

د. أحمد رجب صميده

دكتورة في القانون العام – جامعة بني سويف

قاضي بمجلس الدولة المصري

الأجهزة القابلة للارتداء وأثرها على الحق في خصوصية البيانات الشخصية

Wearable devices and its impact
on the right to privacy of personal data

■ **المراسلة:** د. أحمد رجب صميده

دكتورة في القانون العام – جامعة بني سويف
قاضي بمجلس الدولة المصري

■ **معرف الوثيقة الرقمي (DOI):** <https://doi.org/10.54873/jolets.v4i1.193>

ar.sd777@gmail.com

■ **البريد الإلكتروني:**

Ahmed011129@law.bsu.edu.eg

■ **نسق توثيق البحث:**

الأجهزة القابلة للارتداء وأثرها على الحق في خصوصية البيانات الشخصية
Wearable devices and its impact on the right to privacy of personal
data، المجلد الرابع، العدد الثاني، أكتوبر ٢٠٢٤ صفحات ١٥٨-١١١

الأجهزة القابلة للارتداء

وأثرها على الحق في خصوصية البيانات الشخصية

Wearable devices and its impact on the right to privacy of personal data

ملخص الدراسة

تتناول هذه الدراسة تعقيدات حماية البيانات الشخصية في مواجهة التحديات والمخاطر الناتجة عن جمع البيانات، ومعالجتها بواسطة الذكاء الاصطناعي، وأثرها على الحق الأساسي في الخصوصية، واستعراض التنظيم التشريعي لخصوصية البيانات الشخصية في الاتحاد الأوروبي، ومدى كفايته في تحقيق الحماية الفعالة لتلك البيانات حال استخدام الأجهزة القابلة للارتداء، المزودة بتقنيات الذكاء الاصطناعي؛ مختتمين إياها بعدد من التوصيات التي تهدف إلى تطوير الإطار التشريعي والصناعي لتوفير الحماية الكافية للبيانات الشخصية في مواجهة تلك الأجهزة.

كلمات مفتاحية: الأجهزة القابلة للارتداء، الذكاء الاصطناعي، الصحة الرقمية، الخصوصية، اللائحة العامة لحماية البيانات، البيانات الشخصية، البيانات الحساسة.

Abstract

This study reveals the complexity of protecting personal data in the face of the challenges and risks that data collection and processing by AI offer to the fundamental right to privacy. It reviews the legislative regulation of personal data privacy in the European Union and its adequacy in achieving effective protection of that data when using wearable devices equipped with (AI) technologies, concluding with several recommendations aimed at developing the legislative and industrial framework to provide adequate protection for personal data in the face of these devices.

Keywords: Wearable devices, Artificial Intelligence, Digital health, Privacy, General Data Protection Regulation, Personal data, Sensitive data

مقدمة:

أدّى ارتفاع تكاليف خدمات الرعاية الصحيّة، وسهولة الوصول إلى الإنترنت، واتجاه الثقافة الحالية نحو إدارة المشاكل الصحيّة إلى قيام الأفراد ببعض الأنشطة الطبيّة بأنفسهم؛ بمساعدة الأجهزة الذكيّة القابلة للارتداء، التي ازدهرت صناعتها في الآونة الأخيرة، وأضحّت أداةً مهمّة تُستخدَم في الصناعات المتعلّقة بالرعاية الصحيّة؛ فقد أصبح الشخص قادراً على الكشف عن الحالة الصحيّة الخاصّة به دون مغادرة المنزل؛ ومن ذلك، على سبيل المثال، هناك حالياً العديد من التطبيقات التي تسمَح باستخدام الهاتف الذكي للكشف عن احتمالات عالية للإصابة بالسرطان ببساطة عن طريق التقاط صورة لمنطقة الجلد المشتبه بها؛- هذه التطبيق يُسمّى UMSkinCheckApp؛ والذي طُوّر في جامعة ميشيغان (الولايات المتحدة الأمريكيّة) ⁽¹⁾.

ونظراً للقدرة الفائقة للذكاء الاصطناعي على تحديد الاحتمالات من خلال مجموعات البيانات؛ فقد استُخدِم لحلّ بعض أكثر التحديات الصحيّة تعقيداً؛ حيث يمكن لهذه التكنولوجيا أن تحدّث ثورة في الرعاية الصحيّة لكبار السن، وتسمح بتقليل تكاليف دُور رعاية المسنّين، وتحسين نوعيّة الحياة لهؤلاء المرَضَى، كما يمكنها أيضاً تحسين عمليات التشخيص للأطباء في الريف أو المواطنين العاديين، أو ذوي الدخول المنخفضة الذين قد لا يتمكّن مرضاهم من الوصول إلى المتخصّصين، كما تسمح بأتمتة مهامّ الرعاية الصحيّة منخفضة المخاطر؛ مما يُحرّر الأطباء من أجل تركيز المزيد من الطاقة على الحالات المعقّدة؛ أي إن الذكاء الاصطناعي يُمكن أن يوفر نوعيّة حياة أفضل، من خلال تمكين المرضى من القيام بالمهامّ النمطيّة التي تستهلك المزيد من الوقت إذا قام بها الأطباء المتخصّصون؛ مثل التحكم في مرض السكري؛ حيث يتمّ التقاط البيانات بواسطة الأجهزة القابلة للارتداء (مثل الساعات الذكيّة).

إلا أنّه، ونظراً لاشتراك كافّة الأجهزة. مثل الهواتف الذكيّة، أو الأجهزة اللوحيّة، حتى لو كانت «قابلة للارتداء». في العديد من المميّزات مع التكنولوجيا القابلة للارتداء، فقد ظهرت تحديات قابلة للمقارنة إلى حدّ كبير؛ حيث تسمح جميعها باستخدام عددٍ

(1) TSCHIDER, Charlotte A. The healthcare privacy-artificial intelligence impasse. Santa Clara High Technology Law Journal, [s. l.], v. 36, n. 4, p. 439-443, 2020. Available at: <https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1689&context=facpubs>. Access on: July. 20, 2024.

متزايد باستمرار من («التطبيقات») التي تجمع أنواعاً عديدة من البيانات، والتي غالباً ما تكون مزيجاً من البيانات التي يقدمها المستخدمون؛ (مثل البيانات المقدمة من الآباء حول أطفالهم، عادات الأكل أو النوم، استهلاك السعرات الحرارية المبلغ عنها ذاتياً.....)، والبيانات التي يتم استقبالها تلقائياً بواسطة الأجهزة؛ منها على سبيل المثال: (البيانات الخاصة بالموقع، أو النشاط عبر الإنترنت، أو جهات الاتصال)؛ الأمر الذي أثار العديد من المشكلات المتعلقة بخصوصية، وأمان البيانات الشخصية الناتجة عن استخدام تلك الأجهزة؛ على الأخص البيانات الصحية، والتي تستأهل حماية قانونية خاصة؛ باعتبارها أهم فئات البيانات الحساسة؛ لا سيما فيما يتعلق بالحصول على البيانات، وإعداد التقارير التي تستند إليها، وإمكانية إعادة تحديد بيانات المريض؛ علاوة على ذلك؛ فقد تم الإبلاغ مؤخراً عن حالات تجاوز الشركات للحدود الأخلاقية إبان سعيها للحصول على بيانات المرضى لتدريب أنظمتها؛ أحدها يتعلق بالشراكة بين Royal Free NHS Foundation Trust و DeepMind التابعة لشركة Google، والتي اعتُبرت غير قانونية من قبل هيئة حماية البيانات بالمملكة المتحدة، والتي تم إنهاؤها بسبب عدم كفاية الموافقة المستنيرة من المريض فيما يتعلق باستخدام الثانوي للبيانات الشخصية - وهذا المثال يوضح الصراع الواضح بين المشرع والصناعة، والمتعلق بجمع البيانات الطبية اللازمة لخوارزميات تدريب أنظمة الذكاء الاصطناعي⁽¹⁾.

إشكالية البحث:

تتمثل مشكلة البحث في تساؤل مفاده: ما الطرق التي يمكن من خلالها تعزيز تشريعات حماية البيانات بأشكال أخرى من الجهود التنظيمية والتشريعية؛ لتغطية العديد من المشاكل التي تنشأ عن التقاط، ومعالجة البيانات الحساسة من قبل الشركات التي تطور الأجهزة والخدمات القائمة على التقنيات المعتمدة على الذكاء الاصطناعي؟ وينبثق منه عدة تساؤلات فرعية:

ما هي المخاطر والتحديات المحددة التي تطرحها الأجهزة القابلة للارتداء المزودة بتقنيات الذكاء الاصطناعي على الحق في خصوصية البيانات الشخصية؟

(1) ROHRINGER, Taryn J.; BUDHKAR, Akshay; RUDZICZ, Frank. Privacy versus artificial intelligence in medicine. University of Toronto Medical Journal, [s. l.], v. 96, n. 1, p. 51-53, Jan. 2019. Available at <https://jps.library.utoronto.ca/index.php/utmj/issue/download/2376/453#page=52>. Access on: July. 20, 2024.

ما هي التحديات التي تواجهها التشريعات المتعلقة بحماية البيانات الشخصية، مثل اللائحة العامة لحماية البيانات (GDPR)، في توفير الحماية الكافية للبيانات الشخصية التي تم جمعها عن طريق الأجهزة القابلة للارتداء؟

ما هي المقترحات الممكنة لتطوير الإطار التشريعي والصناعي لحماية البيانات الشخصية في ظل استخدام الأجهزة القابلة للارتداء المزودة بتقنيات الذكاء الاصطناعي؟

منهج البحث:

اعتمد البحث على المنهج الوصفي التحليلي الذي يقوم على أساس تحديد مفهوم الأجهزة القابلة للارتداء، وتحليل المخاطر والتحديات الناجمة عن استخدام الأجهزة المزودة بتقنيات الذكاء الاصطناعي، أثرها على الحق الأساسي في الخصوصية؛ بغية الوقوف على مدى كفاية التشريعات المتعلقة بحماية البيانات الشخصية في حماية هذه البيانات في سياق الأجهزة القابلة للارتداء، وصولاً إلى تكوين نهج قانوني مكتمل يحقق التوازن بين المزايا التي توفرها الأجهزة القابلة للارتداء وما يتطلبه ذلك من وسائل وإجراءات تستهدف تطويرها والحفاظ على قدرتها التنافسية، وحماية الحق في خصوصية البيانات الشخصية.

أهداف البحث:

يحاول البحث تحقيق هدف رئيسي يتمثل في دراسة مدى تعقيد حماية البيانات الشخصية في مواجهة التحديات والمخاطر التي تتعرض لها أنشطة التقاط البيانات والمعالجة بواسطة تقنيات الذكاء الاصطناعي (AI) على الحق في الخصوصية؛ ويندرج تحت هذا الهدف مجموعة من الأهداف الفرعية أبرزها:

- رصد المخاطر والتحديات الناجمة عن استخدام الأجهزة القابلة للارتداء المزودة بتقنيات الذكاء الاصطناعي على حق الأفراد في خصوصية بياناتهم الشخصية.
- تحليل مدى كفاية التشريعات المتعلقة بحماية البيانات الشخصية في حماية هذه البيانات في سياق الأجهزة القابلة للارتداء.

- اقتراح مبادرات وتوصيات لتطوير وتكييف الإطار التشريعي والصناعي لحماية البيانات الشخصية في مواجهة التحديات الناجمة عن استخدام هذه الأجهزة.
- ولتحقيق هذا الهدف قُسمَت الدراسة إلى أربعة أقسام.
- **يتناول القسم الأول:** مفهوم الأجهزة الذكية القابلة للارتداء وأقسامها ودورها في مجال الرعاية الصحية، والعلاقة بين تطوير الذكاء الاصطناعي في التطبيقات، وبين أجهزة ما يُسمَّى بالصحة الرقمية، وكذلك الطرق التي مثلت - من خلالها - هذه التقنيات الجديدة وعوداً مثيرة للاهتمام، مع الأخذ في الاعتبار المخاطر التي قد تُسببها، ويحلل القسم الثاني منها المخاطر والتحوُّلات التي تفرضها التقنيات المعتمدة على الذكاء الاصطناعي (التعلم العميق، البيانات الضخمة) على الحق في الخصوصية، في عصر الاتصال المُفرط، وانتشار تقنيات المراقبة في كل مكان، والاستثمار الضخم من قبل الشركات والدول في هذه التقنيات، ويدرس القسم الثالث اللائحة الأوروبية لحماية البيانات العامة (GDPR)؛ مشيراً إلى العديد من المشكلات المتعلقة بالموافقة المطلوبة من مستخدمي التطبيقات، وأجهزة التقاط البيانات المستخدمة في تدريب الذكاء الاصطناعي. وأخيراً، يتناول القسم الرابع منها المقترحات الجديدة المتعلقة بتنظيم الذكاء الاصطناعي ومعالجة البيانات، إلى جانب الأنظمة الحكومية التقليدية.

المبحث الأول

الذكاء الاصطناعي والصحة الرقمية وخصوصية البيانات

سابقا، كان استخدام التكنولوجيا القابلة للارتداء قاصرا على المجالات العسكرية، وبمرور الوقت أثبتت فاعليتها في مجال الرعاية الصحية، وقد شهد العصر الحالي نموا كبيرا في صناعة هذه الأجهزة التي تُستخدم بشكل أساسي في قطاعات (الصحة، اللياقة البدنية، النظام الغذائي)، وبحسب وظائفها وطبيعة المهام التي تقوم بها، التي تتطلب بطبيعة الحال قيامها بأنشطة تتعلق بجمع ومعالجة البيانات الشخصية وتخزينها، وهو ما يستتبع التعرف على مفهوم الأجهزة القابلة للارتداء، تأثير تقنيات الذكاء الاصطناعي المُستخدمة في المجالات الصحية على الحق في خصوصية البيانات الشخصية.

لذا سوف نتناول دراسة هذا المبحث في مطلبين على النحو التالي:

المطلب الأول

مفهوم الأجهزة القابلة للارتداء

يُمكن تعريف الأجهزة القابلة للارتداء بأنها مُلَحَقَاتُ أو عناصر من ملابس تتضمن إلكترونيات، أو برامج، أو أجهزة استشعار تتصل عادةً بشبكة، وتتخذ تلك الأجهزة أشكالاً عديدة؛ مثل الساعات الذكية، وأجهزة تتبع اللياقة البدنية، والملابس الذكية، وأساور المعصم، وما إلى ذلك⁽¹⁾.

أقسامها:

- يمكن تقسيم الأجهزة القابلة للارتداء إلى فئتين⁽²⁾:
- الفئة الأولى: أجهزة قابلة للارتداء تستخدم مستشعرا، ويدخل ضمن هذه الفئة: سوار المعصم الذكي والساعة الذكية، وتنقسم إلى فئتين فرعيتين بحسب وظيفة كل منها:

الأجهزة الخاصة بمؤشرات الصحة وتتبع الحركة:

تستخدم هذه الفئة أجهزة استشعار لتسجيل حركة المستخدم ومؤشرات صحته البدنية، ثم يتم توصيلها بجهاز طرفي ذكي حتى يتمكن المستخدم من تحليل تلك البيانات وإدارتها بعمق لفهم حالته الخاصة بوضوح.

الأجهزة المرتبطة بالهواتف الذكية:

تستخدم هذه الأجهزة عادة جنبا إلى جنب مع الهاتف الذكي، وتمكن مستخدميها من أداء مجموعة من الوظائف مثل إجراء المكالمات وإرسال واستقبال رسائل البريد الإلكتروني والتحكم في الرسائل والتطبيقات الموجودة على الهاتف الذكي.

- الفئة الثانية: أجهزة تجمع بين الإنسان والحاسب الآلي باستخدام تقنيات التفاعل والمثال الأبرز لهذه الفئة هو: النظارات الذكية

(1) Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. Journal of Sensor Actuator networks, 1(3), 217-253.

(2) Dawei Jiang, Guoquan Shi.(2021) « Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare Journal of Healthcare Engineering, Volume 2021, p.3.

وهذا النوع من المعدات لا يستخدم أجهزة استشعار لجمع البيانات فحسب، بل تستخدم كذلك تقنيات تفاعل معقدة بين الإنسان والحاسب الآلي، وعادة ما يتم تحسين تلك المعدات بعد ربطها بالهواتف الذكية، وتستخدم مجموعة متنوعة من تقنيات التفاعل بين الإنسان والحاسب (HCI) Human-computer interaction مثل تكنولوجيا العرض الحديثة، تقنيات التفاعل الصوتي، تقنيات الواقع المعزز، وتقنية التعرف على الصور لتلبية تجربة المستخدمين الافتراضية والواقعية^(١).

دورها في مجال الرعاية الصحية:

للأجهزة القابلة للارتداء عدة استخدامات في المجال الصحي يُمكن إيجازها في الآتي:

- **مراقبة الصحة:** يمكن للأجهزة القابلة للارتداء تتبع العلامات الحيوية للإنسان؛ مثل معدل ضربات القلب، وضغط الدم، ومستويات الأكسجين في الدم، وحتى قراءة تخطيط القلب؛ ومن ثم تُمكن هذه المراقبة المستمرة المستخدمين من مراقبة صحتهم؛ بحيث يمكنها تنبيههم، أو تنبيه مقدم الرعاية الصحية الخاص بهم إلى أية مشكلات مُحتملة.
- **إدارة الأمراض المزمنة:** تلعب الأجهزة القابلة للارتداء دوراً مهماً في إدارة الأمراض المزمنة؛ مثل مرض السكري، وارتفاع ضغط الدم، وأمراض القلب؛ عن طريق تتبع المقاييس الحيوية ذات الصلة؛ مما يُمكن المستخدمين من إدارة حالتهم الصحية بشكل أفضل، واتخاذ قرارات مستنيرة بشأن نمط حياتهم، وخطط العلاج^(٢).
- **تتبع النشاط البدني:** أجهزة يُمكن ارتداؤها لمراقبة الجوانب المختلفة للنشاط البدني؛ مثل عدد الخطوات التي يخطوها الشخص، وسرعة الجري، والسرعات الحرارية المحروقة، وأنماط النوم، كما توفر تحليلاً لتلك البيانات؛ مما يسمح للمستخدمين بمراقبة تقدمهم نحو أهداف اللياقة البدنية، وتعديل نمط حياتهم حسب الحاجة^(٣).

(1) Dawei Jiang, Guoquan Shi, Op.Cit, p.3.

(2) <https://strongholddata.com/wearable-technology-in-healthcare/>

(3) Garcia-Mancilla, J., & Gonzalez, V. M. (2015). Stress quantification using a wearable device for daily feedback

المطلب الثاني

تأثير تقنيات الذكاء الاصطناعي المستخدمة في المجالات الصحية على الحق في خصوصية البيانات الشخصية

ذهب البعض إلى أن الذكاء الاصطناعي يلعب دوراً هاماً في مجال الصحة الرقمية؛ حيث يُقدّم عدداً لا يُحصى من التقنيات المتقدمة التي يجب أن تكون متوافرة لمساعدة الأطباء عن طريق السماح بتحليل البيانات؛ لتسهيل الوصول إلى أنماط مختلفة من المعرفة في المجالات المختلفة للعلوم الصحية؛ ومن ثمّ يجب السعي إلى إنتاج البيانات الصحية، ومشاركتها دون أي عوائق، حتى يتواجد الذكاء الاصطناعي في كل مراحل تلك العملية، ويؤدي بالتالي إلى الوصول إلى معلومات جديدة من جميع مصادر تلك البيانات؛ يكون من شأنها إحداث اكتشافات ثورية في مختلف مجالات الصحة^(١).

ولتحقيق تلك النتيجة؛ يجب أن يشترك فريق من الأطباء (الذين يفهمون السياق الطبي للبيانات)، ومحللو البيانات (الذين يمتلكون المعرفة التقنية) في القيام بتحليل تلك البيانات لزيادة المعرفة الناتجة عنها، مع زيادة ذكاء التكنولوجيا، كما يتعين إيجاد طرق جديدة لإشراك المستخدمين؛ (بما في ذلك الأطباء، ومقدمي الخدمات) مع الأجهزة؛ ومن ثم تصبح تجربة مستخدمي تلك الأجهزة في غاية الأهمية لأية شركة تقنية تُقدّم خدمات مستمرة لمستخدميها من خلال الأنظمة الأساسية أو التطبيقات^(٢).

كما أضحت طبيعياً أن يتفاعل المرضى مع تلك الأدوات الصحية الرقمية؛ لأن عدم الامتثال لتلك الأدوات، من شأنه أن يؤثر سلباً على صحتهم، بالإضافة إلى أن السلوك البشري يميل في كثير من الأحيان إلى التصرف بأريحية تجاه المتطلبات والأوامر الصادرة عن تلك الأدوات، حتى مع إمكانية حدوث آثار سلبية؛ فضلاً عن المزايا الناتجة عن استخدامها؛ كالقدرة على الارتداء، والراحة التي توفرها من خلال دمجها في

to improve stress management. Paper presented at the ICSH; Sano, A., & Picard, R. W. (2013). Stress recognition using wearable sensors and mobile phones. Paper presented at the 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction.

(1) CHANG, Anthony. The role of artificial intelligence in digital health. In: WULFOVICH, Sharon; MEYERS, Arlen (ed.). Digital health entrepreneurship. Cham: Springer, 2020. p. 71-81. (Health Informatics).

(2) KAZGAN, Mehmet. Real challenge in digital health entrepreneurship: changing the human behavior. In: WULFOVICH, Sharon; MEYERS, Arlen (ed.). Digital health entrepreneurship. Cham: Springer, 2020. p. 7-15. (Health Informatics).

الروتين اليومي؛ مما يُشعر المستخدمين بالتمكين الذي يُحفّزهم على الالتزام بالعادات الصحيّة⁽¹⁾؛ للوصول إلى معدلات جيّدة من القيم الصحيّة، أو الإنتاجية، أو النشاط البدني.

ولكي تحقّق تلك الأنظمة الأغراض المنشودة منها؛ يجب مشاركة البيانات التي تُعدّ من قبيل «البيانات الحساسة»؛ لذا يجب الحفاظ على أمان هذه البيانات وتخزينها بواسطة شركات معالجة البيانات، كما يتعيّن تسمية هذه البيانات بشكل صحيح وتسجيلها؛ لتكون مفيدة حقاً للذكاء الاصطناعي؛ لأن البيانات عالية الجودة هي الأساس لتحقيق نماذج عالية الدقة - على الرغم من صعوبة الحصول على تلك النماذج في البيانات الضخمة «Big Data» دون وجود مُيول تمييزيّة، أو إمكانية تحديد هويّة صاحب البيانات - لذا يجب أن يقوم رُواد الأعمال باستثمارات كبيرة؛ من أجل إنشاء بيانات نظيفة، وتنظيم الحصول عليها، مع إعطاء الأولوية لبروتوكولات التخزين والوصول الآمنة.

وتجدر الإشارة إلى أن تقنية blockchain قد تُساعد في الحفاظ على أمن وخصوصية البيانات، مع الحفاظ على دقة المعلومات؛ كما يجب على رُواد الأعمال «مُصنّعي الأجهزة القابلة للارتداء» إنشاء حلقات نقاشية مع الخبراء من مُصنّعي تلك الأجهزة؛ لتعديل منتجاتهم من الأخطاء؛ لتلافي المسؤولية الناتجة عن الأخطاء والانتهاكات التي قد تتسبّب بها تلك الأجهزة.

وبالإضافة للأجهزة القابلة للارتداء؛ مثل الساعات الذكيّة؛ هناك العديد من الأجهزة الأخرى المُصمّمة من أجل الصحة والبيانات؛ فهناك العديد من تقنيات المراقبة والرعاية الصحيّة القائمة على جمع البيانات من الأجهزة التي يُمكن نشرها أو ابتلاعها من الأشخاص الخاضعين للمراقبة، والتي يُمكنها جمع بيانات الفرد وتخزينها، وتحليلها باستخدام خوارزميات الذكاء الاصطناعي عن طريق نقل البيانات عبر شبكة Wi-Fi إلى أجهزة الكمبيوتر التي تُعالج تلك الخوارزميات والبرامج؛ على سبيل المثال: هناك - على ما يبدو - تطبيقات غير محدودة للتقنيات القابلة للابتلاع لمراقبة الصحة؛ من خلال أنواع عديدة من المستشعرات والعلاجات؛ مثل: الروبوتات الصغيرة والمجهرية التي تقوم بإجراء الجراحات الدقيقة، والأقراص الذكية التي

(1) LUPTON, Deborah. Wearable devices: sociotechnical imaginaries and agential capacities. In: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). Embodied computing: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 49-69.

تُدير الأدوية بشكل صحيح، وما إلى ذلك، التي - من المحتمل - أن تقلل الانتقال إلى عيادات الأطباء، المختبرات الطبية لإجراء التحاليل، والعيادات الخارجية، وكذا غرف العمليات؛ الأمر الذي من شأنه إنقاذ المزيد من الأرواح بطرق أكثر أماناً، ومع ذلك؛ فقد يترتب على استخدام تلك التقنيات آثار سلبية لا تتعلق بالصحة والسلامة الطبية؛ وإنما في مجالات أخرى يجب مراعاتها بعناية.

وفي سياق متصل، هناك عدد قليل من مُطوِّري المنتجات القابلة للابتلاع قد أولى اهتماماً كبيراً بقضايا الخصوصية المتعلقة بالبيانات الصحية للمستخدم، أو الطرق التي يمكن من خلالها استخدام المنتجات القابلة للابتلاع لإخراج المستخدمين، أو إلزامهم من قبل شركات التأمين الصحي⁽¹⁾؛ فالأجهزة القابلة للابتلاع يمكن أن تخلق مشاكل مستقبلية إذا لم يمنح العملاء الموافقة المناسبة، بالإضافة إلى أن المرضى قد يُجبرون على استخدام الأجهزة القابلة للابتلاع التي تُنتج بيانات قيمة عن مستخدميها يمكن بيعها أو مبادلتها، أو استخدامها ضد إرادة أصحاب تلك البيانات - والذي قد يحدث، في أغلب الأحوال، بطرق لا يمكن تصورها، في الوقت الذي يوافق فيه هؤلاء على شروط استخدام تلك التكنولوجيات؛ حيث تتعرض خصوصية الفرد للخطر عند استخدام تلك الأجهزة لحفظ البيانات في شكل صور، أو أصوات، أو معلومات بيولوجية (معدل ضربات القلب، درجة حرارة الجسم، الحركة..... إلخ)؛ فهذه البيانات يمكن استخدامها ضد أصحابها - على سبيل المثال: تطلب شركات التأمين من الأشخاص تتبع أنفسهم من أجل دفع المطالبات؛ ومن ثم أضحت الأجهزة القابلة للابتلاع أشكالاً جديدة من المراقبة المعززة بالذكاء الاصطناعي.

وفي الاتجاه ذاته، يرى Pedersen⁽²⁾ أن الجسد البشري أصبح منصة لجمع البيانات وتحليلها بدعم من التطورات التكنولوجية للأجهزة القابلة للارتداء؛ بحيث لا تبدو الفكرة القائمة على وجود (جسد مترابط) - متصلة بالشبكة يعمل بشكل مستقل - إنها صورة لمستقبل بعيد لا يمكن تصوُّره.

(1) ILIADIS, Andrew. Computer guts and swallowed sensors: ingestibles made palatable in an era of embodied computing. In: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). Embodied computing: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 1-20.

(2) PEDERSEN, Isabel. Will the body become a platform? Body networks, datafied bodies, and AI futures. In: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). Embodied computing: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 21-48.

وقد أدّت شعبية الاتصالات اللاسلكية، ونجاحها التجاري إلى زيادة التوقعات حول كيفية فهم الناس للتواصل البشري، ومشاركة التجارب الشخصية؛ كما اكتسبت الأجهزة القابلة للارتداء القائمة على هذه التقنيات تصميمات أكثر عمليّة وراحة، وأصبحت أكثر انتشاراً؛ ليس فقط نتيجة للاستثمار الكبير الذي تقوم به شركات التكنولوجيا، ولكن أيضاً بسبب قابليتها للاستخدام المستمر.

وفي الوقت نفسه، كانت الصحافة تُعجّد الأتمتة، أنظمة القرار الخوارزمية، التعلم العميق على الرغم من الإنذارات المتكررة حول الغموض، وعدم الوضوح المحيط بتلك الأنظمة وعملياتها المختلفة.

وتجدر الإشارة إلى أنّ اتصالات وسائل الإعلام العامة حول الإمكانيات التكنولوجية (في أفلام الخيال العلمي الناجحة، والمسلسلات، أو في ألعاب الفيديو على سبيل المثال) ليست مجرد رخصة خياليّة؛ وإنما هي انعكاسٌ للتعاون بين الصناعة العسكرية المعقدة، والثقافة الأمريكيّة التي تُعجّد التكنولوجيا في منتجاتها.

كما تُعزّز العقيدة العسكرية ما بعد البشرية - المتعلقة بربط البشر بالآلات - أجهزة الحوسبة الخياليّة؛ مما يجعلها تبدو مثيرة ومُصمّمة للظهور في العالم الحقيقي؛ لذا فإنّ هناك مَنْ يتواصل بشكل كبير حول المستقبل الذي سيتحول فيه الإنترنت إلى واقع جديد مُشرق لن تكون فيه حاجة إلى الأجهزة اللوحية، أجهزة الكمبيوتر، الهواتف الذكيّة؛ حيث تملأ المكونات الإلكترونية الأجساد والفضاء المادي؛ الأمر الذي يترتب عليه حصول الشبكات غير المرئية على بيانات الأشخاص بشكل سلبي، والتي تكون مُعرّضة للخطر بالضرورة عن طريق الهجمات التي تقوم بها الأطراف الثالثة؛ الأمر الذي يترتب عليه تبادل تعابير الوجه، وبيانات المراقبة الطبيّة والأفكار والعواطف والذكريات والأحاسيس والبيانات السلوكيّة العامة على نطاق واسع خارج نطاق سيطرة المستخدمين الذين يمتلكون مثل هذه المعلومات الحساسة والخاصّة.

كما أنّ أجهزة التتبّع الذاتي القابلة للارتداء تلتقط البيانات الصحيّة مُنعدّة الأبعاد؛ ممّا يُوفّر العديد من المزايا؛ بما في ذلك توفير طرق جديدة لتسهيل البحث، ومع ذلك؛ فهي تُؤدّي كذلك إلى ظهور تضارب بين المصالح الفرديّة - التي تتجنب الإضرار بالخصوصيّة - والمصالح الجماعيّة - التي تتعلق بجمع، واستخدام البيانات

الصحية الضخمة للمنفعة العامة، وبرغم وجود بعض ممن يدافع عن آليات المساءلة والشفافية لحل هذا الخلاف؛ فإن المستخدمين العاديين غير قادرين على الوصول إلى المعلومات ومعالجتها فيما يتعلق بعواقب الموافقة على الاستخدام الجديد لبياناتهم.

وفي هذا السياق، يدافع Arora⁽¹⁾ عن العلاقات الائتمانية التي تلقي مسؤولية تداول البيانات الصحية على مراقبي البيانات؛ للحفاظ على مصالح الأشخاص «موضوع البيانات» في المقدمة؛ بهدف وضع الحق في الخصوصية في السياق الصحيح، وبمعنى آخر؛ يجب الاعتراف بالعلاقة بين المستخدمين، وأصحاب البيانات الصحية، ومراقبي البيانات الرقمية على أنها علاقة ائتمانية؛ بحيث يبقى مراقبو البيانات الصحية مصالح المستخدمين في المقدمة؛ الأمر الذي من شأنه أن يضمن المشاركة الجماعية لبيانات المستخدم في (تحسين تطبيقات الصحة الرقمية، المساهمة في البحث العلمي ... إلخ)، وتقليل المخاطر المتعلقة بالحق في الخصوصية.

وفي بعض الأحيان قد يتم دفع مستخدمي الأجهزة القابلة للارتداء لمشاركة بالبيانات المتعلقة بهم في وسائل التواصل الاجتماعي / أو إلى جمهور غير محدد؛ ومن ثم فإن العديد من الجهات التي تشترك في عملية جمع تلك البيانات، والتي تمتد من مطوري التطبيقات، وأنظمة التشغيل، ومصنعي الأجهزة، ومتاجر التطبيقات، والأطراف الثالثة الأخرى. غالباً ما يكون لديهم اهتمام كبير بالوصول إلى البيانات التي تم جمعها ومعالجتها؛ حيث تستند نماذج أعمالهم، في الغالب، على تدفقات البيانات المنبثقة من الأجهزة القابلة للارتداء، وتتمتع التطبيقات ذات الصلة بجاذبية خاصة لقطاعات الإعلان، الصيدلة، التأمين، التوظيف، وكذلك مجال البحث الطبي الذي يفترض أن يحقق فائدة كبيرة؛ نتيجة لتدفق البيانات غير المسبوق⁽²⁾؛ حيث يسهم التحليل الحسابي لمجموعات البيانات المتعددة «البيانات الطبية الحيوية الضخمة» (BBD) القادمة من الأجهزة القابلة للارتداء، أو إنترنت الأشياء، أو المسارات السريرية، أو وسائل التواصل الاجتماعي - في تطوير المعرفة الطبية، وتحسين جودة الرعاية الصحية⁽³⁾.

(1) ARORA, Chirag. Digital health fiduciaries: protecting user privacy when sharing health data. Ethics and Information Technology, [s. l.], v. 21, n. 3, p. 181-196, Feb. 2019. DOI: <https://doi.org/10.1007/s10676-019-09499-x>. Available at: <https://link.springer.com/content/pdf/10.1007/s10676-019-09499-x.pdf>. Access on July. 20, 2024.

(2) European Data Protection Supervisor (EDPS), Opinion 1/2015: Mobile Health - Reconciling Technological Innovation with Data Protection, 21 May 2015, Brussels, p. 9.

(3) Nagtegaal et al. (2015), Internet of Things: Wearable Technology, Business Innovation Observatory, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, European Commission, February 2015, p. 2.

وبصفة عامّة، قد يؤدي التوسّع في استخدام تلك التقنيات إلى عدم إدراك مُستخدميها لمقدار البيانات التي يتم إنتاجها وتجميعها؛ ومن يُمْكِنُ أن يستخدم تلك البيانات، أو يسعى لاستخدامها، ولأي غرض، الطرق التي يتمُّ بها معالجة البيانات، الوقوف على العواقب المحتملة لهذه الممارسات على حياتهم، (وعلى المجتمع بشكل عام)^(١)؛ وبالتالي فإنّ الافتقار إلى الشفافية حول تلك العناصر من شأنه أن يتعارض مع المبادئ القانونيّة الخاصّة بحماية البيانات الشخصية المعمول بها داخل الاتحاد الأوروبي؛ كما يؤثر على قدرة المستخدمين على منح موافقة مُستتيرة على أنشطة معالجة بياناتهم الشخصية، أو رفض تلك الأنشطة حال تعارضها مع رغبتهم، وأخيراً، هناك العديد من المشاكل الناجمة عن حقيقة قيام بعض مستخدمي الأجهزة القابلة للارتداء، والتطبيقات المُلحقة بها بجمع معلومات عن أشخاص آخرين. على سبيل المثال؛ قد يتم بيع تطبيقات، أو أجهزة للآباء لمراقبة موقع أطفالهم وأنشطتهم.

(1) Gloria González Fuster and Amandine Scherrer (2015), 'Big Data and Smart Devices and their Impact on Privacy', under the coordination of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and the Centre for European Policy Studies (CEPS), Policy Department C - Citizens' Rights and Constitutional Affairs European Parliament.

المبحث الثاني

الخصوصية في عصر انتشار جمع البيانات والذكاء الاصطناعي

انتشرت في العصر الحديث تكنولوجيا مُتقدِّمة أسهمت في تغيير المجتمع بشكلٍ كلي، وأبرز صورها (الذكاء الاصطناعي، التعلم الآلي)، فقد تم تنفيذها في كل مكان، وفي مجالات عدَّة منها (الطب، النقل، التمويل، المؤسسات القانونية والاجتماعية، تطوير الأسلحة،)^(١)، كما عهد إليها - في بعض الصناعات - بمسؤولية اتخاذ القرارات، بدلاً من البشر؛ ونتيجةً لذلك، فقدت الحياة الحديثة الغموض، أو ما يُسمَّى «إخفاء الهوية»؛ الذي كان يُميِّزها على مرَّ القرون؛ حيث أضحت الكاميرات، أجهزة الاستشعار، الهواتف النقالة، ومنصات التواصل الاجتماعي المزودة بتقنيات الذكاء الاصطناعي لديها القدرة على قراءة وتفسير المجموعات الكبيرة من البيانات المستقاة من كافة المصادر، ومع ازدياد التطوُّر التكنولوجي؛ فقد أضحت الحياة الحديثة تُسم بالشفافية في الوقت الذي تطوَّرت فيه معايير الخصوصية، وحماية البيانات.

وذهب Keller^(٢) إلى أنَّ تفسير التناقض بين الحقِّ في الوصول إلى المعلومات، والحقِّ في الخصوصية يجب أن يتمَّ من خلال المفهوم الواسع للاقتصاد السياسي؛ حيث يسعى الحقُّ في الوصول إلى المعلومات إلى تقييد التشريعات الخاصة بحماية البيانات الشخصية.

وعلى الرغم من أنَّ النموذج الليبرالي السائد للمعلومات يتمحور حول عاملين رئيسيين هما:

١- ضمان ما يُمكن الدولة من الوصول في نهاية المطاف إلى المعلومات.

٢- أنَّ السوق قد يتعامل - على الأقل بشكلٍ مُحتمَل - مع البيانات.

ومن ثم؛ فإنَّ الخطر الذي تتعرَّض له البيانات الشخصية أمام طلبات الوصول إليها من قِبَل الدولة أو السوق هو أكثر بكثيرٍ من مُجرَّد عدم توازن في القوة السياسية أو

(1) YANISKY-RAVID, Shlomit; HALLISEY, Sean K. «Equality and privacy by design»: a new model of artificial intelligence data transparency via auditing, certification, and safe harbor regimes. Fordham Urban Law Journal, [s. l.], v. 46, n. 2, p. 428-486, 2019. Available at: <https://ir.lawnet.fordham.edu/ulj/vol46/iss2/5>. Access on: July, 20, 2024.

(2) KELLER, Perry. The reconstruction of privacy through law: a strategy of diminishing expectations. International Data Privacy Law, [s. l.], v. 9, n. 3, p. 132-152, Aug. 2019. DOI: <https://doi.org/10.1093/idpl/ipy012>.

الاقتصادية؛ لأن الحق في الوصول إلى المعلومات تطوّر من خلال علاقة ديناميكية بين استخدام المعلومات الحكومية والتجارية، وكذلك الاستخدام المستمر للتقنيات الحديثة لجعل المعلومات أكثر قابلية للاستخدام والوصول إليها.

بالإضافة إلى أن إعادة بناء الحق في الخصوصية من خلال القانون مليء بالثغرات، ومن شأنه أن يعرّض هذا الحق إلى المزيد من المخاطر⁽¹⁾ وعلى الأخص من خلال:

تحوّل المفاهيم الخاصّة بالفضاء العام والملك العام: لتبرير الوصول إلى البيانات الخاصّة، مع توفير حد أدنى من الحماية لتلك البيانات.

التعارض بين مبادئ الموافقة والاختيار الفردي: يعتمد مفهوم الموافقة المستنيرة على تعقيد ممارسة جمع البيانات؛ إلا أنه في غالب الأحيان يفقر المستهلكون لخيارات بديلة عند التعامل مع مقدّمي الخدمات الذين يجمعون بياناتهم الشخصية.

٢- البناء الضعيف لقوانين الخصوصية وحماية البيانات الشخصية: غالباً ما ينظر إلى قوانين حماية البيانات الشخصية على أنها خاضعة لقانون المعلومات بمعناه الواسع.

ومن ناحية أخرى، تتمتع الشركات صاحبة الامتياز العاملة في مجال تقديم الخدمات العامّة (الكهرباء، المياه،) بمكانة متميّزة تُتيح لهم الحصول على البيانات الشخصية للمستهلكين؛ ويرجع ذلك في معظم الأحوال إلى أن هؤلاء المستهلكين ليس لديهم أي خيار في السوق؛ إما بسبب عدم وجود بديل يُمكن أن يُقدّم ذات الخدمة، أو أن العملاء في تلك الحالات يكون من المستحيل عليهم اختيار الخدمة المقدّمة في مجالات؛ مثل (الصحة، التعليم،)⁽²⁾، مع تزايد الاحتمالات حول استخدام التقنيات الحديثة، وإنترنت الأشياء (IOT)؛ للوصول إلى المزيد من البيانات الشخصية؛ مثل: العدادات الذكية، أجهزة استشعار تعمل على الحصول على المعلومات المتعلقة بنمط الاستخدام، ودعم التطبيقات الذكية لاستهلاك، وتسعير الخدمات المقدّمة؛ لا سيّما أنه - من المعلوم - أن أنظمة الذكاء الاصطناعي تعمل بشكل أفضل كلما زادت

(1) Ibid.

(2) STEIN, Amy L. Artificial intelligence and climate change. Yale Journal on Regulation, [s. l.], v. 37, n. 3, p. 890-939, 2020. Available at: <https://www.yalejreg.com/print/artificial-intelligence-and-climate-change/> Access on: July. 20, 2024.

كمية البيانات التي يمكنها الوصول إليها -؛ وبالتالي ستكون مشاركة البيانات ضرورية للتنفيذ الناجح لتقنيات الذكاء الاصطناعي؛ وبالتالي فإن الاستخدام المتزايد لمثل هذه الأجهزة يُثير مخاوف بشأن البيانات الشخصية التي يمكن الحصول عليها عن الأفراد من خلال أنماط سلوكهم؛ مما يجعل مالكي هذه البيانات يخشون المراقبة العرضية، أو غزو المنزل المستهدف، أو إنشاء ملفات تعريف، أو تتبع السلوك، أو سرقة الهوية؛ الأمر الذي من شأنه أن يضع مسؤوليات إضافية على عاتق هذه المرافق؛ بصفتها أمينة على تلك البيانات، وتُثير هذه الحقيقة أسئلة مهمة حول تخزين هذه البيانات، واستخدامها، ونقلها، والتخلص منها^(١).

وهذه المسائل المتعلقة بالخصوصية تتعارض مع الجهود المبذولة لتقليل التدريب المتكرر للذكاء الاصطناعي، وتسهيل مشاركة البيانات، تلك الخطوات، والتي تعد ضرورية، تمكن تلك الشركات من تحديث خدماتها، ويمكن اتخاذ بعض الإجراءات لتلافي الآثار السلبية الناتجة عن استخدام البيانات الشخصية؛ منها:

اعتماد إجراءات صارمة لإخفاء هوية البيانات: يتم تنفيذ عمليات إزالة هوية البيانات؛ بحيث لا يمكن التعرف على المعلومات، أو ربطها، أو وصفها، أو الرجوع إليها، أو ربطها بشكل مباشر، أو غير مباشر بفرد معين، أو قابل للتحديد - وتعد تقنية شائعة الاستخدام لحماية الخصوصية؛ إلا أن التجربة العملية أثبتت أن مثل هذه التقنيات ليست فعالة بنسبة ١٠٠٪ من الناحية الفنية.

تنظيم ملكية البيانات: حيث يحق لأصحاب البيانات الوصول إلى بياناتهم الخاصة، إلا أن الرأي انقسم حول ما إذا كان بإمكان الأطراف الثالثة الوصول إلى هذه البيانات، وكذلك من تؤول إليه ملكية تلك البيانات.

وفي السياق ذاته؛ فإن التطبيقات البسيطة التي تستخدم الذكاء الاصطناعي - على سبيل المثال التطبيقات التي تُستخدم لتحديد مواقع السيارات من خلال صور المركبات؛ والتي تعرف بـ «محددات الموقع العالمي» - يمكن أن تُثير مخاوف تتعلق بالخصوصية^(٢)؛ أهمها:

(1) Ibid, p.923

(2) TUCKER, Catherine. Privacy, algorithms, and artificial intelligence. In: AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi (ed.). The economics of artificial intelligence: an agenda. Chicago: The University of Chicago Press, 2019. p. 423-438. (National Bureau of Economic Research Conference Report).

استمرار البيانات المخزّنة: حيث إن البيانات الشخصية التي يُنشئها أصحابها تظلّ مخزّنة لفترةٍ طويلةٍ تتجاوز حياة أصحابها؛ وذلك بسبب التكلفة المنخفضة نسبياً لتخزين البيانات.

إمكانية إعادة استخدام البيانات الشخصية: قد تتجاوز عملية جمع البيانات الشخصية الهدف المرجوّ منها؛ مما يُثيرُ مخاوف بشأن العواقب غير المقصودة؛ المتمثلة في إعادة استخدام البيانات الشخصية التي أنشئت فيما بعد (بواسطة خدمات الأمن، أو من قِبَل الدولة، أو عن طريق شركات التسويق أو التأمين.. إلخ).

تدفّق البيانات: فهذه التطبيقات قد تُسجّل بيانات شخصية أخرى لا تتعلق بالشخص «موضوع البيانات» - التي تتعلق به البيانات المسجّلة -؛ فقد تكشف صورة سيلفي (selfie) التقطها أحد الأشخاص لوحة ترخيص سيارة تابعة لشخص آخر متوقّفة في ذات المكان، ويُمكن بالتالي معرفة الشخص صاحب السيارة عن طريق قواعد بيانات لوحة الترخيص؛ على الرغم من أن هؤلاء الأشخاص لم يختاروا إنشاء بيانات شخصية عنهم؛ الأمر الذي قد تكون له تداعيات مستقبلية سلبية.

فهذه المشاكل الثلاثة تُشكّل تحديات جديدة للمعالجة القانونية للبيانات الشخصية؛ لتعارضها مع الطرق التقليدية التي يُمكن للأشخاص «موضوع البيانات» أن يقرّروا من خلالها إنشاء بيانات شخصية يُمكن استخدامها فيما بعد، وعلى الأخص قيمة الموافقة التي يمنحها الشخص «موضوع البيانات» لتخزين ومعالجة البيانات الشخصية المتعلقة به؛ ففي الوقت الحالي تمكّن العديد من التطبيقات والخدمات المقدمة عبر الإنترنت من جمع وتخزين كميات كبيرة من البيانات الشخصية من خلال توفير مجموعة واسعة من الخدمات بسرعة وسهولة⁽¹⁾.

حيث يعتمد النموذج الحالي لتلك التطبيقات والخدمات على ما يُسمّى بـ «شروط الاستخدام واتفاقيات الخصوصية» - التي يسعى التطبيق من خلالها إلى الحصول على موافقة الشخص «موضوع البيانات» إلى الوصول إلى تخزين ومعالجة بياناته الشخصية - التي غالباً ما يتم صياغتها بطريقة مُربكة؛ بهدف حث المستخدمين على

(1) PELTZ, James; STREET, Anita C. Artificial intelligence and ethical dilemmas involving privacy. In: MASA-KOWSKI, Yvonne R. (ed.). Artificial intelligence and global security: future trends, threats and considerations. Bingley, UK: Emerald Publishing, 2020. p. 95.

قبول مخاطر معينة تلقائياً مقابل الراحة والسهولة التي توفرها تلك التطبيقات، والتي يمكن إتاحتها لأطراف ثالثة؛ كالحكومة، أو شركات التسويق؛ مما يؤدي إلى تآكل الخصوصية الفردية؛ حيث يعمل الذكاء الاصطناعي على إنشاء ملف رقمي لكل شخص يحتوي على خصائصه وتفضيلاته وميوله؛ استناداً إلى البيانات التي تم جمعها من سلوكه، وقد يعمل على تحليل وصقل تلك البيانات لأجل إعادة استخدامها لاستهداف ذات الأشخاص أصحاب البيانات.

وأبرز الأمثلة على ذلك: (عقود التأمين من المخاطر)؛ حيث أدى التنبؤ الخوارزمي في مجال صناعة التأمين إلى الدخول في حقبة جديدة من تخصيص السياسات، والأقساط، والمطالبات، والتغطية؛ بناءً على سلوك الفرد، ومستوى المخاطر التي يتعرض لها من خلال ما تم جمعه من بيانات شخصية حول نمط معيشته؛ وبالتالي يتم استبدال المتغيرات الخارجية (الجنس، والعمر، والعرق، والعنوان، وما إلى ذلك) بمتغيرات داخلية؛ أي السلوك الفردي، مما أدى إلى إعادة صياغة عقود التأمين بالكامل وفقاً لذلك؛ ومن ثم لن تكون الأسعار المتعلقة بعقود التأمين مرجعية؛ وبناءً عليه، سوف يتعين على الجميع الدفع فقط مقابل تعرضهم الحقيقي للمخاطر⁽¹⁾.

وتجدر الإشارة إلى أن السباق حول تطوير الذكاء الاصطناعي قد بدأ بالفعل، ويبدل العديد من الدول جهوداً لتكون رائدة على مستوى العالم في هذا القطاع؛ بينما يحمل الذكاء الاصطناعي وعداً بعالم أكثر ذكاءً واستقلالية؛ إلا أن هناك العديد من المخاوف القانونية المتعلقة بتطوره؛ من بينها تلك المتعلقة بالخصوصية، وحماية البيانات الشخصية للمستهلك.

وبرغم تبني دول العالم المختلفة لدرجات متفاوتة من حماية البيانات الشخصية؛ إلا أن الاتحاد الأوروبي (EU) يعد رائداً في مثل هذا التنظيم؛ من خلال اللائحة العامة لحماية البيانات (GDPR)، ومع هذا؛ فإن العديد من جوانب هذا التنظيم يُثير مخاوف بشأن تأثير تطبيقه على الخوارزميات، والتعلم الآلي الضروري لتطوير الذكاء الاصطناعي.

(1) CEVOLINI, Alberto; ESPOSITO, Elena. From pool to profile: social consequences of algorithmic prediction in insurance. Big Data & Society, [s. l.], v. 7, n. 2, p. 1-11, July/Dec. 2020. DOI: <https://doi.org/10.1177/2053951720939228>. Available at: <https://journals.sagepub.com/doi/pdf/10.1177/2053951720939228>. Access on: July. 20, 2024.

فالحفاظ على القدرة التنافسية لقطاع الذكاء الاصطناعي في بلد أو منطقة ما يعتمد على التوازن السلس لمثل هذا الهدف مع حماية الخصوصية⁽¹⁾.

والجدير بالذكر أن هناك سياسات عامة يمكن أن تحقق مثل هذا التوازن؛ مثل التمويل العام لتطوير الذكاء الاصطناعي الأقل تعرضاً للحق في الخصوصية - مثل برنامج OpenAI من Google؛ والذي - على الرغم من عدم فعاليته، مقارنة بالذكاء الاصطناعي غير المحدود في الوصول إلى البيانات - إلا أنه يتسم بالحد في تطوير واحترام خصوصية المستهلك.

ومع ذلك؛ فإن تنظيم استخدام البيانات الشخصية دون إنشاء وسائل لتسهيل استخدامها لتدريب أنظمة الذكاء الاصطناعي سيؤدي بدلاً من ذلك إلى إضعاف النظام القياسي لحماية البيانات الشخصية الذي يختار ببساطة حماية خصوصية المستخدمين دون أي توازن في مواجهة الحاجة إلى الحفاظ على الابتكار التكنولوجي في المنطقة التي ينطبق فيها هذا القانون؛ الأمر الذي يؤدي إلى قيام المنظمات والشركات الخاصة بمحاولة تطوير الذكاء الاصطناعي عن طريق التحايل على تشريعات حماية البيانات الشخصية التي تحظر استخدام ومعالجة البيانات الشخصية؛ نظراً لأن تطوير الذكاء الاصطناعي يعتمد بالضرورة على تحليل كميات هائلة من البيانات.

(1) HUMERICK, Matthew. Taking AI personally: how the E.U. must learn to balance the interests of personal data privacy & artificial intelligence. Santa Clara High Technology Law Journal, [s. l.], v. 34, n. 4, p. 393-418, 2018. Available at: <https://digitalcommons.law.scu.edu/chtj/vol34/iss4/3/>. Access on: July. 20, 2024.

المبحث الثالث

مُغالطة الموافقة وخصوصية التصميم؛ مفاهيم رئيسة تتعلق بحماية البيانات في عصر الذكاء الاصطناعي

لكي تكون معالجة البيانات الشخصية مشروعة، يجب أن تتم لأسباب قانونية، وهو ما يعرف بـ«الأساس القانوني للمعالجة»، والتي عددها عليها المادة (٦) من اللائحة العامة لحماية البيانات «GDPR»^(١)، فإذا تحقق أحدها كان سبباً قانونياً كافياً لمعالجة البيانات الشخصية، ومن بين تلك الأسباب «(أ) الموافقة: إذا وافق الشخص «موضوع البيانات» على معالجة البيانات الشخصية الخاصة به».

إلا أنه، ونتيجة لانتشار الأجهزة القابلة للارتداء المعتمدة على البيانات الشخصية للمستخدمين كأساس لعملها، والتي استندت إلى موافقة صاحب البيانات كأساس قانوني لمعالجة البيانات الشخصية معولة على سهولة الحصول عليها كشرط لاستفادة المستخدم بالمهام والوظائف التي يوفرها الجهاز القابل للارتداء، الأمر الذي اقتضى دراسة مدى كفاية الموافقة كأساس قانوني لمعالجة البيانات في ظل هذه التحديات، وسوف نستعرض ذلك فيما يلي:

مُغالطة الموافقة:

استند البناء القانوني للحق في حماية البيانات الشخصية إلى موافقة صاحب البيانات الشخصية على معالجة تلك البيانات، والتي يجب أن تتخذ مظهراً حراً مستنيراً لا لبس فيه؛ يوافق من خلاله أصحاب البيانات الشخصية على جمع ومعالجة بياناتهم الشخصية لغرض محدد، ويُعد ذلك السبب الرئيسي في وجود ما يُسمى بـ«إذن معالجة البيانات الشخصية»؛ مما أدى إلى إدخال الخوارزميات الخاصة بمعالجة البيانات بشكل متزايد في المجتمع؛ إلا أن قواعد حماية خصوصية البيانات الشخصية وجدت صعوبة في دمج خصوصية مجتمع المعلومات في ظل الاستخدام

(1) Art. 6 «1- Processing shall be lawful only if and to the extent that at least one of the following applies:

1- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
2- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

المُكثَّف للبيانات، ونتيجةً لذلك؛ فإن التحديات التي تُواجهُ دورَ ومفهوم الموافقة تبدو واضحةً بشكلٍ جليٍّ^(١).

- يرى Cotino Hueso^(٢) أن مثل هذه القاعدة أصبحت عُرضَةً للخطأ في عصر البيانات الضخمة، والذكاء الاصطناعي؛ ويرجع ذلك لعدة أسباب:
- أولاً: التراكم الهائل للبيانات والتقاطها سوف يُثقلُ كاهل المبادئ القانونية المتعلقة بالإجماع على حماية البيانات الشخصية.
- ثانياً: الأفراد غير مُستعدين للتخلي عن استخدام تكنولوجيا المعلومات والاتصالات.
- ثالثاً: المجتمعات لا تمتلك ثقافةً قويةً بشأن الخصوصية؛ مما يجعل الضمانة الخاصة بالموافقة غير حقيقية، وتفتقرُ للفعالية الكافية. علاوة على ذلك؛ فإن الموافقة - من الناحية العملية - ذات نمطٍ مُوحَّد؛ مما يُثيرُ العديد من الشكوك؛ حيث إنه من الخطأ الاعتقاد بوجود سيطرة فعّالة على البيانات الشخصية من خلال الموافقة، وكذلك مقدار الحقوق التي يَمْلِكُها «صاحب البيانات» - وتصبح الموافقة، في الممارسة العملية، «تفويضاً مطلقاً» لـ«التدفق غير المنضبط للبيانات الشخصية»؛ الأمر الذي من شأنه أن يُؤدِّي إلى ضَعْفِ دور «الموافقة»؛ حتى يُصَبِّحَ دورها رمزياً؛ مما يترتب عليه - في نهاية المطاف - إلى الانتهاك المقصود للخصوصية، وإضعاف أنظمة الحماية.

خصوصية التصميم:

جرت مناقشة العديد من الطرق لتحقيق الحماية الكافية للبيانات الشخصية؛ ومن بين الطرق التي جرت مناقشتها على نطاق واسع ما يُسمَّى بتنظيم التصميم، الذي يعني في صورته البسيطة: استخدام التدابير الفنية والتنظيمية لتحقيق أهداف حماية البيانات^(٣).

(1) GIANOPOULOU, Alexandra. Algorithmic systems: the consent is in the detail? Internet Policy Review, [s. l.], v. 9, n. 1, p. 1-19, Mar. 2020. DOI: <https://doi.org/10.14763/2020.1.1452>. Available at: <https://policyreview.info/articles/analysis/algorithmic-systems-consent-detail>. Access on: July. 20, 2024.

(2) COTINO HUESO, Lorenzo. Big data e inteligencia artificial: una aproximación a su tratamiento jurídico desde los derechos fundamentales. Dilemata, [s. l.], año 9, n. 24, p. 131-150, 2017. Available at: <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104>. Access on: July. 20, 2024.

(3) RUBINSTEIN, Ira S.; GOOD, Nathaniel. The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law, [s. l.], v. 10, n. 1, p. 37-56, Feb. 2020. DOI: <https://doi.org/10.1093/idpl/izp019>.

على سبيل المثال؛ يمكن الالتزام ببرمجة الأدوات التكنولوجية بطريقة تجعل من المستحيل معها انتهاك قانون حماية البيانات الشخصية، وعلى غرار تنظيم التصميم أنشئ مفهوم «خصوصية التصميم» الذي يُشير إلى إعطاء الأولوية للخصوصية؛ ابتداءً من تصميم المنتج، أو الخدمة^(١). وتجد فكرة الخصوصية حسب التصميم مجالاً لها في ضمان خصوصية البيانات الشخصية؛ بعيداً عن الامتثال للإجراءات أو المعايير؛ فالخصوصية الآن يجب أن تتوافق مع معايير تنظيمية، والتي يجب أن تدمج في طريقة عمل كل شركة.

وفي ذات السياق، قام منظمو الخصوصية بإقرار تقنيات من شأنها تعزيز الخصوصية؛ كـ (إخفاء الهوية، التسمية المستعارة). وعلى سبيل المثال؛ ما نصّت عليه المادة (٢٥) من اللائحة العامة لحماية البيانات التي ساهمت في تحويل تلك الفكرة إلى التزام قانوني ملزم^(٢)؛ كما يجب أن يؤخذ في الاعتبار الوسائل المعقولة المتاحة وقت المعالجة، حتى ولو ظهرت تقنيات أفضل لاحقاً؛ بسبب التقدم الهائل للتكنولوجيا بمرور الوقت، وما يعتبر معقولاً اليوم، قد لا يُعتبر كذلك لاحقاً.

وتجدر الإشارة إلى أن الجهاز الأوروبي التنظيمي - اللائحة العامة لحماية البيانات الشخصية - لا تتوافق بشكل كاف مع أساليب هندسة الخصوصية، وتقنيات إنفاذ الخصوصية - خاصة فيما يتعلق بتقنيات الإنفاذ «الصارمة»؛ وهو ما يؤدي في النهاية إلى التسبب في تقليل الثقة في الأطراف الثالثة؛ (بما في ذلك وكلاء مراقب البيانات) التي تستخدم تقنية التشفير لتقليل الوصول إلى البيانات^(٣).

ونخلص إلى أنه - من أجل تعزيز حماية البيانات، بدلاً من مجرد تعزيز المبادئ العامة لللائحة العامة لحماية البيانات (GDPR) - يجب تفسير نص المادة (٢٥) على أنه يتطلب تنفيذ هندسة خاصة، وتقنيات صارمة لإنفاذ الخصوصية، ومن أكثر الطرق

(1) SOARES, Paulo Vinícius de Carvalho. A diluição das esferas de privacidade e de intimidade diante da era dos dados. In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovanni dos Santos (coord.). Direito, processo e tecnologia. São Paulo: Revista dos Tribunais, 2020. p. 555-574. (Coleção Direito e Novas Tecnologias).

(2) EUROPEAN UNION. 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). Brussels : EUR-Lex, 2016. Available at : <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Access on: July. 20, 2024; RUBINSTEIN, Ira S.; GOOD, op.cit, p.37.

(3) RUBINSTEIN; GOOD, ibid.

وُضوحًا للقيام بذلك، إلزام المتحكم في البيانات باستخدام التقنيات المتاحة لتقليل البيانات.

- وبناءً عليه؛ لكي يتحقق التنفيذ التدريجي لتقنيات الخصوصية، يجب اتخاذ عدّة خطوات تتمثل في:

إنشاء هيئات تنظيمية لحماية البيانات؛ تلعب دوراً مركزياً في هندسة الخصوصية، وتقنيات تعزيز الخصوصية في المشاريع القادمة من القطاع العام.

إصدار المبادئ التوجيهية بشأن نصّ المادة (٢٥) من اللائحة العامة لحماية البيانات تتضمن عبارات صريحة وقوية، تطلب من خلالها بوضوح تنفيذ تقنية الخصوصية.

مكافأة الأمثلة الجيدة لهندسة الخصوصية بدلاً من معاقبة الإخفاقات.

وبالرغم من ظهور الذكاء الاصطناعي بشكل متكرر في النقاشات العامة في السنوات الأخيرة، إلا أنه ما زال من غير المعلوم معرفة العوامل التي تشكل مواقف الناس تجاه هذه التكنولوجيا، وفي هذا السياق، تناولت الدراسة التي أجراها، Lobera, Fernández Rodríguez and Torres-Albero⁽¹⁾ هذه العوامل عن طريق تحليل البيانات الناتجة من دراسة استقصائية أجريت في إسبانيا؛ والتي أظهرت أن القيم والمواقف الثقافية تجاه العلم تُقدّم تفسيراً فعالاً لمعارضة الناس للذكاء الاصطناعي، ومن ثم؛ فإنّ مَنْ يتحدثون عن قيم المساواة ومخاوف الخصوصية هم أكثر الفئات التي يُحتمل أن تُعارض الذكاء الاصطناعي، وكذلك الأشخاص الذين يُعبّرون عن ثقة أقل في التطبيق العملي للعلم، وكذا الأشخاص الأقل استعداداً للابتكار والتغيير؛ وأمثلة الأبرز المتعلق بمعارضة الذكاء الاصطناعي ارتبط بالتطور التكنولوجي الذي أدّى إلى ظهور الإنسان الآلي (الروبوت) في أماكن العمل؛ الأمر الذي اعتبر بمثابة عنصر تهديد جديد.

وقد أثار - الاستخدام واسع النطاق للذكاء الاصطناعي في اتخاذ القرارات بشأن مختلف جوانب حياة الإنسان - جدلاً واسعاً بسبب المخاطر والقيود المتعلقة بهذه التكنولوجيا؛ فقد شكّل الذكاء الاصطناعي مصدر قلق كبير للخصوصية؛ نتيجة لعدة

(1) LOBERA, Josep; FERNÁNDEZ RODRÍGUEZ, Carlos J.; TORRES-ALBERO, Cristóbal. Privacy, values and machines: predicting opposition to artificial intelligence. Communication Studies, [s. l.], v. 71, n. 3, p. 448-465, Mar. 2020. DOI: <https://doi.org/10.1080/10510974.2020.1736114>.

عوامل أهمها: جمع البيانات الشخصية من كل مكان، المشاكل المتعلقة بتحديد الهوية، الافتقار إلى المساءلة القانونية.

ومع ذلك يقترح Els ⁽¹⁾ أن الذكاء الاصطناعي يمكن أن يساعد في التخفيف من معظم التحديات المتعلقة بالخصوصية الرقمية، التي يُعتبر استخدامها وتطويرها بمثابة تهديد للخصوصية؛ حيث تعمل التقنيات الحديثة المدمجة في الخصوصية التفاضلية، والتعلم العميق على تقليل كمية البيانات الحساسة التي يتم جمعها وتخزينها، ومشاركتها مع الأطراف الثالثة؛ مما يسمح للشركات بمواصلة التعلم بطريقة قيمة حول أنشطة مستخدميها، ويمكن للمدققين، ومسؤولي الذكاء الاصطناعي تمثيل مصالح المستهلكين خلال جمع البيانات وتصحيح الدوافع، ومراقبة إمكانية إعادة تحديد الهوية، أو النتائج التي تُسَمَّ بطابع ينطوي على تمييز بين الأفراد في الأنظمة الأخرى. أضف إلى ذلك أن الذكاء الاصطناعي يمكن أن يساعد في تحديد ماهية الخصوصية، إلا أن الأمر يبدو أنه بعيد المنال، ومن شأن التسليم به تقويض القدرة على سن حماية أكثر أهمية للحق في الخصوصية.

وتجدر الإشارة إلى أن التنفيذ الناجح لتلك التقنيات يعتمد على تنسيق التشريعات والإجراءات الخاصة لضمان تحقيقها لإمكاناتها الكاملة.

كما تُقدِّم التحليلات الخاصة بالبيانات الضخمة والذكاء الاصطناعي توقعات واستنتاجات ليست بديهية وغير مُحَقَّقة حول البيانات الشخصية للأفراد؛ (سلوكياتهم، تفضيلاتهم، حياتهم الخاصة)؛ والتي تستند إلى بيانات غنية ومتنوعة؛ الأمر الذي من شأنه خلق فرص جديدة لاتخاذ القرار بطريقة تمييزية جائرة.

وتجدر الإشارة إلى أنه، ولما كانت اللائحة العامة لحماية البيانات، وكافة التشريعات المتعلقة بحماية البيانات تهدف إلى حماية خصوصية الأشخاص وهويتهم وسمعتهم واستقلاليتهم؛ إلا أنها لم تتطرق إلى حماية الشخص «موضوع البيانات» من المخاطر الحديثة الناشئة عن التحليل الاستنتاجي، ووفقاً لـ Wachter and Mittelstadt ⁽²⁾

(1) ELS, Andrea Scripa. Artificial intelligence as a digital privacy protector. Harvard Journal of Law & Technology, [s. l.], v. 31, n. 1, p. 217-235, 2017. Available at: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech217.pdf>. Access on: July. 20, 2024, p234-235.

(2) WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, [s. l.], v. 2.019, n. 2, p. 494-620, May 2019. DOI: <https://doi.org/10.7916/cblr.v2019i2.3424>. Available at: <https://journals.library.columbia.edu/index.php/>

فإنَّ الأفراد لا يتمتَّعون إلا بقدر ضئيل من التحكم أو الإشراف على الطرق التي يتم بها استخدام بياناتهم الشخصية لعمل استنتاجات عنها، وبمقارنة الأنواع المتعددة لبيانات الشخصية، يتَّضح أنَّ الاستنتاجات تُعدُّ - فعلياً - بيانات شخصية من «الفئة الاقتصادية» وفقاً للتصنيف الذي وضعته اللائحة العامة لحماية البيانات (GDPR)؛ يملكُ الشخص «موضوع البيانات» بشأنها كافة الحقوق التي تضمَّنتها اللائحة؛ وأبرزها: الحقُّ في المعرفة (المواد ١٢-١٥)، الحقُّ في التصحيح (المادة ١٦)، الحقُّ في الإلغاء (المادة ١٧)، الحقُّ في الاعتراض (المادة ٢١)، نقل البيانات (المادة ٢٠) البيانات الشخصية تُعتبرُ مُقيَّدة بشكل كبير للاستدلالات، ومما يجدرُ التنويه إليه أنَّ اللائحة العامة لحماية البيانات (GDPR) لا تُوفِّرُ حمايةً كافيةً للاستدلالات الحسَّاسة (المادة ٩)، والحلول اللازمة للطعن على تلك الاستنتاجات، أو القرارات المتخذة وفقاً لها (المادة ٢٢).

وبناءً عليه؛ فإنَّ حقاً جديداً للشخص «موضوع البيانات» وهو «الحقُّ في الاستدلالات المعقولة» يُمكنُ أن يسدَّ فجوة المسؤولية التي تمثلها حالياً «الاستنتاجات عالية الخطورة» الناتجة عن تحليل البيانات الضخمة التي تضرُّ بالخصوصية، أو سمعة الشخص «موضوع البيانات»^(١)، والذي قد يتطلب قيام مراقب البيانات بتقديم تبرير؛ لتحديد ما إذا كان الاستنتاج معقولاً، والذي ينبغي أن يتعرَّض إلى:

- لماذا تُشكِّلُ بعضُ البيانات أساساً مقبولاً لتكوين استنتاج؟
 - لماذا تُعدُّ هذه الاستنتاجات ملائمة ومقبولة معيارياً للاعتماد عليها في اتخاذ القرار بطريقة آليّة؟
 - الدقّة والموثوقية الإحصائية للبيانات، والطريقة التي استُخدمت في عمل استنتاجات عنها.
- ولا شكَّ أنَّ من شأن هذا التبرير أن يدعم آلية لاحقة تسمح لأصحاب البيانات بالطعن على «الاستنتاجات غير المعقولة».

المبحث الرابع

تنظيم جمع البيانات الشخصية والذكاء الاصطناعي: «مقترحات جديدة»

تعد البيانات الشخصية أهم جانب من جوانب تدريب أنظمة الذكاء الاصطناعي؛ حيث تتعلم الخوارزميات من مجموعة ضخمة من البيانات الموجودة مسبقاً، ومع ذلك؛ فإن البيانات - التي تستخدمها أنظمة الذكاء الاصطناعي - قد تكون في بعض الأحيان غير قانونية، أو تمييزية، أو معدلة، أو غير موثوقة، أو ببساطة غير مكتملة. ونتيجة لذلك؛ فإنه كلما تم توفير المزيد من البيانات لأنظمة الذكاء الاصطناعي، زاد احتمال قيام تلك الأنظمة بإصدار قرارات تمييزية؛ ومن ثم انتهاك الحق في الخصوصية من خلال استخدام تلك البيانات، ولحل تلك المشكلة اقترح Yanisky-Ravid and Hallisey⁽¹⁾ إيجاد نموذج للذكاء الاصطناعي، يعتمد على شفافية البيانات يركز على الكشف عن البيانات، وليس على البرنامج الأساسي ومبرمجه؛ وبالتالي فإن أنظمة التدقيق، وبرامج الشهادات التي تديرها جهة حكومية يمكن أن تتحقق من شفافية الخوارزمية أو في حالة - غياب تلك المؤسسة - عن طريق إحدى المؤسسات الخاصة، والتي من شأنها - حال وجودها - أن تشجع القطاع الصناعي؛ ليكون سباقاً في اتخاذ خطوات لضمان موثوقية قواعد البيانات الشخصية الخاصة بهم، وبناءً عليه؛ فإن «هيئة حماية البيانات» لن تكون مسؤولة فقط عن تنظيم الممارسات المتعلقة بحماية البيانات؛ بل سوف تُسأل أيضاً عن تشجيع القطاع الخاص على إيجاد آليات للتدقيق والشفافية، والاستفادة من أحدث التقنيات لتحقيق هذا الغرض؛ بهدف تحقيق التوازن بين الحاجة إلى حماية البيانات الشخصية، واستخدام البيانات لصالح الابتكار التكنولوجي في هذا القطاع، مع الأخذ في الاعتبار أن هذه الآليات قد تصبح عمليات وأدوات قابلة لتسويق للمنتجات والخدمات الأمنية.

وقد أظهر Alamäki, Mäki and Ratnayake⁽²⁾ أن جودة البيانات ترتبط بعوامل وأبعاد عديدة تؤثر على موثوقيتها - (الدقة، الصلاحية القانونية، القيمة التجارية)؛

(1) Yanisky-Ravid and Hallisey, Op. cit.

(2) ALAMÄKI, Ari; MÄKI, Marko; RATNAYAKE, R. M. Chandima. Privacy concern, data quality and trustworthiness of AI-analytics. In: FAKE INTELLIGENCE ONLINE SUMMIT, 1., 2019, Pori, FI. Proceedings [...]. Pori, FI: Satakunta University of Applied Sciences, 2019. p. 37-42. Available at: <http://urn.fi/URN:NBN:fi-fe2019051315372>. Access on: July. 20, 2024.

فالقلق بشأن الخصوصية من شأنه أن يؤثر على موثوقية البيانات؛ حيث يمكن للمستخدمين التلاعب بالمعلومات التي يقدمونها؛ ويتمثل التحدي الأكبر الذي يواجه معظم أنظمة الذكاء الاصطناعي اليوم في عدم القدرة على التمييز بين البيانات المتحيزة أو التالفة، من البيانات عالية الجودة؛ فتلك الأنظمة قادرة على معالجة البيانات، لكنها لا تملك القدرة على تقييم عملية تكوين تلك البيانات، فقد تلبّي تلك البيانات متطلبات معينة من الناحية الفنية، إلا أنه - في الواقع - قد يكون محتواها متحيزاً أو تالفاً، بالإضافة إلى ذلك؛ لا يستطيع المتخصصون في مجال معالجة البيانات - دائماً - التمييز بين البيانات الفاسدة، أو البيانات عالية الجودة؛ خاصة إذا لم يتمكنوا من معرفة الكيفية التي تمّ من خلالها جمع ومعالجة تلك البيانات؛ وبالتالي فقد أوضح المؤلفون أن جودة البيانات تؤثر على موثوقية النتائج، بالإضافة إلى القلق بشأن الخصوصية؛ والذي يعدّ عاملاً من شأنه أن يؤثر في تلك الموثوقية؛ ومن ثمّ يقترح هؤلاء المؤلفون أن يتمّ التركيز على المراحل المبكرة من عملية جمع البيانات؛ حيث تؤدي العوامل البشرية، وندرة التكنولوجيا المستخدمة في جمع البيانات إلى إفساد جودتها. وتعدّ واحدة من المشاكل الرئيسة المتعلقة بأمان وخصوصية بيانات المستهلك: عدم مساءلة الشركات التي تتعامل مع تلك البيانات أو المخاطر التي تمثلها تلك الشركات؛ نتيجة انتهاكها للأصول القانونية⁽¹⁾.

- ويفترض إنشاء نظام للمسؤولية الكاملة التغلب على ثلاث صعوبات:
 - مراقبة العمل الحقيقي للشركات في جمع واستخدام وتخزين البيانات.
 - قياس العواقب الناتجة عن ممارسة أنشطتها المتعلقة بالبيانات الشخصية للمستهلكين؛ وعلى الأخص الإدراك المسبق للأعمال الضارة المنخفضة الاحتمالية.
 - إنشاء علاقة سببية بين ممارسة البيانات عن طريق الشركات والعواقب الناشئة عنها.
- وبالرغم من أن الخصوصية قد يُنظر إليها على أنها عقبة أمام الابتكار، والتي تُعدّ

(1) JIN, Ginger Zhe. Artificial intelligence and consumer privacy. In: AGRAWAL, Ajay; GANS, Joshua; GOLD-FARB, Avi (ed.). The economics of artificial intelligence: an agenda. Chicago: The University of Chicago Press, 2019. p. 439-462. (National Bureau of Economic Research Conference Report).

من منظور الكثيرين شيئاً قد يزيد من تكلفة إدارة البيانات دون تقديم فائدة حقيقية؛ إلا أن موقف العديد من أصحاب المصلحة في العلاقة بين الخصوصية والابتكار قد تغير، فقد اعتُبرَ حقاً أساسياً جرى الاعتماد عليه كميسر للابتكار؛ تأسيساً على أن ثقة المستخدم تُعدُّ أمراً أساسياً للقيام بالأعمال التجارية، والخدمات التي تقوم على البيانات⁽¹⁾.

بالإضافة إلى بناء الثقة من خلال إثبات المسؤولية في عملية معالجة البيانات الشخصية؛ حيث تستخدم الشركات أدوات حماية الخصوصية في عدة مجالات؛ منها: تخزين البيانات، الأرشيف. النهج الاستباقي للخصوصية: يعني أن الإطار القانوني لم يتمّ تقليصه؛ بل أخذ على محمل الجد، مما يجعل الأمر أسهلّ كثيراً، وبعبارة أخرى؛ فإنّ النظرة الكاملة لا تقتصر على القانون وحده؛ بل تمتدُّ إلى الإجراءات الإضافية المتخذة لحماية الخصوصية، والتي قد تتطلب جهداً أكبر، لكنه سوف يعود بالنفع على المدى المتوسط والطويل، بالإضافة إلى المواقف المسؤولة لتلك الشركات - من وجهة اجتماعية - سوف تُرضي العملاء، وستخضع مسؤولية خصوصية البيانات لتحوّل مماثل.

لكن الخصوصية كمحرك للابتكار لا تزال تواجه تحديات؛ أبرزها:

- **الرُّبُحِيَّة:** قد لا تكون الحلول المتوائمة مع الخصوصية مُربحة مثل النماذج التقليدية.
- **نماذج الأعمال:** قد تتعارض القواعد الجديدة للخصوصية مع نماذج الأعمال المتواجدة.
- **القيمة الفردية:** انخفاض قيمة الخصوصية بالنسبة للأفراد؛ فقد لا يُقدِّم المستخدمون الأولوية للخصوصية بشكل كافٍ على نحوٍ يبرّر دفع مبلغٍ إضافي يقابلها.
- **الاختلافات الثقافية:** يُمكن أن تختلف توقّعات الخصوصية باختلاف الثقافات.

(1) BACHLECHNER, Daniel; VAN LIESHOUT, Marc; TIMAN, Tjerk. Privacy as enabler of innovation. In: FRIE-DEWALD, Michael; ÖNEN, Melek; LIEVENS, Eva; KRENN, Stephan; FRICKER, Samuel (ed.). Privacy and identity management: data for better living: AI and privacy. Cham: Springer, 2020. p. 3-16. (IFIP AICT Tutorials, v. 576).

الفارق في المهارات: قد لا تكون هناك قوّة عاملة تمتلك الخبرة والمعرفة اللازمة في مجال الخصوصية.

الثغرات التنظيمية: قد لا تُعالج اللوائح الموجودة مخاوف الخصوصية بشكل كافٍ.

ومن ثم؛ فإن القيود التقنية ليست وحدها السبب في وجود هذه الصعوبات، ولكن أيضاً التنظيم غير السليم قد يتسبب كذلك في حدوث تلك الصعوبات، وحالياً؛ فإن الممارسة التي تقوم بها تلك الشركات تُعتبر ضعيفة التنظيم؛ مما يؤدي إلى قيامها بإخفاء الممارسات الحقيقية عن الجمهور، التعتميم على المعلومات التي يتم الكشف عنها للمستهلكين، أو إلقاء اللوم على عوامل أخرى متعددة (القضاء والقدر، القوّة القاهرة، فعل المستهلك)؛ باعتبار أنها من تسببت بذلك الضرر.

وفي هذا الصدد، هناك حاجة إلى مزيد من التغييرات؛ لتوفير مزيد من الشفافية في تقديم ممارسة البيانات نحو النتائج الضارة، ولترجمة النتائج إلى حوافز تؤثر بشكل مباشر على اختيار الشركات لممارسة البيانات؛ فهذه التغييرات لا تستطيع إبطاء التقدم التكنولوجي، أو إنهاء جدوى الشركات، ومع ذلك؛ فإن اللوائح ينبغي أن تهدف إلى المساعدة في بناء ممارسة بيانات صديقة للمستهلك، تتفّ بعيداً عن الممارسات الضارة، ومن ثمّ تعزز الابتكارات التي تحترم حاجة المستهلك إلى الخصوصية، وأمن البيانات.

وتجدر الإشارة إلى أن هناك العديد من الطرق للتعامل مع الحوافز غير المناسبة من خلال «التشريعات الجديدة»؛ حيث يمكن سنّ قوانين لفرض حماية خصوصية البيانات. التنظيم الذاتي للصناعة: يمكن للصناعات تطوير معايير الخصوصية الخاصة بها وإنفاذها. أحكام المحاكم: يمكن للمحاكم أن ترسي سوابق قانونية من خلال القضايا المميزة. تدابير حماية المستهلك: يمكن اتخاذ تدابير لتمكين المستهلكين من حماية خصوصيتهم؛ ولعل أهمها ما يلي⁽¹⁾:

التنظيم الأمني: التحكم غير المناسب في جودة الخصوصية، أمن البيانات قد يترتب عليه عواقب عشوائية مُزعجة؛ مثل (سرقة الهوية، الاحتيال)، بالإضافة إلى أن الطرق التي تُقرّر الشركات استخدامها للتعامل مع بيانات المستهلكين لا يمكن ملاحظتها - في معظم الحالات - من قبل المستهلكين النهائيين.

(1) JIN, Op. Cit.

وَيُمْكِنُ حُلُّ تلك المشكلة في القيام بالتنظيم المباشر لعملية معالجة البيانات عن طريق (وضع شروط مُسَبَّقة يجب أن تتقيّد بها الشركات عند تخزين ومعالجة البيانات الشخصية، المعايير التي يجب مراعاتها فيما يتعلق بعمليات التفتيش والتدقيق الدورية.... وما إلى ذلك)، لكن هذه اللوائح تقوم على افتراض مفادُه أنَّ الممارسة الجيدة أو السيئة سوف تكون معلومة، إلا أنه من الناحية الواقعية ليس من السهل إيجادها في مجال البيانات؛ ويرجع ذلك إلى أنَّ التطور التكنولوجي السريع للقطاع سوف يُؤدّي بالضرورة إلى صعوبة قيام السلطات العامة (القضاة، السياسيين، اللجان الفنية) بتقييم الممارسات الجيدة؛ ومن ثم يكون من الصعب ضمان تحديث اللوائح مع كل جولة من التقدم التكنولوجي.

إفصاح الشركة والنهج المعتمد على الاختيار المستقل للمستهلك: يُمكن هذا النهج المستهلكين من اتخاذ خيارات مستنيرة من خلال مطالبة الشركات بالكشف عن ممارسات بياناتها، وحتى يُحقّق هذا النهج الفعالية المرجّوة منه يجب أن يكون المستهلكون قادرين على اتخاذ أفضل الخيارات؛ بشرط أن يكون لديهم معلومات كافية للقيام بذلك.

لكن هذا النهج غير فعال بالنسبة للخصوصية، وأمن البيانات؛ لعدّة أسباب تكمن في:

١- ثبت علمياً - وعلى نطاق واسع - أن معظم المستهلكين لا يقرأون الشروط المتعلقة بممارسات الخصوصية.

٢- معظم الشركات كثيفة البيانات قد لا يكون لديها تفاعل مباشر مع المستهلك؛ مما يُؤدّي إلى صعوبة قيامهم بالاختيار السليم؛ بسبب عدم قدرتهم على تقييم الممارسات المختلفة للبيانات، بالإضافة إلى عدم معرفتهم بالخيارات المتاحة لتخفيف الضرر المحتمل.

٣- ممارسات البيانات الخاصة بالشركات قد تتغيّر في كثير من الأحيان - في ضوء التقدم التكنولوجي -؛ لذا فإن تقديم إخطارات محدّثة للمستهلكين قد يكون غير عملي، أو - في كثير من الأحيان مستحيل.

التنظيم الذاتي: يفترض هذا النهج - أنه نظراً للمعرفة الكبيرة للشركات بتكنولوجيا

وممارسة البيانات -؛ فإنها سوف تكون في وضع أفضل من سلطات الدولة لتحديد أفضل الممارسات.

في الواقع، يرى المؤلفون كـ Katyal⁽¹⁾ أنه من غير المُجدي النظر فقط إلى دور الدولة - المترددة جداً - في معالجة المسائل المتعلقة بالمساءلة القانونية؛ كما ينبغي أن يغطي التركيز على تنظيم المساءلة القانونية طرقاً أخرى لضمان الشفافية والمساءلة التي نشأت في ظل الصناعة الخاصة.

إلا أن الواقع الحالي يُشير إلى أن الأنشطة التي تُثير أكبر المخاوف بشأن (معالجة البيانات، التمييز، الخصوصية وأمن البيانات) هي تلك المتعلقة بالشركات دون الدول؛ ومن ثم فإن ممارسات التنظيم الذاتي؛ مثل مدونات السلوك، والبيانات الرسمية ذات التأثير، وحماية المبلغين، يمكن أن تُشجّع على الاهتمام الناشئ من الداخل نحو تطبيق الحقوق الأساسية، لكن التاريخ يُشير إلى أن التنظيم الذاتي قد لا يحدث بدون التهديد الذي يُشكله التنظيم القانوني للدولة، ومن ثم يرى البعض أن جهود الحكومة يجب أن تستكمل ولا تستبدل بمحاولات الشركات الصناعية بناءً التنظيم الذاتي⁽²⁾.

ومع ذلك؛ فإن هناك عقبات فنية فيما يتعلق ببناء تنظيم ذاتي فعال؛ حيث يحاول العديد من المنظمات تطوير أنظمة التصنيف المتعلقة بممارسة البيانات؛ إلا أنه لا توجد معلومات شاملة ومُحدّثة تتعلق بممارسة البيانات الخاصة بكل شركة؛ مما يجعل من الصعب تقييم جهودها في مجال التنظيم الذاتي.

تعريف ومتطلبات الالتزامات المتعلقة بالخصوصية واستخدام البيانات كحقوق: لتحقيق الالتزامات المتعلقة بالخصوصية في الممارسة العملية، اتبع الاتحاد الأوروبي نهج الخصوصية؛ باعتباره جزءاً من حقوق الإنسان؛ مما يقيد حقوق النقل والتعاقد؛ لذا فقد اعترف الاتحاد الأوروبي بالحق الفردي في الوصول إلى البيانات ومعالجتها وتصحيحها ومسحها في اللائحة العامة لحماية البيانات (GDPR)؛ لأنه من المبكر جداً الحديث عن أن هناك تأثيراً بارزاً ملموساً لللائحة العامة لحماية البيانات حتى الآن.

(1) KATYAL, Sonia K. Private accountability in the age of artificial intelligence. UCLA Law Review, [s. l.], v. 66, n. 1, p. 54-141, Jan. 2019. Available at: <https://www.uclalawreview.org/private-accountability-age-algorithm/>. Access on: July. 20, 2024.

(2) JIN, Op. Cit.

إلا هناك العديد من التحديات التي تواجه قابليتها للتطبيق - والتي قد تُعيق الابتكارات المُستندة إلى البيانات -؛ إذ يجب على المُبتكر أن يحصل مُقدِّماً على حقوق استخدام البيانات من عدة أطراف:

فيما يتعلق بالعديد من المنتجات التي تستخدم البيانات (السيارات ذاتية القيادة على سبيل المثال)؛ فإن البيانات لا تنشأ إلا في الوقت الذي يتفاعل فيه المُستخدم مع النظام؛ لذا فإنه يتم الحصول عليها من أطراف ثالثة؛ مثل (الشركات التي تُقدِّم خدمات الـ GPS، وشركات التأمين على المركبات....)، والذي من شأنه أن يُثير شكوكاً جديّة حول مَنْ يجب أن تُسبب إليه البيانات؛ سواء كان (المستخدم، أو المنتج، أو الطرف الثالث).

٢- على فرض، تحديد ملكية البيانات بوضوح في اللوائح العامة؛ فإن ذلك لا يعني الالتزام الكامل؛ فالقرصنة والتزوير أمثلة جيّدة على الانتهاكات التي قد تحدث.

وأخيراً، تُصبح مسألة تنظيم الخصوصية أكثر تعقيداً بسبب الخصوصية التي تتمتع بها كل مُنظمة تعمل معها؛ فعلى سبيل المثال: عندما يتعلق الأمر بالمنظمات التي تُقدِّم مساعدات إنسانية (مثل الصليب الأحمر)؛ فإن الامتثال لمبادئ حماية البيانات ليس كافياً؛ حيث يجب أن تمتثل هذه الجهات الفاعلة أيضاً للمبادئ الإنسانية لضمان تقديم مساعدة مُحيّدة ومُحيّدة لا تُضرُّ بالمستفيدين بأيّة طريقة؛ لذلك قام Barboza، Jasmontaitè-Zaniewicz and Diver⁽¹⁾ بتحليل نظام افتراضي للتعرف على الوجه يعتمد على الذكاء الاصطناعي، والذي يساعد المنظمات في جهودها لتحديد الأشخاص المفقودين، وقد أدرك العلماء أن مثل هذه الأنظمة يُمكن أن تُخلق مخاطر، من خلال توفير معلومات عن الأشخاص المفقودين يُمكن استخدامها من قبل أطراف ثالثة، لتحديد تلك الفئات الضعيفة واستهدافها؛ لذا لا ينبغي تنفيذ هذا النظام إلا بعد تقييم شامل للآثار المترتبة عليه؛ لضمان التزامه بحماية البيانات والمبادئ الإنسانية معاً؛ وبالتالي يجب أن تُوائم المبادئ الإنسانية؛ مثل (الالتزام بعدم التسبب بضرر، مشاركة المستفيدين، بناء القدرات المحلية، المسؤولية) مع تلك المتعلقة بحماية البيانات؛ مثل: تقييد الغرض من الاستخدام، أمن البيانات، العدالة في مواجهة النزاعات التمييزية المحتملة.

(1) BARBOZA, Júlia Zomignani; JASMONTAITÈ-ZANIEWICZ, Lina; DIVER, Laurence. Aid and AI: the challenge of reconciling humanitarian principles and data protection. In: FRIEDEWALD, Michael; ÖNEN, Melek; LIEVENS, Eva; KRENN, Stephan; FRICKER, Samuel (ed.). Privacy and identity management: data for better living: AI and privacy. Cham: Springer, 2020. p. 161-176. (IFIP AICT Tutorials, v. 576).

النتائج:

خلص البحث إلى النتائج الآتية:

التطبيقات التي تُستخدم الذكاء الاصطناعي يُمكن أن تُثير مخاوف تتعلق بالخصوصية؛ أهمها:

- استمرار البيانات المخزنة: البيانات الشخصية التي يُنشئها أصحابها تظل مُخزّنة لفترة طويلة تتجاوز حياة أصحابها؛ وذلك بسبب التكلفة المنخفضة نسبياً لتخزين البيانات.

- إمكانية إعادة استخدام البيانات الشخصية: قد تتجاوز عملية جمع البيانات الشخصية الهدف المرجو منها؛ مما يثير مخاوف بشأن العواقب غير المقصودة؛ المتمثلة في إعادة استخدام البيانات الشخصية التي أنشئت فيما بعد (بواسطة خدمات الأمن، أو من قبل الدولة، أو عن طريق شركات التسويق أو التأمين.. إلخ).

- تدفق البيانات: قد تُسجّل هذه التطبيقات بيانات شخصية أخرى لا تتعلق بالشخص «موضوع البيانات» - التي تتعلق به البيانات المُسجّلة -؛ على الرغم من أن هؤلاء الأشخاص لم يختاروا إنشاء بيانات شخصية عنهم؛ الأمر الذي قد تكون له تداعيات مستقبلية سلبية تتعلق بالحق في الخصوصية.

- مبدأ موافقة صاحب البيانات على معالجة بياناته الشخصية فقد قوّته بشكل كبير في عصر البيانات الضخمة والذكاء الاصطناعي؛ ويرجع ذلك لعدة أسباب: أولاً: التراكم الهائل للبيانات، والتقاطها الذي يترتب عليه إقبال كاهل المبادئ القانونية المتعلقة بالإجماع على حماية البيانات الشخصية. ثانياً: أن الأفراد غير مستعدين للتخلي عن استخدام تكنولوجيا المعلومات والاتصالات. ثالثاً: المجتمعات لا تمتلك ثقافة قوية بشأن الخصوصية؛ مما يجعل الضمانة الخاصة بالموافقة غير حقيقية، وتفقر للفعالية الكافية؛ الأمر الذي تضخى معه الموافقة بمثابة «تفويض مطلق» لـ«التدفق غير المنضبط للبيانات الشخصية»؛ مما يُضعف دور الموافقة حتى يصبح دورها رمزياً؛ الأمر الذي يترتب عليه في نهاية المطاف إلى الانتهاك المقصود للخصوصية، وإضعاف أنظمة الحماية.

- إذا كان استخدام الذكاء الاصطناعي يهدد الحق في الخصوصية لعوامل عدة؛ أبرزها: (جمع البيانات الشخصية من كل مكان، المشاكل المتعلقة بتحديد الهوية، الافتقار إلى المساءلة القانونية)؛ إلا أنه يمكن أن يساعد في التخفيف من معظم التحديات المتعلقة بالخصوصية الرقمية - التي يُعتبر استخدامها وتطويرها بمثابة تهديد للخصوصية - حيث تعمل التقنيات الحديثة المدمجة في الخصوصية التفاضلية والتعلم العميق على تقليل كمية البيانات الحساسة التي يتم جمعها وتخزينها ومشاركتها مع الأطراف الثالثة؛ مما يسمح للشركات بمواصلة التعلم بطريقة فعالة حول أنشطة مستخدميها، ويمكن للمُدققين، ومسؤولي الذكاء الاصطناعي تمثيل مصالح المستهلكين خلال جمع البيانات وتصحيح الدوافع، ومراقبة إمكانية إعادة تحديد الهوية، أو النتائج التي تُسَم بطابع ينطوي على تمييز بين الأفراد في الأنظمة الأخرى.
- أدى التوسع في استخدام الأجهزة القابلة للارتداء المزودة بتقنيات الذكاء الاصطناعي إلى جمع كميات ضخمة من البيانات الشخصية حول مستخدميها، كما قدمت التحليلات الخاصة بها توقعات واستنتاجات ليست بديهية وغير مُحَقَّقة حول تلك البيانات؛ مما أدى إلى خلق فرص جديدة لاتخاذ القرار بطريقة تمييزية جائرة، على نحو يضر بخصوصية وسُعة الأشخاص « موضوع البيانات ».
- يلعب الذكاء الاصطناعي دوراً هاماً في مجال الصحة الرقمية؛ حيث يُقدّم عدداً لا يُحصى من التقنيات المتقدمة التي يجب أن تكون متوافرة لمساعدة الأطباء عن طريق السماح بتحليل البيانات؛ لتسهيل الوصول إلى أنماط مختلفة من المعرفة في المجالات المختلفة للعلوم الصحية، ولكي يحقق الذكاء الاصطناعي ذلك الهدف المنشود يجب أن تكون البيانات التي جمعها « نظيفة » لأن البيانات عالية الجودة هي الأساس لتحقيق نماذج عالية الدقة، إلا أن التحدي الأكبر الذي يواجه معظم أنظمة الذكاء الاصطناعي يتمثل في عدم القدرة على التمييز بين البيانات المتحيزة أو التالفة، من البيانات عالية الجودة؛ فتلك الأنظمة قادرة على معالجة البيانات، لكنها لا تملك القدرة على تقييم عملية تكوين تلك البيانات؛ فقد تلبّي تلك البيانات متطلبات معينة من الناحية الفنية، إلا أنه - في الواقع -

قد يكون محتواها متحيزاً أو تالفاً، بالإضافة إلى ذلك؛ لا يستطيع المتخصصون في مجال معالجة البيانات - دائماً - التمييز بين البيانات الفاسدة، أو البيانات عالية الجودة؛ خاصةً إذا لم يتمكنوا من معرفة الكيفية التي تم من خلالها جمع ومعالجة تلك البيانات.

- أدى استخدام الخوارزميات التنبؤية إلى تغيير واقع الأنواع المختلفة للتجارة والخدمات؛ فالأسعار يُمكن أن تُحتسب الآن وفقاً للمتغيرات الخارجية والسلوكية دون المتغيرات الخارجية العامة وحدها، ومع ذلك، وبقدر ما يبدو تفريد الأسعار عادلاً، يُمكن أن يؤدي إلى إنشاء أشكال جديدة وغير مُتوقعة من التمييز، تختلف عن أنواع التمييز الحالية القائمة على التقسيم الاجتماعي الطبقي العام.

التوصيات:

- لمعالجة المخاوف المتعلقة بالخصوصية التي تثيرها التطبيقات التي تُستخدم الذكاء الاصطناعي، وبهدف تحقيق الموازنة بين الحق في الخصوصية، والمحافظة على القدرة التنافسية لقطاع الذكاء الاصطناعي، يُمكن تبني سياسات عامة يُمكن أن تحقق مثل هذا التوازن؛ مثل: التمويل العام لقطاعات الصحة الرقمية، وتشجيع تطوير الذكاء الاصطناعي الأقل تعرّضاً للبيانات الشخصية؛ مثل برنامج OpenAI من Google.
- نظراً لفقدان مبدأ موافقة صاحب البيانات على معالجة بياناته الشخصية لقوّته بشكل كبير في عصر البيانات الضخمة والذكاء الاصطناعي، مما جعل الضمانة الخاصة بالموافقة غير حقيقية، وتفتقر للفعالية الكافية، ولمعالجة هذه المشكلة يُمكن استخدام طريقة «خصوصية التصميم»؛ والتي تعني: الالتزام ببرمجة الأدوات التكنولوجية بطريقة تجعل من المستحيل عليها انتهاك قانون حماية البيانات؛ الأمر الذي يضمن خصوصية البيانات الشخصية؛ بعيداً عن الامتثال للمعايير والإجراءات المتعلقة بقانون حماية البيانات. ولكي يتحقق التنفيذ التدريجي لتقنيات الخصوصية؛ يجب اتخاذ عدة خطوات: ١- إنشاء هيئات تنظيمية لحماية البيانات، تلعب دوراً مركزياً في هندسة الخصوصية، وتقنيات تعزيز الخصوصية في المشاريع القادمة من القطاع العام. ٢- إصدار المبادئ

التوجيهية بشأن نص المادة (٢٥) من اللائحة العامة لحماية البيانات، تتضمن عبارات صريحة وقوية؛ يُطلب من خلالها، بوضوح، تنفيذ تقنية الخصوصية. ٣- مكافأة الأمثلة الجيدة لهندسة الخصوصية، بدلاً من معاقبة الإخفاقات.

- استخدام التقنيات الحديثة، وإنترنت الأشياء (IOT)؛ للوصول إلى البيانات الشخصية يُمكن أن يهدد الحق في الخصوصية؛ لذا يُمكن اتخاذ بعض الإجراءات لتلافي الآثار السلبية الناتجة عن استخدام هذه البيانات؛ ومن بين تلك الإجراءات:

- اعتماد إجراءات صارمة لإخفاء هوية البيانات: تنفيذ عمليات إزالة هوية البيانات؛ بحيث لا يُمكن التعرف على المعلومات، أو ربطها، أو وصفها، أو الرجوع إليها، أو ربطها بشكل مباشر أو غير مباشر بفرد معين، أو قابل للتحديد.
- تنظيم ملكية البيانات: حيث يحق لأصحاب البيانات الوصول إلى بياناتهم الخاصة.

- لم تتطرق اللائحة العامة لحماية البيانات، وكافة التشريعات المتعلقة بحماية البيانات الشخصية إلى حماية الشخص «موضوع البيانات» من المخاطر الحديثة الناشئة عن التحليل الاستنتاجي؛ لذا يجب إجراء تعديل تشريعي بإدراج حق للشخص موضوع البيانات يُسمى «الحق في الاستدلالات المعقولة»؛ حتى يمكن تلافي المخاطر التي تمثلها «الاستنتاجات عالية الخطورة»؛ الناتجة عن تحليل البيانات الضخمة، والتي تضر خصوصية وسمعة الشخص «موضوع البيانات»؛ عن طريق توفير آلية تمكن أصحاب البيانات من الطعن على الاستنتاجات غير المعقولة.

- يجب ألا يقتصر تنظيم الحق في الخصوصية وأمن البيانات المتعلق باستخدام البيانات من قبل الشركات - خاصة البيانات التي تُستخدم كأساس للتطوير والابتكار التكنولوجي القائم على الذكاء الاصطناعي - على منع الممارسات الضارة بالخصوصية وأمن البيانات فحسب؛ بل ينبغي أن يُشجع الممارسات الجيدة التي تطوّر من خلال عملية الابتكار.

- نظراً للتقدم في تقنيات الحصول على البيانات الشخصية ومعالجتها، وكذلك

تكنولوجيا المعلومات والاتصالات - التي من بينها الذكاء الاصطناعي - بات من الضروري أن تُصاغ التشريعات المتعلقة بحماية الحق في الخصوصية بشكل تفصيلي وصارم؛ بحيث تُعتمد فيها تقنيات إخفاء الهوية والتسمية المستعارة فيما يتعلق باستخدام تقنيات الذكاء الاصطناعي.

- يتمثل التحدي الأكبر الذي يُواجه معظم أنظمة الذكاء الاصطناعي اليوم - كما أسلفنا - في عدم القدرة على التمييز بين البيانات المتحيزة أو التالفة، من البيانات عالية الجودة؛ وللتغلب على هذه المشكلة:
- يجب التركيز على المراحل المبكرة لعملية جمع البيانات؛ حيث تُؤدّي العوامل البشرية، ونُدرة التكنولوجيا المستخدمة في جمع البيانات إلى إفساد جودتها، لذا يجب إنشاء نظام للمسؤولية الكاملة يساهم في: ١- مراقبة العمل الحقيقي للشركات في جمع واستخدام وتخزين البيانات. ٢- قياس العواقب الناجمة عن ممارسة أنشطتها المتعلقة بالبيانات الشخصية للمستهلكين؛ وعلى الأخص الإدراك المُسبق للأعمال الضارة المنخفضة الاحتمالية. ٣- إنشاء علاقة سببية بين ممارسة البيانات عن طريق الشركات، والعواقب الناشئة عنها.
- العمل على إيجاد نموذج للذكاء الاصطناعي، يعتمد على شفافية البيانات يركّز على الكشف عن البيانات؛ وبالتالي فإن أنظمة التدقيق، وبرامج الشهادات التي تُديرها جهة حكومية يمكن أن تتحقق من شفافية الخوارزمية أو في حالة - غياب تلك المؤسسة - عن طريق إحدى المؤسسات الخاصة، والتي من شأنها - حال وجودها - أن تُشجّع القطاع الصناعي؛ ليكون سباقاً في اتخاذ خطوات لضمان موثوقية قواعد البيانات الشخصية الخاصة بهم.
- يجب ألا يقتصر تنظيم استخدام أدوات الذكاء الاصطناعي التي تتعامل مع البيانات الشخصية على حماية البيانات، ومبادئ الخصوصية؛ بل ينبغي أن يمتد هذا التنظيم إلى مسائل أخرى تتعلق بطبيعة نشاط المؤسسة التي تتعامل مع هذه التقنيات؛ لذا يجب بناء نهج تعاوني مُتعدد التخصصات يأخذ في اعتباره نوع المؤسسة التي تتعامل مع هذه التقنيات.
- شكلت المخاوف المتعلقة بالحق في الخصوصية - التي سببتها التطبيقات التي

تستخدم الذكاء الاصطناعي - تحديات جديدة للمعالجة القانونية للبيانات الشخصية؛ لتعارضها مع الطرق التقليدية التي يُمكن للأشخاص «موضوع البيانات» أن يقرروا من خلالها إنشاء بيانات شخصية؛ يُمكن استخدامها فيما بعد؛ لذا يجب تعديل التنظيم التشريعي للحق في الخصوصية؛ ليكون تنظيمًا شاملاً يأخذ في اعتباره كافة المخاطر الناتجة عن استخدام تقنيات الذكاء الاصطناعي؛ للوصول إلى حماية كاملة للحق في الخصوصية.

المراجع

References

- ALAMÄKI, Ari; MÄKI, Marko; RATNAYAKE, R. M. Chandima. Privacy concern, data quality and trustworthiness of AI-analytics. In: FAKE INTELLIGENCE ONLINE SUMMIT, 1., 2019, Pori, FI. Proceedings [...]. Pori, FI: Satakunta University of Applied Sciences, 2019. p. 37 -42. Available at: <http://urn.fi/URN:NBN:fi-fe2019051315372>. Access on: July. 20, 2024.
- ARORA, Chirag. Digital health fiduciaries: protecting user privacy when sharing health data. Ethics and Information Technology, [s. l.], v. 21, n. 3, p. 181-196, Feb. 2019. DOI: <https://doi.org/10.1007/s1067609499--019-x>. Available at: <https://link.springer.com/content/pdf/10.1007/s1067609499--019-x.pdf>. Access on July. 20, 2024.
- BACHLECHNER, Daniel; VAN LIESHOUT, Marc; TIMAN, Tjerk. Privacy as enabler of innovation. In: FRIEDEWALD, Michael; ÖNEN, Melek; LIEVENS, Eva; KRENN, Stephan; FRICKER, Samuel (ed.). Privacy and identity management: data for better living: AI and privacy. Cham: Springer, 2020. p. 316-. (IFIP AICT Tutorials, v. 576).
- BARBOZA, Júlia Zomignani; JASMONTAITÈ-ZANIEWICZ, Lina; DIVER, Laurence. Aid and AI: the challenge of reconciling humanitarian principles and data protection. In: FRIEDEWALD, Michael; ÖNEN, Melek; LIEVENS, Eva; KRENN, Stephan; FRICKER, Samuel (ed.). Privacy and identity management: data for better living: AI and privacy. Cham: Springer, 2020. p. 161176-. (IFIP AICT Tutorials, v. 576).
- CEVOLINI, Alberto; ESPOSITO, Elena. From pool to profile: social consequences of algorithmic prediction in insurance. Big Data & Society, [s. l.], v. 7, n. 2, p. 111-, July/Dec. 2020. DOI: <https://doi.org/10.11772053951720939228/>. Available at: <https://journals.sagepub.com/doi/pdf/10.11772053951720939228/>. Access on: July. 20, 2024.
- CHANG, Anthony. The role of artificial intelligence in digital health. In: WULFOVICH, Sharon; MEYERS, Arlen (ed.). Digital health entrepreneurship. Cham: Springer, 2020. p. 71- 81. (Health Informatics).
- COTINO HUESO, Lorenzo. Big data e inteligencia artificial: una aproximación a su tratamiento jurídico desde los derechos fundamentales. Dilemata, [s. l.],

año 9, n. 24, p. 1312017 ,150-. Available at: <https://www.dilemata.net/revista/index.php/dilemata/article/view/412000104>. Access on: July. 20, 2024.

- Dawei Jiang, Guoquan Shi. « Research on Data Security and Privacy Protection of Wearable Equipment in Healthcare Journal of Healthcare Engineering, Volume 2021.
- ELS, Andrea Scripa. Artificial intelligence as a digital privacy protector. Harvard Journal of Law & Technology, [s. l.], v. 31, n. 1, p. 2172017 ,235-. Available at: <https://jolt.law.harvard.edu/assets/articlePDFs/v3131/HarvJLTech217.pdf>. Access on: July. 20, 2024, p234235-.
- European Data Protection Supervisor (EDPS), Opinion 12015/: Mobile Health - Reconciling Technological Innovation with Data Protection, 21 May 2015, Brussels.
- EUROPEAN UNION. Regulation (EU) 2016679/ 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 9546//EC (General Data Protection Regulation). Brussels : EUR-Lex, 2016. Available at : <https://eur-lex.europa.eu/eli/reg/2016679/oj>. Access on: July. 20, 2024.
- Garcia-Mancilla, J., & Gonzalez, V. M. (2015). Stress quantification using a wearable device for daily feedback to improve stress management. Paper presented at the ICSH; Sano, A., & Picard, R. W. (2013). Stress recognition using wearable sensors and mobile phones. Paper presented at the 2013 Humaine Association Conference on Affective Computing and Intelligent Interaction.
- GIANNOPOULOU, Alexandra. Algorithmic systems: the consent is in the detail? Internet Policy Review, [s. l.], v. 9, n. 1, p. 119-, Mar. 2020. DOI: <https://doi.org/10.147632020.1.1452/>. Available at: <https://policyreview.info/articles/analysis/algorithmic-systems-consent-detail>. Access on: July. 20, 2024.
- Gloria González Fuster and Amandine Scherrer (2015), 'Big Data and Smart Devices and their Impact on Privacy ', under the coordination of the Centre d'Etudes sur les Conflits, Liberté et Sécurité (CCLS) and the Centre for European Policy Studies (CEPS), Policy Department C - Citizens' Rights and Constitutional Affairs European Parliament.

- HUMERICK, Matthew. Taking AI personally: how the E.U. must learn to balance the interests of personal data privacy & artificial intelligence. Santa Clara High Technology Law Journal, [s. l.], v. 34, n. 4, p. 3932018 ,418-. Available at: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss43/>. Access on: July. 20, 2024.
- ILIADIS, Andrew. Computer guts and swallowed sensors: ingestibles made palatable in an era of embodied computing. In: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). Embodied computing: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 120-.
- JIN, Ginger Zhe. Artificial intelligence and consumer privacy. In: AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi (ed.). The economics of artificial intelligence: an agenda. Chicago: The University of Chicago Press, 2019. p. 439462-. (National Bureau of Economic Research Conference Report).
- KATYAL, Sonia K. Private accountability in the age of artificial intelligence. UCLA Law Review, [s. l.], v. 66, n. 1, p. 54- 141, Jan. 2019. Available at: <https://www.uclalawreview.org/private-accountability-age-algorithm/>. Access on: July. 20, 2024.
- KAZGAN, Mehmet. Real challenge in digital health entrepreneurship: changing the human behavior. In: WULFOVICH, Sharon; MEYERS, Arlen (ed.). Digital health entrepreneurship. Cham: Springer, 2020. p. 715-. (Health Informatics).
- KELLER, Perry. The reconstruction of privacy through law: a strategy of diminishing expectations. International Data Privacy Law, [s. l.], v. 9, n. 3, p. 132152-, Aug. 2019. DOI: <https://doi.org/10.1093/idpl/ipz012>.
- LOBERA, Josep; FERNÁNDEZ RODRÍGUEZ, Carlos J.; TORRES-ALBERO, Cristóbal. Privacy, values and machines: predicting opposition to artificial intelligence. Communication Studies, [s. l.], v. 71, n. 3, p. 448465-, Mar. 2020. DOI: <https://doi.org/10.1080/10510974.2020.1736114/>.
- LUPTON, Deborah. Wearable devices: sociotechnical imaginaries and agential capacities. In: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). Embodied computing: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 49- 69.
- Nagtegaal et al. (2015), Internet of Things: Wearable Technology, Business Innovation Observatory, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, European Commission, February 2015.

- PEDERSEN, Isabel. Will the body become a platform? Body networks, datafied bodies, and AI futures. In: PEDERSEN, Isabel; ILIADIS, Andrew (ed.). Embodied computing: wearables, embeddables, ingestibles. Cambridge, MA: The MIT Press, 2020. p. 21- 48.
- PELTZ, James; STREET, Anita C. Artificial intelligence and ethical dilemmas involving privacy. In: MASAKOWSKI, Yvonne R. (ed.). Artificial intelligence and global security: future trends, threats and considerations. Bingley, UK: Emerald Publishing, 2020.
- ROHRINGER, Taryn J.; BUDHKAR, Akshay; RUDZICZ, Frank. Privacy versus artificial intelligence in medicine. University of Toronto Medical Journal, [s. l.], v. 96, n. 1, p. 51- 53, Jan. 2019. Available at <https://jps.library.utoronto.ca/index.php/utmj/issue/download/2376453#/page=52>. Access on: July. 20, 2024.
- RUBINSTEIN, Ira S.; GOOD, Nathaniel. The trouble with Article 25 (and how to fix it): the future of data protection by design and default. International Data Privacy Law, [s. l.], v. 10, n. 1, p. 3756-, Feb. 2020. DOI: <https://doi.org/10.1093/idpl/ipz019>.
- SOARES, Paulo Vinícius de Carvalho. A diluição das esferas de privacidade e de intimidade diante da era dos dados. In: LUCON, Paulo Henrique dos Santos; WOLKART, Erik Navarro; LAUX, Francisco de Mesquita; RAVAGNANI, Giovani dos Santos (coord.). Direito, processo e tecnologia. São Paulo: Revista dos Tribunais, 2020. p. 555574-. (Coleção Direito e Novas Tecnologias).
- STEIN, Amy L. Artificial intelligence and climate change. Yale Journal on Regulation, [s. l.], v. 37, n. 3, p. 8902020 ,939-. Available at: <https://www.yalejreg.com/print/artificial-intelligence-and-climate-change/> Access on: July. 20, 2024.
- Swan, M. (2012). Sensor mania! the internet of things, wearable computing, objective metrics, and the quantified self 2.0. Journal of Sensor Actuator networks, 1(3), 217 -253.
- TSCHIDER, Charlotte A. The healthcare privacy-artificial intelligence impasse. Santa Clara High Technology Law Journal, [s. l.], v. 36, n. 4, p. 4392020 ,443-. Available at: <https://lawecommons.luc.edu/cgi/viewcontent.cgi?article=1689&context=facpubs>. Access on: July. 20, 2024.
- TUCKER, Catherine. Privacy, algorithms, and artificial intelligence. In:

AGRAWAL, Ajay; GANS, Joshua; GOLDFARB, Avi (ed.). The economics of artificial intelligence: an agenda. Chicago: The University of Chicago Press, 2019. p. 423438-. (National Bureau of Economic Research Conference Report).

- WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. Columbia Business Law Review, [s. l.], v. 2.019, n. 2, p. 494620-, May 2019. DOI: <https://doi.org/10.7916/cblr.v2019i2.3424>. Available at: <https://journals.library.columbia.edu/index.php/CBLR/article/view/3424>. Access on: July. 20, 2024.
- YANISKY-RAVID, Shlomit; HALLISEY, Sean K. «Equality and privacy by design»: a new model of artificial intelligence data transparency via auditing, certification, and safe harbor regimes. Fordham Urban Law Journal, [s. l.], v. 46, n. 2, p. 4282019 ,486-. Available at: <https://ir.lawnet.fordham.edu/ulj/vol46/iss25/>. Access on: July. 20, 2024.
- B- websites:
- <https://strongholddata.com/wearable-technology-in-healthcare/>

