2007, n° 05-17.407.

بسلوك بالغ الخطورة يصل إلى حد الغش ويدل على عدم قدرة المدين على القيام بالمهمة التعاقدية التي قبلها.

كما قضي بأنه لا يجوز للمدين الذي يكون التزامه الأساسي تسليم عمل معين أن يعفي نفسه من التزامه من خلال شرط إعفاء المسئولية بطريق المراوغة، ويجب اعتبار هذا الشرط باطلاً بما يتعارض مع نطاق التزامه(١٦٨).

وفي نطاق عقد التأمين يمكن إبطال شرط استبعاد الضمان إذا كان يتعارض هذا الاستبعاد مع جوهر التزام المؤمن(١٦٩)، كما يجب التقيد بنطاق استبعاد الضمان وفقاً لما هو مقرر قانوناً بشرط ألا يفرغ الضمان من جوهره(١٧٠).

وعلى ذلك، وفي نطاق معالجة البيانات الحساسة، وحالة تنظيم العلاقة القانونية بين صاحب البيانات والمتحكم في البيانات، وكذلك العلاقات العقدية الأخرى بين المتحكم والمعالج للبيانات، وكذلك تنظيم علاقة المعالج من الباطن فإن أي بند في شروط التعاقد يفرغ الالتزام الأساسي على عاتق المتحكم أو المعالج أو المعالج من الباطن يكون باطلاً ولا يعتد به في مواجهة الطرف الأولى بالرعاية وهو صاحب البيانات.

ويظهر ذلك، بشكل جلي، حال إخلال المتحكم في البيانات أو المعالج لها لالتزاماته بشكل متعمد أو نتيجة ارتكابه لخطأ جسيم أو غش، مما ترتب عليه الإضرار بصاحب البيانات سواء أضرار مادية أو أدبية.

---

(168) Cour de cassation, Chambre commerciale, 9 juin 2009, n° 08-10.350.

(169) Cour de cassation, Deuxième chambre civile,12 octobre 2023, n° 22-13.759.

(170) Cour de cassation, Deuxième chambre civile, 1 décembre 2022, n° 21-19.342.

كما يمكن إبطال أي شرط في بنود التعاقد يخل بالمبادئ الأساسية لمعالجة البيانات، مثل مبدأ مشروعية المعالجة، والتناسب، وتقليل البيانات، والتقيد بنطاق وغرض المعالجة.

كما يمكن إبطال الشروط الواردة بالتعاقد والتي من شأنها الإخلال بالحقوق والحريات الأساسية للشخص المعني بالبيانات.

المطلب الثالث

طبيعة المسئولية وأحكامها

يمكن تحديد طبيعة المسئولية المدنية عن معالجة البيانات الشخصية الحساسة بالنظر للعلاقات الحاكمة لهذه المسئولية.

وتتحدد هذه العلاقات والروابط من خلال عدة صور، منها علاقة المتحكم في البيانات بصاحب البيانات، وعلاقة المتحكم في البيانات بمعالج البيانات، وعلاقتهما بصاحب البيانات.

ويترتب على ذلك آثار قانونية فيما يتعلق بمسائل التضامن، والتعويض، وتوزيع عبء المسئولية.

الفرع الأول

طبيعة المسئولية

تتقرر مسئولية مراقب البيانات أو المتحكم بموجب القواعد القانونية المنظمة لحماية البيانات الشخصية بما فيها البيانات الحساسة.

ولتنظيم مسئولية المتحكم في البيانات، يجب أن نبين علاقة المتحكم بصاحب البيانات، وكذلك علاقة المتحكم بالمعالج للبيانات، ونوضح ذلك فيما يلي:

أولاً: علاقة المتحكم في البيانات بصاحب البيانات:

وفقاً للائحة العامة لحماية البيانات الشخصية (GDPR) فإن مسئولية مراقب البيانات أو المتحكم فيها هي مسئولية مفترضة حيث يسأل عن تعويض الأضرار الناجمة عن معالجة البيانات الشخصية بالمخالفة لأحكام وقواعد ومبادئ المعالجة المقررة باللائحة وقوانين حماية البيانات الشخصية(١٧١).

كما يسري هذا الأمر على مسئولية كل مراقب أو متحكم شارك في المعالجة بالمخالفة للقواعد المنظمة لحماية البيانات الشخصية الحساسة.

كما يجوز مساءلة المتحكم في البيانات، وفقاً لأحكام القانون المصري، في مواجهة صاحب البيانات، حال إخلاله بالالتزامات القانونية المفروضة عليه قانوناً،

(171) GDPR, art. 82 (2), "Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller."

ويستوي في ذلك أن تكون هناك علاقة عقدية تربط بينهما، أو الرجوع بالمسئولية التقصيرية في حالة عدم وجود عقد بينهما ويكون الرجوع وقتئذ بمقتضي الإخلال بالتزامات قانونية(١٧٢).

وفي حالة وجود أكثر من متحكم في البيانات فإن لصاحب البيانات ممارسة حقوقه تجاه كل متحكم على حدة، دون وجود تضامن بينهم، ويلتزم كل منهم في مواجهة صاحب البيانات بالالتزامات القانونية المقررة على عاتق المتحكم.

ثانياً: علاقة المتحكم في البيانات بمعالج البيانات:

تتقرر مسئولية المعالج للبيانات الحساسة في حالتين: (١) إخلاله بالتزامات المعالجين المقررة باللائحة العامة لحماية البيانات، (٢) المعالجة بشكل خارج أو متعارض مع التعليمات القانونية لوحدة التحكم(١٧٣).

كما أن تفويض المعالج للبيانات للقيام بعملية المعالجة إنما يستند لتعاقد مكتوب بموجب أحكام القانون المصري، وهو ما يتطلب معه وجود عقد يربط بين المتحكم في البيانات بالمعالج(١٧٤).

ويوضح ذلك بأن مسئولية المعالج تتقرر دائماً بالنظر للرابطة العقدية التي تربط بين المراقب أو المتحكم في البيانات بالمعالج، وعندئذ يجب الرجوع لأحكام هذا التعاقد لتقرير التزامات المعالج، ولتحديد الخطأ الذي يمكن نسبته إليه، كما يلتزم المعالج

(١٧٢) بشأن التزامات المتحكم في البيانات، راجع: المادة (٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(173) GDPR, art. 82 (2).

(١٧٤) المادة (٣/٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

للبيانات، بشكل عام، بالالتزامات القانونية المقررة باللائحة العامة وقوانين حماية البيانات الشخصية.

وعلى ذلك، فإن مسئولية المعالج تكون في مواجهة المتحكم مسئولية عقدية، وقوامها إخلال المعالج بالتزام عقدي تم تقريره بموجب العقد المنظم لحقوق والتزامات المعالج بوحدة التحكم، أو إخلال بالتزام قانوني فرضه المشرع على المعالج للبيانات.

بينما قد تكون العلاقة القانونية بين المعالج للبيانات وصاحب البيانات تظل خاضعة لنطاق المسئولية التقصيرية، لعدم وجود عقد يربط بينهما، وتنشأ هذه المسئولية بتوافر شرائطها من خطأ يتمثل في إخلال بالتزام قانوني، وضرر مادي أو أدبي لحق بالشخص المعني بالبيانات، وتوافر علاقة السببية بين الخطأ والضرر.

الفرع الثاني

أحكام المسئولية

أولاً: التضامن:

يعد التضامن وصف من أوصاف الالتزام، فيحول دون انقسام الالتزام في حالة تعدد الدائنين أو تعدد المدينين، كما يعد الأصل في الالتزام انقسامه على عدد أطرافه إذا تعددوا، والاستثناء هو أن يكونوا متضامنين، ولذلك يجب أن تكون العبارات المستخدمة لتقرير التضامن دالة عليه بطريقة لا تقبل الشك، يستوي في ذلك أن يرد بعبارة صريحة أو ضمنية(١٧٥).

(١٧٥) د. محسن عبد الحميد إبراهيم البيه، النظرية العامة للالتزامات، الجزء الثاني، أحكام الإلتزام، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠١-٢٠٠٢، ص ٤١١.

ووفقاً للقواعد العامة، فإن التضامن سواء بين الدائنين أو بين المدينين لا يفترض، وإنما يكون بناء على اتفاق أو نص في القانون(١٧٦).

وتقرر اللائحة العامة الأوروبية لحماية البيانات الشخصية أنه عندما يشارك أكثر من وحدة تحكم أو معالج، أو كلاً من وحدة التحكم والمعالج، في نفس المعالجة فإنهم يكونوا مسئولين عن أي ضرر ناتج عن المعالجة، ويتحمل كل وحدة تحكم أو معالج المسئولية عن الضرر بأكمله من أجل ضمان التعويض الفعال لصاحب البيانات(١٧٧).

ولم يقرر المشرع المصري بقانون حماية البيانات الشخصية نصاً يتعلق بالتضامن في حالة المسئولية المدنية عن معالجة البيانات، بل قرر المشرع المصري أنه في حال وجود أكثر من متحكم فإنه يلتزم كل منهم بكافة الالتزامات المقررة بقانون حماية البيانات الشخصية، ويحق للشخص المعنى بالبيانات مباشرة حقوقه في مواجهة كل متحكم على حدة(١٧٨).

كما قرر المشرع المصري أنه في حالة وجود أكثر من معالج فإنه يلتزم كل منهم بكافة الالتزامات المقررة بقانون حماية البيانات الشخصية، وذلك في حالة عدم وجود عقد يحدد بوضوح التزامات كل منهم(١٧٩).

---

(١٧٦) المادة (٢٧٩) من القانون المدني المصري.

(177) GDPR, art. 82 (4), " Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject."

(١٧٨) المادة (٤) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

(١٧٩) المادة (٥) من القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

ويجوز لوحدة التحكم في البيانات الشخصية، وكذلك البيانات الشخصية الحساسة، الاستعانة بمعالج يقوم نيابة عنها بمعالجة البيانات، وفرضت اللائحة العامة قيداً على وحدة التحكم في ذلك وهو أن تستخدم فقط المعالجات التي توفر ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تلبي المعالجة متطلبات هذه اللائحة وتضمن حماية حقوق موضوع البيانات(١٨٠).

ولا يجوز للمعالج إشراك معالج آخر دون الحصول على إذن كتابي محدد أو عام مسبق من وحدة التحكم، وفي حالة التفويض الكتابي العام، يجب على المعالج إبلاغ وحدة التحكم بأي تغييرات مقصودة تتعلق بإضافة أو استبدال معالجات أخرى، مما يمنح وحدة التحكم الفرصة للاعتراض على هذه التغييرات(١٨١).

وفي علاقة وحدة التحكم بالمعالج فإنها علاقة عقدية حيث تخضع المعالجة بواسطة المعالج لعقد، وهو عقد ملزم للمعالج فيما يتعلق بوحدة التحكم، ويجب أن يشتمل هذا العقد على موضوع المعالجة، ومدتها، وطبيعتها، والغرض من المعالجة، ونوع البيانات الشخصية، وفئات أصحاب البيانات، وكافة الالتزامات المختلفة.

وفي مجال المسئولية العقدية فإن التضامن لا يفترض بل يجب أن يتم الاتفاق عليه في العقد أو يقرره نص القانون، وفي هذه الحالة، حتى ولو لم يتم الاتفاق على شرط التضامن في العقد، فانه مفترض بموجب اللائحة العامة لحماية البيانات الشخصية.

وفي حالة قيام المعالج الأصلي بتفويض معالج غيره للقيام بعملية المعالجة، فإن نفس التزامات حماية البيانات المنصوص عليها في العقد أو أي إجراء قانوني آخر بين

(180) GDPR, art. 28 (1).
(181) GDPR, art. 28 (2).

وحدة التحكم والمعالج تُفرض كذلك على المعالج الآخر عن طريق عقد أو إجراء قانوني آخر، ولا سيما توفير ضمانات كافية لتنفيذ التدابير الفنية والتنظيمية المناسبة بطريقة تجعل المعالجة تلبي المتطلبات القانونية(١٨٢).

وفي حالة فشل ذلك المعالج الآخر في الوفاء بالتزاماته المتعلقة بحماية البيانات، يظل المعالج الأصلي مسئولاً مسئولية كاملة أمام وحدة التحكم عن أداء التزامات ذلك المعالج الآخر.

ويمكن تأسيس ذلك وفق القواعد العامة في عقد المقاولة، والتي تجيز للمقاول أن يكل تنفيذ العمل في جملته، أو في جزء منه إلى مقاول من الباطن إذا لم يمنعه في ذلك شرط تعاقدي أو لم تكن طبيعة العمل تفترض الاعتماد على كفايته الشخصية، ويظل المقاول الأصلي مسئولاً عن المقاول من الباطن في مواجهة رب العمل(١٨٣).

ولا يتحمل المعالج من الباطن، من جانبه، المسئولية إلا إذا لم يمتثل للالتزامات الخاصة بالمعالجين من الباطن أو إذا تصرف خارج نطاق التعليمات القانونية للمراقب أو يتعارض معها، كما يجوز إعفاؤه من المسئولية إذا أثبت أن الحدث المسبب للضرر لا يعود إليه.

ومن أجل حماية الشخص المعني بالبيانات، فإن اللائحة العامة لحماية البيانات الشخصية تقرر مبدأ التضامن بين وحدة التحكم في البيانات والمعالج لها في مواجهة صاحب البيانات حال رجوعه بالتعويض عن الأضرار التي لحقت به.

---

(182) GDPR, art. 28 (4).

(١٨٣) المادة (٦٦١) من القانون المدني المصري.

ويتقرر التضامن في المسئولية المدنية وفقاً للائحة العامة لحماية البيانات حال تعدد وحدات التحكم، وحال تعدد المعالجين للبيانات، وحال اشتراك وحدة التحكم مع معالج البيانات، ففي كل هذه الحالات يكون المدينون بدين التعويض متضامنون في مواجهة الدائن وهو الشخص المعنى بالبيانات.

ويترتب على ذلك، أنه يحق للشخص المعنى بالبيانات (المضرور) الرجوع من خلال دعوى مباشرة ضد وحدة التحكم (المتحكمين) في المعالجة، والمعالج للبيانات، وكذلك المعالجين من الباطن الذين تقررت مسئوليتهم بموجب القواعد المنظمة لعملهم، ولا تتطلب هذه المسئولية ضرورة وجود عقد بين الشخص المعني بالبيانات والمتحكم والمعالج والمعالجين من الباطن.

وتستند مسئولية هؤلاء جميعاً في مواجهة صاحب البيانات المضرور لقواعد المسئولية القانونية أو التقصيرية، والناشئة عن الإخلال بالتزامات فرضها القانون حماية لأصحاب البيانات، ولا تستجيب هذه المسئولية لأي خصوصية غير خصوصية النص الذي يشرعها(١٨٤).

وتطبيقاً للقواعد العامة فإن التضامن مفترض بنص القانون في المسئولية التقصيرية، حيث إذا تعدد المسئولون عن الفعل الضار كانوا متضامنين في التزامهم بتعويض الضرر، وتكون المسئولية فيما بينهم بالتساوي، ما لم يعين القاضي نصيب كل منهم في التعويض(١٨٥).

(184) Laurence Legris, Larcier Le Data Protection Officer, La désignation d'un DPO, Dalloz, 2020.

(١٨٥) المادة (١٦٩) من القانون المدني المصري.

وحسناً ما فعلت اللائحة الأوروبية العامة لحماية البيانات الشخصية من تقرير مبدأ التضامن لحماية الطرف الأولى بالرعاية والحماية وهو الشخص المعني بالبيانات، ولذلك فإن مسئولية المعالج من الباطن تعتبر خطوة ضرورية إلى الأمام، في سياق الحوسبة السحابية والتداول الهائل للبيانات، ومع ذلك، من المستحيل التحكم في إمكانية تتبع عمليات تبادل البيانات، لذا فمن الصعب ضمان المساءلة الحقيقية عبر سلسلة التعاقد من الباطن بأكملها(١).

كما تكمن فائدة تقرير التضامن بين معالج البيانات والمعالج من الباطن في إرساء مبدأ المسئولية المشتركة بين الفاعلين عندما يشاركون في نفس المعالجة.

كما تظهر أهمية التضامن وضروريته في حالة كون الشخص المعني بالبيانات (المضرور) غير قادر على التمييز بين المسئوليات - ولا حتى تقاسم الأدوار - بين معالج البيانات والمعالج من الباطن، ومن ثم، يمكنه أن يطلب التعويض من أحدهما أو الآخر أو كليهما، حيث أن التزامهما المشترك هو الأكثر حماية، ومن ثم يحق للمحكوم عليه الرجوع على الآخرين، في إطار اللجوء إلى الدعوى، بحصة التعويض المنسوبة إليهم بموجب تقاسم المسئولية التي تحددها القوانين.

ثانياً: التعويض:-

يتقرر الحق في التعويض لصالح الشخص المعني بالبيانات، ويعتبر دائناً به، ويخضع تحديد وتقدير مبلغ التعويض (مقدار التعويض المالي) المستحق للقواعد الداخلية

(1) Céline Castets-Renard , Brève analyse du règlement général relatif à la protection des données personnelles, Dalloz, IP/IT, 2016, p. 331.

التي تنظمها القوانين الوطنية، وقررت هذا المبدأ وأكدت عليه محكمة العدل الأوروبية[١].

ويجب أن يرتكز تعويض صاحب البيانات على مبدأ التعويض الكامل عن الضرر نتيجة الإخلال بالالتزامات والحقوق المقررة بقوانين حماية البيانات الشخصية.

ويكون لصاحب البيانات (المضرور) دعوى مباشرة ضد وحدة التحكم (المتحكمين) في المعالجة والمعالج للبيانات وكذلك المعالجين من الباطن الذين تقررت مسئوليتهم بموجب القواعد المنظمة لعملهم، ولا تتطلب هذه المسئولية ضرورة وجود عقد بين الشخص المعني بالبيانات والمتحكم والمعالج والمعالجين من الباطن.

ويكون الأساس القانوني الذي تستند عليهم مسئولية هؤلاء جميعاً في مواجهة صاحب البيانات المضرور هي المسئولية القانونية أو التقصيرية، والناشئة عن الإخلال بالتزامات فرضها القانون حماية لأصحاب البيانات، ولا تستجيب هذه المسئولية لأي خصوصية غير خصوصية النص الذي يشرعها[٢].

وتجدر الإشارة في هذا السياق إلى أن النظام القانوني الذي تبنته اللائحة العامة لحماية البيانات الشخصية هو نظام الديون "التضامنية"، وهذا يعني أنه في مرحلة الالتزام بالديون، يجب على أي شخص يُعلن أنه مسئول أن يعوض الضحية بالكامل من أجل ضمان جبر الضرر الفعال للشخص المعني[٣].

(1) CJUE 4 mai 2023, no C-300/21.

(2) Laurence Legris, Larcier Le Data Protection Officer, La désignation d'un DPO, Dalloz, 2020.

(3) Regulation (EU) 2016/679 of the European Parliament and of the Council on on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) art. 28 (4).

ولكي يتم اتخاذ إجراء ضد معالج البيانات أو المعالج من الباطن، يجب أن يتم تقرير مسئوليته، وبالتالي، لا يمكن رفع دعوى تعويض ضد معالج البيانات أو المعالج من الباطن الذي تم إعفاؤه من المسئولية، والذي يسمى كضمان، من قبل الشخص المعني، لعدم وجود علاقة تعاقدية تربط بين صاحب البيانات والمعالج، أوالمعالج من الباطن، بينما قد توجد العلاقة العقدية بشكل مباشر بين صاحب البيانات والمتحكم.

ومع ذلك إذا تمت معالجة البيانات الشخصية الحساسة بالمخالفة لقواعد المشروعية والقانونية والشروط والضوابط المقررة لمعالجتها، سواء من قبل المعالج الأصلي، أو المعالج من الباطن، يمكن للمضرور في هذه الحالة (صاحب البيانات) الرجوع عليهم جميعاً وفقاً لأحكام المسئولية التقصيرية وبالتضامن فيما بينهم.

وبناء على التضامن بين المدينين في مواجهة الدائن المضرور، يجوز للمضرور الرجوع عليهم جميعاً أو على أي منهم بالمطالبة بحقه في التعويض كاملاً.

وبالنسبة للعلاقة بين المتحكم والمعالجين (الأصلي، من الباطن) وكذلك في علاقة المعالجين بعضهم ببعض، في مرحلة المساهمة في الدين، ووفقًا لنظام الديون المشتركة، فإنه يحق لمن قام بإصلاح الضرر وسداد التعويض المطالبة من المدينين الآخرين الذين شاركوا في نفس المعالجة بحصة التعويض المقابلة لحصتهم في المسئولية عن الضرر، ويحدد القاضي حصة كل شخص من المسئولية عن الضرر.

ووفقاً للائحة العامة لحماية البيانات الشخصية، يجب على المراقبين المشتركين تحديد التزاماتهم بشفافية لأغراض ضمان الامتثال لمتطلبات هذه اللائحة بالاتفاق فيما بينهم وإلى الحد الذي تكون فيه هذه الالتزامات متوافقة مع أحكام القانون، علاوة على ذلك، تخضع المعالجة من قبل معالج من الباطن لعقد أو إجراء قانوني آخر يربط المعالج من الباطن بمراقب البيانات والذي ينص، على وجه الخصوص، على حقوق والتزامات

مراقب البيانات والمعالجين، وهذا التوزيع للحقوق والالتزامات يمكن أن يكون مفيداً للقاضي في تحديد حصة كل شخص من المسئولية فيما بينهم(١).

وكما يشير البعض إلى أنه لا ينبغي أن يكون تفسير مصطلح "المراقبون المشتركون" للمعالجة الذي تستخدمه اللائحة العامة مضللاً فيما يتعلق بطبيعة دين المسئولية، حيث إن دين التعويض مشترك بالفعل، أي أنه يمكن للشخص المعني أن يتصرف دون مبالاة، وبكامل مبلغ التعويض، ضد واحد أو أكثر من المسئولين، ويفسر مصطلح "المراقبون المشتركون" بأنهم المعالجون الذين نظموا التزاماتهم تعاقديًا في عملية المعالجة، وهو أمر مفيد في تحديد حصة مسئولية كل منهم في مرحلة المساهمة في الدين(٢).

كما يمكن تفسير هذا مصطلح "مشترك" من خلال الترجمة الحرفية لعبارة "وحدات التحكم المشتركة" المستخدمة في النسخة الإنجليزية من المادة ٢٦ من اللائحة العامة لحماية البيانات والتي تقرر عندما يحدد مراقبان أو أكثر بشكل مشترك أغراض ووسائل المعالجة، يجب أن يكونوا مراقبين مشتركين، ويجب عليهم أن يحددوا بطريقة شفافة مسئولياتهم فيما يتعلق بالامتثال للالتزامات بموجب هذه اللائحة، لا سيما فيما يتعلق بممارسة حقوق صاحب البيانات وواجبات كل منهم في تقديم المعلومات ....، ويجب أن يعكس الترتيب المشار إليه على النحو الواجب الأدوار والعلاقات الخاصة بالمراقبين المشتركين تجاه أصحاب البيانات. يجب أن يكون جوهر الترتيب متاحًا لصاحب البيانات(٣).

(1) GDPR, art. 28 (3).

(2) Laurence Legris, Larcier Le Data Protection Officer, La désignation d'un DPO, Dalloz, 2020.

(3) GDPR, art. 26 (1-2).

كما يتبين من حيثيات اللائحة العامة لحماية البيانات أنه في حالة اشتراك أكثر من وحدة تحكم في البيانات، وكذلك حالة اشتراك معالج للبيانات بجانب وحدة التحكم، فيتطلب ذلك تحديداً واضحاً للمسئوليات، وذلك حماية لحقوق وحريات أصحاب البيانات، وكذلك لمسئوليات المتحكمين والمعالجين للبيانات، كما يهم ذلك السلطات الإشرافية في عمليات المراقبة واتخاذ التدابير المناسبة(٤).

ثالثاً: حق الرجوع:

عندما تدفع وحدة التحكم أو المعالج تعويضًا كاملاً عن الأضرار التي لحقت بالشخص المعني، يحق لوحدة التحكم أو المعالج المطالبة بالاسترداد من وحدات التحكم أو المعالجين الآخرين المشاركين في نفس المعالجة ذلك الجزء من التعويض المقابل لمسئوليتهم عن الضرر(٥).

إذا قام الشخص المسئول، بعد أن عوض الشخص المعني بالكامل، بممارسة حق الرجوع الشخصي على الأطراف المسئولة الأخرى، فقد يكون لتصرفه أساس تعاقدي، ولا يشكل تطبيق شروط تحديد المسئولية، بشرط صحتها، أي إشكالية.

---

(4) GDPR, Whereas (79).

(5) Regulation (EU) 2016/679 of the European Parliament and of the Council on on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) art. 82 (5), " Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2."

ويحل المتحكم أو المعالج الذي قام بدفع التعويض كاملاً لصاحب البيانات المضرور محل حقوق صاحب الشأن، أي أن تصرفه سيكون هو نفس ما اتخذه الشخص المعني ضده في البداية، ومع ذلك، لا ينشأ هذا الإجراء من عقد بين المتحكمين المشتركين أو بين المتحكم والمعالج إنما استناداً للقواعد القانونية المقررة لذلك.

الخاتمة

عرضنا من خلال هذه الدراسة لمسألة أصبحت في الوقت الحالي من أكثر المسائل خطورة على حقوق الأشخاص، وتتمثل في الاستدلالات على البيانات الحساسة.

وتحظى الاستدلالات بحماية قانونية أقل من تلك المقررة لأنواع البيانات بموجب القواعد التشريعية المنظمة لحماية البيانات الشخصية، على الصعيدين الدولي والمحلى.

كما تكمن خطورة عمليات الاستدلالات على البيانات الحساسة بتأثيراتها البالغة على حقوق الأفراد الأساسية، وباشكاليتها المتعددة التي تنعكس على أحكام المسئولية المدنية وحماية الأشخاص المعنيين بالبيانات.

كما بينا من خلال هذه الدراسة لمفهوم البيانات الحساسة، سواء التعريف التشريعي، أو ضرورة تعريفها في عصر الاستدلالات بشكل مختلف، والمعيار الذي تم انتهاجه بشكل تشريعي في تحديد هذا المفهوم، بالإضافة للمعايير الأخرى، وضرورة الاعتماد على مفهوم موسع للبيانات الحساسة.

كما عرضنا لعمليات جمع البيانات والاطلاع عليها ومعالجتها والاستدلالات الناشئة عنها من خلال الوسائل التكنولوجية الحديثة، وإمكانية معالجتها حتى بدون علم المستخدم للأجهزة والتطبيقات المختلفة والمنتشرة بشكل متزايد في السنوات الأخيرة.

كما عرضنا لعمليات الاستدلالات على البيانات الحساسة، وتأثيراتها على الحقوق الأساسية للأفراد، خاصة في عصر الذكاء الاصطناعي والبيانات الضخمة، وشروط صحة عمليات الاستدلالات المعقولة، وحاولنا إيجاد أساس قانوني للاستدلالات سواء المعقولة أو عالية المخاطر، وقمنا بعرض تقييم لمدى ملائمة قواعد حماية البيانات الحالية لمواجهة عمليات الاستدلالات على البيانات الحساسة.

وعرضنا كذلك لصور حماية البيانات الحساسة خاصة المبدأ العام لحظر معالجة البيانات الحساسة، ومدى انطباقها على عمليات الاستدلالات، كما عرضنا في صور الحماية لضرورة الاعتراف بحقوق أصحاب البيانات في مجال الاستدلالات.

ومن صور حماية أصحاب البيانات أيضاً المسئولية المدنية بما تكفله من تعويض عادل وكامل لأصحاب البيانات المضرورين من انتهاك القواعد الخاصة بحماية بياناتهم الحساسة، وعرضنا لأحكام هذه المسئولية، وبينا كذلك لإشكالات المسئولية المدنية في ظل عمليات الاستدلالات.

وقد توصلنا للنتائج الآتية:

أولاً: إن الاستمرار في الاعتماد على معايير الحساسية وإمكانية تحديد الهوية، أو على التمييز غير الواضح بين البيانات الشخصية والبيانات الحساسة (معيار طبيعة البيانات) كمقياس لمستوى الحماية الممنوحة للبيانات هو أمر لم تثبت فعاليته في ظل التطورات المتلاحقة في عمليات المعالجات الالكترونية والاستدلالات من خلال استخدام تقنيات الذكاء الاصطناعي والبيانات الضخمة.

ثانياً: ضرورة تدخل القضاة من خلال سلطتهم التقديرية بهدف توسيع نطاق الحماية المقررة بقانون حماية البيانات لضمان اتخاذ قرارات دقيقة وعادلة حين تعتمد عملية الاستدلالات على بيانات غير شخصية أو مجهولة المصدر.

ثالثاً: يمكن للقضاة الاستعانة في ذلك بالتفسير الموسع لتعريف البيانات الحساسة مثلما فعلت محكمة العدل الأوروبية.

رابعاً: تأثر حماية الحق في الخصوصية، وكذلك سائر الحقوق الأخرى للأفراد من خلال عمليات الاستدلالات على البيانات الحساسة، ومن ذلك إنشاء الملفات التعريفية للأشخاص والمجموعات بما تؤثر على حقوقهم ولم يكن في الوقت الحالي فسيكون مستقبلاً.

خامساً: قصور القواعد القانونية الحالية المنظمة لحماية البيانات الحساسة في مواجهة عمليات الاستدلالات واسعة النطاق، وبصفة خاصة في منح حقوق لأصحاب البيانات فيما يتعلق بنتائج الاستدلالات المتعلقة بهم.

سادساً: قصور القواعد التشريعية الحالية لحماية البيانات الحساسة، حيث قصر المشرع نطاق الحماية على البيانات الحساسة التي يتم جمعها واستخدامها في عمليات المعالجة، دون النص على الأشكال الأخرى للبيانات التي يمكن الاستدلال من خلالها على بيانات ذات طبيعة حساسة، مثل البيانات العادية والبيانات مجهولة المصدر، مما جعل النص التشريعي قاصراً على مواجهة التغيرات السريعة والمتلاحقة في عمليات الاستدلال على البيانات الحساسة.

سابعاً: اهتمام تشريعات حماية البيانات، سواء في مجالات المعالجة أو كذلك الاستدلالات على البيانات المدخلة، دون إعطاء اهتمام وحماية مماثلة

للبيانات المستنتجة من عملية الاستدلال، بما قد تمثله من خطورة أكبر من البيانات المدخلة.

كما توصلنا لأهم التوصيات الآتية:

أولاً: ضرورة النص صراحة على عمليات الاستدلالات على البيانات الحساسة، مع وضع تنظيم قانوني لعملية الاستدلال من خلال ربطها بالحق في الخصوصية.

ثانياً: ضرورة تقرير حماية أكثر فعالية للحق في الخصوصية في قانون حماية البيانات، في ظل التطورات الحديثة التي تشهدها عمليات الاستدلالات على البيانات الشخصية بصفة عامة، والبيانات الحساسة بصفة خاصة.

ثالثاً: يجب إعادة النظر في المعيار المحدد لطبيعة البيانات الشخصية والحساسة، وضرورة تجنب المعيار الذي انتهجه المشرع في تحديد البيانات الحساسة وهو معيار طبيعة البيانات، وضرورة الاعتداد بمعياري سياق الاستخدام والغرض، بهدف تقرير حماية أعم وأشمل لما يعد من البيانات الحساسة.

رابعاً: نوصي كذلك، بهدف تقرير وتفعيل الحماية الهادفة للبيانات الحساسة، أن ينص المشرع المصري على ضرورة خضوع كل البيانات (الشخصية، الحساسة، العادية، ومجهولة المصدر)، وهى ما تعتبر ببيانات مدخلات، للقيود المقررة لعمليات جمع ونقل وتخزين ومعالجة وإتاحة البيانات الحساسة، طالما كانت عمليات الاستدلال منها تؤدى لاستنتاجات بشأن البيانات ذات الطبيعة الحساسة، مما مؤداه-وقتها- بتمتعها بذات الطبيعة.

خامساً: ضرورة النص صراحة على حماية البيانات الحساسة المستنتجة من عمليات الاستدلالات، وخضوعها لذات الحماية المقررة للبيانات الحساسة.

سادساً: ضرورة وضع تنظيم قانوني صريح بشأن الأجهزة والتطبيقات الحديثة التي يمكن من خلالها التوصل لاستدلالات على البيانات الحساسة.

سابعاً: نوصي بضرورة النص على حقوق صاحب البيانات التي تم الاستدلال عليها، وبصفة خاصة حقوقه المتعلقة بالبيانات المستنتجة، ومنها حقه في معرفة الاستدلالات ونتائجها، وحقه كذلك في الاعتراض على نتائج الاستدلالات، وإمكانية الطعن عليها وتصحيحها وحقه في طلب المحو، ومعرفة الأسباب والمعايير التي قامت عليها عملية الاستدلالات.

ثامناً: يجب التركيز على إدارة بيانات المخرجات، أو الاستدلالات والقرارات، لإعادة تشكيل الخصوصية كمفهوم شمولي، دون الاعتداد والاكتفاء فقط بحساسية البيانات وقابليتها للتعرف والتحديد والتي أصبحت لا تجدي في عصر البيانات الضخمة والذكاء الاصطناعي.

قائمة المراجع

أولاً: المراجع العربية:

١) د. بولين أنطونيوس أيوب، الحماية القانونية للحياة الخاصة في مجال المعلوماتية، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٩.

٢) د. تامر محمد الدمياطي، الرضا الرقمي بمعالجة البيانات الشخصية دراسة مقارنة، مجلة القانون والتكنولوجيا، الجامعة البريطانية، كلية القانون، عدد (١)، مجلد (٢)، ٢٠٢٢.

٣) د. ثروت عبد الحميد، النظرية العامة للالتزامات في القانون المدني المصري، الجزء الأول، مصادر الالتزام، بدون دار نشر، بدون سنة نشر.

٤) د. سامح عبد الواحد التهامي، الحماية القانونية للبيانات الشخصية، دراسة في القانون الفرنسي، مجلة الحقوق، جامعة الكويت، مجلد ٣٥، عدد ٣، ٢٠١١.

٥) د. سامح عبد الواحد التهامي، نطاق الحماية القانونية للبيانات الشخصية والمسئولية التقصيرية عن معالجتها: دراسة في القانون الإماراتى، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، عدد ٦٧، ٢٠١٨.

٦) د. طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية، دراسة تحليلية مقارنة، المجلة القانونية، كلية الحقوق فرع الخرطوم، جامعة القاهرة، العدد ١٢، مجلد ٨، ٢٠٢٠.

٧) د. عبد الرزاق أحمد السنهوري، الوسيط في شرح القانون المدني، الجزء الأول، مصادر الالتزام، منشأة المعارف، الاسكندرية، طبعة ٢٠٠٤.

٨) د. عبد العزيز اللصاصمة، المسئولية المدنية التقصيرية عن الفعل الضار، الدار العلمية الدولية ودار الثقافة للنشر، عمان، ٢٠٠٢.

٩) د. محسن عبد الحميد إبراهيم البيه، النظرية العامة للالتزامات، الجزء الثاني، أحكام الإلتزام، مكتبة الجلاء الجديدة، المنصورة، ٢٠٠١-٢٠٠٢.

١٠) د. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي، دراسة مقارنة، مجلة كلية الشريعة والقانون، جامعة طنطا، العدد الثالث والثلاثون، الجزء الرابع، ديسمبر ٢٠١٨.

١١) د. مشعل محمد أحمد سلامة، الحق في محو البيانات الشخصية، دراسة تحليلية في ضوء لائحة حماية البيانات بالاتحاد الأوروبي وأحكام المحاكم الأوروبية، مجلة الدراسات القانونية والاقتصادية، كلية الحقوق، جامعة مدينة السادات، مجلد ٣، عدد ٢، ٢٠١٧.

١٢) د. نبيل إبراهيم سعد، مصادر وأحكام الالتزام، منشورات الحلبي الحقوقية، بيروت، ٢٠٠٣.

ثانياً: المراجع الأجنبية:

1) A Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits, 2002.

2) A.LECOURT, RGPD : nouvelles contraintes, nouvelles stratégies pour les entreprises, Dalloz IP/IT 2019.

3) Aaron Smith, Record shares of Americans now Own smartphones, have home broadband, PEW RSCH. CTR. (Jan. 12, 2017),

4) Alessandro Mantelero & Giuseppe Vaciago, Data Protection in a Big Data Society. Ideas for a Future Regulation, 15 Digital Investigation, 2015.

5) Alessandro Mantelero, Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection, 32 Computer L. & Security Rev., 2016.

6) Alessandro Mantelero, Regulating Big Data. The Guidelines of the Council of Europe in the Context of the European Data Protection Framework, 33 Comp. L. & Security Rev., 2017.

7) Alexander Nguyen, Videouberwachung Insensitiven Bereichen, 35 Datenschutz und Datensicherheit,2011.

8) Alexander Schiff, Besonderer Kategorien personenbezogener Daten, in Datenschutz-Grundverordnung, 2017.

9) Andrew D. Selbst & Solon Barocas, The Intuitive Appeal of Explainable Machines, 87 Fordham L. Rev., 2018;

10) Andrew G. Reece & Christopher M. Danforth, Instagram Photos Reveal Predictive Markers of Depression, 6 EPJ DATA SCI., no. 15, 2017.

11) Andrew Tutt, An FDA for Algorithms, 69 Admin. L. Rev., 2017.

12) Bart Custers & Helena Ursic, Big Data and Data Reuse: A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection, INT'L DATA PRIV. L., 2016.

13) Brent Daniel Mittelstadt & Luciano Floridi, The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts, 22 Sci. & Engineering Ethics, 2016.

14) Brent Mittelstadt, Chris Russell & Sandra Wachter, Explaining Explanations in AI, in FAT "19: Conference on Fairness, Accountability, and Transparency (FAT '19), January 29-31, 2019, Atlanta, GA, USA, 2019.

15) Brent Mittelstadt, From Individual to Group Privacy in Big Data Analytics, 30 Phil. & Tech., 2017.

16) C. De Terwangne, « Les cabinets d'avocats et la loi sur la protection des données à caractère personnel », Cabinet d'avocats et technologies de l'information : balises et enjeux, coll. Cahiers du CRID, no 26, Bruxelles, Bruylant, 2005.

17) C. Tucker, The Economic Value of Online Customer Data, OECD (2011).

18) C. Cadwalladr et E. Graham-Harrison, « Revealed : 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », The Guardian, 17 mars 2018.

19) C. Gayrel, « Chronique de jurisprudence en droit des technologies de l'information, Dalloz, (2009-2011).

20) Cathy O'neil, weapons of math destruction: how big data increases inequality and threatens democracy, 2016.

21) Céline Castets-Renard , Brève analyse du règlement général relatif à la protection des données personnelles, Dalloz, IP/IT, 2016.

22) Christopher Kuner, Fred H. Cate, Christopher Millard & Dan Jerker B. Svantesson, The Challenge of "Big Data" for Data Protection, 2 Int'l Data Privacy L., 2012.

23) Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 San Diego L. Rev., 2007.

24) Daniel J. Solove, Regulating Based On Harm And Risk Instead Of Sensitive Data, 118 Nw. U.L. Rev., 2024.

25) Daniel J. Solove, The Limitations of Privacy Rights, 98 NOTRE DAME L. REV., 2023.

26) Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 Wash. L. Rev., 2014; Peter Grindrod, Beyond Privacy and Exposure: Ethical Issues Within Citizen-Facing Analytics, Phil. Transactions Royal Soc'y A, Dec. 28, 2016.

27) Dara Hallinan, Michael Friedewald, & Paul De Hert, Genetic Data and the Data Protection Regulation: Anonymity, Multiple Subjects, Sensitivity and a Prohibitionary Logic Regarding Genetic Data?, 4 COMPUT. L. & SEC. REV., 2013.

28) David Lazer, Ryan Kennedy, Gary King & Alessandro Vespignani, The Parable of Google Flu: Traps in Big Data Analysis, 343 Science, 2014.

29) Doshi-Velez & Mason Kortz, Accountability of AI Under the Law: The Role of Explanation (Berkman Klein Ctr. Working Grp. on Explanation and the Law Working Paper, 2017.

30) Douwe Korff, Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of

Technological Developments 41 (European Comm'n Directorate-General Justice, Freedom and Security, Working Paper No. 2, 2010).

31) Douwe Korff, The Proposed General Data Protection Regulation: Suggested Amendments to the Definition of Personal Data, EU Law Analysis (Oct. 15, 2014).

32) E. Degrave, « Le Règlement général sur la protection des données et le secteur public », Rev. Droit communal, 2018; Égal. Groupe 29, Guidelines on transparency under Regulation 2016/679, revised and adopted on 11 April 2018.

33) Edward J. Janger, Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy, 44(4) WM. & MARY L. REV., 2003.

34) Frank Pasquale, The Black Box Society: The Secret Algorithms that Control Money and Information (2015).

35) Gianclaudio Malgieri & Giovanni Comandé, Sensitive-by-Distance: Quasi-Health Data in the Alogrithmic Era, 3 INFO., COMMC'N & TECH. L., 2017.

36) Gianclaudio Malgieri, Trade Secrets v. Personal Data: A Possible Solution for Balancing Rights, 6 Int'l Data Privacy L., 2016.

37) Gunther Eysenbach, The Continued Use of Mobile Health Apps: Insights From a Longitudinal Study, JMIR MHEALTH UHEALTH, Aug. 2019.

38) Hans-Georg Kamann and Martin Braun, Recht auf Berichtigung, in Datenschutz-Grundverordnung Bundesdatenschutzgesetz, 2017.

39) Harold Demsetz, Toward a Theory of Property Rights, 57(2) THE AMERICAN ECONOMIC REV, 1967.

40) Hideyuki Matsumi, Predictions and Privacy: Should There Be Rules About Using Personal Data to Forecast the Future?, 48 CUMB. L. REV., 2017.

41) Ira S. Rubinstein & Woodrow Hartzog, Anonymization and Risk, 91 Wash. L. Rev., 2016.

42) Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, 3 Int'l Data Privacy L., 2013.

43) Isak Mendoza & Lee A Bygrave, The Right Not to Be Subject to Automated Decisions Based on Profiling (Mar. 9, 2018).

44) J.-M. Van Gyseghem, « L'économie collaborative et la protection des données : quel partage de

données ? », Aspects juridiques de l'économie collaborative, Limal, Anthemis, 2017.

45) Janneke Gerards, The Discrimination Grounds of Article 14 of the European Convention on Human Rights, 13 Hum. Rts. L. Rev. 99, 2013.

46) Jay Hancock, Workplace wellness programs put employee privacy at risk, CNN HEALTH (Oct. 2, 2015.

47) Jina Kim, Jieon Lee, Eunil Park & Jinyoung Han, A Deep Learning Model for Detecting Mental Illness from User Content on Social Media, 10 SCI. REPS., 2020.

48) Joanne Hinds & Adam N. Joinson, What Demographic Attributes Do Our Digital Footprints Reveal? A Systematic Review, 13 PLOS ONE, Nov., 2018.

49) Johnny Ryan, Regulatory Complaint Concerning Massive, Web-Wide Data Breach by Google and Other "Ad Tech" Companies Under Europe's GDPR, Brave (Sept. 12, 2018).

50) Joris van Hoboken, Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines, 2012.

51) Jose Gonzalez Cabanas, Angel Cuevas & Ruben Cuevas, Facebook Use of Sensitive Data for Advertising in Europe (Feb. 14, 2018.

52) Joshua A. Kroll et al., Accountable Algorithms, 165 U. Pa. L. Rev., 2017.

53) Julie Cohen, Examined lives: informational privacy and the subject as object, 52 STANF L. REV, 2000.

54) Karen McCullagh, Data Sensitivity: Proposals for Resolving the Conundrum, 2 J. INT'L COM. L. & TECH., 2007.

55) Kean Birch, DT Cochrane and Callum Ward, Data as an asset? The measurement, governance and valuation of digital personal data by big tech, 1(15) BIG DATA & SOCIETY, 2021.

56) Laurence Legris, Larcier Le Data Protection Officer, La désignation d'un DPO, Dalloz, 2020.

57) Leon Trakman, Robert Walters & Bruno Zeller, Is Privacy and Personal Data Set to Become the New Intellectual Property?19(70) UNSW LAW RESEARCH PAPER, 2019.

58) Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a "Right to an Explanation' Is Probably Not the

Remedy You Are Looking For, 16 Duke L. & Tech. Rev., 2017- 2018.

59) Luciano Floridi, Four Challenges for a Theory of Informational Privacy, 8 Ethics & Info. Tech., 2006.

60) Luciano Floridi, The Informational Nature of Personal Identity, 21 Minds & Machines, 2011.

61) M. Rosenberg, N. Confessore et C. Cadwalladr, « How Trump Consultants Exploited the Facebook Data of Millions », The New York Times, 17 mars 2018.

62) M. Van Overstraeten et S. Depré, « Le traitement automatisé des données à caractère personnel et le droit au respect de la vie privée en Belgique », Rev. trim. dr. h., 2003.

63) M.-H. Boulanger et al., « La protection des données à caractère personnel en droit communautaire », J.D.E., 1997.

64) Mai Arlowski, Personal Data as a New Form of Intellectual Property, 102 J. Pat. & Trademark Off. Soc'y, 2022.

65) Marion Oswald, Algorithm-Assisted Decision-Making in the Public Sector: Framing the Issues Using Administrative Law Rules Governing Discretionary Power, Phil. Transactions Royal Soc'y A, Aug. 6, 2018.

66) MARK A. LEMLEY et. El., Intellectual Property in the New Technological Age, 2016.

67) Martin Abrams, The Origins of Personal Data and its Implications for Governance (Nov. 24, 2014).

68) Mary Anne Franks, "Revenge Porn" Reform: A View from the Front Lines, 69 FLA. L. REV., 2017.

69) Michal Kosinski, David Stillwell & Thore Graepel, Private Traits and Attributes Are Predictable from Digital Records of Human Behavior, 110 PNAS, 2013.

70) Mireille Hildebrandt, Primitives of Legal Protection in the Era of Data-Driven Platforms, 2 Geo. L. Tech. Rev., 2018.

71) Mireille Hildebrandt, Profiling: From Data to Knowledge, 30 Datenschutz und Datensicherheit, 2006.

72) Moni Wekesa, What is SUI GENERIS System of Intellectual Property Protection?13 TECHNOLOGY BRIEF, 2006.

73) Munmun De Choudhury, Scott Counts, Eric J. Horvitz & Aaron Hoff, Characterizing and Predicting Postpartum Depression from Shared Facebook Data, in Ass'n for computing mach., cscw '14: proceedings of the 17th acm

conference on computer supported cooperative work & social computing, 2014.

74) Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 Law Innovation & Tech, 2018.

75) Nadezhda Purtova, Do Property Rights in Personal Data Make Sense after the Big Data Turn?: Individual Control and Transparency, 10 J.L. & Econ. Reg., 2017.

76) Niels van Dijk, Raphaël Gellert, & Kjetil Rommetveit, A Risk to a Right? Beyond Data Protection Risk Assessments, 32 COMPUT. L. & SEC. REV., 2016.

77) Norbert Nolte & Christoph Werkmeister, Recht auf Loschung ("Recht auf Vergessenwerden"), in Datenschutz-Grundverordnung VO (EU) 2016/679, 2017.

78) Paul Quinn & Gianclaudio Malgieri, The Difficulty of Defining Sensitive Data the Concept of Sensitive Data in the EU Data Protection Framework, 22 GERMAN L.J., 2021.

79) Paul Quinn & Liam Quinn, Big Genetic Data and Its Big Data Protection Challenges, 34 COMPUT. L. & SEC. REV., 2018.

80) Paul Quinn, Ann-Katrin Habbig, Eugenio Mantovani & Paul De Hert, The Data Protection and Medical Device Frameworks? Obstacles to the Deployment of mHealth Across Europe?, 20 EUR. J. OF HEALTH L., 2013.

81) Pauline T. Kim, Essay, Auditing Algorithms for Discrimination, 166 U. Pa. L. Rev. Online, 2017.

82) Ph. Jestaz, L'obligation et la sanction: A la recherche de l'obligation fondamentale: in Ph. Jestaz, Autour du droit civil. Écrits dispersés, idées convergentes, Dalloz, 2005.

83) Priscilla M. Regan, Privacy as a Common Good in the Digital World, 5 Info., Comm'n. & Soc'y , 2002.

84) S. C. Olhede & P.J. Wolfe, The Growing Ubiquity of Algorithms in Society: Implications, Impacts and Innovations, Phil. Transactions Royal Soc'y A, Aug. 6, 2018.

85) S. Gutwirth, « De toepassing van het finaliteitbeginsel van de privacywet van 8 décember 1992 tot de bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens », T.P.R., 1993/4 ; Th. Léonard et Y. Poullet, « Les libertés comme fondement de la protection des données nominatives », in F. Rigaux, La vie privée, une

liberté parmi les autres ?, Travaux de la Faculté de droit de Namur, no 17, Bruxelles, Larcier, 1992.

86) Samuel E. Trosow, Sui Generis Database Legislation: A Critical Analysis, 7 YALE J.L. & TECH., 2004.

87) Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, COLUM. BUS. L. REV., 2019.

88) Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 Harv. J.L. & Tech., 2018.

89) Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Privacy L., 2017.

90) Serge Gutwirth & Paul De Hert, Regulating Profiling in a Democratic Constitutional State, in Profiling the European Citizen, 2008.

91) Solon Barocas & Andrew D. Selbst, Big Data's Disparate Impact, 104 Calif. L. Rev., 2016.

92) Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 Seton Hall L. Rev, 2017.

93) Tal Z. Zarsky, Understanding Discrimination in the Scored Society, 89 Wash. L. Rev., 2014.

94) Thomas Mouritz, Comparing the Social Contracts of Hobbes and Locke, 1 THE WEST AUSTRALIAN JURIST, 2010.

95) Tim Miller, Explanation in Artificial Intelligence: Insights from the Social Sciences, Artificial Intelligence, Feb. 2019.

96) V. Verbruggen, Les Codes commentés. La protection des données, Bruxelles, Larcier, 2011.

97) Vaclav Janececk & Gianclaudio Malgieri, Commercialization of Data and the Dynamically Limited Alienability Rule, 21 GERMAN L. J., 2020.

98) Vaclav Janecek, Ownership of Personal Data in the Internet of Things, 34 COMPUTER LAW & SECURITY REVIEW, 2018.

99) Viktor Mayer-Schonberger, Delete: The Virtue of Forgetting in the Digital Age, 2009.& Brent Daniel Mittelstadt & Luciano Floridi, The Ethics of Big Data: Current and

Foreseeable Issues in Biomedical Contexts, 22 Sci. & Engineering Ethics, 2016.

100) Wim Schreurs. Mireille Hildebrandt, Els Kindt & Michael Vanfleteren, Cogitas, Ergo Sum., The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector, in Profiling the European Citizen, 2008.

101) Wu Youyou, Michal Kosinski & David Stillwell, Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans, 112 PNAS, 2015.

102) Yeshimabeit Milner & Amy Traub, Data For Black Lives & Demos, Data Capitalism + Algorithmic Racism 16, 2021.

103) Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., Aug. 20, 2021).

ثالثاً: مواقع الانترنت:

✓ http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm.

- ✓ http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files /2007/wp136_en.pdf (on file with the Columbia Business Law Review).
- ✓ http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826.
- ✓ http://eulawanalysis.blogspot.com/2014/10/the-proposed-general-data-protection.html.
- ✓ http://hudoc.echr.coe.int/eng?i=001-142673.
- ✓ http://hudoc.echr.coe.int/eng?i=001-57491.
- ✓ http://hudoc.echr.coe.int/eng?i=001-90051.
- ✓ http://hudoc.echr.coe.int/rus?i=001-57533.
- ✓ http://hudoc.echr.coe.int/rus?i=001-58033.
- ✓ http://www.crid.be/pdf/public/6539.pdf.
- ✓ http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML +TA+P8-TA-2017-0051+0+DOC+PDF+V0//EN.
- ✓ https://arxiv.org/abs/1802.05030 [https://perma. cc/V2C8-FY3W].

- ✓ https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf [https://perma.cc/5MG4-6LED]
- ✓ https://curia.europa.eu/juris/liste.jsf?num=C-136/17.
- ✓ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [https://perma.cc/J3P5-GUL2].
- ✓ https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/X6PC-825X].
- ✓ https://ec.europa.eu/newsroom/article29/items/612053/en [https://perma.cc/YW6D-87ED].
- ✓ https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf [https://perma.cc/5BS2-4VJE].
- ✓ https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_ wp29_documents.pdf [https://perma.cc/8H9A-RQR3]
- ✓ https://edps.europa.eu/sites/edp/files/publication/18-03-19_online__manipulation_en.__pdf [https://perma.cc/3KJ6-VSUD].

- ✓ https://files.consumerfinance.gov/f/201409_cfpb_report_proxy-methodology. pdf [https://perma.cc/5CY4-NK3L].
- ✓ https://hudoc.echr.coe.int/fre#[%22itemid%22:[%22001-174441%22.
- ✓ https://medium.com/mydata/five-loopholes-in-the-gdpr-367443c4248b [https://perma.cc/L8EM-8YPM]
- ✓ https://papers. ssrn.com/abstract=2964855 [https://perma.cc/NPK5-MGE2].
- ✓ https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510927[https://perma.cc/9YZ5-FT96]
- ✓ https://perma.cc/38L5-ATQ8]; Vijay Pandurangan, On Taxis and Rainbows, Medium (June 21, 2014),
- ✓ https://perma.cc/SRY9-JDW8]; Robert Madge, Five Loopholes in the GDPR, Medium (Aug. 27, 2017),
- ✓ https://rm.coe.int/09000016806845af [https://perma.cc/BB87-NZQR].
- ✓ https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a.

- ✓ https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a [https://perma.cc/G5SZ-J77A].
- ✓ https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1.
- ✓ https://techscience.org/a/2015092903.
- ✓ https://www.brave.com/blog/adtech-data-breach-complaint/.
- ✓ https://www.cnil.fr/fr/definir-une-finalite.
- ✓ https://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive /index.html
- ✓ https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_ Capitalism_Algorithmic_Racism.pdf.
- ✓ https://www.dwt.com/blogs/privacy--security-law-blog/2023/06/florida-digital-bill-of-rights-data-privacy [https://perma.cc/BAN9-3MNA].
- ✓ https://www.grandviewresearch.com/industry-analysis/mhealth-market
- ✓ https://www.idc.com/getdoc.jsp?containerId=prUS46138520 .

- ✓ https://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/
- ✓ https://www.spiceworks.com/tech/devops/articles/what-is-metadata/.
- ✓ https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/.
- ✓ https://www.theatlantic.com/technology/archive/2020/07/defund-facial-recognition /613771/ [https://perma.cc/5B84-AJAD]
- ✓ https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election ;
- ✓ https://www.verywellhealth.com/track-health-information-phone-1739148.