جامعة الأزهر
كلية الشريعة والقانون
بالقاهرة

مجلة الشريعة والقانون

مجلة علمية نصف سنوية محكمة

تعنى بالدراسات الشرعية والقانونية والقضائية

تصدرها
كلية الشريعة والقانون بالقاهرة
جامعة الأزهر

العدد الثالث والأربعون
أبريل ٢٠٢٤م

توجه جميع المراسلات باسم الأستاذ الدكتور: رئيس تحرير مجلة الشريعة والقانون

جمهورية مصر العربية - كلية الشريعة والقانون - القاهرة -الدراسة - شارع جوهر القائد

ت: ٢٥١٠٧٦٨٧

فاكس: ٢٥١٠٧٧٣٨

http://fshariaandlaw.edu.eg

جميع الآراء الواردة في هذه المجلة تعبر عن وجهة نظر أصحابها، ولا تعبر بالضرورة عن وجهة نظر المجلة وليست مسئولة عنها

رقم الإيـــداع

١٨٠٥٣ / ٢٠٢٤

الترقيم الدولي للطباعة

ISSN: 2812–4774

الترقيم الدولي الإلكتروني:

ISSN: 2812–5282

تقنية الذكاء الاصطناعي وحماية البيانات الشخصية

دراسة مقارنة

إعداد

د. وفاء حلمي السعيد

مدرس القانون التجاري والبحري

كلية القانون - الأكاديمية البحرية للعلوم والتكنولوجيا والنقل البحري

تقنية الذكاء الاصطناعي وحماية البيانات الشخصية دراسة مقارنة

وفاء حلمي السعيد
قسم القانون التجاري والبحري، كلية القانون، الاكاديمية البحرية للعلوم والتكنولوجيا والنقل البحري.
البريد الالكتروني: Wafaahelmy1984@gmail.com

ملخص البحث:

لما كان دمج تقنيات الذكاء الاصطناعي والبيانات الضخمة سيؤدى إلى تحقيق العديد من المزايا، ومثال ذلك تيسير الوصول إلى المعلومات وإنشاء المعارف وتوزيعها على كافة أنحاء العالم وتوفير التكاليف المالية وزيادة نطاق الوظائف الإبداعية، وزيادة الشفافية والحد من التحيز والتمييز بين أفراد المجتمع دون وجه حق. كما يسهم هذا الدمج في زيادة نطاق توقع الشركات لاتجاهات السوق واتخاذ القرارات المناسبة وتمكين المستهلك من اتخاذ القرارات الاكثر فائدة وتمكين السلطات العامة من توقع المخاطر ومنع وقوع الضرر. وبناء على ذلك، تريد الباحثة من هذه الدراسة تسليط الضوء على العلاقة بين تقنية الذكاء الاصطناعي وحماية البيانات على ضوء لائحة حماية البيانات الصادرة عن الاتحاد الأوربى عام ٢٠١٦، فتقنية الذكاء الاصطناعي انتشرت في العالم بصور مختلفة، ومثال ذلك الروبوتات الصناعية، وروبوتات الخدمة في المنازل ومنشآت الرعاية الصحية، والطائرات بدون طيار والوكلاء الإلكترونيين في مجال التجارة الإلكترونية، وهو ما يعنى أن تقنية الذكاء الاصطناعي أضحت إحدى آليات التغيير الاقتصادي والاجتماعي لأفراد المجتمع. وبالتالي يجب تطوير وتغيير القواعد القانونية لكى تتناسب مع هذا التطور التقني المذهل على ضوء المخاطر المترتبة على استخدام هذه التقنية في كافة مجالات الحياة، فقد يزيد نطاق خطر السيطرة والتلاعب والتمييز بين أفراد المجتمع قدر أهمية هذه التقنية في تسهيل حياة أفراد المجتمع، ولذلك يزيد نطاق الضرر الذى قد يصيب الفرد لو أخفقت هذه التقنيات الحديثة في عدم احترام الحقوق الفردية أو عدم مراعاة القيم الاجتماعية السائدة. وقد تناولت هذه الدراسة تقنية الذكاء الاصطناعي وتطورها على المستوى التكنولوجي والاجتماعي وعلاقتها بالمعالجة الفنية للبيانات الشخصية من خلال بيان مفهوم الذكاء الاصطناعي والعلاقة بينه وبين المعالجة التقنية للبيانات الشخصية.

وقد اعتمدت الدراسة على المنهج التحليلي لنصوص لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي عام ٢٠١٦ لبيان حقيقة العلاقة القانونية بين تقنيات الذكاء الاصطناعي وضرورة الحماية القانونية للبيانات الشخصية.

كلمات مفتاحية: الذكاء الاصطناعي، البيانات الضخمة، لائحة حماية البيانات، الاعتداء على البيانات، تقنية.

Artificial intelligence technology and protection of personal data - a comparative study

Wafaa Helmy Saeed
Department of Commercial and Maritime Law, College of Law, Maritime Academy for Science, Technology and Maritime Transport.
Email: Wafaahelmy1984@gmail.com

Abstract:

The integration of artificial intelligence and big data technologies will bring many advantages, such as facilitating access to information, creating and distributing knowledge worldwide, saving financial costs, increasing the scope of creative functions, increasing transparency and reducing prejudice and discrimination among members of society unjustly. This integration also contributes to increasing the scope for companies to anticipate market trends, make appropriate decisions, enable consumers to make the most beneficial decisions, and enable public authorities to anticipate risks and prevent harm. Accordingly, the researcher wants this study to highlight the relationship between artificial intelligence technology and data protection in light of the data protection regulation issued by the European Union in 2016, as artificial intelligence technology has spread in the world in different ways, for example, industrial robots, Service robots in homes and healthcare facilities, drones and electronic agents in the field of e-commerce, which means that artificial intelligence technology has become one of the mechanisms of economic and social change for members of society. Therefore, legal rules must be developed and changed to suit this amazing technical development in light of the risks resulting from the use of this technology in all areas of life, the scope of the risk of control, manipulation and discrimination between members of society may increase as much as the importance of this technology in facilitating the lives of members of society, and therefore the scope of harm that may affect the individual increases if these modern technologies fail to respect individual rights or do not take into account the prevailing social values. This study dealt with artificial intelligence technology and its development at the technological and social level and its relationship to the technical processing of personal data by explaining the concept of artificial intelligence and the relationship between it and the technical processing of personal data.

The study relied on the analytical approach of the texts of the Data Protection Regulation issued by the European Union in 2016 to clarify the reality of the legal relationship between intelligence technologies. artificial and the necessity of legal protection of personal data.

Keywords: Artificial Intelligence, Big Data, Data Protection Regulation, Data Abuse, Technology.

المقدمة

يقصد بالذكاء الاصطناعي تلك التقنية التي تحاول القيام بوظائف تتطلب ذكاء الأشخاص العادية، وقد جرت العادة على استخدام مصطلح الخوارزميات للتعبير عن تطبيقات الذكاء الاصطناعي، فعلى سبيل المثال: استخدام المواقع لاتخاذ القرار الحسابي، ومع ذلك مفهوم الخوارزمية أكثر عمومية من مفهوم الذكاء الاصطناعي؛ لأنه يتضمن تسلسل من التعليمات المحددة بصورة لا لبس فيها لتنفيذ مهمة معينة. وقد تكون الخوارزميات بسيطة بحيث تحدد كيفية ترتيب قوائم الكلمات بالترتيب الأبجدي، أو كيفية العثور على العنصر المشترك بين رقمين، وقد تكون الخوارزميات معقدة للغاية، ومثال ذلك: خوارزميات تشفير الملفات وخوارزميات ضغط الملفات الرقمية وخوارزميات التنبؤ المالي[١].

وقد يجري استخدام البيانات الشخصية لعمل التوقعات والتقييمات المستمدة من الذكاء الاصطناعي، ثم تحليل المخاطر والنتائج المترتبة على ذلك، وهو ما يساعد على اتخاذ القرارات الخاصة بالأفراد شريطة مراعاة المساواة وعدم التمييز، ومثال ذلك: ربط النموذج الطبي لأعراض المرض ذاته، وربط نموذج القياسي النفسي بسلوك الفرد على مواقع التواصل الاجتماعي[٢].

ويؤدى دمج تقنيات الذكاء الاصطناعي والبيانات الضخمة إلى تحقيق العديد من المزايا، ومثال ذلك: تيسير الوصول إلى المعلومات وإنشاء المعارف وتوزيعها على كافة أنحاء العالم، وتوفير التكاليف المالية وزيادة نطاق الوظائف الإبداعية، وزيادة الشفافية والحد من التحيز والتمييز بين أفراد المجتمع دون وجه حق. كما يسهم هذا الدمج في زيادة نطاق توقع الشركات لاتجاهات السوق واتخاذ القرارات المناسبة وتمكين المستهلك من اتخاذ القرارات الأكثر فائدة، وتمكين السلطات

(١) فريدة بن عثمان، الذكاء الاصطناعي، مقاربة قانونية، دفاتر السياسة والقانون، المجموعة ١٢، الجزء الثاني، ٢٠٢٠، ص١٥٦.

(٢) كريم على سالم، الجوانب القانونية للذكاء الاصطناعي، مجلة جيل الأبحاث القانونية المعمقة، العدد ٥٤، أكتوبر ٢٠٢٢، ص٥٣.

العامة من توقع المخاطر ومنع وقوع الضرر[١].

وبناء على ذلك، تريد الباحثة من هذه الدراسة تسليط الضوء على العلاقة بين تقنية الذكاء الاصطناعي وحماية البيانات على ضوء لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي عام ٢٠١٦م، فتقنية الذكاء الصناعي انتشرت في العالم بصور مختلفة، ومثال ذلك: الروبوتات الصناعية، وروبوتات الخدمة في المنازل ومنشآت الرعاية الصحية، والطائرات بدون طيار والوكلاء الإلكترونيين في مجال التجارة الإلكترونية، وهو ما يعنى أن تقنية الذكاء الاصطناعي أضحت إحدى آليات التغيير الاقتصادي والاجتماعي لأفراد المجتمع[٢].

وبالتالي، يجب تطوير وتغيير القواعد القانونية لكى تتناسب مع هذا التطور التقني المذهل على ضوء المخاطر المترتبة على استخدام هذه التقنية في كافة مجالات الحياة، فقد يزيد نطاق خطر السيطرة والتلاعب والتمييز بين أفراد المجتمع قدر أهمية هذه التقنية في تسهيل حياة أفراد المجتمع، ولذلك يزيد نطاق الضرر الذى قد يصيب الفرد لو أخفقت هذه التقنيات الحديثة في عدم احترام الحقوق الفردية أو عدم مراعاة القيم الاجتماعية السائدة[٣].

وبناء على ذلك، ظهرت العديد من المسائل القانونية والأخلاقية في نطاق الاستخدامات المختلفة لتقنية الذكاء الاصطناعي في مجالات المسئولية المدنية والتأمين وحماية البيانات الشخصية. وتشغل الحماية القانونية للبيانات الشخصية مكانة هامة في نطاق العلاقة بين الذكاء الاصطناعي والقانون، فقد تتضمن العديد من تطبيقات تقنية الذكاء الاصطناعي معالجة إلكترونية للبيانات الشخصية بما في ذلك استهداف الأفراد ومعالجة بياناتهم الشخصية.

---

(١) إيناس خلف الخالدي، حوكمة استخدام الذكاء الاصطناعي في العمل القضائي، قراءة قانونية في الميثاق الأخلاقي الأوربي بشأن استخدام الذكاء الاصطناعي في النظم القضائية وبيئتها، مجلة البحوث والدراسات الشرعية، العدد السادس عشر بعد المائة رجب ١٤٤٢، ص١٦٢.

(2) D.L DALKE, Can Computer Replace Lawyers, Mediators and Judges? in The Advocate, 1, 2013, p.12

(3) Aletras N, Tsarapatsanis D, Preoţiuc-Pietro D, Lampos V. 2016. 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', Peer Computer Science 2:e93 https://doi.org/10.7717/peerj-cs.93.

وهو ما يستوجب زيادة فعالية الحماية القانونية لهذه البيانات في حالة استخدام تقنية الذكاء الاصطناعي، أي بحث آليات حماية البيانات الشخصية على ضوء المخاطر التي تهدد هذه البيانات نتيجة استخدام تقنيات الذكاء الاصطناعي[١].

موضوع البحث:

سوف نتناول في هذه الدراسة تقنية الذكاء الاصطناعي وتطورها على المستوى التكنولوجي والاجتماعي وعلاقتها بالمعالجة الفنية للبيانات الشخصية من خلال بيان مفهوم الذكاء الاصطناعي والعلاقة بينه وبين المعالجة التقنية للبيانات الشخصية. وفى نطاق الحماية القانونية المقررة للبيانات الشخصية، يتعامل الذكاء الاصطناعي مع هذه البيانات ويعالجها، وهو ما يستوجب وجود تنظيم قانوني محكم لآليات حماية البيانات في مثل هذه الأحوال، وخاصة أنها تكثر في المجال الطبي والرعاية الصحية.

وما يعضد ذلك، أن معالجة البيانات الشخصية يمثل اعتداء كبير وخطير على صاحب هذه البيانات؛ لأنها ستفضى إلى تبنى صورة كاملة عن هذا الشخص، ودون علمه بذلك. علاوة على ذلك، تحيط المخاطر البيانات الشخصية بسبب استخدام الحاسب الآلي وتقنيات الذكاء الاصطناعي لإنشاء قواعد البيانات الشخصية وتكوين العديد من الشبكات بين الجهات المعنية لتيسير تبادل هذه البيانات فيما بينها.

أيضا، تتطور آليات الدعاية والتسويق بحيث أصبحت البيانات الشخصية هي الأساس الذى يجرى بناء هذه الآليات عليه من أجل الدعاية للشركات التجارية، فظهرت نظرية التسويق المباشر التي تنهض على فكرة إنشاء دعاية خاصة لكل عميل من خلال المعلومات التي يجرى تجميعها عنه، وهذه المعلومات هي بمثابة البيانات الشخصية للعميل.

ولذلك، أضحت هذه البيانات الشخصية ذات قيمة مالية كبيرة لهذه الشركات، وهو ما ترتب عليه ظهور ما يمكن تسميته بتجارة البيانات الشخصية،

(1) C. BARBARO, Y. MENECEUR, Issues in the use of artificial intelligence (AI) algorithms in judicial systems, 1, 2018, p.23

والتي أضحت سبباً لتحقيق ربح وفير للكثير من الشركات والأفراد.

إشكالية البحث:

تدور إشكالية هذا البحث حول مدى إمكانية صياغة إطار قانوني من أجل حماية البيانات الشخصية في نطاق الاستخدام المشروع لتقنيات الذكاء الاصطناعي، والتي قد تثير العديد من المشكلات القانونية، ومثال ذلك:

١- ما مدى مشروعية معالجة البيانات الشخصية عبر تقنية الذكاء الاصطناعي؟ فهل هذه المعالجة أمر قانوني ويجوز القيام به دون ضابط قانوني لذلك، أم أنه أمر غير قانوني ولا يجوز القيام به بصورة مطلقة، أم هناك شروط وضوابط يجب مراعاتها حتى تكون معالجة البيانات الشخصية عبر تقنيات الذكاء الاصطناعي صحيحة؟

٢- لو كانت معالجة البيانات الشخصية عبر هذه التقنيات المتطورة مشروعة، فما هي الواجبات التي تقع على عاتق الشخص الذى يقوم بهذه المعالجات حتى تكون مشروعة ومحققة لكافة النتائج المرجوة منها؟

٣- ما هي حقوق الشخص الذى يجرى معالجة بياناته عبر تقنية الذكاء الاصطناعي، وكيف تتم حماية هذه البيانات بصورة قانونية سليمة في ظل التطور التقني الكبير؟

منهج البحث:

سوف نعتمد على المنهج التحليلي لنصوص لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي عام ٢٠١٦ لبيان حقيقة العلاقة القانونية بين تقنيات الذكاء الاصطناعي وضرورة الحماية القانونية للبيانات الشخصية. وما يعضد ذلك العلاقة الوثيقة بين ضرورة حماية البيانات الشخصية من ناحية وحماية الحياة الخاصة من ناحية أخرى على أساس أن هذه البيانات هي عنصراً من عناصر الحياة الخاصة لأفراد المجتمع.

خطة البحث:

تنقسم دراسة هذا البحث إلى مقدمة، ومبحثين، وذلك على النحو الآتي:

أما المقدمة: فاشتملت على أهمية الموضوع، وأسباب اختياره، وإشكالية البحث، والمنهج، والخطة.

وأما المبحث الأول: مفهوم الذكاء الاصطناعي وعلاقته بالبيانات الشخصية

والمبحث الثاني: الحماية القانونية للبيانات الشخصية

المبحث الأول
مفهوم الذكاء الاصطناعي وعلاقته بالبيانات الشخصية

تمهيد وتقسيم:

لا يخفى على أحد العلاقة الوثيقة بين الذكاء الاصطناعي والبيانات الشخصية، فهذه التقنية الحديثة تعتمد على هذه البيانات بصورة كلية بحيث لا تقوم لها قائمة بدون هذه البيانات، هذا من ناحية أولى.

ومن ناحية أخرى، أصدر المشرع المصري التشريعات التي تحمى البيانات الشخصية من كافة صور الاعتداء عليها، والتي تشكل في غالبية حالتها جريمة يعاقب عليها القانون، وبناء على ذلك تنقسم دراسة هذا المبحث إلى مطلبين، وذلك على النحو الآتي:

المطلب الأول ـ المقصود بتقنيات الذكاء الاصطناعي.

المطلب الثاني ـ المقصود بالبيانات الشخصية.

المطلب الأول
المقصود بتقنيات الذكاء الاصطناعي

لم تتفق الآراء على تحديد المقصود بتقنيات الذكاء الاصطناعي بسبب التطور المستمر والمتلاحق للتكنولوجيا، إلا أن هذه الآراء تتفق على أنه يقصد بهذه التقنيات استخدام الآلة الحديثة بطريقة مماثلة للعمل البشرى بحيث تتضمن سلوكاً ذكياً من خلال تحليل الوقائع والبيانات التي أدخلها العنصر البشرى من أجل اتخاذ الإجراءات المناسبة وبصورة مستقلة[١].

كما عرفها البعض بأنها: "استجابة الآلة بصورة توصف بأنها ذكية"، أو "هو العلم الذى يسعى نحو إنتاج آلة أو أنظمة ذكية لها قدرات شبيهة بقدرات العقل البشرى"، أو "هو العلم الذى يبحث في كيفية جعل الحاسب يؤدى الأعمال التي يؤديها البشر بطريقة أفضل منهم"[٢].

ويترتب على ما سبق أن تقنيات الذكاء الاصطناعي تشتمل على ما يلى:

١- أنظمة الكمبيوتر ذات المهام المحدودة.

٢- أنظمة الذكاء الاصطناعي ذات المهام المتوسطة.

٣- أنظمة الذكاء الاصطناعي ذات الأداء القوى، والذى يتضمن أنظمة تقنية تتجاوز قدرات البشر[٣].

أهمية الذكاء الاصطناعي:

تتعدد مظاهر أهمية الذكاء الاصطناعي في نطاق الخدمات الواسعة التي

---

(1) Lorenzo Picotti, Questionnaire - Section I (Droit pénal - partie générale) Catégories traditionnelles de droit pénal et IA: crise ou palingénésie? http://www.penal.org › files › p.15

(٢) محمد بومديان، الذكاء الاصطناعي تحد جديد للقانون، مسارات في الأبحاث والدراسات القانونية، العدد ١٠، ٢٠١٩، ص١٩٨.

(3) Lorenzo Picotti, Questionnaire - Section I (Droit pénal - partie générale) Catégories traditionnelles de droit pénal et IA: crise ou palingénésie? http://www.penal.org › files › p.15

تشتمل على مجالات عديدة، ومثال ذلك:

١- الحديث مع الحاسب الآلي شفاهة، وهو ما يعنى التواصل مع الحاسب سهل، وخاصة أنه علم مفيد لمن لا يتقن التعامل مع هذه التقنية، فضلاً عن سرعته العالية في الكتابة بحيث يستطيع كتابة مئات الكلمات في دقيقة واحدة[١].

٢- أداء العمل بصورة دقيقة، وبدون تعب أو ملل.

٣- تقديم الاستشارات للمستخدم في كافة التخصصات العلمية والعملية، ودون تكاليف باهظة.

٤- التخفيف عن أفراد المجتمع في الكثير من المخاطر والضغوطات النفسية، وخاصة في المجالات التي تحتوى على تفاصيل تتسم بأنها معقدة، وتحتاج إلى تركيز عقلي كبير، وحضور ذهني متواصل[٢].

خصائص الذكاء الاصطناعي:

تتميز تقنية الذكاء الاصطناعي بمجموعة من الخصائص، ومن أهمها:

١- الاجتهاد: تتميز تطبيقات الذكاء الاصطناعي بالقدرة على الاجتهاد، فإن البيانات التي يجرى إدخالها في هذه التطبيقات لا يحكمها خطوات من أجل الوصول للمشكلة أو اتخاذ القرار[٣].

٢- التعامل مع البيانات المتضاربة: تملك تقنية الذكاء الاصطناعي القدرة على التعامل مع البيانات المتضاربة، والتي تتناقض بعضها البعض بحيث يستطيع المتعامل الوصول لنتيجة لا تتعارض مع سائر علوم المعرفة.

---

(1) Katz, Daniel Martin et al. A General Approach for Predicting the Behavior of the Supreme Court of the United States (January 16, 2017). SSRN: https://ssrn.com/abstract=2463244

(٢) محمد فتحي محمد إبراهيم، التنظيم التشريعي لتطبيقات الذكاء الاصطناعي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد ٨١، سبتمبر ٢٠٢٢، ص١٠٢٥.

(٣) محمد القطب مسعد، دور قواعد الملكية الفكرية في مواجهة تحديات الذكاء الاصطناعي، دراسة قانونية تحليلية مقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد ٧٥، مارس٢٠٢١، ص١٦٢٨.

٣- القدرة على التعلم: تمثل القدرة على التعلم من الأخطاء أحد معايير السلوك التي يتميز بها الذكاء الاصطناعي كنتيجة للاستفادة من الأخطاء السابقة[1].

(1) L. Julia. L'intelligence artificielle n'existe pas (AI does not exist). First Edition, Paris 2019, p. 123

المطلب الثاني
المقصود بالبيانات الشخصية

تبنت المادة الثانية من القانون الفرنسي رقم ٧ لسنة ١٩٧٨ والمعدل بالقانون رقم ٨٠١ لسنة ٢٠٠٤ والمتعلق بحماية البيانات الشخصية تعاريف للبيانات الشخصية، فذكرت أنه "يعتبر بياناً شخصياً كل معلومة تتعلق بشخص طبيعي محدد هويته أو من الجائز تحديد هويته بصورة مباشرة أو غير مباشرة، وسواء تم ذلك من خلال الرجوع إلى الرقم القومي أو بالرجوع لأي شخص يخصه".

ووفقا لرأى أحد الفقهاء، يعد هذا التعريف تعريف حديث لفكرة البيانات الشخصية، وهو تعريف واسع بسبب موقف الفقه والقضاء الفرنسي الذى كان يأخذ بتعريف ضيق للبيانات الشخصية، وهو ما انعكس أثره على موقفه من خلال تبنى تعريف مرن لهذه العبارة القانونية الحديثة بحيث تشتمل على كافة صور البيانات الشخصية[١].

كما أخذت اللجنة القومية للمعلوماتية والحريات الفرنسية بالمفهوم الواسع لفكرة البيانات الشخصية على الرغم من أن المفهوم الضيق الذى تبناه القانون، فقد أخذت الفقه والقضاء لتفسير النص تفسيراً واسعاً؛ ليسمح بدخول الكثير من البيانات تحت مسمى فكرة البيانات الشخصية، وبالتالي تخضع للحماية القانونية[٢].

كما كان القانون رقم ١٧ لسنة ١٩٧٨ قبل التعديل بالقانون رقم ٨٠١ لسنة ٢٠٠٤ يمنح البيانات الشخصية تعريفاً ضيقاً، فقد كان يعرفها بأنها "معلومات تسمح بصورة مباشرة أو غير مباشرة لتحديد هوية الأشخاص الطبيعية".

كما أوضحت المادة الأولى من القانون المصري لحماية البيانات الشخصية المقصود بالبيانات الشخصية، فذكرت "أي بيانات متعلقة بشخص طبيعي محدد،

(1) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier 1, 2003, p.15

(٢) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، دراسة القانون الفرنسي، القسم الأول، مجلة الحقوق، جامعة الكويت، سبتمبر ٢٠١١، مج ٣٥، ع٣، ص٣٨٥.

أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الانترنت، أو أي بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية".

وجدير بالذكر أن الحماية القانونية للبيانات الشخصية تقتصر على البيانات الشخصية للأشخاص الطبيعية، فالبيانات الخاصة بالشخص الاعتباري تخرج عن نطاق الحماية القانونية[١].

ويقصد بالبيانات المادة الأساسية والخام التي يستمد منها المعلومات، وتمثل مجموعة الحقائق والأفكار والمشاهدات والملاحظات والقياسات، وعادة ما تكون في صورة أعداد أو كلمات أو رموز خاصة[٢]، وتنتج المعلومة بعد معالجة البيانات وتحليلها، فالعلاقة بين البيانات والمعلومات هي علاقة دورية بحيث يجرى تجميع البيانات وتشغيلها للحصول على المعلومات، ويجرى استخدام هذه المعلومات لاتخاذ القرارات التي قد تؤدى لتنفيذ مجموعة من الإجراءات التي قد تحتاج لمجموعة إضافية من البيانات؛ ليجري تجميعها مرة أخرى ومعالجتها للحصول على معلومات إضافية أخرى لاتخاذ قرار آخر[٣].

صور البيانات الشخصية:

تبنى القانون الفرنسي تعريفاً للبيانات الشخصية، والذى يتضمن معياراً يجوز تطبيقه لتحديد ما إذا كانت المعلومة الخاصة بشخص ما بياناً شخصياً من عدمه، وبالتالي، هل تخضع للحماية القانونية التي تبناها المشرع الفرنسي من عدمه؟

ولذلك، ليس من السهل تحديد الصور المختلفة للبيانات الشخصية بطريقة مسبقة؛ لأنه من المتوقع أن يظهر في المستقبل صور معلومات يمكن اعتبارها بيانات

(1) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier 1, 2003, p.15

(2) C. BARBARO, Y. MENECEUR, Issues in the use of artificial intelligence (AI) algorithms in judicial systems, 1, 2018, p.23

(٣) كريم على سالم، الجوانب القانونية للذكاء الاصطناعي، مرجع سابق، ص٥٣.

شخصية، وتطبيقا لذلك تظهر شبكة المعلومات الدولية الرقم الخاص بالكمبيوتر الشخصي (IP) كبيان شخصي، وهى مسألة لم تكن معروفة من قبل، ولم تكن تدخل في البيانات الشخصية[١].

وبناء على ذلك، لا تخضع صور البيانات الشخصية لحصر، فهناك العديد من الأمثلة التي يمكن إيرادها للتوضيح، وبالتالي تخضع للحماية القانونية المقررة للبيانات الشخصية، وقد تظهر صور أخرى للبيانات الشخصية في المستقبل، ويجب إخضاعها للحماية القانونية المقررة في مثل هذه الأحوال، وهو ما يمكن أن يصلح كتبرير للمفهوم الواسع الذى أخذ به القانون الفرنسي للبيانات الشخصية حتى تقبل الصور الحديثة التي قد تظهر في المستقبل، وهو ما يعد موقفاً موفقاً للمشرع الفرنسي[٢].

وبناء على ذلك، تكون المعلومات الآتية بيانات شخصية، ويجب حمايتها قانوناً:

الاسم:

يعد الاسم وسيلة لتمييز الأشخاص عن غيرهم، ويمكن تقسيم الاسم إلى اسم أصلى وأسم شهرة وأسم مستعار، ويقصد بالاسم الأصلي هو الاسم المذكور في شهادة الميلاد وبطاقة تحقيق الشخصية، ويظهر في المعاملات الرسمية، بينما يقصد باسم الشهرة الاسم الذى يختلف عن الاسم الأصلي ويشتهر به الشخص بين أفراد المجتمع، ولا يمكن ذكره في شهادة الميلاد أو بطاقة تحقيق الشخصية، والاسم المستعار هو الاسم الذى يتخذه الشخص لنفسه غير الاسم الأصلي بمناسبة نشاط مهني أو فني أو أدبي بغاية إخفاء الشخصية الحقيقة للشخص. ويقصد باللقب اسم الأسرة التي ينتمى إليها الشخص[٣]. واتفقت كافة التشريعات المعنية بحماية البيانات الشخصية على أن اسم الشخص ولقبه بيان شخصي، ويجب حمايته قانوناً.

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٨٥.

(٢) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٨٦.

(3) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.15

الصورة والصوت:

ترى اللجنة القومية الفرنسية للحريات أن صورة الشخص الطبيعي سواء الثابتة أو المتحركة هي بيان شخصي ويخضع للحماية المقررة قانوناً، وهو ذات ما تسري أحكامه على صوت الشخص، فقد رأته هذه اللجنة أن بيان شخصي ومحمي قانوناً، وقد أسست هذه اللجنة وجه نظرها على أن التكنولوجيا الحديثة تسمح بمعالجة الصورة والصوت، وتحميلهم على دعامة واحدة مما يعني اعتبارهما بيانات شخصية قابلة للمعالجة وبصورة منفصلة(١).

وقد استندت الحماية القانونية لبيان الصورة والصوت على التوجيه الأوروبي الخاص بحماية البيانات الشخصية والصادر في ٢٤ أكتوبر ١٩٩٥ قبل إصدار القانون الفرنسي المعنى بحماية هذه البيانات كنوع من الحماية المستقلة، وبناء على ذلك، اعتبار صورة الفرد وصوته بياناً شخصياً هو بمثابة مفهوم جديد وحديث للبيانات الشخصية، فقد كان نطاق هذه البيانات يقتصر على البيانات الأساسية كبيان الاسم واللقب والسن والوظيفة(٢).

كما أن التكنولوجيا الرقمية الجديدة تسمح بمعالجة الصورة والصوت من خلال الحاسب الآلي بحيث يجرى إضافة نص لصورة معينة أو إضافة صوت لنص معين من خلال استخدام برامج الحاسب الآلي، بحيث يؤدى ذلك إلى اعتبار الصورة والصوت بيانات شخصية ويجوز معالجتها، وهو ذات ما يسري على صوت الشخص بحيث يعتبر بياناً شخصياً ويجب إخضاعه للحماية القانونية للبيانات الشخصية على أساس أنه مفهوم حديث لمثل هذه البيانات(٣).

الرقم الشخصي:

يعد الرقم الذى يمنح لكل شخص طبيعي بيان شخصي بحيث يكون خاص به

---

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٨٧.

(2) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.16

(3) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.17

ويميزه ويحدد هويته، ومثال ذلك: الرقم القومي بحيث يكون لكل شخص رقم خاص به على مستوى الدولة، وهو ذات ما يسري على الرقم التأميني، ويقصد به رقم التأمين الاجتماعي الخاص بالشخص الطبيعي، وهو ذات ما تسري أحكامه على رقم التأمين الصحي، ورقم الاشتراك في وسائل المواصلات طالما أنه رقم خاص بالشخص وغير قابل للتكرار وفقا لتعدد الأشخاص[١].

العنوان:

يعد البيان الخاص بالعنوان بيان شخصي سواء كان عنوان المنزل أو عنوان العمل أو عنوان المكان المخصص لقضاء العطلات، فمثل هذا البيان محمي بقواعد القانون المقررة لحماية البيانات الشخصية.

الحالة الاجتماعية:

هي كافة البيانات المتعلقة بالحالة العائلية لأفراد المجتمع، وتشكل بيان شخصي، ومثال ذلك حالة الشخص كمتزوج أو أعزب أو مطلق، وتسري الحماية القانونية المقررة للبيانات الشخصية على كافة بيانات الحالة الاجتماعية[٢].

الحالة الصحية:

وفقا لنص المادة ٨ من قانون حماية البيانات الشخصية الفرنسي تعد الحالة الصحية بيان شخصي ومحمى قانوناً، ولم يكن القانون الفرنسي ينص على ذلك قبل تعديله بحيث لم تكن المعلومات الخاصة بالحالة الصحية بيانات شخصية، إلا أن اللجنة القومية للحريات الفرنسية اعتبرت أن المعلومات الخاصة بالحالة الصحية بيانات شخصية[٣].

الأصول العرقية:

تؤكد المادة الثامنة من قانون حماية البيانات الشخصية الفرنسية على أن

---

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٨٨.

(2) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.18

(3) Ibid. p.19

المعلومات الخاصة بالأصول العرقية للإنسان هي بيانات شخصية محمية قانوناً.

الجنسية:

تعتبر اللجنة القومية للحريات الفرنسية أن المعلومات الخاصة بجنسية الفرد هي بيانات شخصية ويجب إخضاعها للحماية القانونية[١].

الآراء السياسية والمعتقدات الدينية:

تطبيقا لحكم المادة الثامنة من قانون حماية البيانات الشخصية الفرنسي، كافة المعلومات الخاصة بالآراء السياسية والدينية هي بيانات شخصية ويحمي القانون، وهو ذات ما يسرى حكمه على البيانات الخاصة بانتماءات الشخص النقابية.

الاختبارات النفسية:

ترى اللجنة القومية للحريات أن نتائج الاختبار النفسي لأي فرد من أفراد المجتمع بيانات شخصية ومحمية قانوناً، فنتائج هذه الاختبارات هي بمثابة معلومات تتعلق بالحالة الصحية للفرد، فالجانب النفسي جزء من صحة الفرد[٢].

البصمة:

ترى اللجنة القومية للحريات في فرنسا أن بصمة الفرد بمثابة بيان شخصي أيا كانت صورة البصمة سواء كانت بصمة صابع أو بصمة بكامل محيط اليد، فهناك بصمات تتباين من شخص لأخر مثل: بصمات الإصبع واليد والعين بحيث يجرى تجميعها بصورة إلكترونية، وبالتالي، تعد بيان شخصي محمي قانوناً[٣].

رقم الهاتف:

يعد رقم الهاتف لأي شخص أحد البيانات الشخصية التي يحمي القانون

(1) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.20

(٢) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩٢.

(3) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.22

سواء كان رقم هاتف المنزل أو رقم هاتف المحمول.

رقم السيارة:

يعد رقم السيارة التي يملكها أحد الأشخاص بيان شخصي ويحمي القانون الفرنسي[١].

رقم الحساب البنكي:

إذا فتح أحد الأشخاص حساب بنكي في أحد البنوك، فإن رقم الحساب بيان شخصي يحميه القانون.

عنوان البريد الإلكتروني:

لكل فرد من أفراد المجتمع بريد إلكتروني على شبكة الانترنت بحيث يعد العنوان الإلكتروني المستخدم لإرسال واستقبال الرسائل الإلكترونية بيان شخصي محمى قانوناً[٢].

عنوان الكمبيوتر (IP):

لكل حاسب آلي متصل بالإنترنت عنوان يتألف من ٣٢ رقماً بحيث يكون هذا الرقم عنوان لتحديد مكان هذا الحاسب الآلي، ويرى الفقه الفرنسي: أن عنوان الحاسب الآلي هو بيان شخصي لأحد المستخدمين لهذا الحاسب؛ لأنه يتعلق بمعلومة غير مباشرة بأحد الأشخاص الذين يجوز تحديد هويتهم.

وجدير بالذكر أن ما سبق ذكره لا يعدو سوى أمثلة لتوضيح بعض البيانات الشخصية وفقا للمعنى الحديث الذى أخذ به القانون الفرنسي، فهذا المعنى قابل للتطبيق على البيانات الأخرى التي لم تشتمل عليها الأمثلة السابقة، وقد تظهر في المجتمع وفقا للمتغيرات الاجتماعية والاقتصادية التي قد تحدث. ولذلك، يعد تاريخ ميلاد أحد الأشخاص ووظيفته وعنوانه البريدي العادي أحد البيانات الشخصية التي يحميها القانون، وهو ذات ما يسرى حكمه على رقم الفاكس ورقم البطاقة

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٨٩.

(2) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.15

الائتمانية[١].

كذلك، تعد هوايات الفرد وسلوكه ووضعه المالي وعلاقته الأسرية أحد البيانات الشخصية بصورة غير مباشرة، ويحميها القانون، شأنها في ذلك شأن البيانات التي تحمل الدلالة المباشرة.

إمكانية تعرض البيانات الشخصية لمخاطر عديدة:

قد تتعرض البيانات الشخصية للعديد من المخاطر التي قد تدفع المشرع الوطني والدولي إلى إصباغ الحماية القانونية على هذه البيانات، ومثال ذلك: قيام الشركات والمؤسسات والجهات الإدارية التابعة للدولة بتجميع بيانات أفراد المجتمع، فتجميع هذه البيانات يعد أول المخاطر التي قد تتعرض لها هذه البيانات[٢].

وفى مرحلة لاحقة على تجميع هذه البيانات الشخصية، تظهر مرحلة تصنيف هذه البيانات من خلال عمل ملف لكل فرد من أفراد المجتمع من خلال صياغة كافة بياناته في هذا الملف عبر تجميعها في مناسبات مختلفة عن ذات الشخص وفى ملف واحد[٣].

وفى مرحلة أخرى، تأتى مرحلة التعامل مع هذه البيانات بحيث تتعامل الجهات والمؤسسات والشركات مع هذه البيانات بعد تجميعها بغاية الوصول إلى صورة غير كاملة عن الشخص صاحب هذه البيانات، وبالتالي الاتجار بهذه البيانات، فقد أضحت هذه البيانات مصدر ثروة كبيرة للشركات التي تقوم ببيعها لجهات أخرى، فضلا عما سبق قد تتعرض البيانات الشخصية للفقدان أو السرقة من جانب أي جهة تملك ملفات أو قواعد بيانات تحوي هذه البيانات[٤].

خطر تجميع البيانات الشخصية:

تتعامل أفراد المجتمع مع جهات كثيرة، والتي تطلب منه الإدلاء ببعض

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩٠.
(٢) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩١.
(٣) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩٢.
(4) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.18

البيانات الشخصية سواء كانت هذه الجهات شركات أو فنادق أو مستشفيات أو بنوك أو جهات إدارية تتعامل مع أفراد المجتمع بصورة متكررة. وقد تتعلق هذه البيانات بالوضع المادي أو الوظيفي أو العائلي أو الصحي أو التعليمي للفرد، وقد تكون هذه البيانات مهمة لضمان حسن سير العمل، وخاصة أمام الجهات الإدارية التي تتبع الدولة. وتزداد خطوة الوضع الذى قد تتعرض البيانات الشخصية لو تم تجميع هذه البيانات بواسطة جهات خاصة، ومثال ذلك: المستشفيات والفنادق والشركات التجارية والبنوك، فالجهات الخاصة لا يقتصر دورها على تجميع هذه البيانات لتقدم خدماتها لأفراد المجتمع، بل تتعدى المسألة نطاق تجميع البيانات[١].

ويجري جمع البيانات الشخصية على شبكة الانترنت من خلال تقنية تسمى كوكيز، وهى عبارة عن موقع خاص للمنشأة التجارية يجرى وضعه على القرص الصلب الخاص بالحاسب الآلي. ويقوم هذا الملف بتخزين العديد من المعلومات عن مستخدم شبكة المعلومات، ومثال ذلك: المواقع التي قام بزيارتها والمنتجات التي يفضل الحصول عليها، واسم وعنوانه ورقم بطاقة الائتمان وعنوان البريد الإلكتروني الخاص به.

ويرسل هذا الملف هذه المعلومات للموقع الخاص بالمنشأة التجارية التي تقوم باستخدام هذه البيانات؛ لإرسال عروض تجارية لمستخدم الإنترنت عبر البريد الإلكتروني[٢].

خطر تصنيف البيانات الشخصية:

يقصد بتصنيف البيانات الشخصية إنشاء ملف لكل فرد ليتضمن كافة بياناته الشخصية عبر إنشاء قاعدة بيانات تحوى كافة البيانات التي تم تجميعها قبل ذلك. وتساعد قاعدة البيانات المنشآت التجارية على التسويق المباشر بحيث تسهم هذه القواعد على تصميم العروض الدعائية لكل عمل حتى تتناسب مع ذوقه، وتساعدها على اتخاذ القرار الصحيح حتى تضمن قبول العميل للعرض بصورة كبيرة. كما

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩٣.

(2) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.19

يسهم الحاسب الآلي في تصنيف البيانات الشخصية التي يجرى تجميعها من جانب المنشأة التجارية بحيث يجرى تخزين هذه البيانات وتحليلها وتصنيفها واسترجاعها ومقارنتها، فالبيانات الشخصية المجمعة يجوز ضمها في قاعدة بيانات كبيرة من خلال الحاسب الآلي.

وبناء على ذلك، يتصل العميل بالمتجر لشراء المنتج، ولا يحتاج هذا المتجر سوى بيانات عن الاسم أو العنوان؛ لأن كافة بيانات العميل يجرى تسجيلها لدى المتجر، ويتم الرجوع إليها من خلال رقم الهاتف[١].

الاتجار بالبيانات الشخصية:

أضحت البيانات الشخصية موضوعاً للتعامل بين الجهات التي تتولى جمعها بحيث تتبادل كل منشأة البيانات التي سبق لها جمعها مع منشأة أخرى بغاية الوصول إلى بيانات كاملة عن كل فرد من أفراد المجتمع[٢].

ويكمن الخطر في مثل هذه الأحوال أن الفرد يمنح بعض بياناته لجهة معينة معتقداً أنها بيانات ضرورية لتقديم خدمة ما له، كما أن هذه البيانات لا ترسم صورة كاملة عنه، فقد يتم إكمال هذه البيانات ببيانات أخرى قام ذات الفرد بتقديمها قبل كذلك لإحدى الجهات بحيث يتم إكمال صورة عن هذا الفرد.

ولذلك، يكون تداول هذه البيانات سهل من خلال استخدام شبكات الانترنت بحيث يجرى تكوين شبكة من الحاسب الآلي التي تحتوى على قواعد بيانات متعددة للعديد من الجهات، بحيث يكون انتقال هذه البيانات سهل جداً، ودون الحاجة إلى عنصر بشرى[٣].

كما أن هذه البيانات الشخصية أضحت موضوعاً لاقتصاد جديد وموضوعاً للإتجار بها من كافة الجهات التي قامت بتجميعها بحيث تجلب المال لها. وبناء على ذلك، سهولة تجميع البيانات الشخصية وانخفاض تكلفتها ومعالجتها أدت إلى

(١) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩٣.

(2) Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, op.cit. p.20

(٣) سامح عبدالواحد التهامي، الحماية القانونية للبيانات الشخصية، مرجع سابق، ص٣٩٩.

قيام المنشآت التجارية إلى جمع هذه البيانات وبيعها للجهات التي ترغب فيها، بل قامت العديد من الشركات ببيع البيانات الشخصية التي تحوزها بعد صدور حكم بإفلاسها وخروجها من البيئة التجارية.

سرقة البيانات الشخصية وفقدانها:

جمع البيانات الشخصية وتصميم قاعدة بيانات لها قد يؤدى إلى إمكانية فقدها أو سرقة ما تتضمنه من بيانات شخصية، فهذه البيانات موجودة على قاعدة بيانات على الحاسب الآلي المتصل بشبكة الانترنت، وهو ما قد يؤدى لتعرضها لعمليات القرصنة التي تدخل لقاعدة البيانات وسرقتها واستخدامها على نحو غير مشروع أو بيعها لجهات أخرى، فالقرصنة عمل غير مشروع، ويظهر نتيجة لضعف التأمين(١).

وتطبيقا لذلك، ذكرت دار نشر تسمى Lex-nexis أنه البيانات الشخصية لأكثر من ٣٢ ألف مشترك تم سرقتها من قاعدة البيانات الخاصة بها عام ٢٠٠٥، كما ذكرت إحدى الشركات الأمريكية أن قرصنة قاعدة بياناتها وقعت في ٢٠٠٦، وهو ما ترتب عليه سرقة بيانات الكرت البنكي لأكثر من ٤٠ مليون عميل(٢).

كما قد تحدث واقعة السرقة للحاسب الآلي الذى يتضمن قاعدة البيانات الشخصية، ففي الولايات المتحدة الأمريكية تم سرقة جهاز الحاسب الآلي لأحد المستشفيات، والذى كان يتضمن بيانات ١٨٥ ألف مريض، كما قد تتعرض البيانات الشخصية لواقعة الفقد نتيجة خطأ أحد الأفراد، ومثال ذلك: فقدت الإدارة الضريبية البريطانية بيانات ٢٥ مليون ممول في عام ٢٠٠٧(٣). كما فقدت أحد

(1) Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, The European 18 Information & Communications Union general data protection regulation: what it is and what it means,
Technology Law. Volume 28, 2019 - Issue 1.p.75

(2) Paul Lanois, Time to forget: EU privacy rules and the right to request the deletion of data on the internet. Journal of Internet Law. October 2014 p. 21

(٣) محمد حسن عبدالله، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً، دراسة تحليلية مقارنة في ضوء اللائحة الأوربية وبعض التشريعات ذات العلاقة، مجلة العلوم

الشركات الفرنسية أسطوانة تحمل بيانات شخصية لأكثر من ٩ الألف عامل فيها عام ٢٠٠٦، وأعلن بنك أمريكي عن فقدان بيانات شخصية لأكثر من مليون عميل[١].

الحماية المدنية للبيانات الشخصية:

تؤكد اللائحة الأوربية لحماية البيانات الشخصية على حق كل فرد من أفراد المجتمع أصابه ضرر مادى أو غير مادى كنتيجة لمخالفة أحكام هذه اللائحة أن يحصل على تعويض مادى من المعالج أو المتحكم الصادر عنه هذا الضرر. ومع ذلك، يعفى المعالج والمحتكم من المسئولية المدنية لو ثبت أنه غير مسئول عن الفعل الذى ترتب عليه الضرر الذى أصاب الفرد الذى يدعى حدوث ذلك[٢].

وتطبيقا لذلك، قضت محكمة العدل الأوربية بأن: "مشغل موقع الويب الذى يحوى على زر الإعجاب بصفحته في الفيس بوك متحكماً في البيانات بالاشتراك مع فيسبوك فيما يتعلق بجمع البيانات الشخصية للزوار على موقع الويب ونقلها إلى فيسبوك. وبمفهوم المخالفة، فإن هذا المشغل ليس متحكماً في البيانات بالنسبة للمعالجة اللاحقة لهذه البيانات التي يقوم بها فيسبوك وحده"[٣].

الحماية الجنائية للبيانات الشخصية:

يتوقف الاطمئنان إلي مصداقية المحررات الالكترونية في الإثبات علي ما يمكن أن توفره التقنيات التكنولوجية من وسائل أمان تمنع اختراق هذه المحررات، أو إحداث أي عبث بها من قبل الغير، وتكفل التحقق من أطراف المحرر الالكتروني وكافة بياناته، وتوفر نظام لحفظ هذه البيانات والمعلومات بحيث يمكن الرجوع

القانونية، جامعة عجمان كلية القانون، يوليو ٢٠٢١، ص٧٣.

(1) Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, The European 18 Information & Communications Union general data protection regulation: what it is and what it means, Technology Law. Volume 28, 2019 - Issue 1.p.75

(2) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.42

(3) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.44

إليها عند الإنكار[١].

ولهذا، يجب إعداد التشريعات التي تكفل حماية المستندات والبيانات الإلكترونية من عبث الغير حفاظا علي أسرار الخصوم التي قد تحويها ملفات القضية، وذلك بتجريم كل فعل ينال من هذه الأسرار أو الخصوصيات الأسرية أو الاقتصادية، مثل: صياغة التشريعات التي تجرم الاعتداء علي أجهزة ونظم وبيانات الحاسب الآلي، وصياغة التشريعات التي تجرم نشر أو بث أوراق القضية عبر المواقع الإلكترونية، فضلا عن توقيع الاتفاقيات الدولية لمكافحة الجرائم المرتكبة باستخدام تكنولوجيا المعلومات وتسليم مرتكبيها[٢].

وتطبيقا لذلك، تنص المادة ٣٣٩ من المرسوم الاتحادي الإماراتي رقم ١٠ لسنة ٢٠١٧ المعدل لأحكام قانون الإجراءات المدنية الاتحادي على أن "تخضع تقنية الاتصال عن بعد المنصوص عليها في هذا القانون، للوائح وسياسات أمن المعلومات المعتمدة في الدولة"، وهو ما جاء به المشرع الإماراتي بموجب المرسوم بقانون اتحادي رقم ٣ لسنة ٢٠١٢ بشأن إنشاء الهيئة الوطنية للأمن الإلكتروني، وتهدف هذه الهيئة إلى تنظيم حماية شبكة الاتصالات ونظم المعلومات في الدولة، وتطوير وتعديل واستخدام الوسائل اللازمة في مجال الأمن الإلكتروني. وتعمل على رفع كفاءة طرق حفظ المعلومات وتبادلها لدى كافة الجهات بالدولة، سواء عن طريق نظم المعلومات أو أي وسيلة إلكترونية أخرى (المادة الرابعة).

كما تنص اللائحة الأوربية على غرامة ١٠ مليون يورو أو ٢% من الدخل السنوي للشركة على مستوى العالم أيهما أعلى في حالة الإخلال الصادر عن المعالج أو المتحكم في البيانات بأحد الالتزامات الآتية:

---

(١) د/أسامة أحمد شوقي المليجي، استخدام مستخرجات التقنيات العلمية الحديثة وأثره على قواعد الإثبات المدني، دار النهضة العربية، القاهرة، ٢٠٠٠، ص ١٣٩.

(٢) ورقة عمل مقدمة من إدارة تقنية المعلومات بالنيابة العامة الاتحادية لدولة الامارات العربية المتحدة حول المحاور المزمع مناقشتها في اجتماع بيروت خلال ٥-٢٠١٢/٣/٧، ولمزيد من التفاصيل حول جرائم المعلوماتية في مجال التقاضي الالكتروني، وجرائم الاعتداء علي النظام المعلوماتي انظر د/خالد ممدوح إبراهيم، التقاضي الالكتروني "الدعوي الإلكترونية وإجراءاتها أمام المحاكم، دار الفكر الجامعي، الإسكندرية، ٢٠٠٨، ص٢٨٩، ما بعدها.

١- الالتزام بشروط معالجة البيانات الشخصية للأطفال.

٢- الالتزام بتنفيذ التدابير التنظيمية والفنية الملائمة لحماية حقوق وحريات أصحاب البيانات.

٣- الالتزام بتحديد المسئولية المشتركة في حالة إجراء المعالجة بين المعالج وبين أكثر من متحكم.

٤- التزام المعالج بعدم إشراك معالج آخر دون أذن كتابة محدد أو عام من المتحكم.

٥- الالتزام بالحفاظ على سرية البيانات الشخصية.

٦- الالتزام بإخطار السلطة الرقابية الوطنية وصاحب البيانات في حالة وقوع مخالفات لأنظمة المتحكم أو المعالج.

٧- الالتزام بتعيين موظف لحماية البيانات الشخصية.

٨- الالتزام بالحصول على شهادة اعتماد لمعالجة البيانات الشخصية من جانب السلطات المختصة[١].

كما يعاقب القانون المصري بغرامة لا تقل عن مائة ألف جنية ولا تجاوز مليون جنية لكل من جمع أو عالج أو أفشى أو أتاح أو تداول بيانات شخصية معالجة إلكترونياً بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانوناً أو بدون موافقة صاحب البيانات[٢].

وبناء على ذلك، تتشكل العلاقة بين الذكاء الاصطناعي والبيانات بحيث تكون علاقة تبادلية طردية، فلا يوجد ذكاء اصطناعي بدون بيانات كبيرة؛ لأن الذكاء الاصطناعي يحتاج لبيانات حتى يتم بناءه على نحو صحيح، ولتزويد هذه المعالجات

(١) محمد حسن عبدالله، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً، مرجع سابق، ص٧٨.

(٢) محمد حسن عبدالله، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً، مرجع سابق، ص٧٩.

التقنية[١]. وكلما زادت مدخلات أنظمة الذكاء الاصطناعي من البيانات الهامة، كلما زادت دقة النتائج التي قد تتحقق، كما أنه لا يمكن الاستفادة من البيانات الضخمة بدون تقنية الذكاء الاصطناعي بسبب عدم قدرة الطرق التقليدية على معالجتها بصورة سليمة[٢].

(1) T. SOURDIN, Judge vs Robot? Artificial Intelligence and judicial decision- making, 41, 2018, 1114

(2) F. RASO, H. HILLIGOSS, V. KRISHNAMURTHY, C. BAVITZ, L. KIM, Artificial intelligence and Human rights, 1, September 25, 2018, 7

المبحث الثاني
الحماية القانونية للبيانات الشخصية

تمهيد وتقسيم:

ترتكز الحماية القانونية للبيانات الشخصية التي يجرى معالجتها عبر تقنية الذكاء الاصطناعي على مجموعة من الخصائص التي يجب أن تتوافر حتى تكون جديرة بهذه الحماية، فضلا عن مجموعة من المبادئ الجوهرية لهذه الحماية القانونية، وبناء على ذلك تنقسم دراسة هذا المبحث إلى مطلبين، وذلك على النحو الآتي:

المطلب الأول ـ خصائص البيانات الشخصية محل الحماية

المطلب الثاني ـ مبادئ حماية البيانات الشخصية

المطلب الأول
خصائص البيانات الشخصية محل الحماية

تتصف البيانات الشخصية التي يجرى معالجتها عبر تقنية الذكاء الاصطناعي بمجموعة من الخصائص حتى تحقق نتائج موثوقة ودقيقة، وهى:

١- الحجم، فكلما كانت هذه البيانات ذات أعداد كبيرة، كلما كانت النتائج أكثر دقة.

٢- التنوع، فكلما كانت البيانات متنوعة بحيث تشتمل على البيانات المكتوبة والصور الرقمية والتسجيلات الصوتية والمرئية وبيانات الخرائط، كلما كانت دقيقة ومفيدة.

٣- السرعة، فكلما كان إنتاج واستخراج البيانات سريعاً، كلما كان ذلك مفيداً لتغطية الطلب، ويعتبر العنصر الحاسم لبناء القرار استناداً عليها[1].

٤- الموثوقية والصحة، وهو ما يعنى أن تكون هذه البيانات دقيقة وصحيحة

(1) C. BARBARO, Y. MENECEUR, Issues in the use of artificial intelligence (AI) algorithms in judicial systems, 1, 2018, p.12

وحديثة، وهو ما يكون ذات تأثير في اتخاذ القرار.

٥- القيمة، وتكمن أهمية قيمة هذه البيانات لاستخدامها واستغلالها، فإذا كانت هذه البيانات مجرد عدد، فلا يمكن الاستفادة منها مالم تكن ذات قيمة[١].

ويجرى تقسيم تحليل البيانات الشخصية إلى قسمين وفقا لطبيعة البيانات والخوارزميات المستخدمة، وذلك على النحو الآتي:

١- التحليل التنبئي، والذى يهدف إلى التنبؤ بالنتيجة على ضوء البيانات المقدمة من جانب ذوى الشأن، ومثال ذلك: التنبؤ بقيام أشخاص بجرائم معينة بناء على البيانات والسجلات الإجرامية الخاصة بهم.

٢- التحليل الوصفي، والذى يهدف إلى وصف الخصائص التي تتمتع بها البيانات، وذلك من خلال تجميع البيانات المتشابهة في الخصائص في صورة مجموعات[٢].

كما أضحى من السهل جمع عدد كبير من بيانات أفراد المجتمع عبر التطبيقات التي يجرى استخدامها بصورة يومية، وهى تجمع بياناتهم ومواقعهم الجغرافية، وقد تستخدمها الحكومات لغايات وأهداف أمنية[٣]. وتطبيقا لذلك، أصدرت الدول تشريعات حماية البيانات الشخصية، بغاية توعية أفراد المجتمع بما يتعلق ببياناتهم وحقوقهم والالتزامات التي تقع على عاتقهم، وتوجيه السلطات المختصة لتبنى الأحكام والضوابط الخاصة بالإجراءات الإدارية والتقنية الخاصة بتخزين البيانات الشخصية على النحو الذى يضمن الحفاظ على البيانات الشخصية، وفقا لطبيعتها ودرجة أهميتها، فقد أصدر المشرع السعودي نظام حماية البيانات الشخصية بموجب المرسوم الملكي رقم ١٩ بتاريخ ١٤٤٣/٢/٩ ه بحيث خولت المادة ٩ من هذا النظام الجهة العامة حق الوصول للبيانات دون إذن صاحبها لو

(1) D.L DALKE, Can Computer Replace Lawyers, Mediators and Judges?, in The Advocate, 1, 2013, p.21

(2) N. CRISTIANINI, On the Current Paradigm in Artificial Intelligence, in AI Communications, 27, 1, January 1st 2014, 3-5.

(3) L. Julia. L'intelligence artificielle n'existe pas (AI does not exist). First Edition, Paris 2019, p. 123

كان ذلك لاستيفاء متطلبات قضائية[١].

ويستثنى من ذلك المادة السادسة من ذات النظام عدم أخذ موافقة صاحب البيانات في المعالجة المطلوبة؛ لأغراض أمنية أو لاستيفاء متطلبات قضائية، ومنح هذه الصلاحيات للقضاة على النحو الذى يضمن سرعة الفصل في القضايا ومثال ذلك الاطلاع على سجلات المتهمين والتحقق من وجود سوابق لهم من عدمه، والتحقق من أحوال الشهود وغيرها[٢].

معالجة البيانات الشخصية:

يقصد بمعالجة البيانات الشخصية من وجه نظر المشرع الأوروبي "أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية أو على مجموعة من البيانات الشخصية، سواء كانت بواسطة وسائل آلية أو غيرها مثل جمعها أو تسجيلها أو تنظيمها أو هيكلتها أو تخزينها أو تعديلها أو تحويرها أو استرجاعها أو مراجعتها أو استخدامها أو الكشف عنها عن طريق إرسالها أو نشرها أو إتاحتها بأي طريقة أخرى أو فرزها أو تجميعها أو تقييدها أو حذفها أو إنهائها"[٣].

وقد عرف المشرع المصري معالجة البيانات الشخصية على أنها: "أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية أو تجميعها أو تسجيلها أو حفظها أو تخزينها أو دمجها أو عرضها أو إرسالها أو استقبالها أو تداولها أو نشرها أو محوها أو تغييرها أو تعديلها أو استرجاعها أو تحليلها، وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك كلياً أو جزئياً".

ويقصد بالمعالج "كل شخص طبيعي أو اعتباري أو سلطة عامة أو وكالة أو أي هيئة أخرى تحدد لوحدها أو بالاشتراك مع غيرها أغراض ووسائل معالجة البيانات

(1) Katz, Daniel Martin et al. A General Approach for Predicting the Behavior of the Supreme Court of the United States (January 16, 2017). SSRN: https://ssrn.com/abstract=2463244

(٢) إيناس خلف الخالدي، حوكمة استخدام الذكاء الاصطناعي في العمل القضائي، قراءة قانونية في الميثاق الأخلاقي الأوربي بشأن استخدام الذكاء الاصطناعي في النظم القضائية وبيئتها، مرع سابق، ص١٦٢.

(3) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.40

الشخصية"، ويعرفه قانون حماية البيانات الشخصية المصري بأنه "أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله الحق في الحصول على البيانات الشخصية، وتحديد طريقة أو أسلوب ومعايير الاحتفاظ بها أو معالجتها والتحكيم فيها طبقاً للغرض المحدد أو نشاطه"[١].

تنص المادة ٣/٢ من القانون الفرنسي لحماية البيانات الشخصية على تحديد المقصود بمعالجة هذه البيانات، فذكرت أنها "أي إجراء يخص البيانات الشخصية أيا كانت الآلية المستخدمة في هذا الإجراء، وخاصة مسألة تجميع وتسجيل وتنظيم وحفظ وتعديل واستخلاص والاطلاع والإبلاغ عن طريق النقل أو الربط أو المحو أو النشر أو التدمير"[٢].

ويعد التعريف السابق الإشارة إليه تعريف واسع لوسائل معالجة البيانات الشخصية بحيث يمكن القول بأنه: لا يمكن توقع أي إجراء يتعلق بهذه البيانات الشخصية، وإلا يعد من وجه نظر القانون معالجة لهذه البيانات، وجدير بالذكر أنه ما ذكره المشرع الفرنسي في النص السابق لا يعدو حصر لهذه الإجراءات، وإنما هي تطبيقات لأهم الإجراءات المتعلقة بالبيانات الشخصية، فلا يوجد ما يمنع من اعتبار أي إجراء جديد غير هذه الإجراءات لمعالجة هذه البيانات[٣].

وتتعدد الإجراءات التي تبناها القانون الفرنسي كأمثلة لمعالجة البيانات الشخصية، ومثال ذلك:

١- تجميع البيانات: وهى أول خطوة للتعامل مع البيانات الشخصية.

٢- تسجيل البيانات: ويقصد بها تدوين البيانات سواء في صورة إلكترونية أو ورقية.

---

(1) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.42

(2) Paul Lanois, Time to forget: EU privacy rules and the right to request the deletion of data on the internet. Journal of Internet Law. October 2014 p. 21

(٣) محمد حسن عبدالله، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونياً، دراسة تحليلية مقارنة في ضوء اللائحة الأوربية وبعض التشريعات ذات العلاقة، مجلة العلوم القانونية، جامعة عجمان كلية القانون، يوليو ٢٠٢١، ص٧٧.

٣- تنظيم البيانات: ويقصد بها تصنيف البيانات الخاصة بكل فرد من أفراد المجتمع حتى تتشكل الصورة الكاملة عنه.

٤- حفظ البيانات: ويكون ذلك بصورة إلكترونية أو ورقية.

٥- تعديل البيانات: هو إجراء لتغيير بيانات الشخص سواء كان ذلك على أحد هذه البيانات أو جميعها.

٦- الاستخلاص: هو استخلاص أحد المعلومات الخاصة بأحد الأشخاص من بيانات أخرى سبق الحصول عليها.

٧- الاطلاع: هو إطلاع أي شخص على البيانات الشخصية.

٨- الاستخدام: أي استخدام أحد الجهات البيانات الشخصية التي تم تجميعها قبل ذلك بغاية الدعاية والتسويق.

٩- الإبلاغ: أي إبلاغ هذه البيانات لجهة جديدة لتحقيق تعاون بينها وبين الجهة التي أعطتها هذه البيانات حتى يتم رسم صورة مكتملة عن الشخص.

١٠- النشر: أي بث وإذاعة البيانات الشخصية بأي وسيلة سواء كانت إلكترونية أم ورقية، بحيث يجرى رفع البيانات الشخصية على شبكة المعلومات الدولية.

١١- الربط: أي ربط البيانات الشخصية المختلفة والمتعلقة بذات الشخص بغاية تكوين ملف مكتمل عنه[1].

موقف القضاء الفرنسي:

توسع القضاء الفرنسي في تحديد نطاق الإجراءات التي قد تمس البيانات الشخصية من خلال آلية المعالجة، ومثال ذلك:

١- تجميع عنوان البريد الإلكتروني بغاية إرسال إعلانات للعملاء حتى ولو لم يحتفظ الراسل بهذا العنوان أو ينشئ قاعدة بيانات لها.

(1) Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, The European 18 Information & Communications Union general data protection regulation: what it is and what it means,
Technology Law. Volume 28, 2019 - Issue 1.p.75

٢- تصميم قاعدة بيانات شخصية عن الحالة الصحية للمرضى من جانب أحد الجهات المختصة بالبحث العلمي في مجال الطلب بغاية إجراء بحث علمي عن حالة المرضى[١].

٣- إنشاء نظام لتنظيم حضور وانصراف موظفي الشركة من خلال أخذ البصمة لكل موظف في حالتي الحضور والانصراف بحيث يجرى تجميع بصمات الأصابع على الجهاز المختص بذلك.

٤- نشر بيانات الاسم والعنوان البريدي والعنوان الإلكتروني وأرقام الهاتف لبعض الأشخاص على شبكة الانترنت[٢].

٥- تصميم نظام رقابة للكمبيوتر الخاص بكل موظف داخل العمل، وهو الذى يسمح لرئيس العمل بمتابعة المواقع الإلكترونية التي استخدمها الموظف والوقت الذى اتصل فيه بكل موقع وعنوان البريد الإلكتروني الذى يرسل الرسائل الإلكترونية.

٦- قيام شركة الاتصالات بإنشاء النظام الداخلي لتسجيل مكالمات الموظف مع العميل، ويتضمن هذا النظام آلية لحفظ هذه المكالمات لتحليلها.

٧- تصميم ملف لكل نزيل بالفندق بحيث يتضمن هذا الملف معلومات عن النزيل، كالاسم والسن والمهنة والأنشطة التي قام بها النزيل خلال فترة وجوده بالفندق والخدمات التي حصل عليها[٣].

شروط مشروعية معالجة البيانات الشخصية بواسطة تقنية الذكاء الاصطناعي:

تناولت المادة السادسة والسابعة من قانون حماية البيانات الشخصية

(1) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.44

(2) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138 International Data Privacy Law,2017, Vol.7, N0. 29

(3) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.300

الفرنسي الشروط اللازمة للمعالجة القانونية لهذه البيانات، وتنقسم هذه الشروط إلى شروط تتعلق بالبيانات الشخصية ذاتها، وشروط في الشخص الذى يقوم بمعالجة هذه البيانات، وشروط تتعلق بأنواع البيانات[١].

وبناء على ذلك، تنقسم هذه الشروط إلى:

١- الشروط المتعلقة بجمع البيانات:

نصت المادة ١/٦، ٢ من قانون حماية البيانات الشخصية الفرنسي على هذه الشروط بحيث يجب أن تجميعها بطريقة مشروعة، وأن يكون تجميعها لغاية واضحة ومحددة. ولذلك، يجب إخبار صاحب البيانات عن تجميعها حتى يكون هذا التجميع مشروع، وإخباره عن وسيلة التجميع والغاية من هذا التجميع وأنواع البيانات التي يجرى تجميعها[٢].

وبناء على ذلك، تتوقف مشروعية تجميع البيانات على إخبار كل شخص بأنه يجرى تجميع بياناته قبل مباشرة التجميع، فإن لم يجرى هذا الإخبار، يكون جمع البيانات غير مشروع، وبناء على ذلك تجميع البيانات الشخصية دون معرفة صاحبها هو إجراء غير مشروع، فاللجنة القومية للحريات ترى أن تجميع البريد الإلكتروني لمستخدمي شبكة الانترنت دون موافقة صاحب البريد الإلكتروني هو إجراء غير مشروع[٣].

وهو ذات ما ذهبت إليه محكمة النقض الفرنسية، فقررت أن تجميع البريد الإلكتروني لأفراد المجتمع دون موافقتهم يعد إجراء غير مشروع، ويجب توقيع العقاب على من يفعل ذلك.

ووفقا لحكم المادة ٢/٦ من القانون الفرنسي، يجب أن يكون تجميع البيانات الشخصية لغرض محدد وواضح ومشروع، وهو ما يمكن أن نعبر عنه بقاعدة الغاية

(1) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.44

(2) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.139. International Data Privacy Law,2017, Vol.7, N0. 29

(3) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.45

من جمع البيانات ومعالجتها من أجل حماية البيانات الشخصية[١]. ولذلك، لا يجوز تجميع البيانات الشخصية دون معرفة الغاية من التجميع، وأن تكون الغاية محددة بحيث يجرى إخبار الشخص بالغرض من تجميع بياناته.

فضلا عما سبق، لا تعد البيانات الشخصية خطراً في ذاتها، إلا أن الخطورة تنتج من استخدامها، وهو ما يمكن تسميته بالغاية من معالجتها، فعلى سبيل المثال: لو تم تجميع بيانات صحية بغاية إجراء بحث علمي، فهو يشكل غاية مشروعة من تجميع هذه البيانات، أما لو تم تجميع هذه البيانات بغاية تجارية بحتة، فتكون الغاية في هذه الحالة غير مشروعة. أيضا، يكون تجميع البيانات الشخصية دون غاية واضحة أو محددة غير مشروع؛ لأن الشخص الذى يقوم بتجميع هذه البيانات دون غاية واضحة، فلا يجوز أن يخطر من يتم تجميع بياناته بهذه الغاية، فيكون قد أخل بالشرط الخاص بتجميع البيانات[٢].

٢- أن يكون حفظ البيانات بآلية تحدد هوية صاحب البيانات:

لا يجوز حفظ البيانات بصورة عشوائية، بل يجب أن يحدد صاحب هذه البيانات حتى يجوز لهذا الشخص بمباشرة حقوقه على بياناته، ومثال ذلك: الحق في الدخول عليها أو الحق في تعديلها.

٣- أن يكون حفظ البيانات لمدة معينة لتحقيق الهدف الذى تم تجميع البيانات من أجله:

هو ما يعنى أنه يجب على الشخص الذى يتولى معالجة البيانات أن يحفظ البيانات لمدة معينة بحيث لا تزيد على المدة الضرورية لتحقيق الغاية من جمع هذه البيانات.

ولذلك، يجب على الشخص المسئول عن معالجة البيانات أن يراجع بصورة

(1) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.301

(2) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139 International Data Privacy Law,2017, Vol.7, N0. 29

دورية هذه البيانات التي جرى تخزينها أو تدميرها في حالة تحقيق الهدف من جمعها، فالمادة ٦٧ من قانون حماية البيانات الشخصية الفرنسي تؤكد على عدم سريان الشرطين السابقين على حفظ البيانات الشخصية لغايات تتعلق بالعمل الأدبي أو الفني أو لغاية مباشرة مهنة الصحافة[١].

٤- أن تكون معالجة البيانات بوسيلة مشروعة:

تشدد المادة ١/٦ من قانون حماية البيانات الشخصية على الوسيلة المشروعة المستخدمة لأي إجراء من إجراءات معالجة البيانات الشخصية، وهو ما يمكن تحققه من خلال إخبار الشخص صاحب الشأن بإجراءات معالجة بياناته الشخصية، بحيث يكون على علم بكافة الإجراءات التي تحدث لبياناته الشخصية. ولذلك، مشروعية إجراء المعالجة تستوجب إخطار الشخص بمعالجة بياناته الشخصية وآليات هذه المعالجة والغاية من ذلك، وقبل القيام بإجراءات المعالجة[٢].

وبناء على ذلك، لو تمت إجراءات المعالجة بدون إخبار الشخص صاحب الشأن، فإن هذه الإجراءات غير قانونية، وتؤدى لتوقيع الجزاء المنصوص عليه قانوناً في مثل هذه الأحوال[٣].

علاوة على ذلك، حددت المادة ٣٢ من قانون حماية البيانات الشخصية الفرنسي بعض البيانات التي يجب إخبار الشخص بها قبل مباشرة إجراءات المعالجة، وهى:

١- بيانات هوية الشخص القائم بالمعالجة.

٢- الغاية من المعالجة.

٣- الشخص الذى يملك صلاحية إرسال البيانات إليه.

٤- الحق في الاطلاع والاعتراض على هذه البيانات.

---

(1) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.44

(2) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.302

(3) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.45

٥- ألا تكون معالجة البيانات بطريقة لا تتماشى مع الهدف من جمعها:

والهدف من هذا الشرط هو تضييق معالجة البيانات الشخصية بالغاية التي يجرى جمع البيانات من أجلها بحيث تتلاءم آلية المعالجة مع الغاية من جمع البيانات. ولذلك، يجب أن يكون إجراء معالجة البيانات مناسباً مع الغاية من جمعها بحيث لا يجوز أن يكون هناك عدم تناسب بين معالجة البيانات والغاية من إجراء المعالجة[١].

وتطبيقا لذلك، لو تعامل أحد الأشخاص مع إحدى الجهات التي تطلب منه بعض البيانات الشخصية لتقديم إحدى خدماتها، فإنه لا يجوز القيام بأي معالجة لهذه البيانات إلا في نطاق تحقيق الغاية القائمة على تقديم الخدمة لهذا الشخص، وبالتالي لو تم معالجتها فإن هذا الإجراء يكون غير مشروع.

٦- يجب أن تكون البيانات ملائمة:

وفقا لنص المادة ٣/٦، ٤ من قانون حماية البيانات الشخصية الفرنسي يجب أن تكون البيانات متلائمة مع الغاية من تجميع البيانات بحيث لا تتجاوز هذا الحد، كما لا يجوز جمع بيانات غير مناسبة للغاية من تجميعها أو تكون أكثر من الضروري، وتطبيقا لذلك لو تم تجميع البيانات الشخصية بغاية تصميم قائمة بعناوين البيوت الخاصة بالعملاء من أجل توصيل السلع إليهم في حالة طلبها، فيجب أن يكون تجميع هذه البيانات قاصراً على مجرد التجميع، ولا يتجاوز إلى جمع معلومات عن العادات الاستهلاكية للعملاء[٢].

كما تشدد اللجنة القومية الفرنسية للحريات على هذا الشرط الخاص بمعالجة البيانات الشخصية في النظام الرقمي لتنظيم دخول المطاعم في المدارس بحيث يكون النظام قائم على بصمة اليد الموجودة على باب المطعم.

٧- يجب أن تكون البيانات كاملة ودقيقة:

تشدد المادة ٤/٦ من قانون حماية البيانات الفرنسي على أنه يجب أن تكون

(1) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.46

(2) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139. International Data Privacy Law,2017, Vol.7, N0. 29

البيانات كاملة ودقيقة بحيث يتعين على المعالج أن يقوم دورياً بمراجعة البيانات الشخصية المراد تخزينها لديه، وتوجد علاقة بين هذا الشرط وحق الشخص في الدخول على بياناته الشخصية على النظام المعلوماتي الخاص بالشخص الذى يقوم بمعالجة البيانات، وحقه في تعديلها أو مسحها لو كانت غير صحيحة[١].

٨- رضا صاحب البيانات بمعالجتها:

تطبيقا لنص المادة ٧ من قانون حماية البيانات الشخصية الفرنسي، يجب أن يكون الشخص صاحب البيانات موافق على معالجة بياناته الشخصية، فالشخص الذى يتولى مهمة المعالجة يجب أن يحصل على رضاء صاحب البيانات على القيام بمعالجتها والهدف من القيام بهذه المعالجة، ولا يشترط القانون شكل معين في هذا الرضا، فقد يكون شفاهة أو كتابة، وقد يكون هذا الرضا صريح أو ضمني، إلا أنه يجب على القائم بالمعالجة أن يثبت رضاء صاحب الشأن بمعالجة بياناته[٢].

أيضا، يجب أن يكون هذا الرضا ناتج عن إرادة حرة من جانب صاحب الشأن، فلا يكون هناك أي شكل من أشكال الضغط على أرادته من جانب الشخص الذى يقوم بمعالجة هذه البيانات.

وجدير بالذكر أن هناك بعض المواقع الإلكترونية تجمع البيانات الشخصية للمستخدمين ومعالجتها وإرسالها لمواقع دعائية، ففي مثل هذه الأحوال يجب إخطار مستخدم الموقع بكافة ما يحدث لبياناته على هذا الموقع وموافقته على ذلك، وإذا تم معالجة البيانات الشخصية لأحد الأشخاص عديم الأهلية أو ناقصها، فلا يمكن الحصول على رضاء مثل هذه الأشخاص، بل يجب الحصول على رضاء الممثل القانوني، ومثال ذلك: الحصول على رضاء الولي بالنسبة للقاصر[٣].

(1) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.303

(2) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.303

(3) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. =

ولقد أكدت اللجنة القومية للحريات الفرنسية على ضرورة الحصول على موافقة الممثل القانوني لأي شخص غير قادر على التعبير عن إرادته في كافة الحالات التي يجرى فيها معالجة بياناته الشخصية.

نطاق سريان تشريعات حماية البيانات الشخصية المعالجة بواسطة تقنية الذكاء الاصطناعي:

يقتصر نطاق تطبيق هذه التشريعات على بيانات الأشخاص الطبيعية، فلا تسري على الأشخاص المعنوية سواء كانت عامة أم خاصة، ولم تفرق هذه التشريعات بين الشخص الوطني أو الأجنبي من حيث نطاق الحماية القانونية، فيجب أن تكون معالجة البيانات لشخص موجود في إحدى الدول الأوربية التي تخضع لتطبيق اللائحة الأوربية المعنية بحماية البيانات الشخصية[١].

ولذلك، تؤكد هذه اللائحة على ضرورة احترام القواعد والمبادئ الخاصة بحماية الأشخاص الطبيعية في نطاق معالجة البيانات الشخصية، وبصرف النظر عن مكان الإقامة أو الجنسية، كما يجرى تطبيق لائحة الاتحاد الأوروبي على كل شخص يقوم بمعالجة بيانات شخصية في إحدى دول الاتحاد الأوروبي أو كان يملك إحدى الأنشطة الاقتصادية بها، كما تسري أحكام هذه اللائحة على كل شخص يقوم بمعالجة البيانات حتى ولو كان موجود خارج الاتحاد الأوروبي طالما أن البيانات موضوع المعالجة تتعلق بمواطن أوروبي أو شخص مقيم بأحد دول الاتحاد الأوروبي[٢].

وتؤكد المادة الثانية من مواد إصدار القانون المصري رقم ١٥١ لسنة ٢٠٢٠ لحماية البيانات الشخصية على أن تسري أحكامه على المعالجة الإلكترونية سواء كانت بصورة جزئية أم كلية لدى أي حائز أو معالج أو متحكم لها، ودون أن يشترط

P.304

(1) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139. International Data Privacy Law,2017, Vol.7, N0. 29

(2) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139. International Data Privacy Law,2017, Vol.7, N0. 29

القانون جنسية المعالج أو المتحكم، وتؤكد لائحة الاتحاد الأوروبي على النطاق الموضوعي لسريان الحماية المنصوص عليها، فقررت أنه "تسري هذه اللائحة على معالجة البيانات الشخصية كلياً أو جزئياً بالوسائل الآلية وبغير الوسائل الآلية للبيانات الشخصية التي تشكل جزءاً من نظام حفظ الملفات أو يقصد منها أن تشكل جزءاً من نظام حفظ الملفات"[١].

وجدير بالذكر، أن هذه اللائحة لا تقتصر على المعالجة التي تتم بواسطة الوسائل الآلية، بل يجوز سريان أحكامها على معالجة البيانات التي تتم بواسطة وسائل يدوية، فقد أكدت هذه اللائحة على ضرورة أن تكون حماية الأشخاص الطبيعية محايدة من الجانب التقني، ولا ينبغي أن تعتمد على التقنيات المعول عليها، بل يجب حماية الأشخاص الطبيعة عند معالجة بياناتهم الشخصية عبر الوسائل الآلية والمعالجة اليدوية لو كانت هذه البيانات جزءاً من نظام حفظ الملفات أو كان يفترض أنها جزء منه[٢].

ولا تسري أحكام لائحة الاتحاد الأوروبي على الملفات أو وسيلة إعدادها، إلا أن سريان هذه الأحكام على المعالجة اليدوية يتوقف على أن يكون الغرض منها الحفظ في نظام تقنى. وبناء على ذلك، لو كانت المعادلة يدوية للبيانات الشخصية، وتم حفظها في أرشيف ورقي، فلا تسري أحكام اللائحة في مثل هذه الأحوال، ويحرص القانون الفرنسي على تحديد نطاق سريان أحكامه على المعالجة الآلية للبيانات الشخصية سواء بصورة كلية أم جزئية، وعلى المعالجة غير الآلية لذات البيانات أو طلب ظهورها في الملفات.

كما حددت المادة الأولى من مواد إصدار القانون المصري لحماية البيانات نطاق سريان أحكام هذا القانون بحيث تسري على المعالجة الإلكترونية للبيانات الشخصية سواء بصورة كلية أو جزئية لدى أي متحكم أو حائز أو معالج لها[٣].

(1) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.46

(2) Petter Carey, Data Protection, fifth edition, Oxford, 2018.p.46

(3) Kart Pormeister, Genetic Data and The research exemption: Is the GDPR going too far? P.138-139. International Data Privacy Law,2017, Vol.7, N0. 29

الإطار التنظيمي لحماية البيانات الشخصية:

تبنت التشريعات المعنية بحماية البيانات الشخصية إطار تنظيمي محكم لمعالجة البيانات الشخصية من كافة جوانبها ولضمان وضع هذه الحماية محل التنفيذ، ودون تهاون بحقوق أصحاب هذه البيانات أو تجاوز الاعتداء عليها.

وينقسم هذا الإطار التنظيمي إلى جانب وقائي وآخر علاجي بغاية توفير حماية حقيقية للبيانات الشخصية، وذلك على النحو الآتي:

١- الجانب التنظيمي الوقائي لحماية البيانات الشخصية:

تنص لائحة الاتحاد الأوروبي على تأسيس مجلس خاص لحماية البيانات الشخصية على مستوى الاتحاد الأوروبي، وفرضت على كل معالج للبيانات بأن يعين مسئول عن حماية البيانات لو تجاوز عدد الموظفين ٢٥٠ موظفاً، وتؤكد المادة ٦٨ من لائحة الاتحاد الأوروبي على تأسيس مجلس خاص لحماية البيانات الشخصية، ويحظى بالشخصية القانونية المستقلة على أساس أنه أحد هيئات الاتحاد الأوروبي[(١)].

أما على المستوى الداخلي، تعد الهيئة الوطنية للمعلوماتية والحريات الفرنسية هي السلطة الإشرافية على تنفيذ قانون حماية البيانات الشخصية، كما يشدد القانون المصري على تأسيس مركز لحماية البيانات الشخصية بحيث يضطلع بمهمة تنفيذ ورقابة تنفيذ أحكام قانون حماية البيانات الشخصية، وهى هيئة عامة اقتصادية، وتحظى بشخصية اعتبارية مستقلة.

وقد أوجبت لائحة الاتحاد الأوروبي الدول بتأسيس سلطة رقابية وطنية لتكون مسئولة عن رقابة تنفيذ اللائحة حتى تضمن توفير حماية حقيقية للحقوق والحريات الأساسية لكافة الأشخاص الطبيعية في نطاق المعالجة للبيانات الشخصية، كما تحظى كل سلطة رقابية بالاستقلالية التامة، ولا يسري عليها سوى أحكام لائحة الاتحاد الأوروبي في أداء مهامها، ويباشر أعضاء اللجنة مهامهم

(1) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.300

الناتجة عن اللائحة بصورة مستقلة، ولا يخضعوا لأي تأثير خارجي[1].

الجانب التنظيمي العلاجي لحماية البيانات الشخصية:

تضمنت لائحة الاتحاد الأوروبي حماية مدنية للبيانات الشخصية وحماية جنائية بحيث يجرى تطبيق هذه الحماية لمواجهة كافة صور الاعتداء غير المشروع على هذه البيانات.

(1) Daphne Keller, The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation, Berkeley Technology Law Journal. Vol.3:297. 2018. P.300

المطلب الثاني
مبادئ حماية البيانات الشخصية

يحكم استخدام الذكاء الاصطناعي في علاقته بالبيانات مجموعة من البيانات التي يمكن تسميتها بالمبادئ الأساسية لحماية البيانات الشخصية، وذلك على النحو الآتي:

١- الإنصاف والشفافية:

وفقا لنص المادة ٥/١/أ من لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي عام ٢٠١٦ يجب أن يكون معالجة الذكاء الاصطناعي للبيانات الشخصية بصورة قانونية وعادلة وشفافة بحيث يحكم هذه المعالجة التقنية نص قانوني يجيز ذلك، وعلى نحو عادل وشفاف بحيث يعلم صاحب الشأن بالخطوات التقنية المتبعة لمعالجة مثل هذه البيانات(١).

وقد عرف أحد الفقه الشفافية بأنها الفكرة التي تستند على الإيجاز وإمكانية الوصول للبيان الشخصي وبصورة مفهومة للكافة، ويتطلب مبدأ الشفافية أن تكون المعلومات موجه للجمهور، وبصورة موجزة، ويجوز الوصول إليها بصورة سهلة ومفهومة من جانب المستخدم. فضلا عما سبق، يجب أن يكون استخدام هذه البيانات بلغة واضحة ومفهومة للمستخدم حتى يسهل عليه استخدامها في مجال الذكاء الاصطناعي(٢).

كما أنه يوجد ارتباط وثيق بين عدالة المعلومات ومبدأ الشفافية التي تعنى عدم الخداع أو التضليل بخصوص الموضوعات التي ترد عليها البيانات التي يجرى معالجتها بواسطة تقنية الذكاء الاصطناعي(٣)، كما توجب مبادئ المعالجة العادلة والشفافة إيضاح موضوع البيانات محل المعالجة والغرض من مباشرة تقنية المعالجة

(1) Aletras N, Tsarapatsanis D, Preoţiuc-Pietro D, Lampos V. 2016. 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', PeerJ Computer Science 2:e93 https://doi.org/10.7717/peerj-cs.93.

(2) Ibid.

(3) T. SOURDIN, Judge vs Robot? Artificial Intelligence and judicial decision- making, 41, 2018, 1114

بحيث يجب على التقني تزويد البيانات بأي معلومات ضرورية وإضافية لضمان المعالجة العادلة والشفافة شريطة مراعاة الظروف المحيطة بمعالجة البيانات الشخصية[١].

كما ترتبط عادلة المعلومات بالمسئولية القانونية عن الأضرار التي تنتج عن الاستخدام الخاطئ لهذه المعلومات، فالمعلومات المستخدمة بواسطة تقنية الذكاء الاصطناعي تثير العديد من القضايا بسبب تعقد المعالجات التقنية التي تتضمن تطبيقات الذكاء الاصطناعي، وعدم اليقين من نتائجها، وتعدد الأهداف والغايات المتوقعة من ذلك، ولضمان معالجة عادلة وشفافة لموضوع البيانات الشخصية، فإنه يجب على التقني استخدام مجموعة من الإجراءات الرياضية والإحصائية المناسبة لتنفيذ التدابير الفنية والتنظيمية المناسبة؛ لضمان تصحيح العوامل التي قد تؤدى لعدم الدقة في البيانات الشخصية بطريقة تأخذ في الاعتبار المخاطر المحتملة، والتي تنطوي عليها مصالح وحقوق صاحب البيانات[٢].

وبناء على ذلك، نضمن عدم التمييز بين أشخاص المجتمع على أساس الأصل العرقي أو الجنس أو الرأي السياسي أو الدين والمعتقدات أو الحالة الصحية، أو أي عامل آخر قد يؤدى إلى اتخاذ مثل هذا التمييز غير الموضوعي.

٢- مبدأ تحديد الهدف:

وفقا لنص المادة ١/٥ ب من لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي، يجب أن يكون جمع البيانات الشخصية لأغراض محددة وصريحة ومشروعة بحيث لا يجوز معالجتها بطريقة تتعارض مع هذه الأهداف، ومثال ذلك: تكون المعالجات التقنية صحيحة لو كانت بهدف المصلحة العامة أو البحث العلمي أو التاريخي أو الغرض الإحصائي[٣].

---

(1) Ibid.

(٢) إيناس خلف الخالدي، حوكمة استخدام الذكاء الاصطناعي في العمل القضائي، قراءة قانونية في الميثاق الأخلاقي الأوربي بشأن استخدام الذكاء الاصطناعي في النظم القضائية وبيئتها، مرع سابق، ص١٦٧.

(3) N. CRISTIANINI, On the Current Paradigm in Artificial Intelligence, in AI Communications, 27, 1, January 1st 2014, 3-5

٣- مبدأ الدقة:

تنص المادة ١/٥ من لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي على مبدأ الدقة أثناء المعالجة التقنية للبيانات عبر تقنية الذكاء الاصطناعي، ويقصد بهذه الدقة أن تكون البيانات التي يجرى تداولها دقيقة، ويجري تحديثها من خلال اتخاذ كل خطوة مناسبة لضمان أن البيانات الشخصية التي يجري معالجتها دقيقة ومصحوبة بمراعاة الأهداف التي يتم المعالجة من أجلها، بحيث يجرى محوها أو تصحيحها دون تأخير[١]، ويسري هذا المبدأ على البيانات الشخصية التي يجرى استخدامها كأساس لاستخدام تقنية الذكاء الاصطناعي، وخاصة في حالة استخدام البيانات الشخصية لاتخاذ القرارات والاستنتاجات الخاصة بأحد موضوعات البيانات الشخصية[٢].

٤- قاعدة تخزين البيانات الشخصية:

وفقا لنص المادة ١/٥ ه من لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي يحظر الاحتفاظ بالبيانات الشخصية في حالة عدم الحاجة إليها لأغراض المعالجة التقنية لها عبر استخدام تقنيات الذكاء الاصطناعي[٣]، كما يجب الاحتفاظ بالبيانات الشخصية في صورة تسمح بتحديد الموضوعات المتعلقة بهذه البيانات لمدة لا تزيد عن اللازم لأغراض معالجة البيانات الشخصية، ومع ذلك يجوز تخزين البيانات الشخصية لمدة أطول لو كان الغرض من ذلك أرشفة المعلومات أو البحث أو لأغراض الإحصائيات التي تقدم نتائج مؤكدة عن مسألة ما[٤].

كما يجوز تخزين البيانات الشخصية لفترات أطول لو كانت معالجة البيانات الشخصية لأغراض الأرشفة الخاصة بالمصلحة العامة أو لغرض البحث العلمي أو التاريخي أو لغرض عمل إحصائيات وفقا لنص المادة ١/٨٩من لائحة الاتحاد الأوروبي المعنية، ومع ذلك يتوقف ذلك على اتخاذ كافة التدابير الفنية والتنظيمية

(1) Ibid.

(2) Ibid.

(3) J.N. KOK, E.J.W. BOERS, W.A. KOSTERS, P. VAN DER PUTTEN, Artificial intelligence: definition, trends Techniques and cases, p.11

(4) Ibid.

المناسبة، والتي تتطلبها هذه اللائحة، ومثال ذلك: التدابير الخاصة بحماية الحقوق والحريات موضوع البيانات[١].

الأساس القانوني لمعالجة البيانات الشخصية عبر تقنية الذكاء الاصطناعي:

أكدت المادة السادسة من لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي على الأساس القانوني لمعالجة البيانات الشخصية عبر تقنية الذكاء الاصطناعي تطبيقا لحكم المادة ٨ من الميثاق الأوروبي للحقوق الأساسية بحيث يجرى معالجة البيانات الشخصية على أساس موافقة الشخص المعنى أو على أساس حكم القانون[٢].

وبناء على ذلك، تؤكد المادة السادسة من اللائحة العامة لحماية البيانات على أن معالجة البيانات الشخصية تكون قانونية لو توافرت الشروط الآتية:

١- موافقة صاحب البيانات أو توافر حالة ضرورة.

٢- تكون غاية البيانات الشخصية إبرام عقد أو تنفيذه أو تنفيذ التزام قانوني أو لحماية مصالح عامة أو مصلحة مشروعة تهم أحد أفراد المجتمع[٣].

٥- مبدأ الرضا:

يكون رضا المستخدم على معالجة بياناته الشخصية عبر تقنية الذكاء الاصطناعي متحققاً لو كانت هذه البيانات متضمنة عناصر تدريبية للمستخدم أو لتوفير نموذج تقنى في مجال محدد[٤]، كما يجب أن يكون الرضا محدد على بيانات شخصية معينة وحر، فلا يكون هناك إجبار على إرادة الشخص، ومع ذلك ليس من السهل استيفاء هذه الشروط في نطاق معالجة البيانات الشخصية عبر

(1) N. CRISTIANINI, On the Current Paradigm in Artificial Intelligence, in AI Communications, 27, 1, January 1st 2014, 3-5

(2) Ibid.

(3) Ibid.

(4) F. RASO, H. HILLIGOSS, V. KRISHNAMURTHY, C. BAVITZ, L. KIM, Artificial intelligence and Human rights, 1, September 25, 2018, 7

تقنية الذكاء الاصطناعي، وهو ما يوجب الاعتماد على أسس قانونية جديدة للسماح بمثل هذه المعالجات التقنية، ومثال ذلك: أن تكون معالجة البيانات الشخصية بهدف علمي أو إحصائي أو لهدف اجتماعي[١].

٦- مبدأ المصلحة المشروعة:

تطبيقا لحكم المادة ١/٦/و من لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي يجب أن تكون معالجة البيانات الشخصية بواسطة تقنية الذكاء الاصطناعي بهدف حماية مصالح مشروعة، أي مصالح يحميها القانون، ومثال ذلك: أن تكون معالجة البيانات بهدف حماية الحقوق والحريات الأساسية[٢].

ويستثنى من ذلك، حالة معالجة البيانات الشخصية بغاية التدريب وتصميم نموذج حسابي، وهو ما يجوز القيام به طالما تم تبنى تدابير أمنية وتقنية قوية، ومثال ذلك: استخدام أسماء مستعارة للبيانات وإخفاء هوية الاطراف. كما يجوز إعادة معالجة البيانات الشخصية لأغراض أخرى غير الأغراض المتعلقة بجمع البيانات الشخصية، وهو ما يمكن تصور حدوثه في حالة المعالجة الإضافية التي تتعلق بالأرشفة أو البحث العلمي أو التاريخي أو لعمل إحصائيات علمية[٣].

وتكون المعالجة الإضافية للبيانات الشخصية بغرض الأرشفة أو البحث العلمي أو التاريخي أو لعمل إحصائيات متفقة مع الأغراض الأساسية لمعالجة هذه البيانات، والقائمة على تحقيق مصلحة مشروعة[٤].

(1) Ibid.

(2) J.N. KOK, E.J.W. BOERS, W.A. KOSTERS, P. VAN DER PUTTEN, Artificial intelligence: definition, trends Techniques and cases, p.14

(3) Ibid.

(4) Ibid.

النتائج والتوصيات

أولا: النتائج

١- لم تتفق الآراء على تحديد المقصود بتقنيات الذكاء الاصطناعي بسبب التطور المستمر والمتلاحق للتكنولوجيا، إلا أن هذه الآراء تتفق على أن هذه التقنيات يقصد بها استخدام الآلة الحديثة بطريقة مماثلة للعمل البشرى.

٢- يقصد بالبيانات الشخصية المادة الأساسية والخام التي يستمد منها المعلومات، وتمثل مجموعة الحقائق والأفكار والمشاهدات والملاحظات والقياسات، وعادة ما تكون في صورة أعداد أو كلمات أو رموز خاصة.

٣- تتصف البيانات الشخصية بمجموعة من الخصائص، كالحجم، والتنوع، والسرعة والموثوقية والصحة.

٤- أصدرت الدول تشريعات حماية البيانات الشخصية، بغاية توعية أفراد المجتمع بما يتعلق ببياناتهم وحقوقهم والالتزامات التي تقع على عاتقهم، وتوجيه السلطات المختصة لتبنى الأحكام والضوابط الخاصة بالإجراءات الإدارية والتقنية الخاصة بتخزين البيانات الشخصية.

٥- يحكم استخدام الذكاء الاصطناعي في علاقته بالبيانات مجموعة من المبادئ التي يمكن تسميتها بمبادئ حماية البيانات الأساسية، كمبدأ الإنصاف والشفافية، وتحديد الهدف، و تحديد تخزين البيانات الشخصية.

ثانيا: التوصيات

١- أوصى المشرع المصري بمواكبة التطورات التقنية من خلال إصدار التشريعات المناسبة لتوفير الحماية القانونية للبيانات الشخصية التي تستخدمها تقنية الذكاء الاصطناعي.

٢- أوصى المشرع المصري بتبني المبادئ الإرشادية التي أخذت بها لائحة حماية البيانات الصادرة عن الاتحاد الأوروبي لربط علاقة تقنية الذكاء الاصطناعي بالبيانات الشخصية، وخاصة مبدأ الشفافية وتحديد الغاية من استخدام البيانات الشخصية ومبدأ المساواة بين أفراد المجتمع.

قائمة المراجع

أولا: المراجع العربية:

١. **إيناس خلف الخالدى**، حوكمة استخدام الذكاء الاصطناعى فى العمل القضائى، قراءة قانونية فى الميثاق الأخلاقى الأوربى بشأن استخدام الذكاء الاصطناعى فى النظم القضائية وبيئتها، مجلة البحوث والدراسات الشرعية، العدد السادس عشر بعد المائة رجب ١٤٤٢، ص١٦٢

٢. **سامح عبدالواحد التهامى**، الحماية القانونية للبيانات الشخصية، دراسة القانون الفرنسى، القسم الأول، مجلة الحقوق، جامعة الكويت، سبتمبر ٢٠١١، مج ٣٥، ع٣، ص٣٨٥

٣. **فريدة بن عثمان**، الذكاء الاصطناعى، مقاربة قانونية، دفاتر السياسة والقانون، المجموعة ١٢، الجزء الثانى، ٢٠٢٠، ص١٥٦

٤. **كريم على سالم**، الجوانب القانونية للذكاء الاصطناعى، مجلة جيل الأبحاث القانونية المعمقة، العدد ٥٤، أكتوبر ٢٠٢٢، ص٥٣

٥. **محمد القطب مسعد**، دور قواعد الملكية الفكرية فى مواجهة تحديات الذكاء الاصطناعى، دراسة قانونية تحليلية مقارنة، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد ٧٥، مارس٢٠٢١، ص١٦٢٨

٦. **محمد حسن عبدالله**، النظام القانونى لحماية البيانات الشخصية المعالجة إلكترونياً، دراسة تحليلية مقارنة فى ضوء اللائحة الأوربية وبعض التشريعات ذات العلاقة، مجلة العلوم القانونية، جامعة عجمان كلية القانون، يوليو ٢٠٢١، ص٧٣

٧. **محمد بومديان**، الذكاء الاصطناعى تحد جديد للقانون، مسارات فى الأبحاث والدراسات القانونية، العدد ١٠، ٢٠١٩، ص١٩٨

٨. **محمد فتحى محمد إبراهيم**، التنظيم التشريعى لتطبيقات الذكاء الاصطناعى، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، العدد ٨١، سبتمبر ٢٠٢٢، ص١٠٢٥

ثانيا: المراجع الأجنبية:

9. A.D. Dory Reiling, Courts and Artificial Intelligence, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3736411
10. A.D. Reiling, Technology for Justice, how information technology can support judicial reform (diss. VU Amsterdam) Leiden: Leiden University Press 2009, p. 111-122.
11. Aletras N, Tsarapatsanis D, Preo□iuc-Pietro D, Lampos V. 2016. 'Predicting judicial decisions of the European Court of Human Rights: a Natural Language Processing perspective', PeerJ Computer Science 2:e93 https://doi.org/10.7717/peerj-cs.93.

12. Baffard William, le système de traitement des infractions constatées et la protection des données personnelles, mémoire de DEA informatique et droit, faculté de droit, université de Montpellier 1, 2003, p.15
13. Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, The European 18 Information & Communications Union general data protection regulation: what it is and what it means,
14. Technology Law. Volume 28, 2019 - Issue 1.p.75
15. C. BARBARO, Y. MENECEUR, Issues in the use of artificial intelligence (AI) algorithms in judicial systems, 1, 2018
16. D.L DALKE, Can Computer Replace Lawyers, Mediators and Judges?, in The Advocate, 1, 2013
17. L. Julia. L'intelligence artificielle n'existe pas (AI does not exist). First Edition, Paris 2019, p. 123
18. Fuso Jovia Boahemaa, The impact of artificial intelligence on justice systems, Paper n25, 2018-2019
19. Katz, Daniel Martin et al. A General Approach for Predicting the Behavior of the Supreme Court of the United States (January 16, 2017). SSRN: https://ssrn.com/abstract=2463244
20. F. RASO, H. HILLIGOSS, V. KRISHNAMURTHY, C. BAVITZ, L. KIM, Artificial intelligence and Human rights, 1, September 25, 2018, 7
21. J.N. KOK, E.J.W. BOERS, W.A. KOSTERS, P. VAN DER PUTTEN, Artificial intelligence: definition, trends Techniques and cases
22. L. Julia. L'intelligence artificielle n'existe pas (AI does not exist). First Edition, Paris 2019, p. 123
23. N. CRISTIANINI, On the Current Paradigm in Artificial Intelligence, in AI Communications, 27, 1, January 1st 2014, 3-5.
24. Paul Lanois, Time to forget: EU privacy rules and the right to request the deletion of data on the internet. Journal of Internet Law. October 2014 p. 20-24.
25. T. SOURDIN, Judge vs Robot? Artificial Intelligence and judicial decision- making, 41, 2018, 1114

List of references

First-Arabic references:

1. Inas Khalaf Al-Khalidi, governance of the use of artificial intelligence in judicial work, a legal reading in the European Ethical Charter on the use of artificial intelligence in judicial systems and their environment, Journal of research and Sharia studies, sixteenth issue after the hundredth Rajab 1442, P. 162
2. Sameh Abdulwahid Tohami, legal protection of personal data, study of French law, section I, journal of law, Kuwait University, September 2011, Vol. 35, P3, P385
3. Farida Ben Othman, artificial intelligence, a legal approach, notebooks of politics and law, Collection 12, Part II, 2020, P. 156
4. Karim A. Salem, legal aspects of artificial intelligence, Journal of in-depth legal research generation, issue 54, October 2022, P. 53
5. Mohammed Al-Qutub Massad, the role of intellectual property rules in facing the challenges of artificial intelligence, a comparative analytical legal study, Journal of legal and Economic Research, Faculty of law, Mansoura University, issue 75, March 2021, P. 1628
6. Mohammed Hassan Abdullah, the legal system for the protection of electronically processed personal data, a comparative analytical study in the light of the European regulation and some related legislation, Journal of Legal Sciences, Ajman University College of Law, July 2021, P. 73
7. Mohamed Boumediene, artificial intelligence is a new challenge to the law, tracks in legal research and studies, No. 10, 2019, P. 198
8. Mohamed Fathi Mohamed Ibrahim, legislative regulation of AI applications, Journal of legal and Economic Research, Faculty of law Mansoura University, Issue 81, September 2022, P. 1025

Foreign references:

9. League Rilling, courts and artificial intelligence, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3736411
10. A. Dr. Rilling, technology for justice, how information technology can support judicial reform (diss. VU Amsterdam) Leiden: Leiden University Press 2009, PG. 111-122.
11. Eletras n, tsarapatsanis d, PRIO ermyuk Petro d, Lambos v. 2016. 'Predicting the judicial decisions of the European Court of human rights: a natural language processing perspective', Berg Computer Science 2: e 93 https://doi.org/10.7717/peerj-cs.93.

12. Baffard William, le système de traitement des infractions constatées et la protection des données personelles, mémoire de anti-narcotics informatique ET droit, Faculty of law de droit, université de Montpellier 1, 2003, p.15
13. Chris Jay Hufnagel, Bart van der Sloot and Frederik zuiderwein burgesius, the General Data Protection Regulation of the European Union 18 for information and Communications: what it is and what it means,
14. The law of technology. Volume 28, 2019-issue 1.P. 75
15. C. Barbaro, Y. minesur, issues in the use of artificial intelligence algorithms in judicial systems, 1, 2018
16. Dr. For Dalek, can a computer replace lawyers, intermediaries and judges?, The Advocate, March 1, 2013
17. L.Julia. Artificial intelligence does not exist (artificial intelligence does not exist). First edition, Paris 2019, P. 123
18. Fosu Juvia buahima, the impact of artificial intelligence on justice systems, Paper No. 25 , 2018-2019
19. Katz, Daniel Martin et al. A general approach to predicting the behavior of the Supreme Court of the United States (January 16, 2017). Sirn: https://ssrn.com/abstract=2463244
20. F. Raso, H. Heligus, F. Krishnamurthy , C. pavitz , L. Kim , artificial intelligence and Human Rights, September 1, 25, 2018 , 7
21. G. N. Cook , E. G. W. Boers , W. A. Koesters , P. van der Putten, artificial intelligence: definition, trend techniques and cases
22. L.Julia. Artificial intelligence does not exist (artificial intelligence does not exist). First edition, Paris 2019, P. 123
23. N. Cristianini, on the current paradigm in artificial intelligence, in artificial intelligence communications, 27, 1, 1 January 2014, 3-5.
24. Paul Lanois, it's time to forget: EU privacy rules and the right to request the deletion of data on the internet. Internet Law Journal. October 2014 p. 20-24.
25. T. Sordin, judge vs robot? Artificial intelligence and judicial decision-making , 41, 2018, 1114

فهرس الموضوعـات

الموضـــــوع **الصفحة**

المقدمة.....١٣٩٣
المبحث الأول مفهوم الذكاء الاصطناعي وعلاقته بالبيانات الشخصية ١٣٩٨
المطلب الأول المقصود بتقنيات الذكاء الاصطناعي ١٣٩٩
المطلب الثاني المقصود بالبيانات الشخصية.....١٤٠٢
المبحث الثاني الحماية القانونية للبيانات الشخصية ١٤١٧
المطلب الأول خصائص البيانات الشخصية محل الحماية ١٤١٧
المطلب الثاني مبادئ حماية البيانات الشخصية.....١٤٣٢
النتائج والتوصيات ١٤٣٧
قائمة المراجع ١٤٣٨
فهرس الموضوعـات ١٤٤٢