القاضى/ عبد الرحمن جمال يعقوب
قاض بمجلس الدولة المصري

الحق المشترك في البيانات في ظل تقنية الذكاء الاصطناعي:

«دراسة نقدية لتنظيم البيانات الشخصية»

المراسلة: القاضى/ عبد الرحمن جمال يعقوب
قاض بمجلس الدولة المصري

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v4i2.206

البريد الإلكتروني: abdelrahman.gamal1@yahoo.com

نسق توثيق البحث:

عبد الرحمن جمال يعقوب، الحق المشترك في البيانات في ظل تقنية الذكاء الاصطناعي: دراسة نقدية لتنظيم البيانات الشخصية المجلد ٤ العدد ٢، أكتوبر ٢٠٢٤.
صفحات ٧٩-١٢٨

الملخص

الدراسة الحالية تتناول بالبحث والنقد فعالية نموذج التحكم الفردي الذي اتبعته اللائحة الأوروبية العامة لحماية البيانات وبالتبعية قانون حماية البيانات الشخصية المصري وذلك في مواجهة تقنية الذكاء الاصطناعي. وتلك فلسفة تشريعية تتخذ من الشخص الفرد محورًا للتشريع وتعني بتحقيق الحماية من خلال تمكينه من التحكم، وفي حالة البيانات الشخصية، تمكين صاحب البيانات من التحكم في بياناته عبر تقرير كيف سيتم جمعها ومعالجتها.

في سبيل ذلك، تعرض الدراسة لتأثير الذكاء الاصطناعي على الخصوصية والبيانات الشخصية من منظور تحليلي مُستحدث بأن قدمت مفهوم «دورة تأثير البيانات» كإطار لفهم مخاطر الذكاء الاصطناعي على الخصوصية والبيانات الشخصية. وفقًا لهذا الطرح، تمر البيانات بأربع مراحل بدءًا بالجمع، ومرورًا بالمعالجة والنشر، ووصولًا للتغذية العكسية والتكيف. تشتمل كل من هذه المراحل على مخاطر مستقلة، إلا أنه بفضل الذكاء الاصطناعي، فإنها مجتمعة تمثل دورة مصممة لضمان الحفاظ على تأثير مستمر على صاحب البيانات.

يتكشف عبر الدراسة الحالية أن التحكم الفردي قد يُضِر بصاحب البيانات نفسه والغير معه، حيث إنه بفضل القدرة التحليلية والاستنتاجية للذكاء الاصطناعي يمكن تكوين مجموعات خوارزمية افتراضية من الأفراد المشتركين في السمات والآراء بحيث تصب البيانات الشخصية لأحدهم في فهم البقية. وبغرض فهم هذه الظاهرة، تستعين الدارسة بقياسٍ اقتصادي بغية فهم علاقة التحكم الفردي بالمجموعة.

تنتهي الدراسة الحالية إلى نتيجتين رئيستين، أولاهما أنه في مواجهة الذكاء الاصطناعي، يفقد صاحب البيانات القدرة الحقيقية على التحكم في بياناته، وثانيتهما أنه من الأجدى النظر إلى الخصوصية والبيانات الشخصية باعتبارهما حق مشترك ذو تأثير مواز على المجموعة، وليس حق فردي فحسب.

Abstract

This study examines and critiques the effectiveness of the individual-control model adopted by the EU General Data Protection Regulation (GDPR) and, subsequently, Egypt's Personal Data Protection Law, in the face of artificial intelligence. This legislative philosophy places the individual at the centre, seeking to protect them by enabling personal control. In the context of personal data, it aims to empower the data subject to determine how their data are collected and processed.

To advance this perspective, the study investigates the impact of AI on privacy and personal data from a novel analytical perspective by introducing the concept of the «Data Influence Cycle» as a framework for understanding the risks AI poses to privacy and personal data. According to this framework, data pass through four phases: collection, processing, dissemination, and eventually feedback and readjustment. While each of these phases involves its own distinct risks, artificial intelligence interconnects them into a continuous cycle designed to exert an ongoing influence on data subjects.

The study reveals that individual control may inadvertently harm not only the data subject but also others. Due to AI's analytical and inferential capabilities, it can create virtual algorithmic groups of individuals who share common traits and beliefs, such that one person's data inform the understanding of everyone else in those groups. To shed light on this phenomenon, the study employs an economic analogy to evaluate how individual control affects these broader groups.

Ultimately, the study reaches two primary conclusions. First, when confronted with AI, data subjects lose meaningful control over their personal data. Second, it is more efficient to regard privacy and personal data as a collective right that affects the group, rather than as a purely individual right.

المقدمة

شهـد العقـدان الماضيان طفـرةً لا تخطئها عين في مجال تقنيـة المعلومات، امتدت أطرافهـا لتمس بكافـة مناحي الحياة، وجعلت الحصول علـى الخدمات وسرعة إنجاز المهام أكبر بكثير مما كانت عليه. إلا أن ذلك التطور لم يكن دون ثمن، إذ برزت البيانات الشخصيـة وخصوصية الأفـراد كوقود لذلك الحراك المتسـارع، فظهرت مفاهيم مثل البيانـات الضخمـة حيث يتم معالجـة كميات ضخمة من البيانـات من خلال حواسيب عملاقة لتتمكن من استخراج أنماط واتجاهات السلوك المختلفة [١].

واقترن ذلك بتطور تقنية الذكاء الاصطناعي التي تربطها بالبيانات عامةً والبيانات الشخصيـة خاصةً علاقـةً مزدوجة يمكن وصفها بأنها علاقة تأثـر وتأثير؛ فمن ناحية يتغـذى الذكاء الاصطناعي على البيانات وذلـك لتدريبه وتطويره، حيث يلزم كي يؤدي الـذكاء اصطناعـي وظيفة معينة أن يتم تعريضه لقدر كبير مـن البيانات المتعلقة بتلك الوظيفة، بذات الشاكلة التي يتم تدريب الموظف الجديد على عمله. وبدون تلك البيانات لم يكـن الذكاء الاصطناعـي ليتطور بالشكل الـذي نشهده الآن، وبالتـالي فإن تقنيات الذكاء الاصطناعي تتأثر بشكل جوهري بكم وجودة البيانات.

ومن ناحية أخرى، فإن الذكاء الاصطناعي قد اكتسب نتيجةً لذلك قدرات فائقة على الرصـد والتحليل والفهم،[٢] فتزايـدت قدرته على فهم البيانات وتحويلها إلى معلومات ذات قيمة يتم إعـادة توجيهها لأصحاب البيانات مرةً أخرى من أجل التأثير عليهم[٣]. وهـو أثناء ذلك صارت لديه القـدرة على إظهار جوانب وأبعـاد للبيانات الشخصية لم تكـن موجـودة أو ملحوظة من قبـل، حتى أن العديد مـن الدراسات قد أشـارت إلى أن تطبيقـات مثل وسائل التواصل الاجتماعي صـارت تفهم المستخدمين وميولهم أكثر من فهم المستخدمين لأنفسهم[٤].

(1) Viktor Mayer-Schönberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (Houghton Mifflin Harcourt 2013), 73.
(2) Michal Kosinski, 'Evaluating Large Language Models in Theory of Mind Tasks' (2024) 121 Proceedings of the National Academy of Sciences.
(3) Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Columbia Business Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829> accessed 12 December 2024.
(4) Wu Youyou, Michal Kosinski and David Stillwell, 'Computer-Based Personality Judgments Are More Accurate than Those Made by Humans' (2015) 112 Proceedings of the National Academy of Sciences 1036.

فـي ظل محاولات اللاحـق بالوثبـات المتتالية فـي مجـال تقنية المعلومـات والذكاء الاصطناعـي والحد مـن آثارها على الخصوصيـة والبيانات الشخصيـة، شرع المشرع الوطنـي والمقارن فـي سـن قوانين حماية البيانـات الشخصية، فنجـد النموذج الرائد للاتحـاد الأوروبـي متمثـلاً فـي اللائحـة العامـة لحمايـة البيانـات (General Data Protection Regulation)[١] التـي تبع نهجها العديد مـن التشريعات الوطنية، بما فـي ذلك قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠.[٢]

وقـد ارتكزت اللائحة الأوروبية علـى نموذج حماية بيانات قوامـه التحكم الفردي، وتلـك فلسفة تشريعية -غـير قاصرة على اللائحة العامة لحمايـة البيانات- تتخذ من الشخصـ الفرد محورًا للتشريع وتعنـي بتحقيق الحماية من خلال تمكينه من التحكم، وفـي حالة البيانات الشخصية، تمكـين صاحب البيانات[٣] من التحكم في بياناته عبر تقرير كيف سيتم جمعها ومعالجتها[٤].

الدراسـة الحالية تتناول بالبحث والنقد فعاليـة نموذج التحكم الفردي الذي اتبعته اللائحـة الأوروبية العامة لحماية البيانات وبالتبعية قانـون حماية البيانات الشخصية المصـري وذلـك في مواجهة تقنيـة الذكاء الاصطناعـي. تنتهي الدراسـة الحالية إلى نتيجتين رئيستين، أولاهمـا أنه في مواجهة الذكاء الاصطناعي، يفقد صاحب البيانات القـدرة الحقيقيـة علـى التحكـم فـي بياناتـه، وثانيتهما أنه مـن الأجـدى النظر إلى الخصوصيـة والبيانات الشخصية باعتبارهما حق عام ذو تأثير مشترك على المجموعة وليس حق فردي فحسب.

إشكالية البحث

فـي ظـل التطور السريع في تقنية الـذكاء الاصطناعي وقدرته التـي تفوق تدريجيًا

(١) اللائحـة العامة لحماية البيانات، الاتحـاد الأوروبي، لائحة رقم (EU) ٦٧٩/٢٠١٦، الصادرة عن البرلمان الأوروبي ومجلس الاتحاد الأوروبي بتاريخ ٢٧ أبريل ٢٠١٦، بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وحرية نقلها، والمنشورة في الجريدة الرسمية للاتحاد الأوروبي بتاريخ ٤ مايو ٢٠١٦، وسارية اعتبارًا من ٢٥ مايو ٢٠١٨.

(٢) ذلك ما ذهب إليه بعض المحللون، ويوافقه استخدام ذات التعريفات، والاعتماد على مزيج من المبادئ والقواعد وهي خصيصة تشريعية سبق فيها الاتحاد الأوروبي، وغير ذلك من المظاهر.

(٣) تستخـدم هـذه الدراسة تعبير «صاحب البيانات» بدلًا من «الشخص المعني بالبيانـات» الذي استخدمه قانون حماية البيانات الشخصية المصري.

(4) Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 478.

استيعـاب الإنسـان، يُنظـر إلى البيانـات الشخصيـة باعتبارهـا بوابة تطويـر الذكاء الاصطناعـي من ناحية، والتأثير على أصحاب البيانات من ناحية أخرى. لما كان ذلك، فإن الدراسة الحالية تدور حول الإشكالية البحثية:

مدى ملائمـة اعتبار الحق في الخصوصية والبيانات الشخصية حق خاص فحسب في مواجهة تطبيقات تقنية الذكاء الاصطناعي.

وفي سبيل تناول هذه الإشكالية، ستعالج الدراسة الأسئلة البحثية التالية:

١- مـا هي العلاقـة بين الـذكاء الاصطناعي مـن ناحيـة والخصوصيـة والبيانات الشخصية من ناحية أخرى؟

٢- مـا مدى جدوى التحكم الفردي كنهج لتشريعات البيانات الشخصية خاصةً في ضوء التنظيم المصري الأوروبي المقارن؟

٣- إلى أي مدى يمكن اعتبار الخصوصية والبيانات حق مشترك؟

أهمية البحث

تأتـي هذه الدراسة بين قليلات في الفقه القانوني العربـي التي تتناول بحثًا قانونيًا تأصيليًـا حول مجال حمايـة البيانات الشخصية. بينما نما هـذا الفرع القانوني بشكل كبير في السنوات القليلة الماضية وزادت الكتابات الفقهية فيه، إلا أن غالبية الدراسات المعنيـة قد انصبت إمـا على التحليل المجـرد لنصوص المواد -إما القانـون المصري أو المقارن وخاصةً الأوروبي- أو مجرد رصد للأثر المادي لتقنيات الذكاء الاصطناعي على الخصوصيـة والبيانـات الشخصية. ما تتميز بـه الدراسة الحاليـة إذن هو أنها تربط ربطًا عميقًا بـين الأثر المادي للذكاء الاصطناعي والمعالجة القانونية لتلك الأثار، فنجد مباحثهـا تشتمل على تأصيل لقانون حماية البيانات الشخصية وبحث حقيقي في مدى ملائمته لتحديات اليوم.

والدراسـة بذلك تعد اسهامًـا مصريًا عربيًا فـي جدليات قانون تقنيـة المعلومات، وخاصـةً فرع قانـون حماية البيانات الشخصيـة، التي تسيطر عليهـا الكتابات الغربية حصـرًا. فالحديث عن فلسفة قانون حماية البيانات الشخصية قد يكون ذو فائدة جمة للجهود المصرية الحالية لإخراج اللائحة التنفيذية لقانون تقنية المعلومات، كما أنه قد

يكـون أساسًا لمجهودات تشريعية مستقبلية متوقعة في هذا الصدد نظرًا لوتيرة التطور التقنـي السريعة، وكذا قد يكون أساسًا لأبحاث مستقبليـة تربط بين النظرة الفلسفية للحق في الخصوصية والبيانات الشخصية في الفقه الغربي والفقه العربي والإسلامي.

منهج البحث

تتبنى الدراسة الحالية المنهج الوصفـي لرصد التطورات والتأثيرات التقنية للذكاء الاصطناعي على البيانـات الشخصية والخصوصية. وتتبنى المنهج التحليلي: أولًا لنقد الأساس الفلسفي لقوانين حماية البيانـات الشخصية، وثانيًـا لتحليل النصوص ذات الصلة من اللائحة الأوروبية العامة لحماية البيانات والقانون المصري. كما تتبع منظورًا مقارنًا في تتبع التنـاول المصري والأوروبي للإشكاليات المتصلة بموضوع البحث وذلك لاعتبـار رئيس وهو أن التنظيم الأوروبي لحماية البيانـات يُعد النموذج الرائد في هذا المجـال وهو لا مفر مرجعًا أساسيًا خاصةً في الحالـة المصرية حيث تم اتباع نهجه من ناحيـة، ومن ناحية أخرى لم تصدر اللائحة التنفيذية للقانون المصري ومعها كثير من التفصيل اللازم للوقوف على شكل التنظيم المصري بالنسبة لحماية البيانات.

خطة البحث

- **المبحث الأول: تأثير الذكاء الاصطناعي على الخصوصية والبيانات الشخصية**

أولًا: مخاطر الخصوصية قبل ثورة الذكاء الاصطناعي

ثانيًا: تأثير الذكاء الاصطناعي على البيانات الشخصية والخصوصية

- **المبحث الثاني: عدم جدوى التحكم الفردي**

أولًا: مظاهر التحكم الفردي في قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠

ثانيًا: نواقص التحكم الفردي

أ) مستخدم الإنترنت ذو العلم والقدرة

ب) المؤثرات الخارجية على إرادة الفرد

- **المبحث الثالث: الحق المشترك في البيانات**

أولًا: تأثير البيانات الشخصية على الغير

ثانيًا: الخصوصية والبيانات الشخصية كمورد مشترك

ثالثًا: التنظيم بناءً على حق مشترك في البيانات

المبحث الأول

تأثير الذكاء الاصطناعي على الخصوصية والبيانات الشخصية

لقد أصبح من المسلمات في مجالات تنظيم الانترنت والذكاء الاصطناعي ومواقع التواصل الاجتماعي أن الذكاء الاصطناعي والبيانات الشخصية أضحيا قرينين، ليس فحسب لأن البيانات هي ما تتغذى عليه تقنية الذكاء الاصطناعي، بل أيضًا للتأثير المركب على الخصوصية نتيجةً لاستخدام تقنية الذكاء الاصطناعي. ولكي نتكمن من تمييز أثر الذكاء الاصطناعي على الخصوصية، نعرض أولًا لتصنيف لمخاطر الخصوصية قبل ثورة الذكاء الاصطناعي ثم نتدرج صعودًا إلى المشهد الحالي.

أولًا: مخاطر الخصوصية قبل ثورة الذكاء الاصطناعي

إن الخصوصية لم تتعرض إلى الخطر حصرًا بتأثير من الذكاء الاصطناعي، وإنما هي اعتبار قائم قبل ظهوره بكثير، وكانت دومًا عرضة لمخاطر تتطور مع كل تطور ومرحلة تقنية جديدة. وفي محاولة لتقديم فهم عملي للخصوصية ومخاطرها، قدم أستاذ القانون الأمريكي دانييل سولوف في ٢٠٠٦، قبل تطور الذكاء الاصطناعي بشكل ملحوظ، ما أسماه مصفوفة خصوصية (A taxonomy of privacy) لتصنيف التهديدات المتعلقة بالحق في الخصوصية[١].

رأى سولوف أن مخاطر الخصوصية تتمثل في أربعة أطوار هم جمع المعلومات، معالجة المعلومات، نشر المعلومات، والتعدي. كل من هذه الأطوار يمثله مجموعة من الممارسات التي تعتبر خطرًا أو تعديًا على الخصوصية[٢].

فبالنسبة لجمع المعلومات يمكن أن يكون ذلك من خلال المراقبة من خلال التصنت أو مراقبة الفيديو مثلًا وهو ما ينطوي على انتهاك، سواءً كان سرًا أو علنًا.[٣] فمراقبة الأفراد دون علمهم ينتقص من كرامتهم، ومراقبتهم وهم يعلمون يقيد حريتهم في التصرف.

وبالنسبة لمعالجة البيانات، تثور إشكاليات مثل تراكم البيانات (Data aggregations)، حيث يتم تجميع قطع من البيانات المتفرقة عن الشخص لتكوين

(1) Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 477.
(2) ibid.
(3) ibid 492.

صـورة كبرى عنه.[١] كما تظهر مشاكل مثل تعريـف أو كشف هوية الشخص دون رغبة منه أو سند قانوني، أو مشكلة تغيير غرض استخدام البيانات.

كمـا يثار فـي المقام الثالـث نشر المعلومـات وما ينطـوي عليه ذلك مـن إشكاليات الإفصاح عن معلومات خاصة أو انتهاك الثقة، وما يتبع نشر المعلومات من مخاطر مثل عدم الشعور بالأمن أو تعريض الشخص للابتزاز[٢].

وأخـيـرًا، قد يؤدي انتهاك الخصوصيـة إلى التعدي (Invasion)، وهو ما قد يحدث مـن خلال التدخل في حق الشخص في أن يكون وحيدًا بحسب تعريف وارين وبراندیز الشهير،[٣] أيًا كان شكل ذلك التدخل، والذي قد يكون ملموسًا، أو غير ملموس مثل حالة المراقبـة، كمـا قد يكون التعدي من خلال التدخل في قـرارات الشخص للتأثير عليه أو إجباره على ما لا يريد.[٤]

ثانيًا: تأثير الذكاء الاصطناعي على الخصوصية والبيانات الشخصية

إن كل مـا ورد تحت مصفوفـة خصوصية سولوف لازال ذو صلة اليوم، إلا أن الذكاء الاصطناعي بما لديه من قدرات غير مسبوقة قد عزز من المخاطر السابقة، بل وأضاف إليهـا مظاهـر جديدة إما في شـكل صور مستحدثة كليةً من تهديـدات الخصوصية أو تطويـر التهديدات الموجـودة سلفًا، وهو ما يؤدي إلى تعريضـ الخصوصية لخطر أكبر بشكل عام والتأثير خاصةً على التحكم الفردي في البيانات.

ولفهم أفضل لمخاطر الذكاء الاصطناعي، تقترح الدراسة الحالية استبدال مصفوفة سولـوف للخصوصيـة بتصنيـف آخـر يمكن النظـر من خلالـه على مخاطـر الذكاء الاصطناعـي اليـوم. وعوضًا عن مجـرد المصفوفة حيث يوجد تصنيـف غير مترابط، يُقترح هنا أن ننظر لمخاطر الخصوصية والبيانات اليوم باعتبارها دورة. وهو ما نسميه «دورة تأثير البيانات» (Data Influence Cycle).

وذلـك الطرح يختلف عن سابقه في أنه ينظر إلى أطوار المصفوفة على أنها حلقات أصبـح يربـط بينهـا الـذكاء الاصطناعي بحيـث أن كل منهـا منفـردًا يحتمل حدوث

(1) ibid 505.
(2) ibid 523.

(٣) لقد عرفوا الخصوصية على أنها «الحق في أن يترك الشخص وحده». انظر
Samuel D Warren and Louis D Brandeis, 'The Right to Privacy' (1890) IV Harvard Law Review, 193.
(4) Daniel Solove, 'A Taxonomy of Privacy' (2006) 154 University of Pennsylvania Law Review 548.

انتهاكات للخصوصية، خاصةً بتأثير الذكاء الاصطناعي، إلا أن أطوارها مجتمعة تمثل دورة ذات خطر معزز على الخصوصية.[١] هذه الدورة تمر بمراحل أولها الحصول على البيانات، وثانيها معالجة البيانات، وثالثها نشر المعلومات، ورابعها التغذية الرجعية وإعادة التكيف.

أ) الحصول على البيانات

يحقق الذكاء الاصطناعي فعالية لا تقارن بالوسائل التقليدية بالنسبة لجمع البيانات فالتصنت والمراقبة كوسائل مستخدمة قديمًا أصبحت معززة بالذكاء الاصطناعي وقادرة على تمييز أصوات معينة وتمييز الأوجه دون تدخل بشري[٢] وبينما قد يمثل ذلك نموذجًا تقليديًا واضحًا لانتهاك الخصوصية، فإن هناك صور أخرى مستحدثة لتأثير الذكاء الاصطناعي أكثر رمادية.

يتبدى ذلك في ممارسة مثل تجريف البيانات (data scraping) حيث يتم جمع كميات ضخمة من البيانات الموجودة عادةً على الانترنت بواسطة طرف ثالث دون رضا أو حتى علم أصحاب البيانات، وعادةً دون علم المتحكمين في البيانات أنفسهم.[٣] هذه البيانات جمعها لتدريب خوارزميات الذكاء الاصطناعي عليها من أجل زيادة الجودة والدقة.

وبينما أن تجريف البيانات كممارسة ليس بالأمر الجديد، إلا أن دور الذكاء الاصطناعي يظهر في كمية البيانات التي يمكن جمعها في المقام الأول، ثم تخزينها، فمعالجتها، واستخراج معلومات دقيقة منها. وما ينذر به ذلك هو أن نوعية البيانات التي لم يكون وجودها في المجال العام -الرقمي في هذه الحالة- يثير إشكاليات بالنسبة للخصوصية أصبحت اليوم قابلة للاستفادة منها بأوجه قد تمثل انتهاكًا للخصوصية.

جمع البيانات ليس بالضرورة أن يكون بغير علم صاحب البيانات، وإنما قد يكون برضاه. ذلك الرضا كي يتم بشكل مشروع تحت قانون الاتحاد الأوروبي أو القانون المصري قد يكون في صورة مباشرة عن طريق الحصول على موافقة (Consent)

(١) لفهم أكثر لترابط تلك المراحل وتأثيرها على صاحب البيانات يرجى الإحالة إلى المبحث الثالث من هذه الدراسة.

(2) Rita Matulionyte, 'Reconciling Trade Secrets and Explainable AI: Face Recognition Technology as a Case Study' (2022) 44 European Intellectual Property Review 36.

(3) Daniel J Solove, 'Artificial Intelligence and Privacy' (Social Science Research Network, 1 February 2024) 24.

صاحب البيانات[١] أو في صورة غير مباشرة كجزء من عقد يدخل فيه صاحب البيانات وينطوي على جمع لبياناته الشخصية[٢] وتلك الصورة مثلًا هي الأكثر شيوعًا بالنسبة لوسائل التواصل الاجتماعي.

يترتب على ذلك النموذج، حيث يمنح صاحب البيانات رضاه عن جمع بياناته، إشكاليتان، الأولى هي مدى إدراك صاحب البيانات لنطاق رضاه وما يلي ذلك من كم البيانات وغرض استخدامها، وهو ما سنتعرض إليه فيما بعد.

والإشكالية الثانية هي استخدام البيانات الشخصية لتدريب خوارزميات الذكاء الاصطناعي لمزود الخدمة، فقد حدثت شركة جوجل (Google) إخطار الخصوصية (Privacy notice) الخاص بها لإشعار المستخدمين بأنها تجمع البيانات الشخصية العامة لتدريب خوارزميات الذكاء الاصطناعي التي تستخدمها في خدمات مختلفة.[٣]

وربما يتجاوز ذلك إلى الحصول على الموافقة لاستخدام البيانات لأي غرض. فنرى مثلًا أن تطبيق زووم (Zoom) قد حدث إخطار الخصوصية الخاص به للحصول على رضا مستخدميه على «الوصول، استخدام، جمع، خلق/ تعديل/ توزيع، معالجة، مشاركة، صيانة، تخزين البيانات المنتجة عبر الخدمة (Service Generated Data) لأي غرض»[٤].

إن اختيار عنوان المرحلة الأولى ليكون الحصول على البيانات جاء ليعبر عن أحد الأثار المباشرة للذكاء الاصطناعي وهو أن البيانات لا يتم الحصول عليها من خلال جمعها من مصادر خارجة عن مقدم الخدمة فحسب، وإنما يتم خلقها، أو بالأدق استنتاجها بواسطة الذكاء الاصطناعي. إن الخطر الذي كان يمكن أن يترتب من قبل على الإفصاح عن بيانات شخصية كان يقتصر على البيان المفصح عنه، أو على أقصى

---

(١) الرضاء الرقمي بمعالجة البيانات الشخصية: دراسة مقارنة، تامر محمد الدمياطي، مجلة القانون والتكنولوجيا الناشئة، العدد ٢، ٢٠٢٢، ص ١٣.

(٢) المادة (٦) من اللائحة العامة لحماية البيانات الشخصية؛ المادة (٦) من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠.

(3) Matt G Southern, 'Google Updates Privacy Policy To Collect Public Data For AI Training' (Search Engine Journal, 3 July 2023) <https://www.searchenginejournal.com/google-updates-privacy-policy-to-collect-public-data-for-ai-training/490715/> accessed 8 December 2024.

(4) Ian Krietzberg, 'Zoom Walks Back Controversial Privacy Policy' (TheStreet, 11 August 2023) <https://www.thestreet.com/technology/zooms-latest-move-may-make-you-reconsider-using-the-service> accessed 8 December 2024.

تقديـر قـدرة متلقي البيان علـى تحليله او ربطـه بغيره من بيانات، وهـو خطر محدود بحـدود القـدرة البشريـة على الاستنتـاج والأدوات التقنيـة غير المتطـورة. أما الذكاء الاصطناعـي بإمكانـه استنتاج بيانات شخصية غير معلنة وذلـك من خلال قدر يسير من بيانات أخرى.

علـى سبيـل المثال، يستطيع بائـع باستخدام نظـام ذكاء اصطناعـي أن يستنتج أن إحـدى زبوناته حامل من خلال تغـير في سلوكها الشرائي كما لو قامت بشراء منتجات معينـة مثـل مستحضرات ترطيب البشـرة غير المعطرة، مكمـلات الكالسيوم، وكميات أكـبر من القطن الطبي، بالإضافة إلى مشترياتهـا المعتادة من البقالة. ذلك الاستنتاج لم يكـن ليحـدث عادةً لو نظر البائع في سجلات شـراء الزبونة بنفسه.[1] تلك القدرة الاستنتاجية تمتد إلى نشاطات غير محصورة، ويترتب عليها توليد بيانات عن الشخص أكثر مما يظن أنه معلوم عنه. ذلك البُعد لم يكن مطروحًا قبل بزوغ الذكاء الاصطناعي، ويترتـب عليه بالطبع أن الخطر على الخصوصية هنا يتجاوز مجرد جمع البيانات، إلى مفهوم أوسع متمثلًا في الحصول على البيانات.

ب) معالجة البيانات[2]

عقب الحصول على البيانات، يتم معالجتها بالشكل الذي يرتئيه المتحكم في البيانات -وربما معالج- البيانات لتحقيق أغراض الخدمة. قد يقتصر ذلك على الغرض المباشر مـن جمع البيانات، وقد يتم التوسـع في استخدام البيانات لأغراض ثانوية. وقد تثور فـي هذه المرحلـة بعض الإشكاليات منهـا مثلًا احتمالية تحيـز الخوارزميات، فأنظمة الـذكاء الاصطناعي قد تعطي نتائج متحيزة ضده فئة معينة كما تم رصده في أكثر من

(1) George Kuhn, 'How Target Used Data Analytics to Predict Pregnancies' (Drive Research, 1 August 2023) <https://www.driveresearch.com/market-research-company-blog/how-target-used-data-analytics-to-predict-pregnancies/?utm_source=chatgpt.com> accessed 8 December 2024.

(٢) نتنـاول هنـا مفهوم المعالجة بالمعنى الضيق بما يشمل تناول البيانات التـي تم تجميعها بغرض استخدامها لاحقًا لهدف معين. لكـن مفهـوم معالجة البيانـات هو بحسب الأصل مفهوم واسع يمتـد ليشمل كافة صور تناول البيانات بـدءًا من جمع البيانات ومـا يليهـا من عمليات، أنظـر Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (European Union 2023) 00569/13/EN <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm>.; انظـر أيضًـا سيـد أحمـد محمود، حماية البيانـات الشخصية الرقمية وفقًـا لأحكام القانون المصـري رقـم ١٥١ لسنة ٢٠٢٠ (حماية البيانات الشخصيـة المعالجة إلكترونيًا) بين الواقع والمأمـول، مجلة العلوم القانونية والاقتصادية، العدد الأول، ٦٦، ٢٠٢٤، ص١٤٥١.

حالة،[١] ذلك التحيز قد يكون نتيجة لفقر جودة البيانات التي تم تغذية الخوارزمية بها كأن يكون غالبية المسجونين من فئة معينة، وعند تغذية الخوارزمية بسمات وخصائص المسجونين فعلًا لاستنتاج الأكثر عرضة لارتكاب الجرائم، تظهر الخوارزمية تحيزًا تجاه أفراد هذه الفئة.[٢] وقد يعكس التحيز عيب في تصميم الخوارزمية ذاتها كما لو لم يتم وضع معايير كافية لمنع التحيز[٣].

تثور بصدد معالجة البيانات إشكالية أخرى تتعلق بعدم شفافية الخوارزميات، فالشفافية هي أحد أهم ضمانات المعالجة القانونية السليمة للبيانات الشخصية، وهي على رأس كفالات قدرة الشخص على التحكم في بياناته. نتيجةً لذلك فإن قانون الإتحاد الأوروبي والقانون المصري على السواء يضعون بعض الالتزامات على المتحكم في البيانات تدور في عمومها حول الإفصاح عن المعالجة. فالاتحاد الأوروبي يضع مثلًا مبدأ عام بأن تكون معالجة البيانات بشكل ذي شفافية لصاحب البيانات.[٤]

ويلاحظ هنا أن القانون المصري لم يُضمِّن مبادئ المعالجة المنصوص عليها في المادة (٣) مبدأ الشفافية تحديدًا، وإنما اكتفى باشتراط أن تجمع البيانات الشخصية لأغراض معلنة لصاحب البيانات. وغني عن البيان أن مجرد الإعلان بأغراض جمع البيانات هو أحد تطبيقات الشفافية كمبدأ وفلسفة عامة لتنظيم المعالجة.

وبشكل عام، فإن الشفافية هي مطلب بيني؛ يشمل مرحلة جمع البيانات، وكذلك معالجتها. وبالرغم من محورية مبدأ الشفافية بالنسبة لحماية البيانات الشخصية، فإن ذلك المطلب يصطدم في مرحلة معالجة البيانات في صخرة عدم وضوح طريقة عمل الخوارزميات، وذلك العائق يقف حتى أمام مصممي الخوارزميات أنفسهم حيث إن المصممين يقومون بإنشاء الخوارزمية اللازمة لتأدية مهمة ما، إلا أنهم لا يفهمون

(1) Aylin Caliskan, Joanna J Bryson and Arvind Narayanan, 'Semantics Derived Automatically from Language Corpora Contain Human-like Biases' (2017) 356 Science 183.

(2) 'Data Driven Policing: Highlighting Some Risks Associated with Predicting Crime' (Human Rights Centre Blog, 8 March 2017) <https://hrcessex.wordpress.com/2017/03/08/data-driven-policing-highlighting-some-risks-associated-with-predicting-crime/> accessed 10 December 2024.

(3) Julia Angwin Mattu Jeff Larson,Lauren Kirchner,Surya, 'Machine Bias' (ProPublica, 23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 8 December 2024; Ian Ho, 'AI Sentencing Cut Jail Time for Low-Risk Offenders, but Study Finds Racial Bias Persisted | Freeman News' (24 January 2024) <https://freemannews.tulane.edu/2024/01/24/ai-sentencing-cut-jail-time-for-low-risk-offenders-but-study-finds-racial-bias-persisted?utm_source=chatgpt.com> accessed 8 December 2024.

(٤) المادة (٥) من اللائحة العامة لحماية البيانات. انظر كذلك المواد (١٢) و(١٣) و(١٤) و(١٥) من اللائحة.

بالضـرورة كيـف توصلت الخوارزميـة بعد ذلـك إلى النتيجة التي توصلـت إليها. تلك الحالـة سميت بالصندوق الأسود للـذكاء الاصطناعي في إشارة إلى تعذر تفسير كيف أن تم التوصل إلى نتيجة ما بالتحديد[١].

وعدم القدرة على تفسير قرار معين ينعكس بالتبعية على قدرة الشخص على التحكم في بياناته إذ هو لا يدري كيف تم استخدامها وبالتالي ما إذا كان يريد مشاركة بياناته، أو قـدر منها، أو وقف معالجتها بالكلية. وفوق ذلك، فإنه يتعذر نتيجةً لعدم القدرة على التفسير نسب المسئولية لفاعل معين[٢].

يضـاف إلى مـا سلف من الإشكاليات التي تثور في مرحلـة المعالجة فكرة استخدام البيانات لغير الغرض الذي جمعت له (Repurposing). وذاك يعني استخدام البيانات التـي جمعـت في الأصل لغرض معـين لتحقيق غرض مختلف لم يكن مذكـورًا أو متفقًا عليـه عند جمعها. على سبيـل المثال، قد تُجمع بيانات شخصية مـن أجل تقديم خدمة معينة، ثم تُستخدم لاحقًا في أبحاث تسويقية أو لتحليل سلوك المستخدمين دون علمهم أو موافقتهـم. تغيير غرض المعالجة يمثل مخالفة صريحة إذا كان هدف المعالجة معلن بوضوح، لكن الإشكالية عادةً في عدم إعلان هدف المعالجة بشكل واضح ومحدد، مما يأخذ صور مثل استخدام عبارات عامة كـ «تحسين الخدمة».

ج) نشر البيانات

فـي المراحل السابقة يتم الحصول على البيانات من مسارات مختلفة، ثم يتبع ذلك معالجتهـا بكل مـا تشمله المعالجة مـن عمليات، بيـد أن كلاً من المرحلتـين السابقتين تحدثـان لغرض ما، ذلك الغرض عادةً ما يتمحور حول المرحلة الثالثة. في تلك المرحلة يتم نشر البيانات، والمقصود بمفهوم النشر هنا أوسع من النشر بقصد العلانية، وإنما يشمـل كذلك استخدام المعلومـات الناتجة عن المعالجة لمخاطبـة ومحاولة التأثير على صاحـب البيانـات نفسه. هنا يبرز الأثر الـذي تجري الدورة كاملةً مـن أجله، حيث إن أهمية البيانات الشخصية تتبدى في أنها تساعد على فهم المستخدمين من أجل التأثير عليهم أو اتخاذ قرارات متعلقة بهم، وهو ما يتجسد عادةً في نشر البيانات.

(1) Yavar Bathaee, 'The Artificial Intelligence Black Box and the Failure of Intent and Causation' (2017) 31 Harvard Journal of Law & Technology (Harvard JOLT) 889.
(2) ibid.

هنـاك ممارسات مرتبطة بمرحلة نشر البيانات تمثل خطرًا كبيرًا على الخصوصية لما تنطوي عليه من تأثير على الأفراد، وخاصةً مستخدمي الإنترنت، ومن بينهم مستخدمي مواقع التواصل الاجتماعي ومحركات البحث. أبرز هذه الممارسات هي التخصيص (Personalisation) حيث يتم إرسال محتوى مصمم خصيصًا لمستقبل هذه المحتوى وذلك بناءً على تفضيلاته التي تم استخراجها من بياناته الشخصية[١].

والتخصيص هو مزية وآفة الذكاء الاصطناعي في آن واحد. فمن ناحية، الوصول إلى فهم لتفضيلات واحتياجات مستخدمي الانترنت والاستجابة لها بالشكل المناسب والقدر المناسب في التوقيت المناسب لم يكن متاحًا بهذه الدقة من قبل. ذلك يكفل أداءً أفضل من قِبَل مقدم الخدمة، وتلبية مرضية لمتلقي الخدمة. ينعكس ذلك على الألوان المختلفة للخدمات التي يتم تقديمها للأفراد بدءًا من ترشيح كلمات ورموز معينة على لوحة المفاتيح بناءً على نمط كتابة الفرد، وعلى ذات الشاكلة يتم تخصيص الأخبار، والموسيقى، والمحتوى المرئي، وترشيحات التطبيقات، وفوق ذلك كله تخصيص ترشيحات السلع في حالة التسوق الإلكتروني، وتخصيص المحتوى بالنسبة للمجال السياسي.

إلا أن هذا التنوع وهذه الدقة ذاتهم هما ما يمثلان خطرًا على قدرة الفرد على صنع قراره باستقلالية (Agency). فذلك الفهم العميق للفرد قد يؤدي إلى استغلاله بإرسال المحتوى الذي يغريه بالشراء في الوقت الذي يكون فيه أكثر استعدادًا للإنفاق على سبيل المثال، أو في الأوقات التي يشعر فيها بالضعف والحاجة إلى مُتَنَفس معين. وقد يؤدي التخصيص إلى التضليل والتلاعب بالشخص بناءً على فهم نقاط ضعفه (Vulnerabilities) وانحيازاته المعرفية (Cognitive biases)، فيقدم له محتوى يتناسب مع ميوله مما يدفعه للتصويت لمرشح معين مثلًا، أو أن يأخذ موقف سلبي من قضية معينة بناءً على تجاربه السابقة أو عن طريق تعزيز انحيازاته[٢].

من المفاهيم وثيقة الصلة بالتخصيص هو التنميط (Profiling)، وتلك الممارسة تمثل العمود الفقري لتخصيص المحتوى، إذ تنطوي على جمع وتصنيف البيانات حول

(1) Ramnath K Chellappa and Raymond G Sin, 'Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma' (2005) 6 Information Technology and Management 181.
(2) Cass R Sunstein (ed), 'Fifty Shades of Manipulation', The Ethics of Influence: Government in the Age of Behavioral Science (Cambridge University Press 2016).

شخص طبيعي بغرض فهمه، وبالتالي فإن جودة التنميط تنعكس مباشرةً على جودة التخصيص، فممارسات مثل التسعير الشخصي كأحد صور التخصيص حيث يتم تغيير السعر استنادًا لحاجة المستخدم بشكل فردي وليس بناءً على سعر السوق الموحد، إنما يحدث من خلال معرفة وتحليل تاريخ بحث المستخدم عن المنتج المقصود مثلا[١].

ويمكن تعريف التنميط على أنه جمع وتصنيف البيانات بشكل منظم ولقصد معين خاص بالأفراد[٢] وأبرز اختلاف بين التنميط التقليدي والتنميط عبر الذكاء الاصطناعي يتمثل في أننا، كمواطنين أو مستهلكين أو موظفين، نجد أنفسنا في موضع يتم فيه تنميطنا دون أن يكون لدينا إمكانية الوصول إلى المعرفة التي تستخدم لتصنيفنا والتعامل معنا. وهذا الأمر يحد من حريتنا الشخصية، لأننا لا نستطيع توقع تصرفات أولئك الذين يعرفون عنا ما قد لا نعرفه عن أنفسنا[٣].

ونظرًا للدور المحوري للتنميط في العديد من الممارسات الإلكترونية اليوم، فقد أولت اللائحة العامة لحماية البيانات اهتمامًا خاصًا بالتنميط، إذ عرفته على أنه «أي شكل من أشكال المعالجة الآلية للبيانات الشخصية التي تتكون من استخدام البيانات الشخصية لتقييم بعض الجوانب الشخصية المتعلقة بالشخص الطبيعي وخاصة لتحليل أو التنبؤ بالجوانب المتعلقة بأداء الشخص الطبيعي في العمل والوضع الاقتصادي أو الصحة أو التفضيلات الشخصية أو الاهتمامات أو الاعتمادية أو السلوك أو الموقع أو الحركات»[٤].

وشملت اللائحة التنميط بضمانات مختلفة إذ ألزمت المتحكم بالإفصاح عنه لصاحب البيانات،[٥] وتمكينه من الاعتراض على وجود تنميط لبياناته،[٦] بل ومنحته الحق في عدم الخضوع للتنميط بالكلية إذا كان من شأن ذلك الإضرار به[٧].

---

(١) فعالية تقنية تنميط البيانات الشخصية في تخصيص التجارة الإلكترونية على ضوء اللائحة العامة رقم ٢٠١٦/٦٧٩ المتعلقة بحماية البيانات، فاطمة سرير، مجلة الدراسات القانونية المقارنة، العدد الثاني، ٢٠٢٢، ص ٧٦.

(2) Moritz Büchi and others, 'Making Sense of Algorithmic Profiling: User Perceptions on Facebook' (2023) 26 Information, Communication & Society 809.

(3) Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer Netherlands 2008).

(٤) المادة (٤.٤) من اللائحة العامة لحماية البيانات الشخصية.

(٥) السابق، المواد (١٣)، و(١٤)، (١٥).

(٦) السابق، المادة (٢١).

(٧) السابق، المادة (٢٢).

د) التغذية الرجعية والتكيف

في هذه المرحلة تغلق الدورة بأن يتم رصد جودة وفعالية المعلومات المنشورة من خلال استشعار ردود أفعال المستخدمين. تلك المرحلة تمثل إضافة كبيرة لم تكن متاحة بهذا الشكل قبل الذكاء الاصطناعي. فإحدى خصائص الذكاء الاصطناعي التي تتبدى هنا هي التأقلم (Adaptability)[1]. حيث تتعلم تقنية الذكاء الاصطناعي من التجارب السابقة لتقوم بتكرار الدورة -دورة تأثير البيانات- بفعالية أكبر؛ فيتم جمع البيانات الأكثر صلة، وإجراء المعالجة بشكل يضمن تخصيصًا أكثر ، وإعادة الاتصال مع المستخدمين بالوسائل التي تضمن تأثيرًا أكبر عليهم.

هنا، تعود تفاعلات المستخدمين وردود أفعالهم لتؤثّر من جديد في الخوارزميات المستخدمة في تجميع المحتوى وترشيحه. ونتيجة لذلك، يتشكل مسار تداول المعلومات مستقبلًا وفقًا لهذه التفاعلات، مما قد يؤدي إلى تعزيز روايات أو اتجاهات محدّدة، وبالتالي التأثير على تشكيل الرأي العام بطرق غير محايدة. وخلال هذه العملية، قد تخضع المعلومات للتعديل أو الإخراج من سياقها الأصلي، أو إعادة توظيفها لأغراض مختلفة، وهو ما يؤثر على المعنى والدلالة التي تُكتسب عند تداولها. وفي النهاية، تستلهم هذه المرحلة ردود الأفعال والحوارات بين الأفراد لتعيد ضبط سياسات وآليات نشر المحتوى في المستقبل، فتتكيّف البيئة المعلوماتية باستمرار مع التدفق التفاعلي للمعلومات[2].

تلك المراحل الأربع هي المراحل الرئيسة في دورة تأثير البيانات، وبإمعان النظر فيها يمكن استنتاج أنها جميعًا تأثرت بالذكاء الاصطناعي. إن كل مرحلة استقلالًا تحمل مخاطر خاصة بالخصوصية، لكن تقنية الذكاء الاصطناعي قربتهم، وأبرزت إمكانية الجمع بينهم بغرض التأثير على صاحب البيانات وتحقيق جمع واستفادة أكبر من البيانات.

(1) Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8 Internet Policy Review.
(2) ibid.

المبحث الثاني

عدم جدوى التحكم الفردي

توصلنا إذن إلى أن الذكاء الاصطناعي قد توغل في مجال تناول البيانات الشخصية، وأثار بالتبعية تحديات لم تعرف في سياق الخصوصية من قبل. لذلك يهمنا في الخطوة التالية أن ننظر في مدى فعالية الأدوات المستخدمة في الحد من هذه التحديات. تلك الأدوات تشمل جوانب مختلفة؛ منها التقنية، وعملية صنع السياسيات المرتبطة بالذكاء الاصطناعي ذاته وكذلك حماية البيانات الشخصية، وسياسات التجارة، إلا أن ما يشغلنا في هذا الصدد الجانب التشريعي/القانوني، وفي القلب منه الأساس الذي بني عليه قانون حماية البيانات الشخصية، وتحديدًا التحكم الفردي.

كما ذكرنا في المقدمة، فإن القانون المصري اقتدى إلى حد بعيد باللائحة الأوروبية العامة لحماية البيانات، وتلك تتبع بقدر ليس باليسير نهجًا يرتكن إلى تحكم الشخص في بياناته كوسيلة لتحقيق حماية فعالة للبيانات. تحت عنوان «إطار عمل (اللائحة العامة لحماية البيانات) يعتمد على التحكم واليقين» تنص اللائحة في الحيثية (٧) (Recital ٧) على أنه «يجب أن يتمتع الأفراد الطبيعيون بالتحكم في بياناتهم الشخصية».

وفي هذا الجزء من الدراسة الحالية سنبحث مظاهر التحكم الفردي في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، مع الإشارة عند اللزوم إلى ما يوازيه في اللائحة العامة، ثم سنبحث كيف أن التحكم الفردي يفقد كثيرًا من جدواه في مواجهة تقنية الذكاء الاصطناعي والبيانات الضخمة. وحجتنا هنا ليست أن التحكم الفردي عديم الجدوى، وإنما أنه لا يحقق حماية فعالة للشخص نفسه، ناهيك عن المجموعة، وهو ما يطرح التساؤل فيما بعد عن البدائل.

أولًا: مظاهر التحكم الفردي في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠

هناك العديد من الحقوق والالتزامات التي نص عليها قانون حماية البيانات الشخصية التي يمكن أن يستنتج منها إقامة التحكم الفردي كنهج لحماية البيانات – ومع ذلك، يكمن موطن التحكم الأكبر في نظرنا في حالات جمع البيانات، وهذا ما

ستوليه الدراسة جزءًا أكبر من الاهتمام فيما بعد.[١]

يأخذ تحكم صاحب البيانات في معالجة بياناته صورتين هما الموافقة والعقد. وتمثل الموافقة الصورة المباشرة للرضا بشأن جمع البيانات ومعالجتها، حيث يتم سؤال صاحب البيانات عن رضاه عن جمع بياناته ومصير هذه البيانات. وهذه ما نقابله عند استخدام للعديد من الخدمات عبر الإنترنت، فنجد مثلًا نافذة صغيرة تسأل صاحب البيانات عند ولوجه موقع إنترنت موافقته عن الاحتفاظ بملفات تعريف. تلك الملفات يتم الاحتفاظ بها على حاسوبه ويسجل عليها تاريخ نشاطه على ذلك الموقع كي يتم استردادها كل مرة يزور فيها الموقع وبالتالي تخصيص الخدمة له.

وبالنظر في قانون حماية البيانات الشخصية، يتضح أن المشرع المصري قد اتخذ منحىً يبرز تركيزًا على التحكم الفردي، وخصوصًا الموافقة، فقد أكد على اشتراط موافقة صاحب البيانات لمعالجة البيانات في ثلاثة مواضع. في المادة (٢) من القانون جعل المشرع من موافقة صاحب البيانات السند الأصيل في تناول البيانات إذ نص على «لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا».[٢] ثم هو عاد في المادة (٤) ونص على الموافقة كالتزام على

(١) كون تحكم الفرد في جمع بياناته ذو الأثر الأكبر في جمع البيانات له سببان، أحدهما نظري، والآخر عملي. فمن ناحية نظرية، وعلى فرض التزام المتحكم ومعالج البيانات بالقانون، إذا تم تطبيق تحكم فعال في جمع البيانات فإن كافة مخاطر البيانات التالية سيتم تحييدها إلى حد مقبول. أو بتعبير آخر، فإن جمع البيانات هو المدخل لكافة عمليات المعالجة التالية، فإذا كان صاحب البيانات واعٍ ومسؤول في منح الموافقة على جمع بياناته بالنظر إلى الغرض منها، والكم الذي سيتم جمعه، ومدة الاحتفاظ بها، فإن المخاطر التالية سيتم الحد منها. أما الاعتبار العملي الذي يعطي أهمية خاصة للتحكم في جمع البيانات فيكمن في أنه من الناحية العملية تعتمد غالبية حالات جمع البيانات التي تحدث على الإنترنت على الموافقة أو العقد، وذلك لأن غالبيتها تكون بهدف تحقيق هدف تجاري، وهو ما لا تنطبق معه الحالات الأخرى لجمع البيانات.

(٢) من الملاحظ هنا أن نص المادة (٢) قد ميز بين جمع البيانات ومعالجتها والإفصاح عنها وإفشائها، وهو في المادة (٦) قد استخدم بصدد حالات معالجة البيانات تعبير «المعالجة» فقط دون أن يخص جمع البيانات أو غيرها من العمليات الفرعية، وكلتاهما تتعلقان بشكلٍ أو بآخر بالأساس القانوني لمعالجة البيانات. وكما أشرنا سلفًا فإن تعبير المعالجة يشمل جميع عمليات تناول البيانات حتى تحت القانون المصري، حيث تم تعريف المعالجة في المادة (١) بشكل شامل كـ «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 جزئيا أو كليًا.» وليس من الواضح لدينا إذا كان التمييز بين الجمع والمعالجة تحت المادة (٢) سهوًا من المشرع، أم أنه بغرض تحديد هذه العمليات باعتبارها ضمن حقوق صاحب البيانات كما يشير عنوان الفصل الثاني، وفي هذه الحالة لا مناص من اعتبار المعالجة مقتصرة على العمليات التي تقع بين جمع البيانات والكشف عنها سواءً بالإفصاح أو الإفشاء.

المتحكم للحصول على البيانات حيث نص على أن يلتزم المتحكم بـ «الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا». وفي المادة (٦) أشار بشكل عام إلى أن المعالجة الإلكترونية تعد مشروعة وقانونية في حال توفرت حالات معينة، أولها «موافقة الشخص المعني بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر».[١] وبصرف النظر عما قد يثار من إشكاليات عن تفسير المواد الثلاث جنبًا إلى جنب، فإن ما يمكن الخروج به من قراءتهم هو اعتبار الموافقة حقًا لصاحب البيانات وفقًا للمادة (٢)، والتزام على المتحكم عند حصوله على البيانات وفق المادة (٤)، وأحد الحالات التي تجوز فيها معالجة البيانات وفق المادة (٦) أيًا كان القائم على المعالجة.

أما العقد فيمثل الصورة غير المباشرة لتحكم صاحب البيانات في جمع ومعالجة بياناته. والمقصود هنا أنه في حالة «الموافقة» ينصب السؤال فقط وبشكل مباشر على جمع البيانات، أما جمع ومعالجة البيانات تحت العقد يأتي كجزء من عقد أو نتيجةً لعقد يبرمه صاحب البيانات، وحينها يكون سؤال صاحب البيانات عن بياناته جزء من عملية أكبر تشمل سؤاله عن بقية تفاصيل العقد. وبتعبير آخر فإن صاحب البيانات عندما يوافق على جمع بيانات عبر العقد فإنه يعطي موافقة على عقد كامل من بينه جزء عن البيانات.

والعقد كأساس لجمع البيانات هو السند القانوني الذي يغلب أن تعتمد عليه وسائل التواصل الاجتماعي في الحصول على بيانات مستخدميها.[٢] والعقد كسند لمعالجة البيانات يجد مرجعه في المادة (٦) من القانون التي تنص على أن المعالجة تكون مشروعة وقانونية في حالة أنها «لازمة وضرورية تنفيذًا لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها».

---

(١) تجدر الإشارة هنا إلى أن المشرع قد جانبه الصواب في عنونة المادة (٦) بـ «شروط المعالجة» وذلك نظرًا إلى أن ما تحويه المادة ليس شروطًا وإنما حالات تصح فيها معالجة البيانات. ومن المعلوم أن الحالات هي بدائل، أم الشروط فكلها لوازم.

(2) 'LinkedIn Hit with 310 Million Euro Fine for Data Privacy Violations from Irish Watchdog' (AP News, 24 October 2024) <https://apnews.com/article/linkedin-microsoft-privacy-european-union-ireland-6769ae3b83ea0d83cab8d8cfd1fa7e68> accessed 11 December 2024.

وبالنسبة لجمع البيانات أو المعالجة بمفهومها الواسع، فإن أحد أساسيات التحكم الفعال هو الشفافية والإفصاح في مواجهة صاحب البيانات. تنص المادة (٢) في هذا الصدد على حق صاحب البيانات في «العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها...». وكذلك «العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية». كما أن المادة (٣) تُوجِبُ لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها أن تجمع البيانات الشخصية لأغراض معلنة لصاحب البيانات.

وبالنظر إلى اللائحة العامة لحماية البيانات الشخصية نجد أنها كانت أكثر تحديدًا وتفصيلًا في هذا الصدد. ففيما يخص علم صاحب البيانات بالمعالجة التي تتم على بياناته عرضت اللائحة ثلاث حالات في ظل إطار عام. أما الإطار العام فيتمثل في إلزام المتحكم (يقابله هنا المتحكم والمعالج) في إيصال المعلومات لصاحب البيانات بخصوص بياناته بصيغة موجزة وواضحة ومفهومة وسهلة الوصول، باستخدام لغة واضحة وبسيطة، وخاصة لأي معلومات موجهة تحديدًا للأطفال.[١] وإعمالًا لذلك فقد أنزلت اللائحة التزامًا باطلاع صاحب البيانات على معلومات محددة في حالة أن الحصول على البيانات كان من خلاله،[٢] وكذلك في حالة عدم الحصول على البيانات من خلاله.[٣] وتلك الحالتين تقومان على مبادرة من المتحكم دون طلب من صاحب البيانات. وفوق ذلك منحت اللائحة صاحب البيانات الحق في الوصول إلى بياناته والمعلومات المتعلقة بها وذلك بطلب منه[٤].

وبمقارنة بسيطة بين التنظيمين يتبين أنه بخلاف شروط الإطار العام للشفافية الغائبة عن القانون المصري، فإن نص المادة (٢) على أن حق صاحب البيانات في «العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها...» قد منح حقًا عامًا في العلم والاطلاع دون تحديد التزام على المتحكم أو المعالج بإعلام صاحب البيانات عند جمعها، مما يترك المجال لتفسيِّر النص على أنه قاصر على الحق في الوصول فقط دون الحق في الإعلام المسبق. وبالنظر إلى

(١) المادة (١٢) من اللائحة العامة لحماية البيانات.
(٢) السابق، المادة (١٣).
(٣) السابق، المادة (١٤).
(٤) السابق، المادة (١٥).

أن اللائحة التنفيذية لم تصدر حتى تاريخه فربما تشتمل حين صدورها على ذلك التفصيل، وهي جدير بها ذلك.

بالإضافة إلى التحكم في معالجة البيانات، والشفافية والإفصاح، فإن المادة (٢) قد نصت على مجموعة من حقوق لصاحب البيانات تتبدى فيها مظاهر للتحكم الفردي إذ أقرت له بالحق في:

«٢ – العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

٣ – التصحيح أو التعديل[١] أو المحو[٢] أو الإضافة أو التحديث للبيانات الشخصية.

٤ – تخصيص المعالجة في نطاق محدد.[٣]

٥- ...

٦ – الاعتراض على معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية (الخاصة به)»[٤].

ثانيًا: نواقص التحكم الفردي

بالرغم من أن تمكين صاحب البيانات يكفل قدرًا من الحماية ويعكس روح إطار حقوق الإنسان العام الذي يعني بالفرد ويتخذه أساسًا للبناء التشريعي لقانون حقوق الإنسان،(٥) إلا أن تأسيس قوانين حماية البيانات الشخصية على سند من التحكم الفردي إنما هو وضعٌ لإمكانيات الإنسان في مواجهة إمكانيات الآلة، وهي مواجهة غير متناسبة. فالفرد الذي يتخذ القرار بالتصرف في بياناته لا يكون مدفوعًا باحتياجاته فحسب، وإنما بأدوات ضغط وتوجيه أخرى تعتمد على تقنية متطورة في القلب منها الذكاء الاصطناعي واستثمارات ضخمة تهدف إلى الحصول على البيانات الشخصية للأفراد لاستخدامها في مواجهتهم لاحقًا. عدم التناسب على ذلك النحو يمكن رصده في غير صورة وممارسة مما يعج به عالم إنترنت اليوم. وفوق ذلك، صاحب البيانات

(١) يقابلهما المادة (١٦) من اللائحة العامة لحماية البيانات.

(٢) يقابلها المادة (١٧) من اللائحة.

(٣) يقابلها المادة (١٨) من اللائحة.

(٤) يقابلها المادة (٢١) من اللائحةS

(5) Jef Ausloos and Pierre Dewitte, 'Shattering One-Way Mirrors – Data Subject Access Rights in Practice' (2018) 8 International Data Privacy Law 28.

الفرد إذ هو يقرر كيف سيتصرف في بياناته، فهو لا يؤثر على خصوصيته هو فحسب، بـل على خصوصية الآخرين كذلك. لذا، فإن التساؤل يثور حول جدوى التحكم الفردي في حماية الفرد نفسه وحماية خصوصية الآخرين.

أ) مستخدم الإنترنت ذو العلم والقدرة

يوفر الذكاء الاصطناعي كما ذكرنا من قبل قدرات تحليلية واستنتاجية فائقة تمكنه ومستخدميـه من توليد بيانات شخصية وربما بيانـات شخصية حساسة عن الشخص لم يتم تقديمها له بواسطة صاحب البيانات نفسه أو أي شخص آخر، وإنما قام الذكاء الاصطناعـي باستنتاجهـا من بيانات غـير ذات صلة أو غير مهمة، وربمـا بيانات غير شخصية من الأساس، أو -كما تم التعبير عنها- من «فتات البيانات».[١]

والقـدرة على ربط البيانات ببعضهـا البعض، واستنتاج معلومات من بيانات مبعثرة أو قليلـة ليس بالأمر المستحدث، لكن ما هو جديد حقًا هو القدرة على استخراج بيانات ومعلومات دقيقة للغاية، ومن أقل كم ممكن من البيانات المتاحة بما يمثل هدية كبرى من الـذكاء الاصطناعي للمسوقين والتجار.[٢] لذلك فإن ما يشترطه قانون حماية البيانات الشخصيـة المصري واللائحة الأوروبية من ضوابط للموافقـة إنما تنصب على الأبعاد المباشـرة أو السطحية للمعالجة. بالأدق، إن العلم الذي ينبني عليه الرضا هنا لا يعكس دائمًا دراية حقيقية وبالتالي رضًا معبر نظرًا للقدرات الفائقة للذكاء الاصطناعي[٣].

إن فرضًـا رئيسًـا وراء التحكم الفـردي هو أنه إذا علم الشخـص بمضمون وغرض المعالجـة، وتم تمكينـه من القرار بناءً على هـذا العلم فإن ذلك يحقـق الحماية؛ سواءً كانت حماية للخصوصية أو للقدرة على التحكم.[٤] إلا أن ذلك الفرض يعيبه افتراض العلـم لدى صاحب البيانات. وذلك افتراض تعوقه العديـد من التحديات. فكما أشرنا للتو، فإن صاحب البيانات قد لا يعي بالضرورة ما يمكن استخراجه من استنتاجات من

(1) Steven M Bellovin and others, 'When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning' [2014] NYU Journal of Law & Liberty 558.

(2) Alicia Solow-Niederman, 'Information Privacy and the Inference Economy' (2022) 117 Northwestern University Law Review 357.

(3) Mireille Hildebrandt, 'Profiling and the Identity of the European Citizen' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer Netherlands 2008).

(٤) نميـز هنـا الخصوصية عن القدرة على التحكم باعتبار أن التحكم والحكم الذاتي هما أحد الأسس الفلسفية التي تميز الحق في البيانات عن الحق في الخصوصية. انظر في هذا الصدد كتابات لي بايجراف، مثل:
Lee A Bygrave, Data Privacy Law: An International Perspective (Oxford University Press 2014).

البيانات التي يقوم بإعطائها طوعًا.[1] فالسيدة التي تشارك بيانات تسوقها الإلكتروني والبيانات الخاصة بوسيلة الدفع فحسب يمكن أن يستنتج منها فئتها العمرية، والطبقة الاجتماعية التي تنتمي إليها، وانتمائها الديني بالنظر إلى الوقت من العام الذي قامت فيه بالشراء ونمط شرائها، أو إذا كان لديها أطفال أم لا، وإذا كانت تعاني من حالة نفسية معينة، وغير ذلك من المعلومات مما لا تتوقع هي استنتاجه.

وإذا نحينا العلم بمآلات البيانات وما يمكن أن ينتج عنها جانبًا، فإن صاحب البيانات عادةً ما لا يهتم بإخطارات الخصوصية لأنه لا يدرك من الأساس مخاطر الخصوصية التي قد تترتب على منحه بياناته،[2] فغالبية مستخدمي الإنترنت والتطبيقات الإلكترونية لم يكونوا ليهتموا بإشعارات الخصوصية وتنبيهات سياسة الخصوصية إلا لو كانوا مضطرين لأخذ قرار بشأنها من أجل الاستمرار في استخدام الخدمة.

وعدم الاهتمام بالبيانات والخصوصية الرقمية هو أمر شائع في مصر، فقد أشارت دراسة حديثة إلى أن (٤٦.٢٪) من مستخدمي تطبيقات الصحة المتنقلة لم يقرأوا أبدا سياسات الخصوصية لهذه التطبيقات قبل تثبيتها على هواتفهم المحمولة.[٣] ذلك مع العلم أننا نتحدث هنا عن بيانات حساسة -متعلقة بتطبيقات صحية- وأن هذه نسبة المستخدمين لم يقرأوا سياسات الخصوصية مطلقًا، دعك ممن اطلع سريعًا دون فهم، أو تصفح فسحب.

وعدم الاهتمام بالخصوصية الظاهر قد لا يعبر بالضرورة عن لا مبالاة، إذ ربما يكون انعكاسًا لصعوبة التعامل مع سياسات الخصوصية وإخطارات الخصوصية حتى وإن توافرت الرغبة. إن تحقق العلم الذي يبنى عليه موافقة حقيقية يفترض أن يكون لدى صاحب البيانات القدرة على التعامل مع إشعارات الخصوصية التي يعطي عليها الموافقة، وقدرة الإنسان في هذا الصدد تثير بدورها عدة إشكاليات. وتلك نتيجة منطقية بالنظر إلى أن إشعارات الخصوصية ووثائق سياسيات الخصوصية تتميز بلغة

(1) Daniel J Solove, 'Artificial Intelligence and Privacy' (Social Science Research Network, 1 February 2024) 32.
(2) Fred H Cate, 'The Failure of Fair Information Practice Principles', Consumer Protection in the Age of the 'Information Economy' (Routledge 2006) 360.

انظر أيضًا: الحق في الخصوصية الرقمية وتحديات عصر التقنية، عزت عبد المحسن سلامة، مجلة العلوم الاقتصادية والقانونية، العدد الأول، ٦٢، ٢٠٢٠، ص ١٠٧٠.

(٣) إدارة الخصوصية المعلوماتية لمستخدمي تطبيقات الصحة المتنقلة: دراسة تحليلية وميدانية، زينب علي البكري، المجلة الدولية لعلوم المكتبات والمعلومات، العدد١١، ٢٠٢٤، ص ١٣.

معقـدة، غالبًا تكون بصياغـات قانونية تتطلب معرفة خاصة أو علـى الأقل انتباهًا من المستخـدم. ومرجع ذلك أن مقدمـي الخدمات بصفتهم متحكمين أو معالجين للبيانات يعتـبرون هذه الإشعـارات بمثابة عقـود ملزمة، وبالتـالي يضيفـون التفاصيل والحذر اللازمين لحماية مصالحهم.[١]

فضلًا على ذلك، وبشكل عام، فإن نموذج حماية البيانات الحالي مبني على افتراض غـير صائب بأن قدرة الإنسان غير محدودة، أو كما يُصاغ اقتصاديًا بـ «المستهلك كامل العقلانيـة ذو الانتبـاه اللامحـدود».[٢] في حين أن عـدد الخدمات التـي يتعامل معها المستخـدم العادي للإنترنـت يوميًا، والتي تتطلـب التواصل بشـأن الخصوصية، سواء لجمـع البيانات أو لتغيـير السياسات والأغراض، هو عدد هائل. لذلك، من غير المعقول أن نتوقـع أن يكون الشخص العادي منتبهًا لـكل هذه المعلومات، حتى وإن رغب.[٣] ومن ثم، فإننـا إن نظرنا إلى عموم جمهور مستخدمي الإنترنت والخدمات الإلكترونية، فإن الاحتمالية الوحيدة المتبقية لبعض الحماية الفعالة بناءً على التحكم الفردي ستكون من شخص حريص على الخصوصية، وليس المستخدم العادي فحسب.

ب) المؤثرات الخارجية على إرادة الفرد

رأينا إذن أن مستخدم الانترنت والتطبيقات الإلكترونية قد يفتقد إلى العلم والدراية الكافيتـين بأهميـة ومضمـون وحدود الحق فـي الخصوصيـة والبيانـات الشخصية، والإنســان فوق ذلـك محدود القدرة، فحتى إذا توافرت الرغبـة، فإن التعامل مع تعقيد وطول إشعارات الخصوصية وسياسات الخصوصية يمثل عبئًا على المستخدم العادي.

يضـاف إلى التحديـات المرتبطة بالقـدرة الذاتية لصاحب البيانـات فئة أخرى من التحديـات أكثر دقة ترتبط بما يتعرض له الفـرد من مؤثرات خارجية دقيقة ومصممة

(1) Brendan Van Alsenoy, Eleni Kosta and Jos Dumortier, 'Privacy Notices versus Informational Self-Determination: Minding the Gap' (2014) 28 International Review of Law, Computers & Technology 190.

(2) ibid 189.

(٣) فـي دراسـة نشرت في ٢٠٢٢، قام الباحثون بدراسة سياسـات الخصوصية لـ ٧٥ من التطبيقات والمواقع الأكثر شهرة وانتهوا إلى أن سياسـات الخصوصيـة أصبحت أطول وأكثر تعقيدًا. تم التوصل إلى أن متوسـط طول سياسة الخصوصية يبلغ حوالي ٤٠٠٠ كلمـة، ممـا يستغرق حـوالي ١٦ دقيقة لقراءتهـا. يشير هذا إلى أن قـراءة جميع سياسات الخصوصيـة التي يواجهها المستخدم يوميًا ستتطلب عدة ساعات. أنظر:

'Privacy Policy Comparison Reveals Half Have Poor Readability' (CHOICE, 27 January 2022) <https://www.choice.com.au/consumers-and-data/protecting-your-data/data-laws-and-regulation/articles/privacy-policy-comparison> accessed 12 December 2024.

للتأثير عليه بحيث تصبح أهمية البيانات بالنسبة إليه ثانوية، وهو مجال يبدو فيه غالبًا دور الذكاء الاصطناعي بشكل أوضح.

مـن الهام أثناء تنـاول مسائل حماية البيانات والخصوصيـة أن يكون في الحسبان دومًـا أن الانترنـت والتطبيقـات الإلكترونية ليسـت تقنية سلبية فيمـا يخص البيانات الشخصيـة؛ تتلقى البيانات إذا منحت لها وهي فيما عدا ذلك ساكنة. على العكس من ذلـك تمامًا، إن تلك التقنيـة في سعي دائم وحثيث للحصول على أكبر كم من البيانات والمعلومـات الشخصية. وهي في سبيـل ذلك تلعب دورًا نشطًا في دفع مستخدميها إلى إعطـاء بياناتهم باستخدام كافة وسائـل التوجيه والضغط المباشر أو غير المباشر، وهو ما يترجم إلى تأثير على إرادة المستخدم الفرد الذي ذكرنا سلفًا أنه ربما لا يملك العلم التام أو القدرة اللا منتهية في الأساس.

لذلك فإنه من الشائع في أوساط البحث والقانون والسياسات العامة وصف النموذج الاقتصادي الحالي علـى أنه اقتصاد البيانات،[١] حيث تحولت البيانات من كونها أداة إلى سلعة في ذاتها،[٢] وهي سلعة عالية الطلب في الأوساط التجارية لأغراض التسويق، وفـي الأوساط السياسيـة على السواء، وهو ما يترجم بالطبـع إلى أدوات تأثير وتوجيه لدفـع الفرد لتسليم بياناته.[٣] وذلك لم يكن ممكنًا إلا بفضل الذكاء الاصطناعي الذي أحدث نقلة في معالجة البيانات مما سرع من عملية تحويل البيانات إلى سلعة.

وقـد تم الإشـارة في هذا الصدد إلى أن الرأسمالية أعـادت ترتيب أوراقها لتحقيق الأربـاح من خـلال المراقبـة الأحادية الجانـب وتعديل السلـوك البشـري. تُعرف هذا الظاهـرة بما أسمته شوشانا زابوف «رأسمالية المراقبـة».[٤] ذهبت زابوف في وصفها تلـك الظاهـرة إلى أن عمليـة الاستهـداف الدقيـق للمستخدمين تتضخـم تحت نظام رأسمالية المراقبة، حيث يتم تسليع سلوك الأفراد عبر الإنترنت وصفاتهم وتفضيلاتهم فـي سوق سلوكي. إن عمالقة التقنية مثـل فيسبوك وجوجل ومايكروسوفت يستخدمون تحليـلات البيانات المستندة إلى الذكاء الاصطناعي ونماذج التنبؤ بالبيانات ليس فقط

(1) Manuel Castells, 'Communication, Power and Counter-Power in the Network Society' (2007) 1 International Journal of Communication 29.

(2) Sandra Wachter and Brent Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Columbia Business Law Review 528.

(٣) التكييف الفقهي لبيع البيانات الشخصية، هالة عبد المحسن شتا، مجلة الزهراء، ٣٣، ٢٠٢٣، ص ٨٢٩.

(4) Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) 30 Journal of Information Technology 75.

«لتوقع ما نشعر به، نفكر فيه، ونفعله»،[١] بل أيضًا «لدفعنا وتوجيهنا وضبط سلوكنا نحو نتائج مربحة»[٢].

تلك الآلة الاقتصادية الضخمة تتخذ من تقنية التخصيص أداة لدفع الأفراد لتسليم بياناتهم، وهي في الواقع أداة فعالة. إن الفرد سواءً كان مستخدمًا للخدمات الإلكترونية أو مستهلكًا يمكن أن يستفيد بل ويستحسن الخدمات المفصلة التي تتيحها تقنية التخصيص. من منا لا يحب أن يظهر له أولًا نوعية الأخبار التي يفضل قراءتها، أو العروض على المنتجات التي يهتم بها، أو حتى أن ترشح له لوحة المفاتيح الكلمة التالية في النص الذي يكتبه بناءً على أسلوبه في الكتابة. لكن في المقابل يتحول المستخدم إلى كتاب مفتوح أمام تلك التقنية، حتى لو كان مهتمًا بالخصوصية.

ذلك التضارب بين الإدراك الظاهري لقيمة الخصوصية وفي الوقت ذاته الاستعداد لمقايضة البيانات الشخصية والخصوصية بالخدمات المخصصة تم رصده في ظاهرة يطلق عليها «مفارقة التخصيص والخصوصية» (Personalisation–privacy paradox)، حيث يبدي المستخدمون اهتمامًا مبدأي بالخصوصية، بينما تنخفض قيمتها لديهم عملًا مقابل تخصيص الخدمات التي يتلقونها.[٣] وتمثل مفارقة التخصيص والخصوصية مثالًا واضحًا للتحدي الذي يواجه قوانين حماية البيانات الشخصية ذلك أن اختيار الأفراد مقايضة البيانات بالخدمة يؤدي إلى تقويض الخصوصية ومع ذلك ليس بالضرورة مما يثير مما يثير مسؤولية المتحكم أو المعالج ذلك أنه يمكن القول بأن تسليم البيانات يتم طوعًا.

يلزم في هذا السياق التمييز بين البيانات اللازمة لتقديم الخدمة والبيانات التي يجبر عليها المستخدم دون ضرورة لتقديم الخدمة، حيث إن الفئة الثانية تعتبر مخالفة للقانون. وفي هذا الصدد، تشترط اللائحة العامة لحماية البيانات أن تكون الموافقة حرة،[٤] أي غير مشروطة بتبعات سلبية. وفي تفسير الموافقة الحرة تم اعتبار أن ذلك

(1) Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (First edition, PublicAffairs 2019) 95.

(2) ibid 25.

(3) Chung Hun Lee and David A Cranage, 'Personalisation–Privacy Paradox: The Effects of Personalisation and Privacy Assurance on Customer Responses to Travel Web Sites' (2011) 32 Tourism Management 987.

(٤) المادة (٦) من اللائحة العامة لحماية البيانات؛ تجدر الإشارة إلى أن المشرع المصري لم يضمن القانون شروطًا معينة لصحة الموافقة، وذلك فيما عدا كون الموافقة صريحة في المادة (٢).

الشـرط غـير متوافر حينما يكـون الشخص مضطـرًا للموافقة على جمـع بيانات غير ضرورية من أجل تقديم الخدمة وذلك كي يتم السماح له بالحصول عليها.[١] وألا تكون الموافقة صحيحة إلا إذا كان بإمكان صاحب البيانات ممارسة اختيار حقيقي، ولم يكن هنـاك خطر من الخـداع أو الترهيب أو الإكـراه أو عواقب سلبية كبـيرة في حال عدم موافقته[٢] .

وحتى إن ميزنا في هذا السياق بين البيانات اللازمة لتقديم الخدمة والبيانات التي يجـبر عليها المستخـدم دون ضرورة لتقـديم الخدمة فإن الأمر لازال يثـير إشكاليات. فمـن ناحية، قد يصعب على المستخدم الفـرد تحديد ما إذا كانت الموافقة التي يعطيها حـرة أم لا. تقدير مثلًا أن بيان معين ضروري لتقديم الخدمة قد يصعب عملًا تحديده مـن قبل متلقي الخدمة، ذلك إذا وضع الجهد للنظر في الأمر من الأساس. وبالإضافة إلى هذا، أليس الإغراق في أكوام من الإشعارات والسياسات التي يجب على المستخدم أن يعالجهـا يوميًا يسلب فكرة التحكم جدواها من الأساس دون الحاجة إلى النظر في مدى جودة شروط الموافقة أو الالتزامات تحت العقد.

إننا حتى مع ذلك كله لا نضع في الاعتبار تحد آخر للتحكم الفردي لا تعالجه قوانين حماية البيانات الشخصية ألا وهو القدرة الهائلة لتلك الآلة الضخمة على الإقناع، وهي مسـار يتجنب حمايـة البيانات القائمة علـى التحكم الفردي، لتجعـل مقدمي الخدمة منفرديـن بالأفـراد يقنعونهم بآراء وتوجهات، مـن بينها تسليم بياناتهـم. إن شوشانا زابـوف وهـي تقدم فكرة رأسماليـة البيانات في ٢٠١٥ وتشير إلى تجـاوز قدرة الذكاء الاصطناعـي مجرد فهمنا إلى التأثير علينا لم يكن مـن السهل تخيل أنه خلال أقل من عقد ستتخلل حياتنا ألوان من تقنيات الذكاء الاصطناعي التي بإمكانها توجينا وتشكيل آرائنـا ووعينـا بالشكل التي هـي عليه اليـوم. ولم يأخذ الأمر طويـلًا، ففي خلال عام واحد فقط وقعت حادثة كامبريدج أناليتيكا (Cambridge Analytica) التي جمع فيها

(١) الحيثية (٤٣) من اللائحة العامة لحماية البيانات

(2) Article 29 Data Protection Working Party, 'Opinion 15/2011 on the Definition of Consent' (2011) 01197/11/EN, 12.

وحيث لم يرد في القانون المصري خصائص للموافقة غير الصراحة، وكانت المعاملات التي يحتاجها الشخص عادةً ما تكون فـي صورة عقـود إلكترونية غير قابلة للتفاوض، فقد اتجه بعض الفقه المصري إلى تكييف هذه العقود على أنها عقود إذعان، وهـو مـا لا يستقيم مع شرط الاحتـكار بطبيعة الحال. انظر: الحمايـة القانونية لخصوصية البيانـات الشخصية في العصر الرقمي، طارق جمعة السيد راشد، مجلة القانون والاقتصاد، ملحق خاص العدد ٩٢، ٢٠١٦، ص ٢٧١.

بيانـات ٥٠ مليون مستخدم فيس بـوك للتأثير عليهم بخصوص الانتخابات الرئاسية الأمريكية التي انعقدت في ٢٠١٦.[١]

إن خطـر الذكاء الاصطناعي في العمـوم وخطره بخصوص قدرته الإقناعية هو ما أزاح قوانـين حماية البيانـات الشخصية من موقعها كخط دفـاع أول ضد تقنية الذكاء الاصطناعي لتصعد قوانـين تنصب على الذكاء الاصطناعي تحديدًا.[٢] فنجد الاتحاد الأوروبي يصدر قانون الـذكاء الاصطناعي (Artificial Intelligence Act) هذا العام، ويضع فـي صدره تقنية الذكاء الاصطناعي التي تتعلق بالإقنـاع وبالتحكم في الإنسان عن طريق التلاعب أو الخداع على رأس مخاطر الذكاء الاصطناعي ويجعلها على رأس أنظمة الذكاء الاصطناعي المحظورة.[٣]

لِنُعـد النظر في دورة تأثير البيانات لفهم لماذا أصبـح الحديث عن إرادة الشخص الحرة بصدد تحكمه في البيانات في غير محله في مواجهة قدرات الذكاء الاصطناعي الاقناعية. إن مستخدم الانترنت يقع منذ دخوله الإنترنت في دورة مغلقة – دورة تأثير البيانات – تضيق عليه تدريجيًا لاعتصار المعلومات والبيانات الشخصية منه -إراديًا- بدءًا من اسمه ووصولًا إلى بث مباشر لصورته وصوته وتطورات ميوله السياسية وحياته العاطفية وحالته النفسية.

ففـي مرحلة أولى مـن الدورة يدفع مقدمـو الخدمات المستخدم لتسليـم بياناته أو يستغلـون ميولـه النفسية ليقوم هو بنفسه بذلك. فهناك قـدر من البيانات لازم لتقديم الخدمـة. وهناك قدر من البيانـات يقدمه المستخدم للحصول علـى خدمات إضافية. لكن فوق ذلك، ينساق المستخدم لترك بيانات ليست هي من ذلك ولا ذاك ليحتفظ بها مقدم الخدمة وهو مدفوع بدافع لا يعلمه.

يعلـم القائمـون على مواقـع التواصـل الاجتماعـي -باعتبارها أبرز مثـال في هذا الصدد- بأن الإنسان في طوره العادي يتحلى برغبة في إثبات الذات والمفاخرة. فتعمل

(1) Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' The Guardian (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 16 November 2024.

(2) Nathalie A Smuha, 'The Paramountcy of Data Protection Law in the Age of AI (Acts)' in EDPS (ed), Two decades of personal data protection. What next? EDPS 20th Anniversary (Publications Office of the European Union 2024) <https://papers.ssrn.com/abstract=4874388> accessed 12 December 2024.

(٣) المادة (٥) من قانون الذكاء الاصطناعي الأوروبي.

تلـك المواقـع على تغذية هذا الشعور وتزيد الرغبة عـن المستخدم في الظهور ومشاركة أخبـاره ومستجداتـه، بل وتشكيـل تلك الأخبـار والمستجدات، وتمنحه أسبـاب وأدوات ذلك.[١] فالمستخدم يُعطىَ الأدوات في صورة القدرة على مشاركة صور وموقع ومقاطع مصـورة وأراء مكتوبة ويمكنه تعديل ذلك بسهولـة وبمخرجات احترافية. تلك الأدوات يجتمـع معهـا دوافع/أسباب النشـر والمشاركة،[٢] فنجد أن المستخـدم يقابل اتجاهات (Trends) مواقـع التواصـل الاجتماعي، اتجاهات الموضـة، واتجاهات التطبيقات مثل تطبيقـات الشبـكات الاجتماعية والألعـاب. كما يتعرض لقضايا عامة ممـا يسمح له بالوصـول للمستخدم. كل ذلك يُقدم للشخص بناءً على تفضيلاته في معظم الأحيان، فتكون النتيجة تبادل تفاعلي للآراء السياسية والدينية والشخصية والتفضيلات بشكل عام بين المستخدمين، في بيئة صممت ليدفع كل منهم الآخر لكشف المزيد من البيانات.

في مرحلة ثانية، معالجة البيانات، بقدر يسير جدًا من الشفافية، إن لم يكن نظريًا فبالطبـع عمليًا، يتم معالجة البيانات بغرض ظاهر وهو تقديم الخدمة ذاتها، وتحسين تلـك الخدمة، وأيضًا بغرض موازٍ وهو فهم أكبر للمستخدم والحرص على إبقائه عالقًا فـي الدورة. هنـا يتم تحويل البيانـات إلى معلومـات، وربط معلومات الفـرد ببعضها البعض وبمعلومات غيره من المستخدمين.

فـي مرحلـة ثالثـة، نشـر البيانـات والمعلومات، يتـم العـودة إلى المستخـدم الفرد والمجموعات التي تشبهه في الميول والصفات، وعموم المستخدمين، بمعلومات مخصصة ومفصلة فرديًا لكل مستخدم بغرض تشكيل اختياراته التالية، سواءً كان ذلك بخصوص مـا سينشـره من بيانات ومعلومات لاحقة، أو بخصوص قضايا أخرى فئوية أو عامة – فيبـدأ هنا حبسه فـي فقاعات التصفيـة (Filter bubbles) وغـرف الصدى (Echo chambers) على سبيل المثال.[٣]

فـي مرحلـة رابعة، التغذيـة الرجعية والتكيـف، تظهر أحد القدرات غـير المسبوقة للـذكاء الاصطناعي وهي بمثابة الحلقة التي تغلق بها الدورة. الذكاء الاصطناعي يقوم

(1) Amanda Nosko, Eileen Wood and Seija Molema, 'All about Me: Disclosure in Online Social Networking Profiles: The Case of FACEBOOK' (2010) 26 Computers in Human Behavior 406.

(2) Jan Fox, 'An Unlikeable Truth: Social Media like Buttons Are Designed to Be Addictive. They're Impacting Our Ability to Think Rationally' (2018) 47 Index on Censorship 11.

(٣) الاستبداد الرقمي من خلال فقاعات التصفية وتأثيره على الحرية الرقمية: دراسة مسحية لعينة من مستخدمي تطبيق فيس بوك، بزيط نورة وعشور بثينة نسرين، رسالة ماجيستير مقدمة لجامعة محمد خيضر بسكرة، ٢٠٢٤.

برصـد ردود الفعـل على ما تم نشـره من معلومـات لفهمها ومن ثـم التأقلم معها عبر التغذيـة الرجعيـة. ذلـك يساعده على إدراك ما هـو الأسلوب أو نوعيـة المعلومات ذات الفعاليـة علـى المستخدمين، وما الـذي يَفتَقِدُ للتأثـير عليهم فيتم تغيـيره بآخر. نظرًا للقـدرات التحليلية الفائقة، تلك المرحلة تضمن شيئـين، الأول هو التأكد من فهم دقيق تمامًا للأفراد من خلال التغذية الرجعية. الثاني هو التجديد المستمر لهذا الفهم بحيث يسير الذكاء الاصطناعي حذو المستخدم في تطوراته وتغيراته، بل ويسبقه.[١]

نستخلص من ذلك أن المستخدم الفرد وهو ضعيف العلم والقدرة أصلًا، يدخل منذ دخولـه الإنترنت في دورة صممت لضمـان تأثير مستمر ومتجدد عليه بشكل مخصص ومفـرد له، تؤثر عليه وتتعلم عنه، وبالتوازي تستخدم تلك المعرفة في التأثير على غيره أيضًـا. فتضحى النتيجة ضعف الفرد أمام الآلـة،[٢] وإضعاف للآخرين كذلك، وهو ما سننظر فيه في المبحث التالي.

(1) Daniel Susser, Beate Roessler and Helen Nissenbaum, 'Technology, Autonomy, and Manipulation' (2019) 8 Internet Policy Review.

(2) Alicia Solow-Niederman, 'Information Privacy and the Inference Economy' (2022) 117 Northwestern University Law Review 357.

المبحث الثالث

الحق المشترك في البيانات

أحد كبرى الإشكاليات هو أنه بفضل الذكاء الاصطناعي على النحو الذي عرضنا له، أصبح العالم قرية صغيرة بحق، وأصبحت أنماط الشخصيات وتشابهاتها ومواطن ضعفها وقوتها مفهومة أكثر من أي وقت مضى. وذلك إذا كان له انعكاس واضح فهو كيف أن القدر القليل من الجهد أصبح يترجم إلى أثر كبير؛ أن القدر اليسير من البيانات أصبح يترجم إلى تأثير أوسع بكثير من صاحب البيانات. إن صاحب البيانات الفرد اليوم حينما يمنح بياناته، فهو لا يمنح بياناته وحده، وإنما أصبح يكشف خصوصية الآخرين ممن يشاركونه الصفات بطريقة ما. في هذا الجزء سنلقي نظرة أعمق على تأثير الذكاء الاصطناعي على نظرتنا التقليدية للخصوصية والبيانات الشخصية باعتبارهم مكنة ومجال تأثير فردي فحسب، ومن ثم نشكل تصور أوضح للحق المشترك في البيانات الشخصية وجدوى التحكم الفردي بشأن حماية الخصوصية – غير الفردية.

أولًا: تأثير البيانات الشخصية على الغير

الفقه والتشريع التقليدي حول البيانات الشخصية كان على مدار العقدين الماضيين ولازال ينظر للبيانات الشخصية باعتبارها حق خاص (Private right)، بمعنى أن بيانات الشخص تعني صاحب البيانات، وتؤثر فيه، وتبعًا هو من يستطيع أن يتحكم فيها.[1] والقانون يعكس ذلك عبر أدوات التحكم الفردي، فجمع البيانات يحدث من خلال الموافقة المباشرة بشكل حر أو من خلال دخول صاحب البيانات في عقد، وهما الحالتان الأكثر شيوعًا، على الأقل للأغراض التجارية، وهو كذلك له الحق في معرفة سياق المعالجة، وله الحق في الاعتراض عليها.

مع التطور التقني الكبير وخاصةً تفجر إمكانيات الذكاء الاصطناعي والبيانات الضخمة في الفترة منذ صدور توجيه حماية البيانات الأوروبي (Data Protection Directive) في ١٩٩٥ تنبه المشرع الأوروبي إلى الحاجة وضع التزامات جديدة وتبني

(1) Nadezhda Purtova, 'Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), Under Observation: The Interplay Between eHealth and Surveillance (Springer International Publishing 2017).

إطار تنظيمي يضمن قدرًا من حماية البيانات بشكل يتجاوز رضا صاحب البيانات، وهو ما تمخضت عنه اللائحة العامة لحماية البيانات كبديل للتوجيه السابق في ٢٠١٦. فبدلًا من الاقتصار على القواعد تم الاتجاه إلى تنظيم يعتمد على القواعد والمبادئ معًا (Rules and principles). [١] ومثلًا تم إضافة مبدأ المسائلة[٢] حيث لا يلتزم المتحكم أو المعالج بالامتثال للائحة فحسب، بل عليه أن يكون على استعداد للمسائلة عن هذا الالتزام، فيجب عليه الاحتفاظ بسجلات أنشطة المعالجة،[٣] وكذلك الالتزام العام بمراعاة ودمج حماية البيانات منذ مرحلة تصميم الخدمات والتقنية فيما عرف بحماية البيانات عبر التصميم وبشكل افتراضي (Data protection by design and by default). [٤] كما أضافت اللائحة الالتزام بإجراء تقييم تأثير بخصوص حماية البيانات (Data protection impact assessment) متى كانت المعالجة التي تشملها الخدمة المقدمة يحتمل أن تنطوي على مخاطر عالية بالنسبة لحقوق وحريات أصحاب البيانات.[٥] لكن مع ذلك استمر التركيز على اعتبار الخصوصية حق خاص، وهو ما انعكس على استمرار الاعتماد على الموافقة مع تعزيزها،[٦] وكذلك الاهتمام بزيادة الشفافية في مواجهة صاحب البيانات.[٧]

لكن مع هذا، يبقى السؤال: هل يحقق ذلك تحكم حقيقي؟ أو حتى حماية للبيانات أو الخصوصية حقيقية؟ والإجابة التي ذهبت إليها الكثير من الكتابات هي (لا). (٨) وأحد الطرق لفهم ذلك هي استيعاب أن البيانات أصبحت تؤثر على الغير -صاحب/ أصحاب بيانات آخرين- كما تؤثر على صاحب البيانات نفسه. هذا التأثير بيانه القدرة على الاستنتاج بالنسبة للغير، وكذلك انعدام القدرة بالنسبة للغير.

---

(١) المادة (٥) من اللائحة.

(٢) السابق.

(٣) السابق، المادة (٣٠).

(٤) السابق، المادة (٢٥).

(٥) السابق، المادة (٣٥).

(٦) فأصبحت ليست فقط حرة، وإنما صريحة، ومبنية على معرفة، انظر:

European Data Protection Board, 'Guidelines 05/2020 on Consent under Regulation 2016/679' (European Union 2020).

(7) Article 29 Working Party, 'Guidelines on Transparency under Regulation 2016/679' (European Union 2018).

(8) Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (Social Science Research Network, 15 December 2017) <https://papers.ssrn.com/abstract=3071875> accessed 19 December 2024.

إن التركيـز علـى البيانات كحـق خاص يجعل النظـر منصبًا على كيـف أن القدرة التحليليـة للـذكاء الاصطناعـي قـد تُخـرج استنتاجات عـن الشخـص لم تكن ممكنة بالطـرق التقليديـة والقدرة البشرية علـى التحليل. إلا أن تلك القـدرة تتجاوز استنتاج معلومات عن الفرد إلى استنتاج معلومات عن المجموعة؛ عن المجموعة التي ينتمي إليها صاحـب البيانات. فإذا كنا نتحدث من قبل عن التنميط كممارسة فردية يتم فيها بناء ملـف إلكـتروني للشخص تركب فيه بياناتـه للخروج بصفات ومعلومـات إضافية عنه والتنبـؤ بتصرفاتـه المستقبلية، فيمكـن للتبسيط القول بأن تقنية الـذكاء الاصطناعي تقوم بتنميط جماعي يتم فيه جمع بيانات الأفراد المشتركين في السمات والخصائص والآراء بحيـث يتـم الخروج بصفات ومعلومـات إضافية عن تلـك المجموعة، وبالتبعية التنبؤ بتصرفاتها في المستقبل، أي التنبؤ بتصرفات أفرادها في المستقبل.[١]

وهـذا يعنـي أن ذلك القـدر اليسير من البيانات الـذي يعطيه شخـص فيعود عليه باستنتاجـات كبرى ودقيقة من الذكاء الاصطناعي قد يكون -أو في الغالب هو كذلك- انعكاسًـا لعملية تنميـط لأشخاص أخر يشاركونه الصفـات النسبية ذات الصلة بحيث تكون مشاركة الفرد لبياناته هي مشاركة غير مباشرة لبيانات غيره، والقدر اليسير من مشاركـة كل شخـص منفردًا إنما يصب في بوتقة أكـبر تخص كل من يشبهونه، يمكن مـن خلالها تعريف كل منهم بقدر أكبر مما كشفه كل منهم عن نفسه منفردًا. ذلك ما عـبرت عنه بريسيـلا ريجان استشرافًا منها للمستقبل بأنـه يصعب على شخص واحد أن يحصـل علـى الخصوصية دون أن يحصـل جميع الأفراد على حـد أدنى مماثل من الخصوصية[٢].

والمجموعـات التـي يمكـن تقسيم الأشخاص إليهـا لا نهائية وتتنوع بتنـوع الخدمة المقدمـة وما إذا كان تصنيـف ما يفيد تلك الخدمة. لذا قد يكـون التصنيف بناءً على سمات معينة مثل الجنس أو السن أو اللغة أو النطاق الجغرافي. كما قد يكون بناءً على الاهتمامات والآراء، وهو ما يمكن تسميته التنميط بالتقارب (Affinity profiling) وهو

(1) Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), Profiling the European Citizen: Cross-Disciplinary Perspectives (Springer Netherlands 2008).»plainCitation»:»Mireille Hildebrandt, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds

(2) Priscilla M Regan, Legislating Privacy: Technology, Social Values, and Public Policy (1st edn, The University of North Carolina Press 2000) 212.

تصنيف الأشخاص حسب اهتماماتهم المفترضة وليس فقط سماتهم الشخصية.[١] وهو ما يثير إشكاليات لا تتصدى لها قوانين حماية البيانات الشخصية بالنسبة للخصوصية، والتمييز، وكذلك خلق مجموعات جديدة غير متعارف عليها تقليديًا قد تخضع للتمييز أيضًا.[٢]

الإشكالية التالية إذن هي أن قوانين حماية البيانات الشخصية بما أنها تحمى الحق الخاص في البيانات، فإنها غير معنية بالقدر الكافي ببيانات المجموعة. وبنظرة أدق، فإن «المجموعة» لا تملك حقوقًا مباشرةً تحت قوانين حماية البيانات الشخصية، إلا من خلال أعضائها فرادى وفيما يخص بياناتهم الشخصية.

وذلك ينعكس بوضوح في عدم جدوى أدوات التجهيل: التجهيل (anonymisation) والاستعارة (pseudonymisation). فبينما أن هذه الأدوات يفترض أنها تخفي شخصية صاحب البيانات، إما بشكل نهائي أو مؤقت، بحيث لا يمكن التعرف عليه،[٣] إلا أن ذلك يصبح غير ذي نفع بالنسبة للمجموعة إذ أن ما تم جمعه من بيانات –غير شخصية الآن– يتم استخدامه في تعريف المجموعة ذاتها، وبالتالي يمكن ان يتحول في أي لحظة إلى بيانات من شأنها تعريف أيًا من أفراد هذه المجموعة بمجرد أن يقدم بيانًا شخصيًا يكفي لنسبه إلى تلك المجموعة. وفكرة «تعريف المجموعة» تلك مما يخرج عن التعريف الذي يتبناه القانونان المصري والأوروبي للبيانات الشخصية[٤] ولا يدخل في نطاق أي من القانونين.

لذلك فنحن إذا كنا نتحدث في الأعلى عن عدم قدرة الفرد على التحكم بشكل

(1) Sandra Wachter, 'Affinity Profiling and Discrimination by Association in Online Behavioural Advertising' (2020) 35 Berkeley Technology Law Journal 367.

(2) ibid at 367, 414; Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 475.

(٣) انظر المادة (٤) من اللائحة للتعريفات، مع العلم بأن القانون المصري لم يرد به هذان المفهومان.

(٤) تعرف المادة (٤.١) من اللائحة البيانات الشخصية على أنها: «أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد» («صاحب البيانات»).

ويُعتبر الشخص الطبيعي قابلاً للتحديد إذا كان بالإمكان التعرف عليه، بشكل مباشر أو غير مباشر، خصوصًا عبر الإشارة إلى معرف مثل الاسم، رقم التعريف، بيانات الموقع، معرف على الإنترنت، أو عبر الإشارة إلى واحد أو أكثر من العوامل الخاصة بالهوية البدنية أو الفسيولوجية أو الجينية أو العقلية أو الاقتصادية أو الثقافية أو الاجتماعية لذلك الشخص.»

كما يعرف القانون المصري البيانات الشخصية على أنها: «أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية.»

حقيقـي، وكان الحديـث بذلك منصبًا علـى وجود وسائل تحكم يقرهـا القانون للفرد، فـإن الحديث عـن التحكم بالنسبة للمجموعة ينعدم تمامًـا. وذلك من ناحية لأن قدرة الشخص الفرد على التحكم الحقيقي في بياناته ضعيفة على نحو ما رأينا، ناهيك عن إدراكـه ومـن ثم تحكمه فيما ينتج عـن تلك البيانات من استنتاجـات تتعلق بالمجموعة التـي ينتمي إليها. وهو حتى إن أراد وحرص على ذلك، فإنه سيصطدم بخروج بيانات ومعلومات المجموعة عن نطاق حماية قوانين البيانات الشخصية إذا تم تجهيلها.[١] هذا مـن ناحية، ومن ناحية أخرى فإن المجموعة ذاتها -أيًا كان شكلها أو الصفات الجامعة لهـا- فإنها ليست مما تعترف به قوانين البيانات الشخصية بالكلية، ولذا ينحسر عنها أي حديـث عن وسائـل حماية قانونية.[٢] لذلـك فإن التحكم الفـردي لا يكفي لحماية المجموعة، وبالتالي لا يكفي لحماية الأغيار ممن يدخلون تحت تلك المجموعة.

ثانيًا: الخصوصية والبيانات الشخصية كمورد مشترك

البنـاء الـذي أقمناه حتى الآن في هـذه الدراسة ينبئ عن شيئـين: الأول هو قصور القدرة الفردية وضعف التحكم الفردي، والثاني هو أن مجال حماية البيانات الشخصية في ظل تقنية الـذكاء الاصطناعي يغفل حماية بيانات وتصنيفات المجموعة. وبحسبان ذلك، ربما ينبغي إعادة النظر في طبيعة البيانات الشخصية والخصوصية باعتبارهما حـق خاص، وتحديدًا هـل ستتحقق حماية أكبر إذا وضع ذلـك البُعد المشترك للبيانات في الاعتبار عند تكييف البيانات والخصوصية.[٣]

يمكـن الاستفادة من الدراسات البينيـة بين الاقتصاد والقانون في هذا الصدد، إذ اتجهت عدة دراسات إلى النظر إلى البيانات باعتبارها سلعة (A good) أسوةً بالموارد الاقتصاديـة - وليس المقصود هنا فكرة تسليع البيانات بمعنى الإتجار فيها كما الحال بالنسبة لسماسرة البيانات، وإنما التحليل الاقتصادي للبيانات كمفهوم قانوني.

النظـرة التقليديـة للحق فـي الخصوصيـة والبيانات علـى أنه حق خاص تنعكس اقتصاديًا يمكن ترجمتها اقتصاديًا باعتبار الخصوصية سلعة خاصة (Private good). والسلـع الخاصة هـي تلك التي تتميز بتنافسية شديدة وكذلـك قابلية كبيرة للاستبعاد

(1) Sandra Wachter, 'Data Protection in the Age of Big Data' (2019) 2 Nature Electronics, 7.
(2) Linnet Taylor, Luciano Floridi and Bart Van Der Sloot (eds), Group Privacy: New Challenges of Data Technologies (Springer International Publishing 2017).
(3) Brent Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics' (2017) 30 Philosophy & Technology 478.

(الإقصائية). ومثالها الملكيات الخاصة كالسيارة والمنزل وخلافه. وبالتطبيق على البيانات الشخصية فإن الخصوصية تكون تنافسية بمعنى أن استخدام صاحب لحقه في الخصوصية ينتقص بحسب الأصل من استخدام الآخرين للبيان أو المعلومة الخاصة. وهو ذو قابلية كبيرة للاستبعاد بحيث إن صاحب البيانات يستطيع أن يتحكم فيمن يرى أو يستعمل بياناته، وبالتالي أن يستبعد من يريد من استعمال ذلك البيان. وهو ما يعني بمفهوم آخر أن صاحب البيانات يستطيع أن يتمتع ببياناته دول تدخل من الغير.

وكما هو واضح من واقع ما تم تناوله قبلاً، فإن ذلك التصنيف للبيانات غير دقيق من الناحية الوصفية – لا يعبر عن الواقع. كما أنه حتى لا يوفر رؤية معيارية (Normative) مناسبة؛ تسعى وتكفل حماية حقيقية للبيانات والخصوصية، نظرًا لأنه لا يخبرنا كيف يمكن حماية بيانات المجموعة.

وبخصوص عدم دقة وصف الخصوصية وحماية البيانات كسلعة خاصة، فإن صاحب البيانات لا يستطيع عملاً أن يتحكم في البيانات، فهي أقرب لعدم القدرة على الاستبعاد. فصاحب البيانات عملاً ينتهي به الأمر مجبرًا على أن يتنازل على بياناته مقابل الحصول على بعض الخدمات مثل خدمات التواصل الاجتماعي وتخصيص المحتوى، وقبل ذلك الخدمات الأساسية مثل الرعاية الصحية والخدمات البنكية وحتى الخدمات العامة. فإن أراد الحفاظ على خصوصيته فإن عليه التنازل عن هذه الخدمات وهو أمر عالي التكلفة بالنسبة له، وسيؤثر على أداء المجتمع الاقتصادي ككل، كما في حالة الخدمات العامة حيث سيتعذر تكوين فهم كامل لاحتياجات المواطنين نظرًا لانتقاص المعلومات. وذلك مما يتنافى مع خصائص السلعة الخاصة التي يمكن استبعاد الأخرين من الاستمتاع بها دون تكلفة.[1] ويضاف إلى ذلك كما رأينا عدم واقعية قدرة الشخص على التحكم في بياناته من الأساس، وأن التغلب على ذلك ومحاولة تحقيق تحكم حقيقي سينعكس أيضًا في تكلفة عالية في صورة وقت ومجهود كبيرين.

يمكن القول أيضًا بأن منطق السوق وقوى العرض والطلب تتنافى مع اعتبار البيانات

(1) Priscilla M Regan, 'Privacy and the Common Good: Revisited' in Beate Roessler and Dorota Mokrosinska (eds), Social Dimensions of Privacy: Interdisciplinary Perspectives (Cambridge University Press 2015) 62.

سلعة خاصة حيث إنه يفترض أن يحقق السوق الحر عرض يتناسب مع الطلب من تلقاء ذاته. إلا أن ذلك لا ينطبق هنا حيث إذا تركت الخصوصية للسوق فإن الراجح هو تقويض الخصوصية، أو بتعبير اقتصادي سيقدم السوق عرضًا دون المستوى الأمثل بالنسبة للخصوصية (Suboptimal supply). وبيان ذلك هو أنه في حالة الخصوصية، لا يستطيع أي شخص بمفرده أن يضمن مستوى الخصوصية الذي يريده، نظراً لأن معلوماته الشخصية غالباً ما تُجمع وتُستخدم بطرق لا يمكنه السيطرة عليها تماماً. وفي المقابل، لا تمتلك الشركات حافزًا قويًا لتوفير مستوى الخصوصية الذي قد يعتبره المجتمع مناسبًا. ونتيجة لذلك، وكما هو الحال مع الهواء النظيف والدفاع الوطني- كسلع عامة-، غالبًا ما تكون هناك حاجة لتدخل حكومي أو تنظيمات أو جهود جماعية أخرى لتحقيق مستوى معقول من الخصوصية.

وبتعبير بسيط، فإن منطق المؤسسات، كانت عامة أو خاصة، يدفعها لجمع أكبر قدر ممكن من المعلومات عن الأفراد، وذلك للحدّ من أي مخاطر تنجم عن اتخاذ القرارات بشأن هؤلاء الأفراد، وهو ما سينطوي عادةً على مساس بالخصوصية بصدد جمع البيانات واستخدامها. وفي المقابل، عادةً ما يكون منطق الأفراد هو عدم الالتفات إلى الآثار المترتبة على الخصوصية في قراراتهم. وغالباً ما تكون الخيارات المتعلقة بالخصوصية تكاليف خفية للمعاملات؛ فالفرد يركّز على عملية الشراء أو الخدمة التي يتفاوض بشأنها، وليس على الفرصة أو الحاجة لاتخاذ قرار بشأن الخصوصية. وبذلك، فإن كلًا من حسابات المؤسسة وحسابات الفرد تؤديان إلى تقليل مستوى الخصوصية — أي توفير دون المستوى الأمثل — وذلك لأن جودة المعلومات المتداولة داخل النظام قد تتردى، كما قد تتضرر الثقة بالنظام ذاته. وإذا ترك الأمر للسوق دون تدخل، فإن انتهاكات الخصوصية تكون نتيجة حتمية لإخفاقات السوق.[1]

ذلك ينقلنا إلى السلع العامة، وهي ما يحتاج إلى تدخل الدولة بصدده لضبط السوق وصولًا إلى المستوى الأمثل. والسلع العامة تتسم بعدم القابلية للاستبعاد، فلا يمكن استبعاد شخص من خدمة الدفاع مثلًا لأنه لم يدفع الضرائب.[2] ويثور بخصوص السلع العامة مشكلة الراكب المجاني (Free-rider problem) حيث قد يتمتع الراكب

(1) ibid.

(2) Katarzyna Śledziewska and Renata Włoch, 'Should We Treat Big Data as a Public Good?' in Mariarosaria Taddeo and Luciano Floridi (eds), The Responsibilities of Online Service Providers (Springer International Publishing 2017).

المجـاني بالخدمات العامـة دون تأدية المقابل، وبينما يستمر هـو في استقبال الخدمة، فإن الأثار السلبية لسوكه تضر بالكافة ويؤثر على الجودة النهائية.[١] وهذا مما ينطبق على الخصوصية وبيئة البيانات (Data ecosystem)[٢] حيث لا يملك صاحب البيانات قـدرة حقيقية على التحكم فيهـا، وصاحب البيانات الذي يعامـل بياناته بإهمال يضر بالخصوصية عامةً، خصوصية المجموعة.

بالإضافـة إلى عـدم القابلية للاستبعـاد، فالسلع العامة كذلك تتميـز بالاستهلاك غـير التنافسي؛ فلا ينتقص استخدام شخص لها من قدرة الآخرين على استخدامها. إلا أن البيانـات الشخصيـة والخصوصيـة لا تدخلان تحت التصنيـف التقليدي للسلع العامة، تحديدًا بسبب تنافسية الخصوصية وحماية البيانات ذلك أن استخدام الأفراد للخصوصيـة وبيئة البيانات على نحو يسمح بجمع مزيد من البيانات يؤدي إلى انتقاص الخصوصية واستنزاف بيئة البيانات.

التصـور الأقرب للواقع والـذي يضع في الحسبان الحاجـة إلى حماية البيانات من قـدرات التحليل الفائقة وكذلـك خصوصية الجماعة هو اعتبار حمايـة البيانات مورد مشـترك (Common pool resource)، أو مـا يمكن تسميتـه بالخصوصية المشتركة. والمـوارد المشتركة هي موارد طبيعية أو مجتمعية يصعب استبعاد الأفراد من الاستفادة منهـا، وفي الوقت نفسه يؤدي استخدام أي فـرد لها إلى تقليص المتاح منها للآخرين، لذا فهي تتميز بصعوبة الاستبعاد، والتنافسية.

وتكمن المشكلة في هذه الموارد في أن غياب قواعد واضحة وإدارة جماعية رشيدة قد يؤدي إلى استنزافها بمرور الوقت، لأن كل فرد يسعى لتعظيم استفادته الشخصية قبل أن ينفـد المورد. يطلق على هذا السلـوك مأساة المشاع (Tragedy of the commons)، حيث يـؤدي الاستخدام غير المقيد وغير المنظم إلى تدهـور الموارد المشتركة على المدى الطويـل.[٣] وبالتالي، تظهر الحاجـة إلى وضع سياسات وتنظيمـات واتفاقات جماعية تضمن استدامة هذه الموارد وتوزيعها العادل بين المستخدمين.

---

(١) المالية العامة، خالد إبراهيم السيد أحمد، ص ١٦.

(٢) في معنى «بيئة البيانات» ارجع لبرتوفا:

Nadezhda Purtova, 'Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), Under Observation: The Interplay Between eHealth and Surveillance (Springer International Publishing 2017).

(3) Garrett Hardin, 'The Tragedy of the Commons' (1968) 162 Science.

ينطبق ذلك على بيئة البيانات والخصوصية إذ تتجلى أوجه الشبه مع الموارد المشتركة من ناحية في صعوبة الاستبعاد؛ إذ لا يمكن لشخص بمفرده أن يعزل نفسه تمامًا عن ممارسات جمع البيانات، حتى لو أراد ذلك وحرص عليه. من ناحية أخرى، فإن الخصوصية قابلة للتدهور بمرور الزمن عند تكاثر أنشطة الجمع والاستخدام المفرط للبيانات دون رقابة. تمامًا كما يتراجع مخزون الأسماك عند الصيد الجائر، تتآكل الخصوصية الجماعية مع كل اختراق بيانات أو جمع معلومات يتجاوز الحد المعقول. هذا التدهور لا يمس الأفراد فحسب، بل ينعكس على المجتمع بأسره، مؤديًا إلى نضوب الخصوصية العامة وما يتبع ذلك من تراجع الثقة في المنصات الرقمية والشركات والحكومات، وإلى شعور عام بالانكشاف والضعف.[١]

وربما أهم ما يمكن أن نخرج به من هذا التصور هو توافق وصف المورد المشترك مع المشهد الحالي للبيانات والخصوصية. في ظل قدرات تحليلية معززة للذكاء الاصطناعي يمكن ربط البيانات ببعضها البعض وكشف الكثير من المعلومات بقليل من البيانات، وكشف الكثير عن الغير الذي لم يعط بياناته، وكذلك تنميط المجموعة. تلك الممارسات يمكن تفسيرها على أنها استهلاك لبيئة البيانات والخصوصية مما يتأثر بالتصرفات الفردية وبالتالي يؤدي للنضوب. فإذا اعتبرنا بيئة البيانات والخصوصية مواردًا مشتركًا، فينبغي يتم حمايتها على النحو الذي يتم حماية الموارد المهددة بالاستنزاف.

يتمثل ذلك في أهمية تحديد حدود الموارد المشتركة (Boundaries of the commons)، في هذه الحالة: البيانات، على نحو واضح، حيث لن تتحقق الحماية دون تحديد نطاق موضوعها. وهنا فالتمييز بين ما يعد بيانًا شخصيًا وبيانًا غير شخصي – لا يمكن تعريف الشخص من خلاله – أصبح غير واضح، فالبيان الذي قد يعتبر غير شخصي يمكن أن يتحول إلى بيان شخصي إذا ما جمع مع بيان آخر بفضل الذكاء الاصطناعي.[٢] لذلك يبدو أن مفهوم البيانات الشخصية ذاته في طريقه لفقد قيمته كنواة لنظام حماية البيانات والخصوصية الرقمية القانوني.[٣] وإذا نظرنا إلى

(1) Nadezhda Purtova, 'Health Data for Common Good: Defining the Boundaries and Social Dilemmas of Data Commons' in Samantha Adams, Nadezhda Purtova and Ronald Leenes (eds), Under Observation: The Interplay Between eHealth and Surveillance (Springer International Publishing 2017) 193.

(2) ibid.

(٣) إن عملية الاقناع على سبيل المثال تعتبر عملية صعبة، وتتطلب معرفة جيدة بالشخص المستهدف، أما تقنية الذكاء الاصطناعي=

البيانـات باعتبارها مورد مشترك يصير من الهام تحديد ما يعد بيئة بيانات مشتركة، مـن يشـارك فيها، وكيف تدار، وما هـي القيود والضوابط المفروضـة على استخدامها استهـداءً بدراسـات الموارد الطبيعيـة المشتركة، حيث يكون من الضـروري رسم حدود جغرافية أو مجتمعية واضحة لتحديد من يحق له استخدام المورد ومن يتحمل مسؤولية إدارته.

ثالثًا: التنظيم بناءً على حق مشترك في البيانات

بالنظـر إلى أن الأسـاس القانوني لقوانـين حماية البيانات -يخصنـا هنا المصري والأوروبي- الذي يتخذ من التحكم الفردي أساسًا للتنظيم قد أثبت حسبما رأينا أنه لا يعكـس طبيعة البيانات ولا يكفي للحماية من أثـار تقنية الذكاء الاصطناعي، كما رأينا البيانات ذات طبيعة مشتركة، فالسؤال الذي ينبغي الإجابة عليه الآن هو ما هي سمات التنظيم القانوني أو الأساس الفلسفي الذي يمكن بناء ذلك التنظيم عليه بحيث يمكن استيعاب أثار الذكاء الاصطناعي؟

ينبغي هنا التأكيد على أننا حينما نتحدث عن التنظيم القانوني لا نعني عدم جدوى قوانـين حماية البيانـات تمامًا في مواجهة الذكاء الاصطناعـي. وتلك إشكالية مشروع أثارتها بالنظر إلى أن بعض الاعتبارات التي كان يكفي بشأنها من قبل الاعتماد على قوانين حمايـة البيانات بدأت تنفرد بقوانين مستقلة.[1] وصـورة ذلك الأبرز هي قانون الذكاء الاصطناعـي الأوروبي ذاته، وكذلك تنظيمه لممارسة مثـل التلاعب (Manipulation) بينما كان يكتفى في شأنها باللائحة العامة لحماية البيانات الشخصية مثلًا. كما رأينا تـوًا بالنسبـة لفعالية قوانين البيانات في حماية الخصوصيـة أنها تعتمد على سند غير فعـال من التحكم الفردي، كما أن اتخاذ الـ «البيانـات الشخصية» كنواة لتلك القوانين يفقد جدواه تدريجيًا أمام التأثير المشترك للذكاء الاصطناعي.

ويمكـن إيجاز الرأي هنا بأن علاقة تنظيم الذكاء الاصطناعي بتنظيم البيانات هي

= قد وصلت إلى قدرة على التحليل متقدمة إلى حد أن أقل القليل من البيانات أصبح كاف للاستهداف النفسي (Psychological targeting) وإقناع مستخدمي الانترنت في مسائل مختلفة بدءًا من التسوق ووصولًا للسياسة. أنظر تلك الدراسة مثلًا:
SC Matz and others, 'The Potential of Generative AI for Personalized Persuasion at Scale' (2024) 14 Scientific Reports 4692

(1) Nathalie A Smuha, 'The Paramountcy of Data Protection Law in the Age of AI (Acts)' in EDPS (ed), Two decades of personal data protection. What next? EDPS 20th Anniversary (Publications Office of the European Union 2024) <https://papers.ssrn.com/abstract=4874388> accessed 12 December 2024.»plainCitation»:»Nathalie A Smuha, 'The Paramountcy of Data Protection Law in the Age of AI (Acts

علاقة تنظيم استخدام المادة الخام بتنظيم استخدام المنتج النهائي. فقانون حماية البيانات يحدد إذا كانت المادة -البيانات- مشروعة أصلا، ويرسم ضوابط استخدامها بما يسمح بقدر من التحكم فيها مما يؤثر حتمًا في ذلك المنتج -تقنية الذكاء الاصطناعي التي تستخدم البيانات. وفي ظل مستوى التقنية الحالي والتنظيمات القانونية القائمة، فإن قوانين البيانات الشخصية لازالت تلعب ولا شك دورًا شديد الأهمية في حماية الخصوصية وكذلك كبح جماح الذكاء الاصطناعي الضار.[١]

وشأننا هنا هو كيف لذلك التنظيم، تنظيم البيانات الشخصية، أن يستمر بفعالية في حماية البيانات والخصوصية في ظل تطور غير مسبوق للتقنية.

لا ريب أن الذكاء الاصطناعي صنع من البيانات شخصية ضررًا غير شخصي. فالغير يتضرر من التعامل غير المسئول أو التعامل المسئول غير القادر في البيانات الشخصية من صاحبها. وذلك التعامل ليس إلا أثرًا للاعتماد على تحكم الفرد. إذا كان الأمر كذلك، فربما من المعقول أن يتم الاعتراف للغير بحق في البيانات إذا كان من شأنها التأثير عليه.

الحديث عن حق للغير (حق مشترك) في البيانات يبدو معقدًا نظرًا لما قد يحتمله من المساس بالحق الخاص في البيانات. فالبيانات الشخصية هي في النهاية بيانات تخص صاحبها وهو الأولى بالتقرير بخصوصها.[٢] إلا أن ذلك وإن صح، وإذا نظرنا من منظور تأصيلي، فسنجد بين القواعد الأصولية الراسخة شرعًا قاعدة لا ضرر ولا ضرار، وهو ما يتخذ صورة «عدم التعسف في استعمال الحق» كأحد مبادئ القانون الطبيعي التي يمكن الارتكان إليها في التشريع.

مع أفكار مثل خصوصية المجموعة على نحو ما رأينا، وتأثير البيانات على الغير، وكذلك وجود بيئة بيانات يتشارك فيها أصحاب البيانات، يصبح من المشروع والمنطقي الحديث عن حق «مشترك» في البيانات. فالبيانات أيًا كانت صورتها، إذا كان من شأن معالجتها الإضرار بحقوق الغير يتعين أن يكون هناك في المقابل مُتَنَفس وسند للانتصاف القانوني.

تلك الحقوق تشمل الخصوصية؛ حيث يمكن كشف معلومات عن المجموعة أكثر مما

---

(١) لفهم أكثر لدور تنظيم البيانات الشخصية بالنسبة للذكاء الاصطناعي في سياق قانون الاتحاد الأوروبي، المرجع السابق.

(2) Bart Custers and Helena Vrabec, 'Tell Me Something New: Data Subject Rights Applied to Inferred Data and Profiles' (2024) 52 Computer Law & Security Review 105956.

يكشفه أفرادها منفردين. كما تشمل عدم التمييز، إذ أن الذكاء الاصطناعي أوجد بسبب قدرته على التحليل وربط المعلومات والتصنيف مجموعات مستحدثة وأسس غير مسبوقة للتمييز. وتشمل فوق ذلك الحق في الكرامة والتحكم الذاتي (Autonomy) فالمجموعة التي ينكشف عنها بيانات قد تصبح عرضة للأحكام المسبقة مما يقيد قدرة أفرادها على التقرير لأنفسهم.

وهو حق في البيانات، وليس بالضرورة حق في البيانات الشخصية؛ فصاحب البيانات الفرد له الحق في التحكم في بياناته الشخصية من حيث المبدأ، إلا أنه حينما تنتقل هذه البيانات إلى حيز المجموعة ينشأ حق مشترك يُمكّن ذوي الشأن من الحد من أثار تلك البيانات بالنسبة لهم. ذلك إذن يفترض وجود حق لصاحب البيانات،[1] وحق للمجموعة أساسه المساس بمصالحهم، وإمكانية للتعارض بين هذين الاعتبارين، والفرضية الآن هي التوفيق بينهما.

ذلك التوفيق قد يتحقق بالتقليل من الاعتماد على التحكم الفردي في مقابل اعتماد أكثر على معالجة مسئولة للبيانات من قبل المتحكم والمعالج (والحائز في القانون المصري) وهو ما يمكن أن ينعكس في صورة التزامات مباشرة في مواجهة المتحكم أو المعالج، سواءً في صورة قواعد أو مبادئ، يكون المتحكم أو المعالج ملزم بها بصرف النظر عن استعداد صاحب البيانات في التنازل عن بياناته.

فإذا كانت الفرضية هي أنه ماذا لو أراد الشخص وأصر على أن يفصح عن بياناته؟ فلا يوجد ما يمنع، حيث إن الخطاب هنا موجه لمزود الخدمة الذي يلتزم بالحصول

(١) جدير بالذكر هنا أن حماية البيانات الشخصية هو حق مستقل معترف به في قانون الاتحاد الأوروبي وفق المادة (٨) من ميثاق الحقوق الأساسية للاتحاد الأوروبي، والميثاق ذو قيمة دستورية باعتباره من القوانين الأساسية للاتحاد الأوروبي. وتنص هذه المادة على أن:

«لكل شخص الحق في حماية بياناته الشخصية.

جب أن تُعالج البيانات الشخصية بشكل عادل ولأغراض محددة، وعلى أساس موافقة الشخص المعني أو أي أساس مشروع آخر يحدده القانون...»

بينما لا يوجد نص مواز صريح في القانون المصري، إلا أنه يمكن اعتبار حماية البيانات الشخصية حق فرعي استنادًا للحق الدستوري في الخصوصية (المادة ٥٤ من الدستور المصري) والحق في الكرامة (المادة ٥١ من الدستور).

انظر في هذا الصدد: التأسيس للحق في حماية البيانات الشخصية كحق مستقل عن الحق في الخصوصية في تشريع الاتحاد الأوروبي، أمال شافعي وأم الحق شافعي، مجلة الباحث القانوني، المجلد ١، العدد ٢، ٢٠٢٢؛ أنظر أيضًا: الحماية الدستورية والقانونية للبيانات الشخصية : دراسة مقارنة بين التشريع المصري والفرنسي، وليد رمضان عبد الرازق محمود، مصر المعاصرة، المجلد ١١٣، العدد ٥٤٦، ٢٠٢٢.

علـى القدر اللازم فقط من البيانات لتقـديم الخدمة بما يضمن عدم الإضرار بالغير. كما أننا نتحدث هنا عن مقدم خدمة يضع نظامًا عامًا لكافة مستخدميه، وليس معاملة فردية تخضع لرغبة صاحب البيانات ومتلقيها – أي أننا ننظر لبيئة البيانات وليس إلى المعاملة الفردية.

وربمـا تكـون أحد أهم انعكاسات هذا الأساس الفلسفي علـى أرض الواقع هو إنزال تنظيم البيانات على عملية «الاستنتاج» (Inference)، ليشمل ليس فقط البيانات كمها وكيفهـا، وإنما أيضًا عملية استنتاج المعلومات. إن استنتاج المعلومات هو في الواقع أحد أبرز تأثيرات الذكاء الاصطناعي كيفما رأينا، إلا إن يخرج عن نطاق التنظيم.[١]

وقد اعتبر البعض ذلك حقًا لصاحب البيانات، مما سُمي بـ «الحق في الاستنتاجات المعقولـة» وهـو حق الفرد في ضمان أن تكون الاستنتاجات أو التنبؤات أو القرارات التي تُتخـذ بشأنه – وغالبًا ما تستند إلى البيانـات أو التحليلات أو الخوارزميات – منطقية وعادلة وقابلة للتبرير. يهدف هذا الحق إلى منع الضرر أو التمييز الناتج عن استنتاجات خاطئـة أو منحـازة أو مفرطـة في التكهـن، ويؤكد علـى أهميـة الشفافيـة والمساءلة والاعتبارات الأخلاقية في العمليات التي تؤثر على حياة الأفراد أو سمعتهم.[٢]

وربمـا ينبغي هنا تطبيق الاستنتاجات المعقولة علـى المجموعة كذلك كحق مشترك. الاستنتـاج المعقـول كحق للمجموعة هـو استنتاج يتم استخلاصه مـن البيانات المتعلقة بمجموعـة معينة من الأفراد، ويكـون مبررًا وموثوقًا وذا صلـة بالغرض المحدد لمعالجة البيانات أو القرارات المؤتمتة (Automated). يجب أن تحترم هذه الاستنتاجات حقوق الأفـراد ضمن المجموعة، مـع ضمان أن المنهجيـات المستخدمة لتحقيـق الاستنتاجات تعتمـد على بيانات دقيقة وموثوقة، وألا تسفر هذه الاستنتاجات عن تمييز غير عادل أو انتهاك للخصوصية الفردية أو الجماعية. بمعنى آخر، يجب أن تتسم العملية بالشمولية

---

(١) انظـر حكـم محكمة العدل الأوروبيـة C-141/12 and C-372/12 - YS and Others (Joined Cases)the controller must not especially provide a copy of the original document which contains the personal data.»,»authority»:»CJEU»,» Sandra Wachter and Brent : language»:»en»,»title»:»C-141/12 and C-372/12 - YS and Others (Joined Cases Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) 2 Columbia Business Law Review <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829> accessed 12 December 2024.\\uc0\\u8216{}A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI\\uc0\\u8217{} (2019

(2) Ibid Wachter and Mittelstadt.

والأمانــة، بحيث لا يساء استخدام البيانات لتكوين استنتاجات تضر بالمجموعة أو تقلل من حريتها فـي اتخاذ القرارات.

الاستنتــاج المعقول فــي هذا السياق يركز علــى ضمــان أن أي استنتاجات تستخدم لتحديد سمات أو أنماط خاصة بالمجموعة مبنية على مبررات قوية وذات صلة بالغرض المعلن لمعالجة البيانات. على سبيل المثال، إذا تم استخدام خوارزمية لتصنيف مجموعة مــن الأفــراد على أنهم عرضة للتأخير في السداد بناءً علــى أنماط معينة في بياناتهم السلوكيــة، يجــب أن تكون هذه الاستنتاجــات شفافة وقابلة للتفســير. يتطلب ذلك من الجهات المعنية تقديم مبررات مسبقة (ex-ante justifications) تحدد سبب استخدام البيانــات، وآلية معالجتها، ومدى ارتباطهــا بالغرض المعلن، وضمان موثوقية ودقة هذه الاستنتاجات.

من خلال تطبيق مفهوم الاستنتاجات المعقولة، يمكن ضمان تقليل المخاطر المرتبطة بالتصنيــف العشوائــي أو التحيز الخوارزمي. كما يمنح الأفــراد داخل المجموعة أدوات قانونيــة للطعــن فـي القرارات التــي تستند إلى استنتاجات غــير موثوقة أو غير مبررة. علــى سبيــل المثال، إذا أُدرج فرد فـي مجموعة تتلقى شروطًــا أقل تفضيلًا فـي القروض بنــاءً على نمط بيانات مجتمعة مع بيانات المجموعــة المنسوب إليها خوارزميًا، فإن هذا الإطار يضمن وجود آليات للطعن في الأساس المنطقي لهذه القرارات. هذا النهج يعزز الشفافيــة والمساءلــة ويقلل من الأضرار الناتجــة عن استخدام البيانــات بأساليب قد تكون غير منصفة أو تمييزية و-الأهم من ذلك- منتهكة للخصوصية.

الخاتمة

قطعت التقنية شوطًا كبيرًا خلال العقدين الماضيين، تتبوأ موقع الرأس منها تقنية الذكاء الاصطناعي التي أحدث ثورة في معايشنا، ولم تبلغ أقصى مداها بعد، وليست حتى قريبة من ذلك. طوال هذه الفترة كانت البيانات الشخصية وحمايتها سؤال مفتوح، ولا زالت. بخصوصه، يكشف التطور التقني شيئًا فشيئًا إمكانات وفرص الاستفادة من البيانات الشخصية وكذا المخاطر التي قد تعود من تناولها بشكل غير مسئول. وفي ظل اعتماد حثيث على البيانات لأغراض التجارة والإدارة والسياسة، والسباق المستمر للتسلح بتقنية الذكاء الاصطناعي، والرغبة في فهم الإنسان والتأثير عليه، تخلفت تنظيمات حماية البيانات الشخصية عن تحقيق أهدافها.

أوضحت هذه الدراسة عبر البحث في تأثير الذكاء الاصطناعي والتنظيم المصري والأوروبي المقارن للبيانات أن الفرضية التي بنيت عليها تشريعات حماية البيانات الشخصية من أن الخصوصية والبيانات الشخصية هما حقٌ خاص، يعني صاحب البيانات وحده، أصبحت غير معبرة واقع التقنية اليوم في ظل تقنية ذكاء اصطناعي ذات قدرة فائقة على التحليل والاستنتاج مما يترك الفرد مواجهًا للآلة في مواجهة غير متكافئة.

لذا، وفي سبيل فهم أدق وأشمل لتأثير الذكاء الاصطناعي على البيانات وأصحاب البيانات، اقترحت هذه الدراسة ما سُمِّيَ «دورة تأثير البيانات»، حيث توجد أربع مراحل لتناول البيانات: جمع البيانات، ومعالجتها، ونشرها، والتغذية الرجعية وإعادة التكيف. كلٌ من هذه الأطوار يشمل مخاطر مستقلة على الخصوصية والبيانات، إلا أنها مجتمعة تُكوِّنُ مراحل أو حلقات دورة مصممة للتأثير على الفرد بغرض توليد بيانات أكثر، بالاستعانة بالذكاء الاصطناعي.

ومن أخص مظاهر هذه القدرات على الإطلاق، وما ينال من فعالية تنظيمات حماية البيانات الحالية هو أن الذكاء الاصطناعي قد بلغ درجات متقدمة من القدرة على التحليل بحيث يستطيع ربط البيانات ببعضها البعض لاستخراج معلومات غير متوقع استخراجها. وهو في هذه الأثناء لا يصل إلى استنتاجات عن صاحب البيانات نفسه فحسب، بل وعن المجموعة الخوارزمية التي تشاركه السمات والخصائص والآراء،

والتـي يكونها الذكاء الاصطناعـي بناءً على قدر من البيانات شاركـه كلٌ من أفرادها. تلك المجموعة متروكة خارج التنظيم القانوني الحالي، المصري والأوروبي.

لذلـك فإن الاعتمـاد على تنظيم قانوني لحماية البيانـات الشخصية قوامه التحكم الفـردي قـد أثبـت عدم جـدواه، إذ تبـين أن تحكم صاحـب البيانات فـي بياناته غير فعـال بالنسبة لنفسـه، ناهيك عن الغير. فتحكم صاحب البيانـات مقيد بحدود قدرته وعلمـه المحدوديـن على متابعـة ومعرفة كيف يتـم استخدام بياناتـه ولأي غرض. وهو فـوق محدودية قدرته وعلمه، يتعرض لمؤثرات خارجة مصممة ومخصصة للتأثير عليه واستخـراج البيانات منه. وهو فوق هذا وذلك وذاك، وإن حرص، لن يستطيع أن يحمي غـيره من تبعـات جمع بياناته، التي لا تظل قادرة على الإضـرار بالمجموعة حتى وإن تم تجهيل البيانات وصارت غير شخصية. وإذا كان الأمر كذلك، فإننا إذا كنا نشكو ضعف العلـم والتحكم الفرد فـي بياناته، فنحن نتحـدث عن انعدام العلـم والتحكم بالنسبة للمجموعة.

يكـون لزامًـا إذن أن نغير تلك النظـرة التقليدية للبيانات الشخصيـة على أنها حق خاصـ، ونفكر فـي حق مشترك في البيانات، مما قد يوفر حماية أكثر فعالية لصاحب البيانات نفسه وللأغيار ممن يتأثرون ببياناته. ونحن بصدد ذلك اقترحنا -استعارةً- أن نفهـم الخصوصية والبيانات على أنهما مـورد مشترك، متاح للجميع، ولا يمكن منع أحـد من استخدامه -نظـرًا لضعف التحكم الفردي- لكن الاستخـدام غير المسئول له يضـر بالكافة. ويترتب على ذلك وضع التزامات علـى مقدمي الخدمات من المتحكمين ومعالجـي البيانـات، دون تقييد حرية الشخص في التعامل فـي بياناته. من بين هذه الالتزامـات ما ينصب علـى الاستنتاجات التي يقوم به الـذكاء الاصطناعي استخدامًا للبيانـات وبخصوص أصحـاب تلـك البيانـات، مـع الوضـع فـي الاعتبـار الحق في الاستنتاجات المعقولة لمجموعة.