التَّحدِّيَّات القانونيَّة للاستخداماتِ المُستحدَثة للأشياءِ المُتَّصلة

"نحو إطارٍ قانونيٍّ مُناسبٍ"

"دراسةٌ مقارنةٌ"

د. بكر عبد السعيد محمد أبو طالب

مدرِّس القانون المدنيِّ- كليَّة الحقوق- جامعة مدينة السَّادات

bakrtalb975@gmail.com

(ISSN: 2537- 0758)

التَّحدِّيَّات القانونيَّة للاستخدامات المُستحدَثة للأشياءِ المُتَّصلة
"نحو إطار قانونيٍّ مُناسب"
"دراسةٌ مقارنةٌ"

د. بكر عبد السعيد محمد أبو طالب

الملخَّص:

يدور موضوع هذا البحثِ ويرتكزُ محورُه حول بيانِ التَّحدِّيَّاتِ القانونيَّةِ للاستخداماتِ المُستحدَثةِ للأشياءِ المُتَّصلةِ افتراضيًّا أو المزوَّدة بأنظمة الذَّكاءِ الاصطناعيّ، من أجلِ إمكانيَّةِ وضع إطارِ قانونيّ مُناسبٍ، حيث تثيرالأشياءُ المُتَّصلةُ عديدًا من الإشكاليَّاتِ والتَّحدِّيَّات؛ كون اتِّخاذِ القراراتِ– في إطار الأشياءِ المُتَّصلةِ المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ– يتمُّ في أغلبِ الأحيانِ من خلالِ البرمجيَّاتِ الحاسوبيَّةِ التي تُوجَد بداخلِ هذه الأشياءِ دون تدخُّلٍ بشريّ، كما أن تشغيل هذه الأشياءِ يحتاج إلى تزويدِها بالبياناتِ المتعلِّقةِ بمُستخدميها وأحيانًا تكون هذه البياناتِ ضخمةً للغاية.

وقد تضمَّن هذا البحثُ فصلين وخاتمة، تعرَّضنا في الفصل الأول إلى المقصودِ بالأشياءِ المُتَّصلةِ ومسألة عدم اليقينِ القانونيّ في ضوء تطوُّرِ أنظمةِ الذَّكاء الاصطناعيّ، بينما تناول الفصلُ الثاني مسألةَ إمكانيَّةِ وجودِ إطارِ قانونيّ خاصّ بالأشياء المُتَّصلة لا سيَّما المزوَّدةُ بأنظمةِ الذَّكاء الاصطناعيّ.

وقد خلصْنا من البحثِ إلى عدَّة نتائجَ يأتي في مقدِّمتها أنه لم تحظَ دراسةُ الأشياء المُتَّصلة المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ بالاهتمام الكافي لا سيَّما في ظلِّ غيابِ التَّنظيم التَّشريعيّ الخاصّ بهذه الأنظمةِ لا سيَّما في مصر، كما أنه إذا كان المُشرِّع المصريُّ قد سنَّ قوانينَ تتعلَّقُ بحمايةِ حقوق الملكيَّة الفكريَّة، وحماية البياناتِ الشَّخصيَّة، لكن التَّطبيقَ الفعليَّ والعمليَّ لاستخدام الأشياء المُتَّصلة يُشير إلى وجودِ كثيرٍ من الإشكاليَّاتِ، لا سيَّما القانونيَّةُ التي تحتاج إلى دراسةٍ متخصِّصةٍ وقواعدَ متعمِّقة؛ كون الأضرارِ النَّاجمةِ عن استخدام الأشياءِ المُتَّصلة أصبحت كثيرةً ومتعدِّدةً، ويُعدُّ قانون تنظيم الذَّكاءِ الاصطناعيّ الأوروبيّ لسنة ٢٠٢٤ خطوةً تاريخيَّةً نحو ضمانِ الاستخدام الآمن والمستدامِ للتِّقنيَّاتِ الحديثة.

وتوصَّلنا من هذه الدِّراسةِ إلى مجموعةٍ من التَّوصياتِ، منها: نُوصي بضرورةِ العملِ على مواجهةِ القضايا التي يُثيرها التطوُّرُ السَّريعُ للأجهزة المُتَّصلة، من خلال إنشاءِ برامجَ بحثيَّةٍ في مجال اتِّصالاتِ المعلوماتِ في كافَّةِ التَّخصُّصاتِ للتأكُّدِ من مراعاةِ الاعتباراتِ الأخلاقيَّةِ والقانونيَّة عند تصميم الجهاز، فضلًا عن تقييمِها، كما نُوصِي بضرورةِ وضع إطارٍ قانونيّ "عربي مشترك" لتنظيم الأشياءِ المُتَّصلةِ في ظلِّ التطوُّرِ الهائلِ لاستخداماتِ الذَّكاء االصطناعيّ، من أجلِ الحدِّ من المخاطرِ المحتملةِ لهذه الأشياء، وأيضًا نهيبُ بالمُشرِّع المصريّ ضرورة سنِّ إطارٍ قانونيّ يتضمَّنُ قواعدَ منسجمةً بشأنِ الأشياءِ المُتَّصلة بشكلٍ عامّ والمزوَّدة بأنظمة الذَّكاء الاصطناعيّ عالية الخطورةِ على وجهِ الخصوص؛ لتعزيز تطويرِ واستخدام واستيعابِ الذَّكاء الاصطناعيّ في السُّوقِ الداخليّ، بما يُلبّي في الوقتِ نفسه مستوًى عاليًا من حمايةِ المصالح العامَّة، مثل الصِّحةِ والسَّلامةِ وحماية الحقوقِ الأساسيَّة. فضلًا عن حمايةِ مُستخدمي الأشياءِ المُتَّصلة.

الكلمات المفتاحيَّة: الأشياء المُتَّصلة– أنظمة الذَّكاءِ الاصطناعيّ– آليَّة تشفيرِ البيانات– المعالجة المُؤتمتة–حماية الخصوصيَّة بحسب التَّصميم– الخصوصة افتراضيًّا– نظام مراقبةِ ما بعد التَّسويق– مقدِّمي الأشياء المُتَّصلة– أنظمة الذَّكاء الاصطناعيّ.

Abstract:

This research focuses on outlining the legal challenges associated with the emerging uses of virtually connected objects or those equipped with artificial intelligence systems, with the aim of establishing an appropriate legal framework. The use of connected objects raises numerous issues and challenges, particularly because decisions within these objects, which are equipped with artificial intelligence systems, are often made through the software embedded within these objects without human intervention. Additionally, the operation of these objects requires the provision of data related to their users, and at times, this data can be extremely vast

This research consists of two chapters and a conclusion. In the first chapter, we addressed the concept of connected objects and the

(ISSN: 2537- 0758)

issue of legal uncertainty in view of the development of artificial intelligence systems. The second chapter discussed the possibility of establishing a specific legal framework for connected objects, particularly those equipped with artificial intelligence systems.

The research concludes with several findings, the foremost of which is that the study of connected objects equipped with artificial intelligence systems has not received adequate attention, especially considering the absence of specific legislative regulation for these systems, particularly in Egypt. While the Egyptian legislator has enacted laws related to the protection of intellectual property rights and personal data protection, the actual implementation of connected objects reveals numerous issues, particularly legal ones, that require specialized study and in-depth rules. This is due to the increasing and diverse harm arising from the use of connected objects. The European Artificial Intelligence Regulation of 2024 is seen as a historic step toward ensuring the safe and sustainable use of modern technologies.

This study has led to a set of recommendations, including the need to address the issues raised by the rapid development of connected devices. This can be achieved by establishing research programs in the field of information communications across all disciplines to ensure that ethical and legal considerations are considered during the design and evaluation of these devices. Additionally, we recommend the establishment of a "unified Arab" legal framework to regulate connected objects in view of the significant advancements in artificial intelligence usage, to mitigate the potential risks associated with these devices. Furthermore, we urge the Egyptian legislator to enact a legal framework that includes coherent rules regarding connected objects in general, and particularly those equipped with high-risk artificial intelligence systems. This would help foster the development, use, and integration of artificial intelligence in the domestic market, while simultaneously ensuring a high level of protection for public interests, such as health, safety, and the protection of fundamental rights, as well as safeguarding users of connected objects.

Keywords: Connected Objects– Artificial Intelligence Systems– Data Encryption Mechanism– Automated Processing– Privacy by Design– Virtual Privacy– Post-Market Surveillance System– Providers of Connected Objects– Artificial Intelligence Systems.

مقدِّمة

ممَّا لا شكَّ فيه أن الاتِّصالَ بالابتكاراتِ التِّكنولوجيَّةِ يُمثِّل تحديًا للقانون، ولهذا يتحتَّم تنظيمُ هذه الابتكاراتِ حتى لا نكونَ أمامَ ما يُسمَّى بالفراغ القانونيّ «vide juridique»[1]، ونظرًا لانتشارِ الأشياءِ المُتَّصلةِ في حياتنا اليوميَّةِ واستخدامها (كأتمتة المنزل، والسَّيارات، والصِّناعة، وكذلك استخدام الأشياءِ المُتَّصلةِ في المجال الطِّبيّ، إلى غير ذلك من المجالات)، ستظلُّ مسألةُ ظاهرةِ التَّزامنِ بين القانونِ والابتكارِ التِّكنولوجيّ ذات صلةٍ، ولهذا من الضَّروريّ الآن الرَّبطُ بين مُصطلحي القانونِ والابتكار[2].

وعلى ذلك، يعدُّ المحرّك البخاريُّ ابتكارًا تكنولوجيًّا مهمًّا في القرن الثامن عشر، حيث سمح للإنسان بدخولِ العصرِ الصِّناعيّ، وكذلك الكمبيوتر في القرن العشرين، وأخيرًا الذَّكاء الاصطناعيُّ في القرن الحادي والعشرين وعصر الروبوتات، والواقع أنَّ المنتجاتِ المبتكرةَ في القرن الحادي والعشرين هي نتيجةٌ لعددٍ كبيرٍ من الاكتشافاتِ، بما في ذلك تصغيرُ المكوِّناتِ الإلكترونيَّةِ وتقنيات الاتِّصالات. وهذا هو الحالُ بشكلٍ خاصّ بالنِّسبةِ للهواتف الذكيَّة، التي تطوَّر وجودُها في السُّوقِ إلى التَّحسينِ والاستقلاليَّة، وتحسين المكوِّناتِ وتصغيرها، ويُمكن أن تأتيَ الابتكاراتُ الأخرى من خلال التَّحسيناتِ على الأنظمةِ الحاليَّة، ولذلك، فإنَّ تعريفَ منظَّمةِ التَّعاونِ

---

(1) Centre de recherche critique sur le droit (CERCRID), Le droit au contact de l'innovation technologique, SaintEtienne, Université Jean Monnet, 1989, p..

د. محمد بومديان، الذَّكاء الاصطناعيُّ تحدٍّ جديدٌ للقانون، مساراتٌ في الأبحاثِ والدِّراسات القانونيَّة، ع٩، ١٠، سنة ٢٠١٩، ص١٩٨– ٢٢١.

(2) Cédric Renaud Claude Bernard, Nicolas Burger, La synchronisation du droit et de l'innovation. Regard sur les objets connectés, Ecole doctorale de droit de l'Université de Lyon 3; Institut universitaire de France; Institut sur les systèmes complexes, Feb 2017, p.2-4.

ويُمكن تعريفُ الابتكارِ من الكلمةِ اللاتينيَّة innovatio التي تعني "التَّجديد" بالمعنى الواسع، على أنه تقدُّمٌ تقنيٌّ ثوريٌّ، لا سيَّما وأن له تأثيرًا على المجتمعِ واقتصادِه

Félix GAFFIOT, Dictionnaire latin-français, Paris, Hachette, 1934, p. 823

(ISSN: 2537- 0758)

الاقتصاديّ والتَّنميةِ (OECD) للابتكاراتِ التِّكنولوجيَّةِ في السِّلع والخدماتِ يبدو أكثر مُلاءمةً؛ لأنه يُغطِّي كلًّا من الجدَّةِ التِّكنولوجيَّة والتَّحسينِ التِّكنولوجيّ للمُنتج أو استخدامه[٣].

ومن المُلاحظِ أن الإنترنتّ يشهدُ الآن توسُّعًا غير مسبوقٍ مع تطوُّرِ الأشياءِ المُتَّصلة[٤]، وفي الحقيقةِ كان يُنظر إلى الإنترنتّ على أنه قدرةُ الناسِ على التَّواصلِ في أيّ وقتٍ وفي أيّ مكانٍ؛ بيد أنه مع ظهورِ وتطوُّرِ الأشياءِ المُتَّصلة، يُمكن للعالم الماديّ الآن التواصل، سواء فيما يتعلَّقُ بالعلاقاتِ من أشخاصٍ إلى أشخاصٍ، أو

---

[٣] ابتكار المنتج هو تقديمُ سلعةٍ أو خدمةٍ جديدةٍ أو محسَّنةٍ بشكلٍ كبيرٍ فيما يتعلَّقُ بخصائصِها أو استخداماتها المقصودة. ويتضمَّن ذلك تحسيناتٍ كبيرةً في المواصفاتِ الفنيَّةِ والمكوِّناتِ والموادِّ والبرامجِ المدمجةِ وسهولة الاستخدامِ أو الخصائصِ الوظيفيَّة الأخرى.

«A product innovation is the introduction of a good or service that is new or significantly improved with respect to its characteristics or intended uses. This includes significant improvements in technical spectifications, components and mateials, incorporated software, user friendliness or other functional characteristics». Voir OCDE, Oslo Manual": Guidelines for Collecting and Interpreting Innovation Data, OCDE et Eurostat, 3e édition, 2005, p. 48, disponible sur http://www.oecdilibrary.org/science-and-technology/oslo-manual_9789264013100-en

[٤] إن القيمة الاقتصاديَّةَ المحتملةَ والقيمة الاجتماعيَّة لإنترنت الأشياءِ تبرِّر التنبُّؤ بالنموِّ الهائل لإنترنت الأشياء في غضونِ بضعِ سنواتٍ. ووفقًا لتقديرات جارتنر، فإن ٦.٤ مليار كائن متَّصل بالفعلِ في عام ٢٠١٦، ومن المتوقَّعِ أن يكونَ هناك ٣٠ مليارًا في عام ٢٠٢٤. وبالنِّسبة لشركةِ اتِّصالاتٍ فإنَّ هذا الرَّقمَ سوف يرتفعُ إلى ٢٨ مليارًا بحلولِ نفسِ الأفق، في حين أنَّ هذا الرَّقمَ وفقًا لشركةِ سيسكو قد يصلُ إلى ٥٠ مليارًا في عام ٢٠٢٤، ويتوقَّع موقع iDATE وجود ٨٠ مليار كائنٍ متَّصلٍ في عام ٢٠٢٤.

https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431

من أشخاصٍ إلى أشياء، أو من أشياءَ إلى أشياءَ[٥]، وأمام هذه الإمكانات الكبيرة التي لا تزالُ في معظمِها قيدَ الاستكشاف، فهل نحن– وبحقّ– على فجرِ ثورةٍ تكنولوجيَّةٍ جديدةٍ وبخاصَّةٍ مع كثرةِ الأشياءِ المُتَّصلة المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر؟

ومع انتشارِ إنترنتّ الأشياء[٦] ظهر سيلٌ من الأشياءِ المُتَّصلةِ التي يجب تعريفُها وبدقَّةٍ. وفي الواقع، محطَّاتُ الكمبيوترهي أشياءُ متَّصلةٌ تقنيًّا، في حين أن بعضَ الأشياءِ هي متَّصلةٌ بالفعل ببعضها البعض لتنفيذِ عمليَّاتٍ مستقلَّةٍ ("آلة إلى آلة)، والبعض الآخر قابلٌ للتَّوصيلِ ببساطةٍ فهي أشياءُ غير تكنولوجيَّةٍ، حيث يتمُّ تعزيزُها بواسطةِ مستشعرِ واحدٍ على الأقل، أو شريحة RFID أو رمز الاستجابةِ السَّريعة. وبالتَّالي فإن مجالَ الأشياءِ المُتَّصلة يحتملُ أن يكون لا نهائيَّ وغيرَ قابلٍ للحصر.

والشَّيء المتَّصلُ هو جهازٌ يُمكِنه الاتِّصالُ بالإنترنت، ويستطيع تبادلَ البياناتِ مع الأجهزة الأخرى، حيث أصبحت الأشياءُ المُتَّصلةُ أكثرَ شيوعًا؛ لأنها تُقدِّم

---

[٥] تتنافسُ التَّحليلاتُ المستقبليَّةُ بقوَّةٍ لتأهيلِ وقياسِ مدى التأثيرِ المستقبليّ لإنترنت الأشياء على حياتنا اليوميَّة، وعلى طرق استهلاكنا، وعلى طرقِ إنتاجنا. فمثلًا أجهزةُ الاستشعارِ والرَّقائق والكاميرات الموجودة على متن الطَّائرةِ تجعل من المُمكنِ إنشاء بياناتٍ من أشياءَ كانت خاملةً ومعزولةً عن بعضِها البعض في السَّابق، لجعل بيئتنا أكثر ذكاءً.

ولذا أصبحَ من الممكنِ جعلُ المنازلِ ووسائل النَّقلِ والأماكن العامَّةُ وأماكنُ العملِ والبنى التحتيَّةُ وحتى الموظفون أكثرَ كفاءة، مع إمكانيَّةِ تقديمِ خدماتٍ جديدةٍ وتحسين السَّلامةِ أو السُّلوكِ من خلالِ جَمْعِ ومعالجةِ البيانات المنقولةِ عن طريق الأشياءِ المتَّصلة.

[٦] **يتضمَّن الاتِّحادُ الدوليُ للاتِّصالات خمسَ خصائصَ أساسيَّة لإنترنت الأشياء:**

١– التَّوصيل البينيُ: يُمكن ربطُ الأشياء ببعضِها البعض وبالبنيةِ التحتيَّةِ للإنترنت بأكملها؛ ٢– خدمات محددة: تقدِّم الأشياءُ خدماتٍ بشكلٍ جوهريّ؛ ٣– عدم التَّجانس: الأجهزة المستخدمة لتشغيلِ الأشياءِ غير متجانسةٍ (البرمجيَّات والشَّبكات والخصائص الفيزيائيَّة)؛ ٤– التغيُّرات الديناميكيَّة: تتطوَّر الأشياءُ في بيئةٍ متطوِّرةٍ (الموقع، السُّرعة) ويتطور أيضًا عدد الأجهزة، مع ظهور موجاتٍ تكنولوجيَّةٍ جديدة؛ ٥– النِّطاق الواسع جدًّا: الأجهزة التي سيتعيَّن إدارتُها والتي ستتواصلُ مع بعضِها البعض ستكونُ أكثرَ عددًا بكثيرٍ من تلك المتَّصلةِ بالإنترنت اليوم.

(ISSN: 2537- 0758)

مجموعةً متنوعةً من المزايا للمستخدمين كالسَّاعاتِ أو الهواتفِ الذكيَّةِ أو أنظمة التَّشغيلِ الآليّ للمنزل أو أيّ نوع آخرَ من الأجهزةِ المُتَّصلةِ بالإنترنت[٧]، وأجهزة الاستشعارِ والمزوَّدة بأنظمة الذَّكاءِ الاصطناعيّ.

وفي الواقع نجد أنَّ الاعتمادَ على الأشياءِ المُتَّصلة قد أضحى ملحوظًا للكافَّةِ في الحياةِ اليوميَّة، حيث ظهر في الأفقِ في الآونةِ الأخيرةِ مناقشاتٌ قانونيَّةٌ وأخلاقيَّة، وممَّا لا شكَّ فيه يثير هذا الابتكارُ عديدًا من الإشكاليَّاتِ في عديدٍ من فروع القانون (قانون البياناتِ الشَّخصيَّة وقانون المستهلك، والأمن السيبراني...إلخ). وجديرٌ بالملاحظةِ أنَّ جمعَ وتحليلَ البيانات التي تُتيحها الكائناتُ المُتَّصلة ليس بالأمرِ التَّافه، بل الأمر قد يؤدّي إلى هجماتٍ أكثر خطورةً على خصوصيَّةِ المستخدمين[٨].

وسرعان ما أصبح الجميعُ وبخاصَّةٍ القانونيُّون يبحثون عن الطَّبيعةِ القانونيَّةِ للأشياءِ المُتَّصلة لا سيَّما من زاويةِ تأمين البياناتِ الشَّخصيَّةِ واحترام الخصوصيَّةِ والملكيَّة الفكريَّة[٩]. ولذلك فإنَّ الاهتمامَ بالأشياءِ المُتَّصلة يعدُّ أمرًا حكيمًا بشكلٍ خاصّ بمجرَّدِ أن ندركَ الإمكاناتِ الاقتصاديَّةَ الهائلة التي تُمثِّلها، حيث تستثمرُ الشَّركاتُ بكثرةٍ في التِّكنولوجيات المعنيَّة؛ نظرًا لإمكانيَّاتِها الاقتصاديَّةِ الهائلة، في جميع القطاعاتِ المجتمعة: التَّشغيل الآليّ للمنزل، والصِّحةِ الإلكترونيَّةِ، والزِّراعةِ، والنَّقل، والأجهزة القابلةِ للارتداء، والتِّجارةِ، وحتى التَّرفيه....إلخ.

---

[٧] د. إيهاب خليفة، "إنترنت الأشياء": تهديداتٌ أمنيَّةٌ متزايدةٌ للأجهزة المتَّصلةِ بالانترنت، مجلة اتِّجاهات الأحداث، ع١٩، مركز المستقبل للأبحاثِ والدِّراسات المتقدِّمة، ٢٠١٦، ص٥٨– ٦١.

[٨] بشار طلال أحمد المومني، التَّحدياتُ القانونيَّةُ المعاصرة لاستخداماتِ "إنترنت الأشياء": دراسةٌ في النِّظامِ القانونيّ الإماراتيّ، مجلة كليَّة القانون الكويتيَّة العالميَّة، مج١٠، ع٤٠، كليَّة القانون الكويتيَّة العالميَّة، ٢٠٢٢، ص٢٧٣– ٣٢٢.

[٩] د. مصطفى بن أمينة، الذَّكاء الاصطناعيُّ التوليديُّ: أزمةٌ جديدةٌ في حقوق الملكيَّةِ الفكريَّة، المجلة الأكاديميَّة للبحوث القانونيَّةِ والسياسيَّة، مج٧،ع٢، جامعة عمار ثليجي الأغواط– كليَّة الحقوق والعلوم السياسيَّة، ٢٠٢٣، ص٧٩٠– ٨٠٤.

وتُعدُّ حمايةُ بياناتِ المستخدم أمرًا حسَّاسًا، حيث يتمُّ في الواقع جمعُ هذه البياناتِ وتحليلها وتخزينُها وإعادتها. وهو الأمرُ الذي قد يؤدِّي إلى اختراقِ البياناتِ الشَّخصيَّة، وانتهاك خصوصيَّةِ المستخدم، وفي هذا الصَّددِ يُمكننا القولُ بأنَّ "كل شيءٍ في المجتمعِ متَّصلٌ «les dérives prévisibles du tout connecté».

وبطبيعة الحال، فإنَّ إنترنت الأشياءِ لا يزالُ في مَهدِه؛ وممَّا لا شك فيه أنَّ ما يجعلُ الشَّيءَ المتَّصل أكثر ثراءً، هو إعطاؤه القدرةَ على مشاركةِ المعلومات، واتِّخاذُ القرارات، وتنفيذُ المهامّ، عن طريق الإنترنت؛ من أجل تحويلِ هذه الأشياءِ من أشياءَ تقليديَّةٍ إلى أشياءَ ذكيَّةٍ مزوَّدةٍ بأنظمةِ الذَّكاء الاصطناعيّ.

ولكن لم تقُمْ أيُّ دولةٍ حتى الآن بإنشاءِ إطارٍ قانونيٍّ واضح، ربما حتى لا يُؤدِّي إلى تقييد الإبداع، وكأنه إغفالٌ متعمدٌ لحين إصدارِ الشَّركاتِ المصنعةِ قائمةً بمسؤوليتها، ولهذا فإنَّ الشَّركاتِ المصنِّعةَ هي التي تتَّخذ أحيانًا الخطوةَ الأولى، فقد صرَّحت Google وVolvo وMercedes، على سبيل المثال، بالفعل بأنها ستوافقُ على تحمُّلِ المسؤوليَّةِ القانونيَّة في وقوعِ حادثٍ بسبب سيارتِهم ذاتيَّةِ القيادة(١٠). وتجدر الإشارةُ إلى أنَّ الاتِّحادَ الأوربيَّ قد أصدر لائحتَه لسنة ٢٠٢٤ والتي تعدُّ وبحقٍّ تنظيمًا تشريعيًّا للأشياءِ المُتَّصلةِ ولأنظمة الذَّكاءِ الاصطناعيّ وبخاصَّةٍ عاليةُ المخاطر.

أهميَّةُ موضوعِ الدِّراسة:

إن خطرَ الهجومِ السيبرانيّ على أيّ شيءٍ متَّصلٍ هو خطرٌ حقيقيٌّ. فقد يتسبَّب الاختراقُ في إساءةِ استخدامِ البياناتِ لصالحِ طرفٍ ثالثٍ غير مسموحٍ له باستخدامها، أو الاستخدام الضار، أو حتى الاستيلاء على الشَّيءِ المتَّصلِ ذاته، فضلًا عن المخاطرِ التي قد تنجمُ عن الشَّيءِ المتَّصلِ ذاته والتي قد لا يكونُ معظمُها غير معروفٍ في وقتنا الحاليّ. ولهذا كان لا بدَّ من البحثِ عن إطارٍ محكمٍ نوعًا ما للأشياءِ المُتَّصلة افتراضيًّا.

(10) http://www.autoguide.com/auto-news/2015/10/volvo-google-and-mercedes-to-accept-responsibility-in-self-driving-car-collisions.html.

(ISSN: 2537- 0758)

وفي الحقيقةِ لم تحظَ دراسةُ الأشياء المُتَّصلة بالاهتمامِ الكافي لا سيَّما في ظلِّ غيابِ التَّنظيمِ التَّشريعيِّ الخاصِّ بهذه التقنيَّةِ في مصر، حيث يتمُّ استخدامُها من خلالِ الشَّركاتِ والعقود الخاصَّة بين طالب الخدمةِ (الشَّيء المتَّصل)، والشَّركة المقدَّمة لها؛ وهو الأمرُ الذي يدعونا إلى البحثِ عن إطارٍ قانونيٍّ خاصٍّ ينظِّم ما نتج وما سينتجُ عن استخدامِ هذه التقنيَّةِ من مخاطر.

وعلى الرغمِ من أنَّ اللَّائحةَ الأوروبيَّةَ لحمايةِ البيانات (GDPR) قد أسهمت بشكلٍ كبيرٍ في أوروبا في تنظيمِ استخداماتِ البيانات والأشياء المُتَّصلة. إلا أنه في ظلِّ الأسئلةِ العديدة التي يُثيرها إدخالُ الأشياءِ المُتَّصلة في الحياةِ اليوميَّة للناس، وعلى جميعِ مستوياتِ المجتمع، لا يزال هناك نقصٌ في تنسيقِ السِّياساتِ العامَّة من أجل التوصُّل إلى تطويرِ إطارٍ قانونيٍّ مشتركٍ بين المؤسَّسات العامَّة والقانونيَّة والاقتصاديَّة[١١].

لذلك، هناك حاجةٌ إلى إطارٍ قانونيٍّ يضع قواعدَ منسجمةً بشأن الأشياءِ المُتَّصلةِ بشكلٍ عامٍّ والمزوَّدة بأنظمةِ الذَّكاء الاصطناعيِّ على وجهِ الخصوص؛ لتعزيز تطويرِ واستخدامِ واستيعاب الذَّكاء الاصطناعيِّ في السُّوق الداخليِّ، بما يلبِّي في الوقتِ نفسه مستوًى عاليًا من حمايةِ المصالحِ العامَّة، مثل: الصِّحةِ والسَّلامةِ وحماية الحقوق الأساسيَّة. ولتحقيقِ هذا الهدفِ، يجبُ وضعُ قواعدَ تنظِّم طرحَ أنظمةِ الأشياء المُتَّصلة في السُّوق ووضعها في الخدمةِ واستخدامها، وبالتَّالي ضمان السَّير السَّلسِ للسُّوقِ الداخليَّةِ والسَّماح لهذه الأنظمةِ بالاستفادة من مبدأ حريَّةِ حركةِ السِّلع

---

[١١] في عام ٢٠٢١، سلطت دراسةٌ أجْرَتها مؤسَّسة Rand الضَّوءَ على النقص الكبير في الحوكمةِ السياسيَّةِ لإنترنت الأشياء في الولاياتِ المتَّحدة، وأظهرت من خلال الاستخداماتِ الملموسة (جهاز تنظيم ضرباتِ القلب المتَّصل، وعدَّاد الخطى، وما إلى ذلك) أهميَّةَ أن تأخذ السِّياساتُ العامَّة في الاعتبارِ المزيد من الخصوصيَّةِ والأمن وقضايا الأخلاق.

Béa ARRUABARRENA, Objets connectés: penser les enjeux des technologies connectées sous l'angle de la médiation infocommunicationnelle, Vol. 15, N° 2-3 | 2ème semestre 2021- 1er semestre 2022 Objets connectés: enjeux technologiques, enjeux de société, p.22. https://doi.org/10.4000/ticetsociete.6262.

والخدمات. وينبغي أن تكونَ هذه القواعدُ واضحةً وقويَّةً في حمايةِ الحقوق الأساسيَّة، وداعمةً للحلول المبتكرةِ الجديدة.

إشكاليَّة الدِّراسة:

تُثير الأشياءُ المُتَّصلةُ عديدًا من الإشكاليَّاتِ والتَّحدِّيَّات؛ كون أنَّ اتِّخاذَ القرارات، في إطارِ الأشياءِ المُتَّصلة المزودة بأنظمةِ الذَّكاء الاصطناعيّ يتمُّ في أغلبِ الأحيان من خلالِ البرمجيَّاتِ الحاسوبيَّة التي توجدُ بداخلِ هذه الأشياءِ دون تدخُّلٍ بشريّ، كما أنَّ تشغيلَ هذه الأشياءِ يحتاجُ إلى تزويدِها بالبياناتِ المتعلِّقة بمُستخدميها وأحيانًا تكون بياناتٍ ضخمةً، فلمن ترسل هذه البيانات؟ وهل يُمكن تخزينها واستخدامُها دون علمِ صاحبها؟ كما تُثير هذه الأشياءُ عديدًا من القضايا؟ فما القضايا القانونيَّةُ التي تطرحُها؟ وما الإطارُ القانونيُّ للأشياءِ المُتَّصلة؟ وهل الحلولُ التي تُوفِّرها القوانين الرَّائدة في هذا المجالِ اليوم، تحدُّ من مخاطرِ استخدامِ الأشياء المُتَّصلة عالية المخاطر، خاصَّةً في مجال حمايةِ الخصوصيَة، والتَّعويض عن أضرارِ الأشياءِ المُتَّصلة، في حال عدمِ استجابتِها للرَّغباتِ المشروعةِ للمستهلك؟ وهل نحن بحاجةٍ إلى تنظيمٍ خاصٍّ أو تشريعاتٍ خاصَّةٍ للأشياءِ المُتَّصلة؟ ما إطارُ المسؤوليَّةِ عن الأشياءِ المُتَّصلة؟ Quel cadre pour la responsabilité du fait des objets connectés?

ومع تأثيراتِ إنترنتّ الأشياء– وخاصةً قدرتَه على التَّأثيرِ على العالمِ الماديّ ما هي أشكال الانتهاكاتِ التي تتسبَّب فيها الأشياءُ المُتَّصلةُ بحقوق مستخدميها؟ لا سيَّما في ظلِّ غموضِ الإطار القانونيّ للمسؤوليَّةِ، والذي لم يتمَّ تحديدُ معالمهِ الدَّقيقةِ بعدُ.

فإذا كانت المسؤوليَّةُ عن الفعلِ الإنسانيّ تبدو بسيطةً في الشَّيءِ المتَّصلِ الذي يحلُّ محلَّه أو يكمله، فهل يمكننا حقًّا أن نقولَ عن الشَّيءِ المتَّصلِ إنه "مسؤولٌ عن أفعاله"؟ أليست الثقةُ في إنترنت الأشياء، بل وحتى الذَّكاء الاصطناعي، موضوعًا اجتماعيًّا قبل أن يُصبح نقاشًا قانونيًّا؟ فهل للشَّيءِ المتَّصل دائمًا حارس؟، " l'objet

(ISSN: 2537- 0758)

connecté a-t-il toujours un gardien"؟[١٢]، وما المقصود بالحراسةِ على الشَّيء في القانون؟qu’est-ce que la garde d’une chose en droit? وكيف يُمكننا أن نتصوَّر أن مستخدمَ الشَّيءِ المتَّصلِ مسؤولٌ عن فشلٍ أو الضَّرر النَّاتج عن الشَّيءِ المتَّصل، رغم أنَّ المستخدمَ في أغلبِ الأحيان ليس لديه قدرةٌ على التحكُّمِ والتَّوجيهِ بسبب الاستقلاليَّةِ للشَّيءِ المتَّصلِ المزوَّد بأنظمةِ الذَّكاء الاصطناعيّ؟ فالأشياء المُتَّصلةُ هي أشياءُ خاصَّةٌ غالبًا ما تتمتَّعُ باستقلاليَّةٍ حقيقيَّةٍ، وبالتَّالي يُمكن التَّشكيكُ في مفهومِ السَّيطرةِ عليها[١٣].

وعلى الجانبِ الآخر، هل يُمكن اعتبارُ الشَّيءِ المتَّصل "معيبًا" إذا أحدث ضررًا؟ l’objet connecté peut-il être considéré comme «défectueux» s’il a causé un dommage ؟ بحيث يُمكن للمضرورِ أيضًا اتِّخاذُ إجراءاتٍ ضدَّ الشَّركةِ المصنِّعة للشَّيءِ مستندًا على المسؤوليَّةِ عن المنتجاتِ المعيبة؟ ولكنْ مع انتشارِ إنترنتِ الأشياء، كيف يُمكننا تحديدُ عيبِ الشَّيء المتَّصل؟[١٤].

---

[١٢] في ظلِّ اختلافِ الآراءِ حول المسؤوليَّة عن الأضرارِ النَّاتجةِ عن الشَّيء المتَّصل، ذهب جانبٌ من الفقه إلى أن عدمَ اليقينِ هذا لا يُشكِّل فراغًا تشريعيًّا؛ لأن ما يُسمَّى بالمسؤوليَّةِ المدنيَّة، المتعلِّقة بالضَّررِ الناجم عن شيءٍ ما، منصوصٌ عليها في المادة ١٢٤٢ من القانون المدنيّ الفرنسيّ: "لا يكون الشَّخصُ مسؤولًا فقط عن الضَّررِ الذي يُسبِّبه بفعلهِ الخاصّ". ولكنه مسؤولٌ عن الأشياءِ التي في حراستهِ وعُهدته. ومن النَّاحيةِ العمليَّة، يُمكننا أن نتخيلَ الضَّررَ الناجمَ عن اصطدامِ طائرةٍ بدون طيارٍ بنافذةٍ وكسرها لم تكُنْ لتكتشفها، أو جراحٍ روبوت يخلطُ بين عضوين أو مَركبةٍ ذاتيَّةِ القيادة تصطدم براكبِ دراجةٍ على سبيل المثال. هناك عديدٌ من الحالاتِ العمليَّة.

Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsable

(13) Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsablee

[١٤] تسردُ المادَّة ١٢٤٥-١٠ من القانون المدنيّ الفرنسيّ الحالاتِ التي تسمحُ بإعفاء المنتجِ من المسؤوليَّة، حيث تنصُّ على أنَّ المنتجَ مسئولٌ تلقائيًّا ما لم يثبتْ أنه لم يتمَّ طرحُ المنتجِ

منهجيَّة الدِّراسة:

في الحقيقةِ لدراسةِ التَّحدِّيَّاتِ القانونيَّة للاستخداماتِ المُستحدَثة للأشياءِ المُتَّصلةِ افتراضيًّا، تمَّ اتِّباعُ المنهجِ التحليليّ والاستقرائيّ، وذلك من خلال بيانِ الإطارِ المفاهيميّ للأشياءِ المُتَّصلةِ وتطوُّرها في ظلِّ ظهور الشَّبكاتِ الجديدةِ؛ وذلك بالرُّجوعِ إلى الحقائقِ العلميَّةِ والعمليَّةِ المختلفة، وتحليل النُّصوصِ والأحكامِ القانونيَّة المطبَّقةِ لمعرفةِ مدى مُلاءمتها للتَّطبيقِ على الأشياءِ المُتَّصلة، كما تمَّ الاعتمادُ على المنهجِ المقارن وذلك بالاعتماد على التَّوجُّهِ الأوربيّ لمسائل الأشياءِ المُتَّصلة، فضلًا عن تناولِ لائحةِ (الاتِّحاد الأوروبيّ) ١٦٨٩/٢٠٢٤ بشأن الذَّكاء الاصطناعيّ[١٥]،

للتَّداول، وإذا كان العيبُ الذي تسبَّب في الضررِ لم يكن موجودًا وقتَ طرحِ المنتجِ للتداول وأن هذا العيبَ نشأ لاحقًا، فضلًا عن أنه إذا كان المنتجُ غير مخصَّصٍ للبيعِ أو أيّ شكلٍ من أشكالِ التَّوزيع، كما أنَّ حالةَ المعرفةِ العلميَّةِ والتقنيَّة في وقتِ طرحِ المنتجِ للتَّداول لم تمكِّن من اكتشافِ وجودِ عيبٍ في المنتج.

Article 1245-10Version en vigueur depuis le 10 octobre 2016
Création Ordonnance n°2016-131 du 10 février 2016- art. 2
Le producteur est responsable de plein droit à moins qu'il ne prouve:
1 °Qu'il n'avait pas mis le produit en circulation;
2 °Que, compte tenu des circonstances, il y a lieu d'estimer que le défaut ayant causé le dommage n'existait pas au moment où le produit a été mis en circulation par lui ou que ce défaut est né postérieurement;
3 °Que le produit n'a pas été destiné à la vente ou à toute autre forme de distribution;
4 °Que l'état des connaissances scientifiques et techniques, au moment où il a mis le produit en circulation, n'a pas permis de déceler l'existence du défaut;
5 °Ou que le défaut est dû à la conformité du produit avec des règles impératives d'ordre législatif ou réglementaire.
Le producteur de la partie composante n'est pas non plus responsable s'il établit que le défaut est imputable à la conception du produit dans lequel cette partie a été incorporée ou aux instructions données par le producteur de ce produit.

[١٥] الغرض من هذه اللَّائحةِ هو تحسينُ أداء السُّوق الداخليَّةِ من خلال وضع إطارٍ قانونيٍ موحَّد خاصَّةً فيما يتعلَّقُ بتطويرِ وطرحِ أنظمة الذَّكاء الاصطناعيّ في السُّوق ووضعها في الخدمةِ واستخدامها في الاتِّحاد، وفقًا لقيم الاتِّحاد، وذلك لتعزيزِ استخدامِ الذَّكاء الاصطناعيّ الذي يركِّز

(ISSN: 2537- 0758)

والقوانين الخاصَّةِ الفرنسيَّةِ والمتعلِّقة بحمايةِ البياناتِ الشَّخصيَّة في ظلِّ التطوُّر الهائلِ لإنترنتّ الأشياء، ومقارنته بالنِّظام القانونيّ المصريّ لحمايةِ البياناتِ الشَّخصيَّة في القانون رقم ١٥١ لسنة ٢٠٢٠م، ودراسة مدى فاعليَّةِ نصوصِ قانون حمايةِ البيانات الشَّخصيَّة سالف الذِّكر لمواجهةِ التَّحدِّيَّات القانونيَّة المعاصرةِ للأشياءِ المُتَّصلة المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ.

خطة الدراسة:

قُسِّمتْ هذه الدِّراسةُ فصلين، تناول الفصلُ الأول: الأشياءَ المُتَّصلةَ وعدمَ اليقينِ القانونيّ في ظلِّ تطوُّر أنظمة الذَّكاءِ الاصطناعيّ، بينما تناول الفصلُ الثاني: مدى إمكانيَّةِ وجودِ إطارٍ قانونيّ خاصّ بالأشياء المُتَّصلة.

الفصل الأول: الأشياءُ المُتَّصلةُ وعدم اليقين القانونيّ في ظلِّ تطوُّر أنظمةِ الذَّكاء الاصطناعيّ

الفصل الثاني: نحو إمكانيَّة وجود إطار قانوني خاص بالأشياء المُتَّصلة.

على الإنسانِ مع ضمانِ مستوى عالٍ من حمايةِ الصحَّةِ والسَّلامة والحقوق الأساسيَّة المنصوص عليها في ميثاقِ الحقوقِ الأساسيَّةِ للاتِّحاد الأوروبيّ، بما في ذلك الديمقراطيَّةُ وسيادة القانونِ وحمايةُ البيئة، للحمايةِ من الآثارِ الضارَّة لأنظمة الذَّكاءِ الاصطناعيّ، ودعم الابتكار.

وتضمن هذه اللَّائحةُ حريةَ حركةِ السِّلع والخدمات القائمة على الذَّكاء الاصطناعيّ عبر الحدود، وبالتالي منع الدُّول الأعضاء من فرضِ قيودٍ على تطويرِ وتسويقِ واستخدام أنظمةِ الذَّكاء الاصطناعيّ، ما لم يتمَّ التَّصريحُ بذلك صراحةً بموجبِ هذه اللَّائحة.

الفصل الأول
الأشياء المُتَّصلة وعدمُ اليقين القانونيٍ في ظل تطوُّرِ أنظمةِ الذَّكاء الاصطناعي

تمهيدٌ وتقسيمٌ:

بعد الثَّورةِ الصناعيَّةِ التي قدَّمت للناس قوَّةً في الآلات، أصبحت الثَّورةُ الرقميَّةُ هي ثورةَ الذَّكاءِ الاصطناعيّ. وتقع الكائناتُ المُتَّصلة لاسلكيًّا بشبكاتِ المعلوماتِ في قلبِ عمليَّةِ التقاطِ البيانات الرقميَّة ونقلها. وممَّا لا شكَّ فيه أن تنفيذَ ومعالجةَ هذه البياناتِ يُؤدِّي إلى تغييرٍ جذريّ في أنماط الحياة، وتعديل طريقةِ إنتاج السِّلع والخدمات في شركاتِ المستقبل، وكذلك تعديل الاستخداماتِ، ولقد لحِقَ هذا التطوُّرُ الإنسانَ نفسَه.

وإذا كان القرن العشرون هو عصرَ الأشياءِ الماديَّةِ التي أراد الجميعُ امتلاكَها، إلا أنه مع القرن الحادي والعشرين أصبح الوصولُ بسرعةٍ إلى الخدمةِ أكثر أهميَّةً من امتلاكِ شيءٍ يكون استخدامه متقطعًا ومكلفًا وتقليديًّا. ويشير إنترنتّ الأشياءِ إلى قدرةِ الأشياءِ اليوميَّة على الاتِّصال بالإنترنت ونقل البيانات واستقبالها. ونعني بالشَّيءِ المتَّصلِ التَّشغيل الآليَّ الذي يسمحُ على سبيلِ المثال، بإضاءةِ الشُّرفةِ تلقائيًّا عند العودةِ إلى المنزلِ من العملِ أو حتى الأساور التي تُشارك مع الأشخاصِ لمعرفةِ عدد خطواتِ السَّير خلال اليوم أو وقت "الجري"[١٦]. ويُشير اسم "إنترنت الأشياء" إلى وجود اتِّصالٍ معيَّنٍ بين الأشياءِ المُتَّصلة ومستخدميها. علاوةً على ذلك، تتواصلُ هذه الأشياءُ أيضًا مع بعضِها البعض.

ويلعب الشَّيءُ المتَّصلُ أدوارًا رئيسةً بالاشتراك مع العناصرِ الأخرى للبنيةِ التحتيَّةِ لإنترنت الأشياء منها: جمع البياناتِ من بيئتهِ بفضلِ الشَّبكةِ التي يتواصلُ بها، كذلك

---

[١٦] علي بن ذيب الأكلبي، تطبيقاتُ إنترنتّ الأشياءِ في مؤسَّساتِ المعلومات، ع١٩، الاتِّحاد العربيُّ للمكتبات والمعلومات، ٢٠١٧، ١٦١– ١٨٠.

(ISSN: 2537- 0758)

نقل البياناتِ من الجهاتِ الفاعلةِ المختلفة، وتمكين تحليلِ المعلوماتِ بفضلِ منصَّةِ إنترنت الأشياء التي يتَّصل بها[١٧].

ويُرسِل الشَّيءُ المتَّصلُ البياناتِ المجمَّعةَ إلى البنيةِ التحتيَّةِ المخصَّصةِ بفضل اتِّصاله. ويتمُّ تخزينُ البياناتِ وتحليلُها عبر خوارزمياتِ الحسابِ، ومن ثمَّ إعادتها إلى المستخدم في شكلِ معلوماتٍ قابلةٍ للاستخدام.

وفي الحقيقة نجد أنَّ تزايدَ الأشياءِ المُتَّصلة في السُّوقِ والاهتمام المتزايد للمستهلكين بهذه المنتجاتِ الإلكترونيَّةِ الجديدة يُثير تساؤلاتٍ حول الطَّريقةِ التي ينظرُ بها القانونُ إلى هذه الابتكارات، وتشكِّل هذه الأشياءُ المُتَّصلةُ في الواقع نظامًا جديدًا، لم يخضعْ بعدُ لمجموعةٍ من القواعدِ القانونيَّةِ المحدَّدة.

وبناءً على ما سبق نبيّن ماهيَّةَ الأشياءِ المُتَّصلة في مبحثٍ أول، ثم نبيّن في المبحثِ الثاني مسألةَ عدم اليقينِ القانونيّ في مجال الأشياءِ المُتَّصلةِ، وذلك وفقًا لما يلي:

المبحث الأول: ماهيَّةُ الأشياءِ المُتَّصلة.

المبحث الثاني: عدمُ اليقينِ القانونيّ في مجالِ الأشياءِ المُتَّصلة.

المبحث الأول
ماهيَّةُ الأشياءِ المُتَّصلة

تمهيدٌ وتقسيمٌ:

تبدو الإمكاناتُ الاقتصاديَّةُ للأشياءِ المُتَّصلةِ بلا حدودٍ، ومِن الملاحَظِ وجودُ الأشياءِ المُتَّصلة في كلِّ مكانٍ بيننا، وبالتالي فإنَّ الأمرَ لا يتعلَّقُ بتحليل الابتكارِ المدمِّر، بل بالأحرى تغييرٌ في الحجم في تأثيرِ الأشياءِ المُتَّصلةِ على أنماطِ الإنتاج والاستهلاكِ في حياتنا اليوميَّة.

[١٧] ولنأخذْ مثالَ الريِّ التلقائيِّ الذي يتمُّ تشغيلُه وفقًا للبياناتِ المرسلةِ بواسطةِ محطَّة أرصادٍ جويَّةٍ متَّصلة، أو كاميرا مراقبةٍ مثبتةٍ في المنزلِ ومتَّصلةٍ بالهاتف.

وتجدر الإشارةُ أيضًا إلى أن الاتِّصالَ بالإنترنتّ يُشكِّل خصوصيَّةً لهذه الأشياء، وبفضل هذا، تعدُّ الأشياءُ المُتَّصلةُ بالضرورة جزءًا من نظامٍ بيئيٍّ أكبر، يتكوَّن من كائناتٍ وشبكاتٍ وخوادم وبرامجَ معالجةٍ وبروتوكولات أمانٍ متصلةٍ أخرى، وهذا الأمرُ لا يخلو من الخطورة.

ولعرضِ الإشكاليَّاتِ القانونيَّةِ والتَّحدِّيَّات الفنيَّةِ والاقتصاديَّة التي يُثيرها استخدامُ هذه التِّكنولوجيا الحديثة والتي تغيِّر في عالمنا الحاليّ، فإن الأمرَ يستدعي الوقوفَ عند المفهوم الاصطلاحيّ والفنيّ الدَّقيق للأشياءِ المُتَّصلة، والتَّدقيق في ارتباطاتِها مع مفهوم الذَّكاء الاصطناعيّ.

وفي هذا الشَّأنِ نوضِّحَ أولًا: مفهومَ الشَّيءِ المتَّصل، وذلك في المطلبِ الأول، ثم نُلحقه ببيانِ مخاطرِ الأشياءِ المُتَّصلةِ في مطلبٍ ثانٍ، **وذلك على النَّحو الآتي:**

المطلب الأول: مفهومُ الأشياءِ المُتَّصلةِ.

المطلب الثاني: مخاطرُ الأشياءِ المُتَّصلةِ.

المطلب الأول
مفهومُ الأشياءِ المُتَّصلةِ افتراضيًّا

تمهيدٌ وتقسيمٌ:

يُمثِّل ربطُ الأشياءِ عبر الإنترنتّ بدايةَ مرحلةٍ جديدةٍ من الثَّورةِ الرقميَّة[١٨] التي بدأت في نهايةِ السبعينيَّاتِ مع ظهورِ الكمبيوتر الشخصيّ والهواتفِ المحمولة، وفي عام ٢٠٢٠ هناك ما يقرُبُ من ٧ أشياءَ متَّصلةٍ لكلِّ شخصٍ في العالم[١٩]. كما أن مجالاتِ التَّطبيقِ عديدةٌ وتستمرُّ في النموِّ (الروبوتات، السيارات، الصِّحة، تخطيط المدن، التأمين، إلخ).

وبالفعل أصبحت الكائناتُ المُتَّصلةُ موجودةً بشكلٍ متزايدٍ في حياتنا اليوميَّة. ووفقًا لعددٍ من الدِّراسات، يُمكن أن يرتفعَ عددُ العناصرِ المُتَّصلةِ المباعة من ٥٠ إلى

(18) Soriano, Préface du livre de F. Forster et A. Bensoussan, Droit des objets connectés et télécom, Bruxelles, Editions Bruylant, 2017, p.147.

(19) https://www.pwc.co.uk/issues/megatrends/technological-breakthroughs.html#4.

(ISSN: 2537- 0758)

٢٠٠ مليار بحلول عام ٢٠٢٥. ومع جلبِ الوعدِ بالابتكار في عددٍ متزايدٍ من الأنشطة، فإن التَّحدِّيَاتِ التي يفرضُها ظهورُ إنترنت الأشياءِ متعدِّدةً وترتبط أكثرَ على نطاقٍ واسعٍ لمسائلِ رقمنةِ المجتمع. ويتمُّ دمجُ هذه الأجهزةِ الجديدة، التي تتيحُ التقاطَ البياناتِ وتحليلها وتصوُّرَها في الوقتِ الفعليّ، بسرعةٍ في جميعِ مجالاتِ الحياةِ اليوميَّةِ[٢٠]. كـ النَّقلِ، أو الإسكانِ (المباني الذكيَّة)، أو المدينةِ الذكيَّة، أو البيئةِ، أو الطاقة (الشَّبكاتِ الذكيَّة) (المياه، أو الغاز، أو الكهرباء)، أو الصِّحةِ، أو الرفاهية[٢١]. ومع ذلك، فإنَّ استخداماتها لا تزال أقلَّ إثارةً للجدل، ولا تزالُ القضايا التِّكنولوجيَّةُ والاجتماعيَّةُ والأنثروبولوجيَّة والأخلاقيَّةُ والقانونيَّةُ التي تُثيرها لم تتمَّ معالجتُها إلا بالقليل[٢٢].

وأمام هذه التَّحدِّيَاتِ المهمَّة، من الضَّروريّ اليوم تحديدُ مزايا وحدودِ الأشياءِ المُتَّصلة، كما يبدو من الضَّروريّ توضيحُ وظائفِها. وللقيام بذلك، لا بدَّ من مراجعةِ تطوُّرِ الكائناتِ المُتَّصلةِ من وجهة نظرِ البنى التحتيَّةِ التقنيَّةِ والأسواق التي تُمثِّلها هذه الأجهزة، ثم دراسة القضايا التقنيَّةِ والقانونيَّة.

وفي واقعِ الأمرِ يتميَّز الشَّيءُ المتَّصلُ بخصائصَ تميِّزُه عن غيرِه كقدرتهِ على جمع البيانات من خلال أجهزةِ الاستشعار. فضلًا عن القدرةِ على نقلِ ومعالجةِ المعلومات واتِّخاذ الإجراءاتِ إذا لزمَ الأمرُ.

وفي الحقيقةِ نرى أن لاستخداماتِ الأشياءِ المُتَّصلةِ خصوصيَّةً تظهرُ من خلالِ البحثِ في تطوُّر السُّلوك البشريّ، من رقابةِ الشَّخص العاديّ إلى ذاتيَّةِ الشَّيءِ في السُّلوكِ الآليّ، وهو الأمر الذي لا يخلو من مخاطرَ يصعُبُ السَّيطرةُ عليها.

---

(20) Saleh, I. Les enjeux et les défis de l'Internet des Objets (IdO). Internet des objets, 1(1) (2017)., 5.

(21) Peyroux, E. et Ninot, O. De la «smart city» au numérique généralisé: la géographie urbaine au défi du tournant numérique. L'information géographique, 83(2),. (2019),40-57.

(22) Simon, PLes leçons apprises des principales études sur les objets connectés en télémédecine. ***European Research in Telemedicine/La Recherche européenne en télémédecine***, 6(2),. (2017). 67-77.

وبناءً على ما سبق نبيّن نشأةَ وتطوُّرَ المقصودِ بالشَّيء المتَّصل، وكذلك أنواعُه وخصائصُه، وذلك وفقًا لما يلي:

الفرع الأول: نشأةُ وتطوُّرُ الأشياءِ المُتَّصلةِ افتراضيًّا.

الفرع الثاني: تعريفُ الأشياءِ المُتَّصلةِ افتراضيًّا.

الفرع الثالث: أنواعُ الأشياءِ المُتَّصلةِ وخصائصُها.

الفرع الأول
نشأةُ وتطوُّرُ الأشياءِ المُتَّصلة

تمهيدٌ وتقسيمٌ:

لقد استمرَّ تنوُّعُ أشكالِ "الأشياء المُتَّصلة" (OC) في النموِّ والتَّضاعفِ منذ تسعينيَّاتِ القرن العشرين، معتمدين على البنى التحتيَّةِ التقنيَّةِ الخاصَّة بها، وتحديدًا إنترنت الأشياء (IOT ،Internet of Things) فضلًا عن ربطِ شبكاتِ أجهزة الكمبيوتر مع بعضِها البعض. والأجهزة التي تعزِّز نموَّ خدماتِ المستخدم "كلُّ شيءٍ متَّصل"، وتتقارب التقنيَّاتُ اليومَ مع تطوُّرِ الذَّكاءِ الاصطناعيّ والبيانات الضَّخمةِ نحو "إنترنت السلوكيَّات" (IOB)، حتى وإن ظلَّ سوقُ الأشياءِ المُتَّصلة غير مُتماثلٍ، فإن تعميمَ هذه الأشياءِ بفضلِ إدراجِها التدريجيّ في عديدٍ من مجالاتِ الأنشطةِ اليوميَّة يبدو أنه يجري على قدم وساقٍ.

أولًا: **البنى التحتيَّةُ التقنيَّةُ لإنترنتّ الأشياء "كلُّ شيء متَّصل"**.

"Des infrastructures techniques de l’Internet des objets ou" tout connecté"

ظهرت الكائناتُ المُتَّصلةُ في التسعينيَّات، سواءٌ كانت تتجسَّد في شكلِ أجهزةِ استشعارٍ بدائيَّةٍ أو كائناتٍ أكثر تطوُّرًا تتضمَّن أجهزةَ استشعارٍ أكثر تعقيدًا، وتتميَّز هذه الأجهزةُ بقدرتِها على أن تكونَ أجهزةَ استقبالٍ وإرسالٍ للبيانات[٢٣]؛ ممَّا يمنحُها

(23) Roxin, I. et Bouchereau, A., (2017). Écosystème de l’Internet des Objets. Dans N. Bouhaï et I. Saleh (dir.), ***Internet des objets: Évolutions et Innovations***. Londres, Royaume-Uni: ISTE Éditions Londres.

(ISSN: 2537- 0758)

شكلًا معيَّنًا من "الذَّكاء". كونها مجهزةً بالبرامج والخوارزميات، حيث تتمثَّل وظيفتُها الرئيسةُ في التقاطِ البياناتِ وتحليلِها واستعادتِها عبر واجهاتٍ بدَهيَّةٍ للمستخدم. وفي واقع الأمرِ يُمكن الرُّجوعُ إليها من خلال تطبيقِ الهاتفِ المحمولِ أو من خلال منصَّةٍ تُوفِّرُ لوحاتِ معلوماتٍ لاستخدام أكثر من استراتيجيَّةٍ لأغراضِ صُنع القرار، والتي يعتمد تشغيلُها على القدرةِ على تجميع البياناتِ المجمَّعةِ على الخوادم وحفظها وتاريخها.

وبين عامي ١٩٩٠ و٢٠٠٠، ركَّز تطوُّرُ الكائناتِ المُتَّصلة بشكلٍ أساسٍ على نشرِ البنى التحتيَّة التقنيَّةِ لإنترنت الأشياء. حيث يُشير إنترنتّ الأشياءِ على أنه نظامُ الأنظمةِ "un systèmede systèmes"؛ كونه يجمعُ بين مجموعةٍ من التِّقنيَّاتِ القادرةِ على تحديدِ الأشياءِ الماديَّةِ (أجهزة الاستشعار، RFID، NFC، وما إلى ذلك) ومعالجة البياناتِ في أيّ مكانٍ وفي أيّ وقتٍ[٢٤]. ومنذ العقدِ الأوَّل من القرنِ الحادي والعشرين، ومع انخفاضِ تكاليفِ أجهزةِ الاستشعارِ والتَّخزين، تمَّ استيلاءُ المُستخدمين على الخدمات[٢٥]، كما أدَّى ذلك أيضًا إلى تطوُّرٍ حقيقيّ لإنترنت الأشياء، لا سيَّما مع وصولِ الأجهزةِ والهواتفِ الذكيَّة. ومع هذا التوسُّع والتطوُّرِ لإنترنت الأشياء، فقد ظهر ما يُسمَّى "بإنترنت كلّ شيءٍ متَّصل" (إنترنت كلّ شيءٍ، IOE)[٢٦]، والذي يعكسُ "التَّقاربَ بين شبكات الأشخاصِ والعملياتِ والبياناتِ والأشياء وسيؤدِّي "كلُّ شيءٍ متَّصل" إلى توليدِ كميَّاتٍ هائلةٍ من البيانات؛ ممَّا يُسْهم في تراكمِ البياناتِ الضَّخمةِ بهدف تقديم خدماتٍ جديدةٍ مخصَّصةٍ لصُنعِ القرار[٢٧].

---

(24) Benghozi, P. J., Bureau, S. et Massit-Folea, F. (2008). L'Internet des objets. Quels enjeux pour les Européens? Paris, France: Éditions de la Maison des sciences de l'homme. Repéré à https://hal.archives-ouvertes.fr/hal-00405070/document.

(25) Thebault, P.. **La conception à l'ère de l'Internet des Objets: modèles et principes pour le design de produits aux fonctions augmentées par des applications** (Thèse de doctorat). Paris, ParisTech. (2013).

(26) «Internet du tout connecté» (Internet of Everything).

(27) Bradley, J., Barbier, J. et Handler, D. (2013). White Paper: Embracing the Internet of everything to capture your share of

ثانياً: تقاربُ "الأشياء المُتَّصلة" مع الذَّكاء الاصطناعيِّ والبيانات الضَّخمة:

Convergence des "objets connectés" avec l'intelligence artificielle et les mégadonnées

في وقتنا الحالي يؤدِّي التقاربُ بين البنى التحتيَّةِ للشَّبكاتِ والبياناتِ الضَّخمة والخوارزميات القويَّة من الذَّكاء الاصطناعيّ إلى إحداثِ نقطةِ تحوُّلٍ جديدةٍ في تطوُّرِ إنترنتّ الأشياء بهدفِ إنشاءِ إنترنت السُّلوك. وهذه الفكرةُ التي طوَّرها جوتي نيمان (٢٠٢٠)، أستاذُ علم النَّفسِ بجامعةِ هلسنكي، والتي تناولتها مؤخرًا شركة Gartner في تقريرِها لأفضلِ اتِّجاهاتِ التِّكنولوجيا الاستراتيجيَّةِ لعام ٢٠٢١، والتي تعدُّ هذا الأمرَ تحدِّيًا جديدًا لإنترنتّ الأشياء، حيث أصبح تحليلُ البياناتِ السلوكيَّةِ ممكنًا من خلالِ التقاطِ "الغبار الرقمي poussières numériques[٢٨]"، الذي خلَّفته السلوكياتُ الفرديةُ، مثل: "بيانات العملاء التِّجاريّين"؛ وبيانات المُواطنين التي تتمُّ معالجتُها من قِبل القطاع العامّ والهيئاتِ الحكومية؛ وبيانات وسائلِ التَّواصلِ الاجتماعيّ؛ وكذلك البياناتُ من عملياتِ نشرِ التعرُّفِ على الوجهِ في المجال العامّ. وكما يسلِّط تقريرُ جارتنر الضَّوءَ على استغلالِ واستخدام هذه البيانات، التي أصبحت متزايدةً، بهدفِ التَّأثيرِ على السُّلوكِ الفرديّ.

وفي عام ٢٠٢٠، أشارت دراسةٌ أجْرَتها مؤسَّسةُ Rand إلى ظهورِ إنترنتّ الجسم Internet of Body لوصفِ ظهورِ الأشياءِ التي تربط جسمَ الإنسان، حيث تمثِّل المستشعراتُ الموجودةُ على الجلدِ أو علامات الجلدِ أو الوشم المرتبطُ به رمزًا لهذا التحوُّلِ نحو إنترنتّ السُّلوكيَّات التي تعتمدُ على البياناتِ القادمةِ من الجسم. ففي عام

$14.4 trillion. Cisco, 318. Repéré à https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf

(28) Banque des territoires. Caisse des dépôts (2020). Rapport État des lieux du marché de l'IOT en France avec un focus sur les zones peu denses. (2020). Repéré à https://www.banquedesterritoires.fr/sites/default/files/2021-01/20201109_LesReseauxIOTenZonePeuDense_Vdef_comm.pdf.

(ISSN: 2537- 0758)

٢٠١٧، قام معهدُ ماساتشوستس للتِّكنولوجيا بالفعلِ بتطويرِ تقنيَّةِ DuoSkin، وهي عبارةٌ عن وشم ملموسٍ يسمح للمستخدم بالتحكُّم في مشغلِ الموسيقى من جسمِهِ. وفي المجال الصِّحيّ، شكلت لصقةُ Freestyle7 الجلديَّةُ المخصَّصةُ لمَرضى السُّكر، والتي تمَّ تسويقُها منذ عام ٢٠١٧، ثورةً حقيقيَّةً في المراقبةِ المستمرَّةِ لمستوياتِ السُّكر في الدم.

لكنَّ هذا الاتِّجاهَ لا يقتصرُ على الصِّحة، حيث يتبيَّن من الاستخدام المكثفِ لرمز الاستجابةِ السَّريعة، أنه يلعب في الصِّين– على سبيلِ المثالِ– دورًا رئيسًا في تطويرِ إنترنتّ الأشياء. كما أن ترميزَ المجتمع بتقنيَّة QR، والذي حدث في غضونِ سنواتٍ قليلةٍ مع تطوُّر المدينةِ الذكيَّة[٢٩]، جعل استخدامها في الحياةِ اليوميَّةِ وعلى الشَّبكاتِ الاجتماعيَّة، والهويَّة الرقميَّة أكثر سهولةً، وكما يُشير جانبٌ من الفقهِ إلى أنه خلالَ الأزمةِ المرتبطةِ بجائحة كوفيد–١٩، كانت البطاقةُ الصحيَّةُ في شكلِ رمزِ الاستجابةِ السَّريعة، والذي يسمحُ بتخزينِ أنواع مختلفةٍ من البيانات والإشارة إليها (الهوية، تحديد الموقع الجغرافيّ، والصِّحة، وما إلى ذلك)، ويُمكن استخدامُها إما عبرَ الهاتفِ الذكيّ أو ارتدائها حولَ الرَّقبةِ من قِبل الأفرادِ الذين ليس لديهم هاتفٌ محمولٌ، مثل كبارِ السنِّ أو الأطفال. ومن ناحية أخرى في إيطاليا، كان لدى شابّ رمز الاستجابةِ السَّريعةِ الخاصّ ببطاقتهِ الصحيَّةِ وشمٌ على ذراعِهِ، وحتى لو ظلَّ هذا المثالُ حالةً فريدةً من نوعها، فهو يرمزُ إلى إمكاناتِ أجهزةِ الاستشعارِ الجلديَّة وظهور "إنترنت الأجسام"[٣٠].

(29) Zhang, Y. L'hégémonie du QR code en Chine. Communication présentée au Congrès de la SFSIC 2020. Repéré à https://sfsic2020.sciencesconf.org/325620/document.

(30) Béa ARRUABARRENA, Objets connectés: penser les enjeux des technologies connectées sous l'angle de la médiation infocommunicationnelle, Vol. 15, N° 2-3 | 2ème semestre 2021- 1er semestre 2022 Objets connectés: enjeux technologiques, enjeux de société, p.16.
https://doi.org/10.4000/ticetsociete.6262

وفي السِّياق ذاته تطوَّرت أنظمةُ الذَّكاء الاصطناعيّ إلى درجةِ الأخذ "بنظام التعرُّف على المشاعر" والذي يعني نظامَ الذَّكاءِ الاصطناعيّ لغرضِ تحديدِ أو استنتاج المشاعرِ أو نوايا الأشخاص الطبيعيّين على أساسِ بياناتِهم البيومترية(٣١).

ثالثاً: نحو تعميم التقنيات المُتَّصلة:

Vers une généralisation des technologies connectées:

على المستوى العالميّ، شهِدَ سوقُ إنترنت الأشياء نموًّا قويًّا في السَّنواتِ الأخيرة. لكنَّ هذا يتعلَّقُ في المقام الأوَّل بالقطاع الصناعيّ الذي أخذ زمامَ المبادرة، منذ عام ٢٠٠٩، في الولايات المتَّحدة وأوروبا والصِّين، كجزءٍ من برامج التحوُّلِ البيئيّ، ولا سيما مع تركيبِ عداداتٍ ذكيَّةٍ لمراقبةِ الموارِدِ عن بُعد: عدادات الكهرباء والمياه والغاز. (الشَّبكات الذكيَّة)، بمجرَّدِ اقترانِها بالخوارزمياتِ التنبؤيَّة، تعملُ على تعزيز الإدارةِ الذاتيَّةِ للاستهلاك (Mpawenimana، ٢٠٢٠).

وفيما يتعلَّقُ بالأشياءِ المُتَّصلةِ بالمستهلك، قبل بضع سنوات، كان بإمكانِنا اعتبارُ الاستخداماتِ التي ظهرتْ من مُمارساتٍ، والتي ظهرت في عام ٢٠٠٧ في وادي السيليكون هامشيَّةً أو مخصصةً للذُّكورِ والشَّبابِ والسُّكان المتميِّزين اجتماعيًّا– كما وصفت الأبحاثُ الحديثة(٣٢)، ويُمكننا في وقتنا الحاليّ أن نرى زيادةَ الاستخداماتِ بشكلٍ تدريجيّ، ولا سيَّما بالنِّسبةِ للأشياءِ العامَّةِ في مجالاتِ الرِّياضةِ والرَّفاهية....إلخ(٣٣). حيث أصبحْنا نجدُ أشياءَ متصلةً في عددٍ من المجالات، بما

(31) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art. (39) 'emotion recognition system' means an AI system for the purpose of identifying or inferring emotions or intentions of natural persons on the basis of their biometric data.

(32) Dagiral, E. Extension chiffrée du domaine de perfectionnement? La place des technologies de quantification du soi dans les projets d'auto-optimisation des individus. ***Ethnologie française***, 176, (2019), 719-734.

(٣٣) وفقًا لشركةِ أبحاثِ السُّوق الأمريكيَّة IoT Analytics، تمَّ نشرُ ١٢.٣ مليار كائنٍ متَّصلٍ في جميع أنحاء العالم في نهاية عام ٢٠٢١ (سينها، ٢٠٢١). في فرنسا، تظهر دراسةُ السُّوقِ للعلامات التجاريَّةِ الرئيسةِ الموزَّعةِ أن توزيعَ المبيعاتِ في عام ٢٠٢١ هو ٥٥% من الأشياء المتَّصلةِ بالمنزل، و٣١% للتقنياتِ المحمولةِ أو القابلةِ للارتداء (الأجهزة القابلة للارتداء)، مثل الملابسِ والسَّاعاتِ المتَّصلة و١٢% للطَّائرات بدون طيارٍ والأجهزة، و٢% للأشياء الصحيَّة.

(ISSN: 2537- 0758)

في ذلك الصحة[٣٤] والرياضة، على سبيل المثال الجري أو كرة القدم أو حتى ركوب الدراجات والسكن (المنزل الذَّكي)، حيث يقومون بتعديلِ "أنماط الحياة" بشكلٍ عميقٍ[٣٥]، وفي هذا المجالِ الأخير، يدلُّ جنون مكبراتِ الصَّوتِ المُتَّصلة المجهزة بمساعدين صوتيَّين (Amazon وGoogle وBaidu وAlibaba و Xiaomi (Canalys, 2020)) على هذا التطوُّرِ الذي يسمحُ بالتَّفاعلِ المباشرِ مع الأشياءِ المُتَّصلةِ الأخرى في قلب المنزل (أجهزة التلفاز، الثلاجات، المكانس الكهربائيَّة، السيارات، إلخ[٣٦].

كما أن الأسعارَ التي كانت تعدُّ في السَّابق من بين العقباتِ الرئيسةِ التي تحولُ دون اعتمادها، أصبحت أيضًا جذابةً بشكلٍ متزايدٍ بسبب العروضِ التي تجمعُ بين شراءِ هاتفٍ ذكيٍّ وساعةٍ متَّصلةٍ بالإنترنت. وهكذا، في عام ٢٠٢١، وفقًا لشركة Strategy Analytics (2021)، ارتفعت مبيعاتُ الساعاتِ المتَّصلة من Apple أو Samsung أو Garmin بنسبة ٤٧%، أو ١٨.١ مليون وحدة تمَّ بيعُها في عامٍ واحدٍ.

Béa ARRUABARRENA, Objets connectés: penser les enjeux des technologies connectées sous l'angle de la médiation infocommunicationnelle, Vol. 15, N° 2-3 | 2ème semestre 2021- 1er semestre 2022 Objets connectés: enjeux technologiques, enjeux de société, p. 17.
https://doi.org/10.4000/ticetsociete.6262.

(34) Arruabarrena, B. (2022). Technologie numérique de quantification des corps à l'épreuve du comportementalisme: vers un design de la médiation homme-données. Dans A. Khatchatourov, O. Avenati, P. A. Chardel, I. Quéval (dir.), ***Corps connectés, figures, fragments, discours*** (p.118-135). Paris, France: Presse des mines.

(35) Marchand, G. et Dufour, S. (2020). L'influence réciproque de la maison intelligente sur les styles de vie et ses implications sur la fonction d'architecte. Communication & management, 17, 53-67. https://www.cairn.info/revue-communication-et-management-2020-1-page-53.htm.

[٣٦] للمزيدِ من الأمثلةِ حول استخداماتِ الذَّكاءِ الاصطناعيِّ راجع: د. حسام الدين محمود حسن، واقع الشخصيَّةِ القانونيَّة للذَّكاءِ الاصطناعيِّ، مجلة روح القانون، العدد ١٠٢، أبريل ٢٠٢٣، ص١٣٠-١٣٤.

ويعدُّ البحثُ في العلوم الطبيَّةِ وبشكلٍ أوسع في علوم التَّمريضِ والصَّيدلة مهمًّا جدًّا أيضًا في مجالِ الأشياءِ المُتَّصلة[٣٧]، وتمثِّل الخدماتُ المُتَّصلةُ في مختلفِ مجالاتِ الصِّحةِ أحدَ القطاعاتِ الأولى لتطبيقِ الأشياءِ المُتَّصلة، مثل التَّطبيبِ عن بعدٍ[٣٨]، وكذلك تطويرُ أجهزةِ قياسِ نسبةِ الجلوكوز في الدَّم ومضخَّات الأنسولين، وأجهزة مراقبةِ ضغطِ الدَّم، وتخطيط القلبِ الكهربائيّ (ECGs)، والسَّماعات الطبيَّة المُتَّصلة، ومقاييس التأكسج النبضيَّة المُتَّصلة، وما إلى ذلك. وتمَّ استخدامُها أيضًا في الأمراضِ المزمنةِ، مثل مرض السُّكريّ أو قصور القلبِ أو انقطاع التنفُّسِ في أثناء النوم، وكذلك الأبعادُ الأخرى للصِّحة، مثل النَّشاطِ البدنيّ ونمطِ الحياةِ غير المستقرّ[٣٩].

الفرع الثاني
تعريفُ الأشياءِ المُتَّصلة افتراضيًّا

تمهيدٌ وتقسيمٌ:

يُظهرُ تطوُّرُ الكائناتِ المُتَّصلةِ منذ التِّسعينيَّاتِ أنها حاضرةٌ بشكلٍ متزايدٍ في حياتنا اليوميَّة. فمن تطوُّرِ بنيتِها التحتيَّةِ التقنيَّة، التي نُطلق عليها "إنترنت الأشياء"، إلى تلك الخاصَّة بـ "إنترنت كلّ شيءٍ متَّصل"،» l'«Internet des objets», à «celles de l'«Internet du tout connecté» وتتقاربُ التِّقنيَّاتُ اليوم مع الذَّكاءِ الاصطناعيّ والبيانات الضَّخمة نحو "إنترنت السُّلوكيَّات" (إنترنت السُّلوك). الذي

---

[٣٧] مها يسري عبد اللطيف عبد اللطيف نصار، المسؤوليَّةُ القانونيَّةُ للذَّكاء الاصطناعيّ، المجلة القانونيَّة (مجلة متخصِّصةٌ في الدِّراساتِ والبحوث القانونيَّة) المجلد ١٧، العدد ٧ أغسطس ٢٠٢٣، ص١٤٩٢.

[38] Mathieu-Fritz, A. et Gaglio, G. (2018). À la recherche des configurations sociotechniques de la télémédecine. ***Réseaux***, 207, 27-63.

[39] Rosenberger, M. E., Buman, M. P., Haskell, W. L., McConnell, M. V. et Carstensen, L. L. (2016). 24 hours of sleep, sedentary behavior, and physical activity with nine wearable. ***Medicine and science in sports and exercise***, 48(3), 457-465.

(ISSN: 2537- 0758)

يتفاعلُ أكثر فأكثر مع الأجسام، والذي يتمثَّل تحدِّيه الآن في التَّحليل السلوكيّ. وتُظهر حالة الفنّ العلميّ أدبيَّاتٍ غزيرةَ الإنتاج حول هذا الموضوع وقضاياه المختلفة، مع أولويَّةِ القضايا الاجتماعيَّة التقنيَّة من علوم الكمبيوتر والعلوم الطبيَّة والتَّسويق التي تقدِّم هذه الأشياءَ الرقميَّةَ الجديدة كوعودٍ بالابتكار في عددٍ متزايدٍ من المجالات، بما في ذلك الصِّحةُ، والرَّفاهيةُ والنَّقلُ والإسكان (المباني الذكيَّة– المدن الذكيَّة) والطاقة (الشبكات الذكيَّة) والبيئة وحتى الرِّياضة.

ومع ذلك، تظلُّ استخداماتُ الكائناتِ المُتَّصلة مثيرةً للجدل، حيث تثيرُ مجموعةٌ من المساهماتِ من العلوم الإنسانيَّةِ والاجتماعيَّةِ قضايا اجتماعيَّةً وسياسيَّةً وأنثروبولوجيَّة فيما يتعلَّقُ ببياناتِ العالم وتأثيراتها على العلاقاتِ الاجتماعيَّة. بالإضافةِ إلى ذلك، لا تزالُ القضايا القانونيَّةُ يتمُّ الاستهانةُ بها إلى حدٍّ كبيرٍ، وحتى أقل تقييمًا، تمامًا مثل تلك المتعلِّقةِ بالطَّفراتِ الأنثروبولوجيَّة التي أدخلتها هذه الأشياءُ الجديدة، والتي تُعدِّل بشكلٍ عميقٍ تصرُّفاتِ الحياةِ اليوميَّة بفضلِ الانغماس المستمرّ القائم على البياناتِ والأتمتة[٤٠].

أولًا: المقصودُ بالشَّيءِ المتَّصل افتراضيًّا:

What is a connected object?

إذا كان مفهومُ الشَّيءِ المتَّصل يبدو واسعَ الانتشارِ، فإن إعطاءَ تعريفٍ له يظلُّ صعبًا ويختلفُ فهمُه باختلافِ آراءِ الفقهاء. ووفقًا لقاموس لاروس، يُشير مصطلحُ "الشَّيء" من ناحيةٍ، أنه شيءٌ ملموسٌ، يُمكن إدراكُه عن طريقِ البصر، أو عن طريق اللَّمسِ، ومخصَّصٌ لاستخدامٍ معيَّنٍ[٤١]، ومن ناحيةٍ أخرى، فإنَّ مصطلحَ "متَّصل"، وفقًا لأصلها اللاتينيّ connexio، Connecte: "مرتبطٌ". وبحسَب هذا

(40) Béa ARRUABARRENA, Objets connectés: penser les enjeux des technologies connectées sous l'angle de la médiation infocommunicationnelle, Vol. 15, N° 2-3 | 2ème semestre 2021- 1er semestre 2022 Objets connectés: enjeux technologiques, enjeux de société, p. 9-35.
https://doi.org/10.4000/ticetsociete.6262.

(41) Larousse Maxipoche 2018, Editions Larousse 2017.

المصدرِ نفسه، فإن مصطلحَ التَّوصيلِ يعني "توصيل الدَّوائرِ أو الأجهزةِ أو الآلات الكهربائيَّة فيما بينها من خلالِ شبكةِ Wi-Fi أو Bluetooth أو غير ذلك من الشَّبكاتِ اللاسلكيَّة.

ويُمكننا تعريفُ الشَّيء المتَّصلِ بأنه شيءٌ ملموسٌ مزوَّدٌ بدائرةٍ كهربائيَّةٍ تسمحُ بربطهِ بجسمٍ آخر، بغضِّ النَّظر عن وضعِ الاتِّصالِ (سلكي أو لاسلكي). ومع ذلك، يبدو أنَّ وضعَ اتِّصالِ الأشياءِ المُتَّصلة يقتصرُ على الاتِّصالِ اللاسلكيّ.

ووفقًا لسابين بيرنهايم-ديسفو، فإن الكائنَ المتَّصلَ هو جسمٌ مادِّيٌّ يتمُّ فيه دمجُ الوسائلِ التقنيَّة، ممَّا يسمحُ له بجَمعِ البياناتِ وتخزينها ومعالجتها ونقلها باستخدامِ التِّقنيَّاتِ اللاسلكية"[٤٢]. وفي الحقيقة لا يُعطي هذا التَّعريفُ معلوماتٍ عن الشَّيءِ الذي يرتبطُ به الكائن، خلافًا للتَّعريفِ السَّابقِ الذي بموجبهِ يكون الكائنُ المتَّصلُ أيضًا جهازًا إلكترونيًّا قادرًا على الاتِّصالِ بجهازِ كمبيوتر أو هاتفٍ ذكيٍّ أو جهازٍ لوحيٍّ عبر شبكةٍ لاسلكيًّا، ممَّا يربطه بشبكةِ الإنترنت.

وبحسب ما سبق فإنَّ الشَّيءَ المتَّصلَ هو أيضًا شيءٌ قادرٌ على التَّواصلِ مع شيءٍ آخر. ولديه القدرةُ على تبادلِ البياناتِ مع كياناتٍ ماديَّةٍ أو رقميَّةٍ أخرى، وفي أغلب الأحيانِ يكونُ هذا التَّبادلُ عبر الإنترنت. وسيُلاحظ أنه من الممكن أيضًا للشَّيءِ المتَّصلِ التمكُّن من التَّواصلِ مع شخصٍ ما. ولهذا نقترحُ الإبقاءَ على التَّعريفِ التالي للشَّيءِ المتَّصل: شيءٌ ماديٌّ تتكاملُ فيه الوسائلُ التقنيَّةُ؛ ممَّا يسمحُ له بجمعِ البياناتِ وتخزينها ومعالجتها وإعادة إرسالها باستخدامِ شبكةٍ لاسلكيَّة، وقادرٌ على التَّواصل مع الإنسانِ والكمبيوتر، والهاتف الذكيّ أو أيِّ شيءٍ آخر عبْر هذه الشَّبكةِ الداخليَّةِ أو الإنترنت.

والأشياءُ المُتَّصلةُ هي أشياءُ ماديَّةٌ تدمج وسائلَ الاتِّصالِ؛ ممَّا يسمح بوظائفَ محدَّدةٍ. ولقد أعلنت شركةُ IoT Analyctics في دراسةٍ أنَّ هناك ما يقربُ من

(42) S. BERNHEIM-DESVAUX, «Objets connectés- L'objet connecté sous l'angle du droit des contrats et de la consommation», Contrats Concurrence Consommation n° 1, Janvier 2017, étude 1. Un réseau sans fil peut être un Wi-Fi, Bluetooth, réseaux de téléphonie mobile etc.

(ISSN: 2537- 0758)

١٢.٣ مليار كائنٍ متَّصلٍ في العالم في نهايةِ عام ٢٠٢١. واليوم، تظهرُ الكائناتُ المُتَّصلةُ بأشكالٍ كثيرةٍ ومتنوّعة، حيث أصبحنا أمامَ أجهزةٍ تلفزيون متَّصلةٍ، سياراتٍ، ساعاتٍ، نظاراتٍ، موازينَ، ثلاجاتٍ وغيرها الكثير. وهناك حوالي ١٠ أشياءَ متَّصلةٍ لكلِّ أسرةٍ في عام ٢٠٢١[٤٣].

وتجدرُ الإشارةُ أيضًا إلى أنَّ الاتِّصالَ بالإنترنت يُشكِّل خصوصيَّةً لهذه الأشياء، وبفضل هذا، تعدُّ الكائناتُ المُتَّصلةُ بالضَّرورة جزءًا من نظامٍ بيئيٍّ أكبر، يتكوَّن من كائناتٍ وشبكاتٍ وخوادمَ وبرامج معالجةٍ وبروتوكولات أمانٍ متَّصلةٍ أخرى[٤٤].

وفي بعضِ الأحيان، تكونُ للأشياءِ المُتَّصلةِ أصولٌ قديمةٌ كالإشاراتِ عن بُعدٍ، مثل: إشارات المرور، وأجهزة استشعار الضَّغطِ عند مداخلِ مواقفِ السيارات، وفي أكشاكِ رسوم الطُّرق. ومع ذلك، فهذه أشياءُ متصلةٌ "تقليديَّة"، حيث يُمكن التحكُّمُ فيها عن بُعدٍ أو تشغيلها آليًّا، ولكن نادرًا ما يُمكنها الاستجابةُ أو نقلُ البياناتِ إلى المستخدم؛ كونُها غير متَّصلةٍ بالإنترنت، أو حتى في بعضِ الأحيانِ بشبكةٍ محليَّةٍ، ونادرًا ما تكونُ متَّصلةً بدون كابلات[٤٥].

ويُنظر إلى الشَّيءِ المتَّصلِ على أنه شيءٌ متَّصلٌ بهاتفٍ ذكيّ أو بشبكةٍ لاسلكيَّة يدمجُ تطبيقًا ذكيًّا، ويُقدِّم خدماتٍ للمستخدم عن طريقِ تحديدِ الهويةِ والتقاط البيانات

(43) https://www-murielle--cahen-fr.translate.goog/objets-connectes-et-donnees-personnelles/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

(٤٤) كما تمَّ تطويرُ المساعدِ الصوتيّ للسَّماعاتِ المتَّصلةِ بشكلٍ كبيرٍ، ومن بينها Alexa الشَّهيرُ من Google Home أو HomePod من Apple. السَّماعة المتَّصلةُ موجودةٌ في حوالي ١ من كلِّ ٤ منازلَ في الولاياتِ المتَّحدة في عام ٢٠١٩. وقد بحثتْ CNIL في هذا الموضوعِ ونشرَتْ تقريرًا تقنيًّا في سبتمبر ٢٠٢٠ حول المساعدين الصَّوتيين.
https://www-murielle--cahen-fr.translate.goog/objets-connectes-et-donnees-personnelles/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

(45) https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431.

(درجات الحرارةِ وتحديد الموقع الجغرافيّ.... إلخ)، ولهذا من المحتملِ أن يكونَ أيُّ شيءٍ متَّصلًا.

ويُمكن اعتبارُ أيّ جهازِ كمبيوتر بمثابةِ كائنٍ متَّصل، وفي حياتنا اليوميَّةِ يُلاحَظ بأن هناك اتِّصالًا دائمًا بمعدَّاتٍ ثابتةٍ أو متنقلةٍ للخدماتِ اليوميَّةِ، كتحديدِ الموقع الجغرافيّ على هاتفنا الذكيّ، وسحب الأموالِ من ماكينةِ الصَّرافِ الآليّ التي تتَّصلُ بمصرفنا أو الدَّفع باستخدام البطاقةِ المصرفيَّةِ في مَتجرٍ.

ويُمكن تعريفُ الأشياءِ المُتَّصلةِ افراضيًّا على أنَّها أجهزةُ استشعارٍ أو كائناتٌ مجهزةٌ بأجهزةِ استشعارٍ قادرةٍ على توصيلِ (إرسال واستقبال) البياناتِ عبر الشَّبكة، وعادةً يتمُّ إرسالُ البياناتِ إلى جهازِ كمبيوتر أو جهازِ لوحيّ أو هاتفٍ ذكيّ أو أيّ جهازِ إلكترونيّ آخر، وأحيانًا عبر الإنترنت، بحيث يُمكن الوصولُ إلى المعلوماتِ على جميع الأجهزةِ التي يُمكنها الاتِّصالُ بها. ولذلك الشَّيءِ المتَّصل هو الشَّيءُ القادر،- بالإضافةِ إلى وظيفتهِ الأساسيَّة- على إرسالِ أو استقبالِ المعلوماتِ عبر شبكةِ اتِّصالاتِ"[٤٦].

فالشَّيء المتَّصلُ هو شيءٌ قادرٌ على توصيلِ معلوماتٍ متنوّعةٍ إلى شيءٍ آخرَ أو إلى الإنترنت، ويُمكنه التقاطُ البياناتِ ونقلها (عبر أنواعٍ مختلفةٍ من الاتِّصال)، وفي بعضِ الأحيان معالجتها للمساعدةِ في اتِّخاذ القراراتِ أو بدء الإجراء.

ويتراوحُ مفهومُ الشَّيء المتَّصل من جهازِ استشعارٍ بسيطٍ إلى كائنٍ ذكيٍّ، أي كائنٍ قادرٍ على المعالجة، إما بشكلٍ مستقلٍّ أو في حوارٍ مع هاتفٍ ذكيٍّ أو منصَّةٍ لجمعِ ومعالجةِ بياناتِ إنترنت الأشياء، وهو يعملُ بفضلِ الاتِّصالِ الذي يُمكن أن يكونَ موجودًا منذ البدايةِ أو تتمُّ إضافتُه لاحقًا، وهو مدمجٌ في البنيةِ التحتيَّةِ لشبكةِ إنترنت الأشياء.

---

[٤٦] المعلوماتُ التي يُمكن للجهازِ إرسالها هي على سبيلِ المثالِ درجة الحرارةِ المُحيطة بمنزلك، والصُّور الداخليَّة، ومعدَّل ضرباتِ القلب، وما إلى ذلك. كلُّ هذا يتوقَّفُ على الكائن، سواءٌ كان كاميرا أو ساعةً أو أيَّ شيءٍ آخر.

(ISSN: 2537- 0758)

ثانياً: العناصرُ الأساسيَّةُ لعملِ الأشياءِ المُتَّصلةِ افتراضياً:

في مقالةٍ عن "فكِّ تشفيرِ الكائناتِ المُتَّصلة"، يُقدِّم جان بول كرين العناصرَ الأساسيَّةَ التي تجعلُ من المُمكن تأهيل الشَّيءِ المتَّصل(٤٧) وهي كالتَّالي:

أ- **وجودُ أجهزةِ الاستشعارِ:** وهي تسمحُ للكائنِ بالتقاطِ المعلوماتِ الواردةِ من بيئته، ويجب أن تكونَ دقيقةً وموثوقةً بدرجةٍ كافيةٍ، كما يجبُ معايرةُ قياساتها بشكلٍ متَّسقٍ مع أجهزةِ الاستشعارِ الأخرى الموجودة على كائناتٍ أخرى متَّصلة؛ حتى يُمكن إجراءُ الحوار، وخلال هذه المرحلةِ تعملُ أجهزةُ الاستشعارِ المزوَّد بها الشَّيءُ المتَّصلُ على التقاطِ بياناتٍ من العالمِ الخارجيّ المحيط بالشَّيء، حيث يقوم برصدِ سلوكيَّاتِ الإنسان، وتعتمدُ موثوقيَّةُ المعلوماتِ المنبعثة من الكائنات المُتَّصلةِ على أجهزةِ الاستشعارِ الخاصَّة بها. ويتمُّ تزويدُ الأشياءِ بهذه الأجهزةِ بالعملِ المشتركِ بين الشَّركاتِ المنتجةِ لأجهزةِ الاستشعار، وكذلك الشَّركاتُ المصنعةُ للأشياءِ المُتَّصلة.

ب- **تجميع البيانات:** يتمُّ تجميعُ البياناتِ الملتقطة، وهذه هي العمليَّةُ التي يتمُّ من خلالِها دمجُ البياناتِ من الأشياءِ المُتَّصلةِ مع بياناتٍ أخرى.

ج- **تحليلاتُ الكائنات:** وتُسمَّى أيضًا تحليلاتُ الأشياءِ (AoT)، وهي التي ستحوّل المعلوماتِ الأوليَّةِ إلى معلوماتٍ مطوَّرةٍ لتمكين اتِّخاذِ القرارِ والتَّنفيذ لاحقًا، وبمعنًى آخر، إنَّها مرحلةُ معالجةِ البياناتِ؛ لجعلها قابلةً للاستخدامِ واستغالها بشكلٍ سليمٍ.

د- **العمل المعرفي:** يتضمَّنُ التَّفكيرُ والتأمُّل، ولا يُمكن تنفيذُه، في جميعِ الحالاتِ تقريبًا، إلا عن طريقِ الذَّكاءِ الاصطناعيّ؛ ممَّا يسمحُ للكائناتِ المُتَّصلةِ بأن

(47) Laura Jounda Sonkwa, Responsabilité civile du fait des objets connectés autonomes Master, Droit des assurances Formation en apprentissage RESPONSABILITE CIVILE DU FAIT DES OBJETS CONNECTES AUTONOMES Mémoire de recherche Par Sous la direction de Monsieur le professeur Louis Perdrix Année: 2018– 2019.

تكونَ مستقلَّةً، وجديرٌ بالذِّكر أن الفعلَ المعرفيَّ يختلفُ باختلافِ مستوياتِ القدرةِ التي يتمتَّعُ بها الشَّيء.

وفيما يتعلَّقُ بالعملِ المعرفيّ، ليس المقصودُ من جميعِ الأشياءِ المُتَّصلةِ أن تكونَ مستقلَّةً. وبالمثل، ليس المقصود من جميعِ الأشياءِ المستقلَّةِ أن تكونَ متَّصلةً. ولكنْ في كثيرٍ من الأحيان، تكون معظمُ الأشياءِ المُتَّصلةِ مستقلَّةً ذاتيًّا. وفي هذه الفرضيَّةِ بشكلٍ أساسٍ، من المرجَّحِ أن يثيرَ الكائنُ المتَّصلُ أسئلةً جديدةً في قانون المسؤوليَّة. وستقتصرُ هذه الدِّراسةُ على الكائناتِ المُتَّصلةِ المستقلَّة؛ أي المجهزة بنظام ذكاءٍ اصطناعيٍّ التي يُسمح لها باتِّخاذِ القراراتِ والتَّفاعل مع بيئتِها في أثناء الاستخدام، والتي من المُحتملِ أن تُسبِّب هذه الأشياءُ ضررًا، بحيث يُمكن للكائن–على سبيل المثال– اتِّخاذُ قرارٍ يضرُّ بالطَّرفِ الثالثِ أو مالكه، مثل مركبةٍ ذاتيَّةِ القيادةِ تصدمُ أحدَ المشاة، أو غسالةٍ متَّصلةٍ تُسبِّب أضرارًا بالمياه. ومن المُمكن أن ينجم الضَّررُ أيضًا عن طريقِ اختراقِ الشَّيء ذاته، مع العلم أن معظمَ الكائناتِ المُتَّصلة لها كلمةُ مرورٍ فريدة وغير قابلةٍ للتَّعديل، أو ببساطةٍ ليس لديها كلمةُ مرورٍ[٤٨].

ثالثًا: استخداماتُ الأشياءِ المُتَّصلة:

في ظلِّ ما يشهدُه عالمُنا المعاصرُ من تقدُّم وتطوُّرٍ تكنولوجيّ غير مسبوقٍ، وما زالت الابتكاراتُ تتوالى إلى يومِنا هذا، فلم تَعُد الأشياءُ الأكثر شيوعًا في حياتنا بسيطةً ومقتصرةً على وظائفِها التقليديَّة، بل أصبح لهذه الأشياءِ دورٌ إيجابيٌّ يعمل ذاتيًّا دون حاجةٍ إلى تدخُّلٍ بشريّ، فمثلًا لم تَعُد النَّظاراتُ أو السَّاعاتُ أو الأجهزةُ المنزليَّةُ مقتصرةً على مُجرَّدِ الاستخداماتِ العاديَّة المعروفة، بل أصبحَ لها دورٌ يجعلنا نندهشُ منه.

وممَّا لا شكَّ فيه تتعدَّدُ استخداماتُ الأشياءِ المُتَّصلة في جميع جوانبِ حياتنا اليوميَّةِ بشكلٍ متزايدٍ، مثل: رقابةِ استهلاكِ المياه والكهرباءِ والغاز، وكذلك حالةُ الطَّقسِ، وتنبيه السَّائقين بالرَّاداراتِ الموجودةِ على الطُّرق، وإلى غير ذلك من

(48) https://www.slideshare.net/slideshow/responsabilit-civile-du-fait-des-objets-connectes-autonomes/234291821.

(ISSN: 2537- 0758)

الاستخداماتِ التي لا حصرَ لها[٤٩]، وفي هذا الشَّأنِ نشيرُ إلى جانبٍ من استخداماتِ الأشياءِ المُتَّصلةِ في حياتنا اليوميَّةِ البسيطة:

١ – أدواتُ المائدةِ المُتَّصلة:

تمَّ تصميمُ Smartplate ليكونَ بمثابةِ "خبير تغذيةٍ شخصيّ". وهو مزوَّدٌ بأجهزةِ استشعارٍ تصويريَّةٍ وحسيَّةٍ، ويتفاعل مع قاعدةِ بياناتٍ غذائيَّةٍ من أجلِ تقديم عدَّة خدماتٍ للمستهلك عبر تطبيقٍ على الهاتفِ الذكيّ، حيث يقومُ بوزنِ كميَّةِ كلِّ طعام على الطَّبق، وتقدير السُّعراتِ الحراريَّةِ التي يحتوي عليها والقيم الغذائيَّة، كما ويُمكنه أيضًا تحليلُ السُّرعةِ التي يأكلُ بها المستهلك.

ومن هذه التطوُّراتِ التِّكنولوجيَّةِ نذكرُ على سبيلِ المثالِ أيضًا: ظهور الحوسبةِ السحابيَّة– الحوسبة السحابيَّة: لم يَعُد نقلُ البياناتِ وتخزينُها ومُعالجتُها يعتمدُ على البنى التحتيَّةِ الماديَّةِ الخاصَّة، بل لها القدرةُ على تحليلِ وحسابِ كميَّاتٍ كبيرةٍ من البيانات.

٢ – السَّاعةُ المُتَّصلةُ:

الكائنُ المتَّصلُ الأكثر عصريَّةً حاليًّا هي السَّاعة، فهو يسمحُ بتخصيصِ عرضِ الوقت، وقياس النَّشاطِ البدنيّ لمُستخدمها، وقراءة الرَّسائلِ النصيَّةِ القصيرةِ ورسائل البريد الإلكترونيّ، والرد عليها، وإدارة جهاتِ الاتِّصالِ الخاصَّة بمُستخدمها، والتحقُّق من الطَّقس، وضبط التَّنبيهات، وغير ذلك الكثير، حيث يُمكن العثورُ على جميع مزيَّاتِ الهاتفِ الخلويّ تقريبًا في السَّاعة. وبما أنَّ هذه السَّاعةَ تكون عادةً متَّصلةً بهاتفنا الذكيّ، تتمُّ مزامنةُ كلِّ شيءٍ، بحيث يُصبح الوصولُ إلى المعلوماتِ الرئيسة على الهاتفِ أكثر سهولةً.

٣ – النَّظاراتُ المُتَّصلة:

تتمتَّعُ النَّظاراتُ المُتَّصلة بنفس إمكانيَّاتِ السَّاعاتِ المُتَّصلة تقريبًا، مع تفاعُلٍ أقلَّ ولكنْ يتمُّ تعويضُها عن طريقِ التعرُّف على الصَّوت. ومع ذلك، فإن لديها وظائفَ

---

[٤٩] د. بشار طلال المومني، د. معمر طرية، التَّحدياتُ القانونيَّةُ المعاصرةُ لاستخداماتِ "إنترنت الأشياء"، مرجع سابق، ص٢٨٧.

مختلفةً: الكاميرا التي تلتقطُ صورةً لما نراه (نظرًا لأنَّ الكاميرا على مستوى العين) والواقع المعزَّز؛ أي إنَّ لديهم إمكانيَّةَ إضافةِ نماذج ثلاثيَّةِ الأبعادِ إلى العالم الحقيقيّ من خلالِ شاشةِ النَّظارات.

٤- السَّيارةُ المُتَّصلة:

تُعدُّ السَّيارةُ من الأشياءِ التي جذبتْ أكبرَ قدرٍ من الاهتمام من الشَّركاتِ المصنِّعةِ للمُعدَّات. ومن المؤكَّدِ أنَّ الأجهزةَ الإلكترونيَّةَ والحوسبة الموجودة على متنِ السَّيارةِ ليست أشياءَ جديدةً، ولكنَّ حركةَ تجهيزِ السَّياراتِ الذكيَّة بأجهزةِ الاستشعارِ والكاميرات تسارعتْ في السَّنواتِ الأخيرة. وبالتالي، تحوَّلت السَّيارةُ من كونِها جسمًا ميكانيكيًّا ومنفصلًا تمامًا إلى أداةٍ ذكية بشكلٍ خاصّ.

ويعدُّ إنتاجُ البياناتِ أمرًا ضروريًّا لنجاح السيارةِ المُتَّصلة، وأبسط البياناتِ تجعلُ من الممكنِ حساب سرعةِ السَّيارةِ وتنظيمها بناءً على الأوامرِ التي يُصدرها السَّائق. وبطريقةٍ أكثر تطوُّرًا، وسيسمح تحليلُ البياناتِ إلى التحوُّلِ من بيئةِ القيادةِ إلى التلقائيَّةِ في القيادة (إشارات صوتيَّة أو فرامل أو حتى قيادة أوتوماتيكيَّة)، وتسمح أحدثُ التطوُّراتِ لبعضِ السياراتِ بقيادةِ نفسِها بشكلٍ مستقلٍّ تمامًا، سواءٌ في أثناءِ التحرُّكِ عبر الاختناقاتِ المروريَّةِ أو في المناطقِ الحرَّة تمامًا. كما أن برنامجَ القيادةِ الأكثر تقدُّمًا يسمحُ بالاتِّصالِ بشكلٍ مستقلٍّ بقيادةِ أسطولٍ من المَركباتِ التي تتبعُ بعضها البعض أو في بيئةٍ حضريَّةٍ، لتجاوُزِ السَّياراتِ الأخرى، سواءٌ أكانت متَّصلةً أم لا.

وفي الحقيقةِ فإنَّ البياناتِ التي تُنتجها السياراتُ المُتَّصلةُ لها استخدام، بالنِّسبةِ لشركاتِ التَّأمين، التي تعتمدُ بشكلٍ كبيرٍ على المعلوماتِ التي تحتفظُ بها حولَ سلوكِ القيادةِ لحاملي وثائق التأمين. وفي هذا الشَّأن يُمكن القولُ بأنَّ هناك موجةً جديدةً من الأشياءِ المُتَّصلةِ التي تدفعُ أفقَ الاحتمالاتِ Une nouvelle vague d'objets connectés qui repousse l'horizon des possibles

ورغم الاستخداماتِ النَّافعةِ للأشياءِ المُتَّصلةِ في حياتنا، حيث أصبحت ضروريَّةً، لا يُمكن للأفرادِ الاستغناءُ عنها، فإنَّ واقعَ الممارساتِ العمليَّة لاستخدامِ الكائناتِ

(ISSN: 2537- 0758)

المُتَّصلة يشيرُ إلى أنَّ هذه الأشياءَ قد تُحدث أضرارًا لا يُمكن توقُّعُها من الشَّركاتِ المصنِّعة، أو المبرمج، ولهذا تحتاجُ هذه التِّقنيَّةُ الحديثةُ إلى مزيدٍ من الضَّوابطِ والتَّنظيم الفعَّالِ بطريقةٍ منسقةٍ ومتماسكةٍ وآمنةٍ ومضمونةٍ.

الفرع الثالث
أنواعُ الأشياءِ المُتَّصلة وخصائصُها

تقسيمٌ:

الشَّيءُ المتَّصلُ هو شيءٌ لديه القدرةُ على تبادُلِ البياناتِ مع كياناتٍ ماديَّةٍ أو رقميَّةٍ أخرى، في أغلبِ الأحيانِ عبْر الإنترنت.

أولًا: **الأنواعُ المختلفةُ للأشياءِ المُتَّصلة**:

يُمكننا مقارنةُ شيءٍ متَّصلٍ بنظام كمبيوتر مدمج لديه القدرةُ على الاتِّصال. وفي الحقيقةِ هناك ثلاثُ فئاتٍ من الأشياءِ المُتَّصلة: الشَّيء المتَّصل البسيط l'objet connecté simple، والشَّيء المتَّصل الذكي L'objet connecté intelligent، والشَّيء المتَّصل المستقلُّ L'objet connecté autonome.

١ – الشَّيءُ المتَّصلُ البسيط:

l'objet connecté simple:

تتلقَّى الأشياءُ "المُتَّصلة ببساطة" عددًا معيَّنًا من العناصرِ أو المعلوماتِ، وهي معلوماتٌ أوليَّة، ولكنَّها تظلُّ سلبيَّةً نسبيًّا، وتعتمدُ القيمةُ المضافةُ لهذا النَّوع من الأشياءِ فقط على قُدرتِها على الاتِّصال. ومن الأمثلةِ على هذه الأشياء: كاشفُ دخانٍ متَّصل يُرسل إشارةً إلى هاتفِ صاحبِ المنزلِ في حالةِ نشوبِ حريقٍ، وكذلك مقياسٌ متَّصلٌ ينقل البياناتِ المسجلةَ إلى قاعدةِ بياناتٍ يُمكن الوصولُ إليها عن طريقِ الكمبيوتر أو الهاتف الذكيّ[٥٠]. وما يُميِّز هذه التِّكنولوجيا أنَّها لا تتمتَّعُ بذكاءٍ كبيرٍ، بل إنَّ دورَها ينحصرُ في وظيفةِ المراقبةِ.

(50) Les objets connectés, https://www.maxicours.com/se/cours/les-objets-connectes/.

٢- الشَّيءُ المتَّصلُ الذكيُّ

L'objet connecté intelligent

الكائنُ الذكيُّ المتَّصلُ ليس متَّصلًا فحسْب، بل سيتمُّ تجهيزُه أيضًا ببرمجياتٍ قادرةٍ على إنتاج معلوماتٍ مطوَّرة، وليس فقط بياناتٍ أوليَّةً. وتشهدُ قدراتُ الشَّيء، خلال هذه المرحلةِ، تحسيناتٍ معتبرةً.

وممَّا لا شكَّ فيه أنَّ إنتاجَ المعلوماتِ المطوَّرة هو تعريفٌ محددٌ للذَّكاء، والذي يُشير إلى مفهوم الذَّكاءِ الاصطناعيّ. وهذا ليس ذكاءً بالمعنى الشَّامل، بل هو قدرةُ الشَّيءِ المتَّصلِ على أداءِ مهامَّ محدَّدةٍ معينةٍ، مثل: تحليلِ البياناتِ أو مُعالجتها. ويتميَّزُ هذا النَّوعُ من الذَّكاءِ Smart، وهو ما أعطى هواتفنا الذكيَّةَ اسمها. ومثال على ذلك، ميزانٌ متَّصلٌ قادرٌ على تحليلِ اختلافاتِ الوزن، ويُمكنه حسابُ مؤشِّرِ كتلة الجسم(٥١). وترتفع قدراتُ الشَّيء، بحيث يكونُ في استطاعتهِ الاستجابةُ والتحكُّم في التَّجربةِ الشَّخصيَّةِ للمستهلك، فضلًا عن التَّفاعلِ بطريقةٍ أذكى.

ومن بين الأشياءِ المُتَّصلةِ الذكيَّة، أنظمةُ الذَّكاءِ الاصطناعيّ للأغراضِ العامَّة (Artificial General Intelligence- AGI) وهو نوعٌ من الذَّكاءِ الاصطناعيّ يهدفُ إلى محاكاةِ الذَّكاءِ البشريّ العامّ، حيث يتمكَّن النِّظامُ من أداءِ أيّ مهمةٍ معرفيَّةٍ يُمكن أن يؤدّيَها الإنسان. كما يُشير إلى الذَّكاءِ الاصطناعيّ للأغراضِ العامَّةِ بأنه المهام متعددة الاستخدامات أو الذَّكاء الاصطناعي للأغراضِ العامَّةِ التجاريَّةِ أو الصناعيَّة مثل (GPT أو Google DeepMind) أو نماذج اللُّغة الأخرى....إلخ.

والجدير بالذِّكر أن الاتِّحادَ الأوروبيَّ يُحدِّد في اللَّائحةِ رقم ١٦٨٩ لسنة ٢٠٢٤ التزاماتٍ على عاتقِ مُقدِّمي نماذج الذَّكاءِ الاصطناعيّ للأغراضِ العامَّة، والتي منها إعدادُ وتحديثُ الوثائق الفنيَّةِ لهذه الأنظمة، بما في ذلك عمليَّةُ التَّدريبِ والاختبارِ ونتائج تقييمه(٥٢).

---

(51) Les objets connectés, https://www.maxicours.com/se/cours/les-objets-connectes/.

(52) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial

(ISSN: 2537- 0758)

٣- الشَّيءُ المتَّصلُ المستقلُّ:

L'objet connecté autonome:

يتضمَّنُ هذا النَّوعُ من الأشياءِ المُتَّصلةِ على جميع خصائصِ الشَّيء الذَّكيّ. ويُمكنه أيضًا أداء مهامَّ أكثر تقدُّمًا، مثل تحليلِ بيئتهِ، كما أنه مزوَّدٌ بخاصيَّةِ التعلُّم والتَّحسين الذاتيّ، وبناءً على هذا التَّحليل، يتَّخذ الشَّيء نفسه عددًا معيَّنًا من القراراتِ والأفعال، وبحسب التَّحليلِ السَّابقِ يُصبح الشَّيءُ مستقلًّا.

ويتمُّ تقديرُ القيمةِ المضافةِ للشَّيء المتَّصل المستقلِّ بدرجةِ التدخُّل المباشرِ من قبلِ الإنسان. فكلَّما قلَّ التدخُّلُ بالضَّرورةِ زادت قيمتُه المضافة، كي يعملَ باستقلاليَّةٍ. ومثال على ذلك، السَّيارةُ ذاتيَّة القيادة، حيث يتمُّ ضمانُ القيادةِ بواسطةِ برامج الذَّكاء الاصطناعيّ.

وفي الواقع تُسهم البياناتُ التي تمَّ إنشاؤها بواسطةِ هذه الأشياءِ المُتَّصلةِ في البيانات الضَّخمة، حيث يتلقَّى نظامُ الكمبيوتر المدمج المعلوماتِ من العالم الحقيقيّ من خلالِ أجهزةِ الاستشعارِ. فهو يحفظُ هذه المعلوماتِ ويُعالجها بواسطةِ المعالج الدَّقيق، ثم يرسلُ المعلوماتِ مرَّةً أخرى إلى العالم الحقيقيّ عبر المحرّكات. وتُشير البياناتُ الضَّخمةُ إلى مجموعةٍ ضخمةٍ جدًّا من البياناتِ التي لا يُمكن لأيّ أداةٍ تقليديَّةٍ التعَّاملُ معها حقًّا.

وتجدرُ الإشارةُ إلى أنَّه تكمُنُ القيمةُ المضافةُ للأشياءِ المُتَّصلةِ في قدرتِها على التَّواصل، حيث يتمُّ استخدامُ وسائلِ الاتِّصالِ اللاسلكيَّة، وهناك ثلاثةُ أنواع رئيسةٍ للشَّبكات، نُشير إليها فيما يلي:

- **شبكات LAN:**

شبكاتُ LAN (الشَّبكة المحليَّة): هي شبكاتٌ قصيرةٌ إلى متوسِّطةِ المدى (بين ١ متر و١٠٠ متر). وأشهرُها هي تقنيَّةُ البلوتوث والواي فاي wifi، والتي تسمحُ باتِّصالاتٍ عاليةِ السُّرعة، ولكنَّها تستهلكُ الكثيرَ من الطَّاقة. وبالتَّالي فإنَّ شبكة

intelligence Article 53, Obligations for providers of general-purpose AI models.

Wifi مناسبةٌ فقط للأجهزةِ المُتَّصلةِ بالتيَّارِ الكهربائيّ أو التي يُمكن أن يكونَ مصدرُ الطاقةِ الخاص بها سهلًا ومتكرّرًا، وهناك صورٌ أخرى غير Bluetooth وwifi، مثل NFC أو RFID.

- **الشَّبكات الخلويَّة (Les réseaux cellulaires):**

الشَّبكاتُ الخلويَّةُ هي شبكاتٌ طويلةُ المدى (تصل إلى ٣٠ كم). وهي تعتمدُ على تقنيَّة GSM مثل 4G على سبيل المثال، وتسمحُ بنقلِ كميَّةٍ كبيرةٍ من البياناتِ (الصُّور ومقاطع الفيديو وما إلى ذلك) بسرعةٍ عاليةٍ جدًّا، وهي تتطلَّبُ تركيبَ بطاقةِ SIM في الجهازِ المُرادِ توصيله، من أجلِ التعرُّفِ عليه على شبكةِ الاتِّصال.

- **شبكات LPWAN:**

هو نوعٌ من الشَّبكاتِ اللاسلكيَّة المصمَّمة لتوفيرِ اتِّصالاتٍ منخفضةِ الطَّاقةِ عبر مسافاتٍ طويلةٍ، وتُستخدمُ بشكلٍ رئيسٍ في تطبيقاتِ إنترنتّ الأشياء (IoT)، حيث تكونُ الحاجةُ إلى نقلِ البياناتِ صغيرةً، ولكن المسافةَ المطلوبةَ طويلة، وفي الواقع شبكات LPWAN (شبكة واسعة النِّطاق مُنخفضة الطَّاقة) هي شبكاتٌ طويلةُ المدى (تصلُ إلى عدَّةِ كيلومترات) واستهلاكٌ منخفضٌ للطَّاقة، مثل شبكاتِ Sigfox وLoRa، ولقد تمَّ تصميمُ هذه الشبكاتِ خِصِّيصًا لنقلِ بياناتِ إنترنت الأشياء بتكلفةٍ منخفضةٍ.

ثانيا: خصائصُ الأشياءِ المُتَّصلة:

يُرسل الشَّيءُ المتَّصلُ البياناتِ المجمَّعةَ إلى البنى التحتيَّةِ المخصَّصة بفضلِ اتِّصاله، ويتمُّ تخزينُ البياناتِ وتحليلها عبرَ خوارزمياتِ الحساب، ومن ثمَّ إعادتُها إلى المستخدم في شكلِ معلوماتٍ قابلةٍ للاستخدام. ويتميَّز الشَّيءُ المتَّصلُ بثلاثِ خصائصَ أساسيَّة: قدرتُه على جمع البياناتِ من خلالِ أجهزةِ الاستشعار: الموقع، المسافة، درجة الحرارة، الاهتزاز. وكذلك قدرتُه على نقلِ ومعالجةِ المعلوماتِ، واتِّخاذ الإجراءاتِ إذا لزمَ الأمر، فضلًا عن قدرتهِ على التَّفاعلِ مع الأشياءِ الأخرى في بيئاتٍ مختلفةٍ.

(ISSN: 2537- 0758)

وتتميَّزُ الأشياءُ المُتَّصلةُ من الجيلِ الجديدِ بعدَّة خصائصَ:

أ- **التفاعليَّة،** بشكلٍ تقريبيّ، تكون متَّصلةً عندما تسمحُ بتبادلِ المعلوماتِ بين مستشعرِ واحدٍ على الأقلِّ ومحطَّة كمبيوتر، بشكلٍ ثنائيّ الاتِّجاه أو في ردودِ الفعل. ولكنْ في أشكالها الأكثر تقدُّمًا، أصبحت الكائناتُ المُتَّصلةُ الآن متصلةً بالبنيةِ الأساسيَّةِ العالميَّةِ بالكامل من خلال شبكةِ الإنترنت، الأمرُ الذي يزيدُ من إمكاناتها الخدميَّة. كما تميلُ هذه الكائناتِ إلى الارتباطِ بالمنصَّاتِ التي تسمحُ أيضًا بتعدُّدِ اتِّجاهاتِ التَّبادلات(٥٣).

ب- تحويلُ الأشياءِ الماديَّةِ التقليديَّة إلى أشياءَ ذكيَّةٍ، ويُمكن أن يشملَ ذلك ربط الطُّرق، والمعدَّات الصناعيَّة، والمُعدَّات الرياضيَّة، والأشياء اليوميَّة والمباني....إلخ.

ج- إنتاج البيانات، بدءًا من جمع المعلوماتِ البسيطةِ إلى التَّفاعلِ المستقلِّ للكائنِ وتحليل البياناتِ الضَّخمةِ عن طريقِ التعلُّم العميق.

د- فتح المجالِ أمام الكائنِ المتَّصلِ لاتِّخاذ القرار، والذي يتجاوزُ في بعضِ الأحيانِ القدراتِ البشريَّةَ(٥٤).

وبناءً على ما تقدَّمَ يُمكننا القولُ بأنَّ الشَّيءَ المتَّصلَ يتميَّزُ بثلاثِ خصائصَ أساسيَّةٍ، وهي:

أولًا: قدرتُهُ على جمعِ البياناتِ من خلالِ أجهزةِ الاستشعار.

ثانيًا: القدرةُ على نقلِ ومعالجةِ المعلومات واتِّخاذ الإجراءاتِ إذا لزمَ الأمرُ.

ثالثًا: القدرةُ على التَّواصلِ مع الكائناتِ الأخرى في بيئاتٍ مختلفةٍ.

---

(53) https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431

(54) https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431

وتجدرُ الإشارةُ إلى أنَّ مزايا الأشياءِ المُتَّصلةِ عديدةٌ، حيث تسمحُ للمُستخدمين بمراقبةِ أجهزتِهم والتحكُّم فيها عن بُعدٍ، وبالتَّالي أتمتةُ مهامَّ معيَّنةٍ وتوفير الطَّاقة. بالإضافةِ إلى ذلك، يُمكن للكائناتِ المُتَّصلةِ تحسين الأمانِ والرَّاحةِ وجمع البياناتِ لتحليلها لاحقًا(٥٥).

فعلى سبيلِ المثالِ، يُمكن للشَّركاتِ استخدامُ الأشياءِ المُتَّصلةِ لمراقبةِ أنشطتها عن بُعدٍ، وتحسين كفاءتها، كما يُمكن للأفرادِ أيضًا استخدامُ هذه التقنيَّةِ لمراقبةِ منازلِهم أو تتبُّع صحَّتِهم في الوقتِ الفعليّ، حيث يُمكن استخدامُ الأجهزةِ القابلة للارتداء(٥٦)؛ لتحسين الأمانِ من خلالِ توفيرِ مراقبةٍ مستمرَّةٍ، وتنبيه المالكين عند ظهورِ مشكلةٍ. فعلى سبيلِ المثال، يُمكن تكوينُ بعضِ أنظمةِ التَّشغيلِ الآليّ للمنزلِ لإرسالِ إشعاراتٍ عند فتح أو إغلاقِ الأبوابِ أو النَّوافذ.

وممَّا لا شكَّ فيه يُمكن للأشياءِ المُتَّصلةِ أن تجعلَ الحياةَ اليوميَّةَ أسهلَ من خلالِ أتمتةِ بعض المهامّ الشاقَّةِ، مثل: تشغيلِ وإطفاءِ الأضواءِ أو التحكُّم في التَّدفئة. ويُمكن أيضًا برمجةُ هذه الأجهزةِ لأداءِ مهامَّ محدَّدةٍ على فتراتٍ منتظمةٍ.

كما يُمكن أن تساعدَ الأجهزةُ القابلةُ للارتداءِ أيضًا في إدارةِ الصِّحةِ والمنزل من خلالِ جمع البياناتِ حول العاداتِ اليوميَّةِ، وتقديم رؤًى مفيدةٍ حول الاتِّجاهاتِ طويلةِ المدى. فعلى سبيل المثال، يُمكن للسِّوار الذكيّ قياسُ معدَّلِ ضرباتِ القلبِ وعدد الخطواتِ التي يتمُّ اتِّخاذُها يوميًّا، بينما يُمكن لنظامِ التَّشغيلِ الآليّ للمنزلِ مراقبة استهلاكِ الطَّاقةِ، وضبط الإعداداتِ تلقائيًّا لتقليلِ الفاتورة.

---

(55) Objets connectés: Définition, bénéfices et astuces pour optimiser leur usage, 1 mai 2023, https://maisonetfinance.fr/smart-home/objets-connectes-definition-avantages-conseils-utiliser/.

(٥٦) الأجهزةُ القابلةُ للارتداء (Wearable Devices) هي أجهزةٌ تكنولوجيَّةٌ صغيرةٌ يُمكن ارتداؤُها على الجسمِ، وغالبًا ما تتَّصلُ بالهواتفِ الذكيَّةِ أو الشَّبكات الأخرى لتوفيرِ وظائفَ متعدِّدةٍ. تتميَّزُ هذه الأجهزةُ بأنها مريحةٌ، وعادةً ما تحتوي على مستشعراتٍ لجمع البياناتِ وتحليلها.

(ISSN: 2537- 0758)

المطلب الثاني
مخاطرُ الأشياءِ المُتَّصلة

تمهيدٌ وتقسيمٌ:

يعدُّ عالمُ الأشياءِ المُتَّصلةِ عالمًا لا يُمكن التنبُّؤ به، حيث إنَّ الاحتمالاتِ لا حصرَ لها، لا سيَّما في ظلِّ ارتباطها الوثيقِ بشبكةِ الإنترنت، حيث يوجدُ عددٌ كبيرٌ من أجهزةِ الاستشعارِ وأجهزة الكشفِ والأجهزة المُتَّصلةِ تعملُ معها على توفُّرِ التحكُّم عن بُعدٍ للمستخدمين، فضلًا عن الوظائفِ الآليَّةِ الأخرى وغيرها من الخدماتِ العمليَّة. ولكنْ على الرَّغم من أنَّ الفوائدَ عديدةٌ، فإنَّ هناك أيضًا بعض المخاطرِ التي يجبُ أخذُها في الاعتبار.

وممَّا لا شكَّ فيه أن حجمَ المعلوماتِ السريَّة، والشَّخصيَّة والعاديَّة الضَّخمَ، عبْرَ الإنترنتّ يُبرزُ مشكلةً حقيقيَّةً بشأنِ كيفيَّةِ الحمايةِ الفنيَّةِ للمعلومات، والمتمثِّلة في عدم قدرةِ برامج التَّأمين على تحقيقِ الحمايةِ الكافيةِ للحفاظِ على المعلوماتِ والأسرار؛ الأمرُ الذي يُهدِّد مستخدمي الأشياءِ المُتَّصلةِ بإفشاءِ أسرارِهم والإفصاح عنها، إضافةً إلى الاستخداماتِ الأخرى غير المشروعةِ التي تُلحقُ ضررًا بالأشخاص، فضلًا عن الأضرارِ الأخرى النَّاجمةِ عن استخدام الكائناتِ المُتَّصلةِ لا سيَّما الذكيَّةُ أو المستقلةُ منها.

وإذا كانت الأشياءُ المُتَّصلةُ نقطةَ تحوُّلٍ رئيسة في علاقتنا بمفهومنا للحياةِ اليوميَّة، إلا أنه سينتجُ عن استخدام هذه الأشياءِ مخاطرُ تكنولوجيَّةٌ تتعلَّق بالمعلوماتِ العامَّة، ومخاطر أخرى خاصَّة ترجعُ إلى طبيعةِ الشَّيءِ المتَّصلِ ذاته[٥٧].

الفرع الأول: مخاطرُ تكنولوجيا المعلوماتِ العامَّة والأشياء المُتَّصلة.

الفرع الثاني: المخاطرُ الخاصَّةُ النَّاجمةُ عن الأشياءِ المُتَّصلة.

---

(57) Les objets connectés: risques généraux et risques particuliers, op. cit https://www.apssis.com/tribune-ssi/88/les-objets-connectes-risques-generaux-et-risques-particuliers.htm.

الفرع الأول
مخاطرُ تكنولوجيا المعلومات العامَّة والأشياء المُتَّصلة

تُواجه الأشياءُ المُتَّصلةُ مخاطرَ الثَّغراتِ الأمنيَّةِ التقليديَّة، كما تُواجه صعوباتٍ في التَّكوين والتَّحديث.

أولًا: **ثغراتُ ضَعف الكمبيوتر**:

كما هو الحالُ في أيّ نظام كمبيوتر، تحتوي الأشياءُ المُتَّصلةُ على برنامج ثابتٍ يسمحُ لها بالعمل، وقد تحتوي هذه البرامجُ الثابتةُ على أخطاءٍ برمجيَّةٍ أو أبوابٍ خلفيَّةٍ تُؤدِّي إلى ثغراتٍ أمنيَّةٍ، والتي تُمكِّن المهاجمَ باستغلالِ الشَّيء مثل أيّ جهازِ كمبيوتر آخر، حيث كانت الغالبيَّةُ العظمى من كلماتِ المرورِ سهلَ الوصولِ إليها، وكانت الهواتفُ الذكيَّةُ والأجهزة اللوحيَّة الأخرى غير مجهَّزةٍ بمضادَّاتِ الفيروسات، ويتفاقمُ هذا الخطرُ بالنِّسبةِ للأشياءِ المُتَّصلة بسببِ عدم مراعاةِ الجانبِ الأمنيّ عند تصميم الجهاز، فلم يكُنْ لمصمِّم الشَّيءِ المتَّصل أن يتخيَّلَ سوءَ الاستخدام الذي يُمكن أن يحدث لهذا الشَّيء. وعلاوةً على ذلك، فإنَّ أخذَ هذه المخاطرةِ في الاعتبارِ من شأنهِ أن يزيدَ من تكلفةِ إنتاج البرامج الثابتة، وبالتالي زيادة ثمنِ الشَّيءِ نفسهِ[٥٨].

ثانيًا: **صعوباتُ التَّكوينِ والتَّحديث**:

للوصولِ إلى عددٍ كبيرٍ من الجمهور، يجبُ أن تكونَ الأشياءُ المُتَّصلةُ سهلةَ الاستخدام والتَّثبيت، إلا أنَّ مسألةَ تحديثِ البرنامج الثابت وتكوين الشَّيءِ يُواجه صعوباتٍ كثيرةً. فمسألة التَّشفيرِ تتطلَّبُ عمومًا تدخُّلًا يدويًّا، وهو أمرٌ قد يكونُ معقَّدًا. وبالإضافةِ إلى هذه المخاطرِ العامَّة، هناك مخاطرُ خاصَّةٌ يُنظر إليها بحسَبِ الطَّبيعةِ الخاصَّة لهذه الأشياء.

---

(58) Les objets connectés: risques généraux et risques particuliers, https://www.apssis.com/tribune-ssi/88/les-objets-connectes-risques-generaux-et-risques-particuliers.htm

(ISSN: 2537- 0758)

الفرع الثاني
المخاطرُ الخاصَّةُ النَّاجمةُ عن الأشياءِ المُتَّصلة

اعتمادًا على الظُّروفِ المتعلّقةِ بتطبيقِ الأشياءِ المُتَّصلةِ واستخداماتها، ومستوى التطوُّرِ التِّكنولوجيّ، قد يُولِّد الذَّكاءُ الاصطناعيُّ مخاطرَ، ويُسبِّب ضررًا للمصالح العامَّةِ والحقوق الأساسيَّة. وقد يكون هذا الضَّررُ مادِّيًّا أو غير مادِّيّ، بما في ذلك الضَّررُ البدنيُّ أو النفسيُّ أو المجتمعيُّ أو الاقتصاديُّ. وهذا ما أشارتْ إليه لائحةُ الاتِّحادِ الأوروبيّ ١٦٨٩/٢٠٢٤ في مادَّتها الخامسة(٥٩).

وترتبطُ المخاطرُ الخاصَّةُ بالأشياءِ المُتَّصلةِ نتيجةَ إساءةِ استخدامِها، وكذلك نقصُ عناوين IP، فضلًا عن إساءةِ استخدام الغرضِ، وإلى غير ذلك من المَخاطرِ.

أولًا: إساءةُ استخداماتِ الأشياءِ المُتَّصلة:

الشَّيءُ المتَّصلُ له استخدامٌ معيَّنٌ، ورغم ذلك من المُمكنِ يُمكن مهاجمتُه، إما بسببِ الاهتمامِ بالمعلوماتِ الموجودةِ على متنهِ أو للاستيلاءِ عليه. فلنأخذْ على سبيلِ المثالِ مقياسَ الحرارة، فهو يتضمَّن إعطاءَ درجةِ الحرارةِ عند نقطةٍ معيَّنةٍ، ويبدو أنَّ المعلوماتِ ليست ذاتَ أهميَّةٍ كبيرةٍ بداهةً، ولكنْ إذا كانت متَّصلةً بالمصراع الدَّوارِ الآليّ(٦٠) الذي يفتحُ عند الوصولِ إلى درجةِ الحرارةِ في الغرفة، فقد يجذُها اللِّصُّ مثيرةً للاهتمام.

---

(59) At the same time, depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm.

(٦٠) المصراعُ الدَّوارُ الآليُّ هو نوعٌ من أنظمةِ الأبوابِ المستخدمةِ في المباني، والتي تعتمدُ على تصميمِ دوارٍ يسمح بفتحِ وإغلاقِ الأبوابِ بشكلٍ تلقائيٍّ. وهذا النَّوعُ من المصاريع عادةً ما يستخدمُ في الأماكنِ ذات الحركةِ العاليةِ مثل المراكزِ التِّجاريَّة، المطارات، والفنادق.

ولقد زادت بالفعلِ المخاطرُ المتعلِّقةُ بأمن نظمِ المعلوماتِ في السَّنواتِ الأخيرة، ونخشى أن يؤدِّيَ تطوُّرُ إنترنتّ الأشياءِ إلى زيادةِ هذه المخاطر.

ثانياً: الافتقارُ إلى الحمايةِ بحسَبِ التَّصميم:

لا تُعدُّ حلولُ تأمين الأشياءِ المُتَّصلةِ من أولويَّاتِ الشَّركاتِ المصنَّعة، ولم يتمَّ تحديدُ موضوع الطَّلب بشكلٍ واضح بعد؛ نظرًا لعدم تضمينِ تدابيرِ الأمانِ من المراحلِ الأُولى لتطويرِ الأنظمةِ أو التَّطبيقات. وللحقيقةِ، إنَّ الافتقارَ إلى الأمانِ للكائناتِ المُتَّصلةِ لا ينجمُ بالضَّرورةِ عن الافتقارِ إلى الحيطة، بل التوسُّع في جعلِ الشَّيءِ المتَّصلِ لا سيَّما المزوَّدُ بخاصيَّةِ التعلُّمِ والتَّحسينِ الذاتيّ يقوم بأداءِ مهامَّ أكثر تقدُّمًا يُضعف الحمايةَ القانونيَّةَ المقرَّرة.

ثالثاً: ضَعفُ الأنظمةِ المترابطة:

la vulnérabilité des systèmes interconnectés

مع زيادة عددِ الأجهزةِ المُتَّصلة، يُصبحُ النِّظامُ أكثرَ تعقيدًا؛ ممَّا يزيدُ من احتماليَّةِ حدوثِ أخطاء أو فشلٍ في التَّواصلِ بين الأجهزة. ومن المُحتملِ أن يتيحَ اختراقُ كائنٍ ضعيفٍ إمكانيَّةَ الوصولِ إلى جميع الكائناتِ المرتبطة به.

كما أنَّه إذا تعطَّلت إحدى الشَّبكاتِ أو الأجهزة، يُمكن أن يؤثِّر ذلك على أداءِ النِّظام بالكامل؛ ممَّا يُؤدِّي إلى توقُّفِ الخدمات، إضافةً إلى أنه قد تُواجه الأنظمةُ صعوباتٍ في التوسُّع عند إضافةِ أجهزةٍ جديدةٍ؛ ممَّا يُؤثِّر على الأداءِ والكفاءةِ. وتعدُّ هذه الأمورُ تحدياتٍ كبيرةً تتطلَّب حلولًا مبتكرةً لتعزيزِ الأمانِ والكفاءةِ والموثوقيَّة.

رابعاً: زيادةُ مخاطرِ الهجماتِ على خصوصيَّةِ المُستخدم:

إذا كان من السَّهلِ أن تتعرَّضَ الأشياءُ المُتَّصلةُ اليوميَّة للتطفُّلاتِ الضارَّة، فإن كميَّةَ المعلوماتِ الشَّخصيَّة التي يُمكن جمعُها عن بعدٍ تزيدُ بشكلٍ كبيرٍ (تحديد الموقع الجغرافيّ، والبيانات الصِّحية، وتدفُّقات الفيديو والصَّوت). وممَّا لا شكَّ فيه أن جمعَ البياناتِ من الأجهزة يُمكن أن يؤدِّيَ إلى انتهاكاتٍ للخصوصيَّة، خاصَّةً إذا لم تكُنْ هناك ضوابطُ صارمةٌ على كيفيَّةِ استخدامِ هذه البيانات.

(ISSN: 2537- 0758)

ولهذا يجبُ تقييمُ المخاطرِ المرتبطةِ باستخدام الأشياءِ المُتَّصلة، فمن المُمكنِ أن تكونَ البياناتُ التي يتمُّ جمعُها بواسطةِ هذه الأجهزةِ عرضةً للقراصنةِ والشَّركاتِ الخبيثة؛ ولذا يتحتَّمُ فهمُ المخاطرِ، مع ضرورةِ اتِّخاذِ الخطواتِ اللَّازمةِ لحمايةِ البيانات.

وممَّا لا شكَّ فيه أنَّ الانغماسَ في تدفُّقاتِ البيانات(٦١)، والتَّغذية الرَّاجعة الآليَّة(٦٢) التي تُمارسُ بشكلٍ مستمرّ على أجسادِ الأفرادِ يزيدُ من حدَّة المواجهةِ المنهجيَّةِ للأخير مع آثارِ نشاطهم(٦٣)، والتي تلعبُ دورًا حاسمًا في الاهتمام والهويَّةِ والعلاقاتِ الانعكاسيَّة مع الذَّات. ولقد ذهب جانبٌ من الفقهِ إلى القول: إنَّ دمجَ التِّكنولوجيا في الجسم ليس مجرَّد زيادةٍ بسيطةٍ، ولكنَّه تجربةٌ جديدةٌ تشوِّش الهويَّةَ والجنسَ والفعل، والتي لا يكونُ الوعي كافيًا دائمًا لاحتوائها(٦٤).

وعلى الرَّغم من أنَّ عددًا معيَّنًا من الدِّراساتِ البحثيَّةِ للمُستخدمين قد أظهرتْ بوضوح أن الأشياءَ المُتَّصلةَ يُمكن اعتبارُها مفيدةً، عندما يتمُّ وضعُها في سياقاتٍ محدَّدةٍ جدًّا لرصدِ الأمراضِ المزمنةِ على سبيل المثال(٦٥)، إلا أنَّ بحوثًا أخرى قد أبرزت أنَّ الأشياءَ المُتَّصلةَ يُمكن أن تحملَ أيضًا مخاطر، لا سيَّما أنَّها تشكِّلُ طرقًا للتدخُّلِ على جسم الإنسان، فضلًا عن إحداثِ تأثيراتٍ متعدِّدةٍ على السُّلوك البشريّ(٦٦).

---

(61) Sadin, E.. ***L'humanité augmentée. L'administration numérique du monde***. Montreuil, France: L'Échappée. (2013).

(62) Arruabarrena, B.. ***Le Soi augmenté: les pratiques numériques de quantification de soi comme dispositif de médiation pour l'action*** (Thèse de doctorat). CNAM, Paris. (2016).

(63) Licoppe, C. Formes de la présence et circulations de l'expérience. ***Réseaux***, 6, 2014) 21-55.

(64) Andrieu, B. **Les avatars du corps. Une hybridation somatechnique.** Montréal, Canada: Editions Liber Canada. **(2011) P.1.**

(65) del Río Carral, M., Schweizer, A., Papon, A. et Santiago-Delefosse, M. Les objets connectés et applications de santé: étude exploratoire des perceptions, usages (ou non) et contextes d'usage. ***Pratiques psychologiques,*** 25(1), 1-16.

(66) Cambon, L. (2016). Le nudge en prévention… troisième voie ou sortie de route? ***Santé Publique***, 28, (2019), 43-48.

خامساً: التأثيرُ على العالم الماديِّ، لا سيَّما على البنى التحتيَّة الحيويَّة:

l'impact sur le monde physique, notamment sur les infrastructures critiques

إن ربطَ الشَّبكاتِ العامَّة (توزيع المياه والغاز) أو محاور المرور (إشارات المرور والأنفاق) يعزّز القضايا الأمنيَّةَ بطريقةٍ غير مسبوقةٍ، فلم يَعد اختراقُ أنظمةِ المعلوماتِ يقتصرُ على التَّأثيرِ "الافتراضيّ" (التحكُّم في البيانات، وحجبِ الأنظمةِ، وتثبيتِ البرامج الضارَّة)؛ بل يُمكنه أيضًا أن يُشكِّل تهديدًا جسديًّا[٦٧].

سادساً: التخوُّفُ من استخدام تقنيَّات الأقمار الصناعيَّة:

أُجري عديدٌ من المناقشاتِ بشأنِ النَّظرِ في مساهمةِ وفاعليَّةِ ربط الأشياءِ المُتَّصلةِ عبر الأقمارِ الصناعيَّة، حيث إنَّ تكنولوجيا الأقمارِ الصناعيَّة ذات أهميَّةٍ خاصَّةٍ للتَّعاملِ مع الأسواقِ ذات العمليَّاتِ على نطاقٍ عالميّ (اللُّوجستيَّات، وتتبُّع البضائع، والنَّقل، والمَركبات المُتَّصلة) أو التي لا تخدمها الشَّبكاتُ الأرضيَّةُ بشكلٍ جيّدٍ (الزِّراعة، واستخراج النِّفط، والأمن البحريُّ والجويُّ، ومناطق الصِّراع).

وجديرٌ بالذِّكر أنَّ تطويرَ الأشياءِ المُتَّصلةِ يعرض المستهلكين بشكلٍ أساسٍ لنوعيْن من المخاطر: الاستخدام التجاريُّ للبياناتِ الشَّخصيَّةِ والهجماتُ على الخصوصيَّة، وممَّا لا شكَّ فيه أن إحدى عواقبِ عالم الشَّبكاتِ والاتِّصالات هو أنَّنا نتركُ المزيدَ والمزيدَ من الآثارِ الرقميَّة. وبعيدًا عن التقدُّم التِّكنولوجيّ، أصبحت مسألةُ ضمانِ عدم الكشفِ عن هويَّةِ البياناتِ التي تجمعُها هذه الأجهزةُ تُواجه إشكاليَّةً كبيرةً.

---

[٦٧] قد أظهر عديدٌ من الهجماتِ الأخيرةِ الخطرَ المحتملَ المتمثِّل في عدمِ كفايةِ الأمن: الزِّيادة الحرجة في درجةِ حرارةِ المسبك؛ انقطاع التيارِ الكهربائيّ في عدَّة بلْدَات؛ السَّيطرة على بعضِ الوظائفِ الحيويَّة لمحطَّةِ الطَّاقةِ النوويَّة. اكتشفت شركة Verizon مؤخرًا ثغرةً أَمنيَّةً في محطَّةِ توزيع المياه الأمريكيَّة: كان من الممكن أن يؤدّيَ استغلالُ هذا الخللِ إلى تعديلِ درجةِ حرارةِ المياه أو تركيبها الكيميائيّ أو حتى قطع التَّوزيع تمامًا.

(ISSN: 2537- 0758)

كما أصبح الاتِّصالُ بالإنترنتّ وظيفةً متكاملةً للأشياءِ اليوميَّة، ولذلك يجبُ على مُصمِّمي هذه المعدَّاتِ مواجهةُ مخاطرِ الهجماتِ "السيبرانيَّة". وإلا سنُواجه خطورةً على بياناتِ الأشخاصِ والشَّركات في ذاتِ الوقت، بل والحكومات أيضًا، وهو الأمرُ الذي يحتاجُ إلى رقابةٍ مشدَّدةٍ؛ منعًا لأيّ اعتداء.

المبحث الثاني
عدمُ اليقين القانونيِّ في مجال الأشياءِ المُتَّصلة

تمهيدٌ وتقسيمٌ:

يُثير استخدامُ الأشياءِ المُتَّصلةِ بشكلٍ خاصّ مسألةَ مخاطر الفشل، والتَّساؤل بشأنِ المسؤوليَّاتِ المتعدِّدة. وإذا كانت القدراتُ التقنيَّةُ والوظيفيَّةُ لهذه الأشياءِ حقيقيَّة، فإنَّها تظلُّ مع ذلك أشياءَ غير مؤهلةٍ من النَّاحيةِ القانونيَّة. وبالتالي، يُمكن أن تكونَ بمثابةِ وسيلةٍ لنقل الموافقة، ولكنْ لا يُمكنها الدُّخولُ في أيّ عقدٍ أو أن تكونَ مسؤولةً مسؤوليَّةً حقيقيَّةً عمَّا يحدث منها[٦٨].

فلنأخذْ مثالًا بسيطًا عن الأشياءِ المُتَّصلةِ، ونتخيَّل أن طرفًا ثالثًا تمكَّن من الوصولِ إلى الأشياءِ المُتَّصلةِ في المنزل، وبالتَّالي يُمكنه التحكُّمُ في إغلاقِ أو فتح الأبواب، وأجهزةِ الإنذارِ، وما إلى ذلك. فما الحلُّ القانونيُّ المزمعُ للوقايةِ من مثل هذه المخاطر؟

وعلى الرَّغم من غيابِ قانونٍ خاصّ بالأشياءِ المُتَّصلةِ الآن في التَّشريع المصريّ فإنَّ عددًا من القوانينِ الأخرى يضعُ بعض الحلولِ الأوليَّةِ في قانونِ حمايةِ حقوقِ الملكيَّةِ الفكريَّة، وقانون حمايةِ البيانات الشَّخصيَّة، فضلًا عن النُّصوصِ الدستوريَّةِ العامَّة التي تقرُّ حرمةَ الحياةِ الخاصَّة، لكن التَّطبيقَ الفعليَّ والعمليَّ لاستخدام الأشياءِ المُتَّصلةِ يُشير إلى وجودِ سيلٍ من الإشكاليَّاتِ لا سيَّما القانونيَّةُ التي تحتاجُ إلى

---

[٦٨] منية نشناش، متعاقدُ الذَّكاءِ الاصطناعي: شخصٌ قانونيٌّ جديد؟، مجلَّة أبحاثٍ قانونيَّةٍ وسياسيَّة، مج٧، ع١ جامعة محمد الصديق بن يحيى جيجل– كليَّة الحقوق والعلوم، السياسيَّة، ٢٠٢٢، ص٤١٤– ٤٢٩.

دراسةٍ متخصِّصةٍ وقواعدَ متعمِّقة؛ كون أنَّ الأضرارَ النَّاجمةَ عن استخدام الأشياءِ المُتَّصلة أصبحت كثيرةً ومتعدِّدةً.

وممَّا لا شكَّ فيه أن الحاجةَ ماسَّةٌ إلى إقرارِ قواعدَ للحمايةِ الوقائيَّةِ سواءٌ من النَّاحيةِ التقنيَّةِ أو القانونيَّةِ تحدُّ نوعًا ما من مخاطرِ وسلبيَّاتِ استخدام الأشياءِ المُتَّصلة، قبل وقوع الضَّررِ على الأشخاصِ، إلا أنَّ هناك تحدياتٍ تعرقلُ مسألةَ وجودِ إطارِ قانونٍ خاصٍ.

وبناءً على ما تقدَّم نقسم هذا المبحثَ إلى مطلبين، وذلك وعلى النَّحو التَّالي:

المطلب الأول: الإشكاليَّاتُ القانونيَّةُ المتعلِّقةُ باستخدام الأشياءِ المُتَّصلة.

المطلب الثاني: تحدِّياتُ وضعِ إطارٍ قانونيٍ محدَّد.

المطلب الأول

الإشكاليَّاتُ القانونيَّةُ المتعلِّقةُ باستخدامِ هذه الأشياءِ المُتَّصلة

إن تزايُدَ الأشياءِ المُتَّصلةِ في السُّوق والاهتمام المتزايد للمُستهلكين بهذه المنتجاتِ الإلكترونيَّة الجديدة يُثير تساؤلاتٍ حول الطَّريقةِ التي ينظرُ بها القانونُ إلى هذه الابتكاراتِ. وتُشكِّل هذه الأشياءُ المُتَّصلةُ في الواقعِ نظامًا جديدًا، لم يخضعْ بعدُ لمجموعةٍ من القواعدِ المحدَّدة، وهناك عديدٌ من الأسئلةِ المُثارة في هذا الشَّأن: فما هي الأشياءُ المُتَّصلة؟ وما هو نظامُها القانونيُّ؟- وكيف سيتمُّ استخدامُ بياناتنا الشَّخصيَّةِ أو الفنيَّةِ أو السريَّةِ أو الجغرافيَّةِ أو الطبيَّة؟- وما هو وضعُ هذه البياناتِ بالنِّسبةِ لقانون "المعلوماتيَّة والحريَّات"؟ وتضافُ إلى كلِّ هذه التَّساؤلاتِ التأمُّلاتُ الأخلاقيَّةُ التي تتعلَّقُ بمخاطرِ الجمعِ المنهجيِّ للبياناتِ فيما يتعلَّقُ باحترامِ الحقوقِ الأساسيَّةِ، وخاصَّةً الحقَّ في النِّسيان[٦٩].

(69) Thierry Piette-coudol, Les objets connectés: Sécurité juridique et technique dans l'Internet des objets (2e édition), Lexisnexis Actualite 15 Novembre 2023.
https://www.librairiedalloz.fr/livre/9782711039371-les-objets-connectes-securite-juridique-et-technique-dans-l-internet-des-objets-2e-edition-thierry-piette-coudol/

(ISSN: 2537- 0758)

ويستدعي الشَّيءُ المتَّصلُ في المقامِ الأوَّل أفكارًا عامَّةً حول حمايةِ البياناتِ واحترام الحياةِ الخاصَّةِ والملكيَّة الفكريَّة. ويتطلَّب اتِّصالُ الشَّيءِ أيضًا تحليلًا محدَّدًا في قانونِ العقودِ وقانون المستهلك. وفي هذا الشَّأنِ تبرزُ عدَّة أسئلةٍ نذكُرُ منها، كيف يتمُّ إبرامُ العقدِ عن طريقِ الشَّيء المتَّصل؟ وكيفيَّة التأكُّدِ من أنَّ المستخدمَ يُعطي الموافقةَ في أثناء العمليَّة؟ ما هي المسؤوليَّةُ في حالةِ حدوث خلل؟ وما هو الحلُ الذي يُمكن للمستخدمِ اللُّجوء إليه عندما لا يلبِّي الشَّيءُ المتَّصلُ توقُّعاته؟ وهل القواعدُ القانونيَّةُ التي تحكُمُ الأشياءَ التي يقتنيها المستهلكُ ويستخدمها تتكيَّفُ مع الشَّيءِ المتَّصل؟ أم ينبغي أن يكونَ من المناسبِ منحُ الشَّخصيَّةِ القانونيَّةِ للأشياءِ المُتَّصلةِ المستقلة؟ وما هي التطوُّراتُ المتوقَّعةُ من إصلاحِ قانونِ المسؤوليَّةِ المدنيَّة؟ وما هي الرُّؤيةُ التي يُمكن أن تُقدِّمها لنا حقوقُ جيراننا وحلفائنا الاقتصاديِّين؟[٧٠].

وفي الواقع، هناك مشكلةٌ في استخدامِ البياناتِ الشَّخصيَّةِ التي يتمُّ جمعُها وتخزينُها بواسطةِ الأشياءِ المُتَّصلة. وفي إحدى الحالات، شجبَتْ شركةُ DoctorBeet، وهي مصمِّمةُ برمجيَّاتٍ، عمليَّةَ التجسُّسِ التي قام بها تلفزيون LG. وبالفعل لاحظت الشَّركةُ عند عرضِ إعلانٍ على شاشةِ التلفزيون، فقامتْ بجمعِ بياناتٍ عن سلوكِ المستخدمِ تُجاه هذا الإعلان. بالإضافةِ إلى ذلك، أدركتْ DoctorBeet أنه حتى بعدَ تعطيلِ خيارِ جمعِ البيانات، استمرَّ الأمرُ. كما تمَّ جمعُ البياناتِ من مفتاح USB المتَّصل بالكمبيوتر، وعليه قامتْ شركةُ LG بعد ذلك بتحديثِ برامجها[٧١].

(70) Objets connectés et consentement de l'utilisateurCycle de Conférences du Club des Partenaires de la Faculté DEG, https://centrejeanbodin-univ--angers-fr.translate.goog/fr/activites/manifestations/manifestations-2019/oc-consentement.html?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

(71) Laure Marino, «To be or not to be connected: ces objets connectés qui nous espionnent. A propos des téléviseurs LG» Recueil Dalloz Sirey, 09/01/2014.

وتتعلَّق المخاطرُ التي قد تظهرُ في استخدامِ هذه الأشياءِ المُتَّصلةِ من ناحيةٍ بالمراقبةِ السريَّةِ (أ)، ومن ناحيةٍ أخرى بمعالجةِ البياناتِ الشَّخصيَّة (ب).

أ- المراقبةُ السِّريَّةُ:

بمُجرَّدِ اتِّصالِ الأشياءِ بالإنترنت، تظهرُ مسألةُ المراقبةِ أو حتى التجسُّس، وهذه البياناتُ هي بالضَّرورةِ ذات أهميَّةٍ للمُتسلِّلين، وبالفعل، كشفت شركةُ Kapersky الأمنيَّةَ في دراسةٍ لها أنَّه بيْن عامي ٢٠١٨ و٢٠١٩، زادت الهجماتُ التي نفذها المتسلِّلون تسعة أضعاف، وبالتَّالي وقَعَ ما يقرُبُ من ١٠٥ مليون هجومٍ ضدَّ الأشياءِ المُتَّصلة. ويعدُّ ذلك هدفًا سهلًا للمُتسلِّلين والجرائم الإلكترونيَّة بشكلٍ عامٍ. وفي عام ٢٠١٤، ذكرت شركة HP أن حوالي ٧٠% من الأجهزةِ المُتَّصلةِ بها فيها ثغراتٌ أمنيَّةٌ كبيرةٌ قد تسمحُ للمُتسلِّلين باستغلالها بسهولةٍ. ومن المتوقَّعِ أيضًا بحلول عام ٢٠٢٥ سيكون هناك ما يقرُبُ من ٣٨ مليار شيءٍ متَّصلٍ في العالم(٧٢).

لذا، قد تكونُ هذه المعلوماتُ مُخيفةً، وقد يكونُ استخدام الأجهزةِ المُتَّصلةِ أمرًا خطيرًا، حيث تقومُ الأشياءُ المُتَّصلة بجمعِ الكثيرِ من البياناتِ الشَّخصيَّةِ، مثل: تحديدِ الموقعِ الجغرافيّ، وهي معلوماتٌ يُمكن أن تكونَ تطفليَّةً للمستخدمِ أو حتى خطيرة، حيث يُمكن جمعُ حياةِ المستخدمِ بأكملها، دون عِلمهِ.

ب- معالجة البيانات الشَّخصيَّة:

Un traitement des données personnelles:

تقوم الأشياءُ المُتَّصلة مثل السَّاعاتِ أو عدادات الخطى بجمعِ الكثيرِ من البياناتِ الصحيَّة. وتعدُّ هذه البياناتُ ضِمن البياناتِ الشَّخصيَّةِ الحسَّاسة. ولذلك، فإنَّ الحمايةَ الممنوحةَ لهذه البياناتِ يجبُ أن تكونَ مهمَّةً.

وقد يتمُّ إرسالُ هذه البياناتِ إلى أطرافٍ ثالثةٍ، وخاصَّةً شركاتِ التَّأمينِ، وتجدرُ الإشارةُ إلى أن البياناتِ الصحيَّةَ ليست الوحيدةَ المعنيَّة، فالبياناتُ المرتبطةُ بتحديدِ الموقعِ الجغرافيّ يجب أن تخضعَ أيضًا لحمايةٍ كبيرةٍ.

(72) OBJETS CONNECTES ET DONNEES PERSONNELLES, https://www-murielle--cahen-fr.translate.goog/objets-connectes-et-donnees-personnelles/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

(ISSN: 2537- 0758)

وهناك عديدٌ من الأشياءِ المُتَّصلةِ التي تُسجِّل موقعَنا الجغرافيَّ، والتي يُمكن أن تكونَ مفيدةً بشكلٍ خاصٍّ في بعضِ الأحيان. وفي سياق الدِّراساتِ الاستقصائيَّة، يُمكن أن تكونَ هذه البياناتُ ذات قيمةٍ كبيرةٍ. ففي عام ٢٠١٩، تمَّ العثورُ في فرنسا على قاتلٍ بفضلِ شيءٍ متَّصلٍ تمكَّن من تزويدِ المحقِّقين بالمعلوماتِ اللَّازمة(٧٣).

ومع ذلك، على الرَّغمِ من أنَّ هذا قد يكونُ مفيدًا، فإنه قد ينتهي الأمرُ بالبياناتِ أيضًا في الأيدي الخطأ، حيث يُمكن لمُجرمي الإنترنتّ أو ببساطةٍ الأشخاص الضَّارّين استخدامُ البياناتِ المتعدِّدة. والعمل على إحداثِ ضررٍ بالأشخاصِ المعنيِّين بها. وإزاء هذا الغموضِ كان من الصَّعبِ وضع إطارٍ قانونيٍّ محدَّدٍ للأشياءِ المُتَّصلة.

المطلب الثاني
تحدِّياتُ وضعِ إطارٍ قانونيٍّ محدَّدٍ

تمهيدٌ وتقسيمٌ:

يجبُ أن نعِيَ أنَّ الشَّيءَ المتَّصل يستخدم البياناتِ الشَّخصيَّةَ؛ لكي يتمكَّن من العمل، حيث تُتيح هذه البياناتُ الشَّخصيَّةُ معلوماتٍ بشأنِ تجربةِ العميل، ويتمُّ إرسالُ هذه البياناتِ أيضًا إلى الشَّركاتِ التي تقومُ بالتَّالي بجمع معلوماتٍ حول عُملائها. وجديرٌ بالذِّكر أنه يتمُّ أيضًا جمعُ الكثيرِ من البياناتِ الصِّحيَّةِ، من خلال المقاييسِ والسَّاعاتِ، وحتى أجهزة قياسِ ضغطِ الدَّم المُتَّصلة.

ولذلك، يثورُ التَّساؤلُ بشأن ما إذا كان لا يزالُ من المُمكنِ حمايةُ بياناتنا الشَّخصيَّة ضدَّ غزوِ الأشياءِ المُتَّصلة في حياتنا اليوميَّة؟

يتطلَّبُ تشغيلُ هذه الأشياءِ معالجةَ الكثيرِ من البيانات، وخاصَّةً البياناتِ الشَّخصيَّة، التي يتمُّ جمعُها بشكلٍ مستمرّ، ويتمُّ تخزينُها غالبًا في واجهاتٍ افتراضيَّة. وبالتالي فإنَّ هذه الأشياءَ المُتَّصلةَ تُشارك في ظاهرةِ البياناتِ الضَّخمة.

(73) OBJETS CONNECTES ET DONNEES PERSONNELLES op. cit.

ونظرًا لارتباطِ هذه الأشياءِ بالشَّبكات، فمن المهمّ وضعُ إطارٍ قانونيٍّ مناسبٍ للحدِّ من المُشكلات، لا سيَّما تلك المتعلِّقةُ بأمنِ وحمايةِ البياناتِ الشَّخصيَّة، وجديرٌ بالذِّكرِ لا يوجدُ حاليًّا إطارٌ قانونيٌّ محدَّدٌ للشَّيءِ المتَّصل؛ حيث يتمُّ استعارةُ الإطارِ الحاليّ من مجالاتٍ قانونيَّةٍ مختلفةٍ دون القدرةِ على الاستجابةِ لقضايا الأمانِ وحماية البيانات.

ومن خلالِ "عالم الأشياء" هذا، أصبح من المُمكن الآن إجراء مقارنةٍ مع الأشياءِ المُتَّصلة. ولقد دفعت حياتُنا شديدةُ التَّرابطِ واستخدامنا للتِّقنيَّاتِ الجديدةِ القانونَ إلى إعادةِ النَّظرِ في أسسهِ ونطاقه(٧٤)، حيث أصبحنا نقرأُ بشكلٍ مستمرٍ أنَّ الأشياءَ المُتَّصلةَ تغمرُ السُّوق، بين الأجهزةِ القابلةِ للارتداء، وأشياء التَّشغيلِ الآليّ للمنزل، ناهيك عن تلك المخصَّصةِ للشَّركات، وتستمرُّ فائدتُها في إثباتِ نفسها: في البلدان، والشَّركاتِ، والمُستشفيات،...إلخ.

إذا كان العنصرُ البشريُّ هو المحرّكَ الفعليَّ بحسَب الأصلِ للأشياءِ المُتَّصلة، إلا أنَّنا أصبحنا نرى أشياءَ متَّصلةً صاحبة قرارٍ بمعزلٍ عن البشر، وهذا يعدُّ من أكبرِ التَّحدِّيَاتِ التي يتوجَّبُ العملُ على حلِّها من خلالِ إصدارِ تشريعاتٍ متقدِّمة.

الفرع الأول
تأثيرُ الأشياءِ المُتَّصلة على التَّنظيم
De l’impact des objets connectés sur la régulation

يتمُّ تفسيرُ مكانةِ الشَّيء المتَّصل في السُّوقِ الرَّقميّ من خلالِ قدرتهِ على تقديمِ الخدماتِ ذات الصِّلة، والتي تُغذِّيها في كثيرٍ من الأحيانِ المعلوماتُ الشَّخصيَّة. وربَّما تكونُ قدرةُ الشَّركاتِ على جمعِ مثل هذه البياناتِ قد كشفت عن مخاطرَ جديدةٍ على الحياةِ الخاصَّة للأفراد، وهي مخاطرُ غالبًا ما يفوقها الوزنُ التِّجاريُّ لهذا النَّوعِ من الأشياء. وبالتَّالي، تطلَّبت هذه الحداثةُ من الجهةِ التنظيميَّةِ إعادة التَّفكيرِ في

(74) Ministère de l’économie et des finances, Marché des objets connectés à destination du grand public, 2018.

(ISSN: 2537- 0758)

الإطارِ القانونيّ، وتسليط الضَّوءِ على فائدةِ الأداةِ التنظيميَّةِ الجديدة التي يُمكن تحسينُها وهي الأخلاق(٧٥).

أولًا: الثَّورةُ الرقميَّةُ والأشياءُ المُتَّصلة:

Révolution numérique et objets connectés

يُعدُّ هذا العالمُ من الأشياءِ المُتَّصلةِ– عمومًا– نتيجةً للثَّورةِ الصناعيَّةِ الرَّابعة. ويُوضِّح هذا التَّعبيرُ قوَّة التَّغييرِ التي تفرضُها هذه التِّكنولوجيا، وهي قوَّةُ انفتاحِ العالمِ الخاصِّ على الشَّركات، وهو شرطٌ لا غِنَى عنه للوصولِ إلى الخدماتِ التي يُقدِّمها الشَّيءُ المتَّصل. ويُشكِّل هذا الابتكارُ جزءًا من حركةٍ تكنولوجيَّةٍ أوسع نطاقًا، والهدف من ذلك هو التدخُّلُ أكثر فأكثر في الحياةِ الخاصَّةِ للأفرادِ لتحسينِ وتسهيلِ عاداتِهم الحياتيَّةِ اليوميَّة، ويجبُ التَّأكيدُ على أنَّ هذا الابتكارَ يتطوَّرُ على حساب الحياةِ الخاصَّةِ للأفراد. ويؤثِّر هذا الوجودُ الكليُّ على كميَّةِ البياناتِ التي يتمُّ جمعُها، وهي ضخمةٌ، وهذه البياناتُ ليست مهمَّةً كما قد يدَّعي البعض، بل الأمرُ يتعلَّقُ بالبياناتِ الشَّخصيَّة. وبالتَّالي تُسهم هذه العمليَّةُ في فكرةِ الحياةِ الخاصَّةِ الرقميَّةِ والقابلة للرَّقمنةِ بشكلٍ متزايدٍ، من خلال العلاقةِ الخاصَّةِ بين المستخدمِ والشَّركةِ التي تقدِّم الشَّيءَ المتَّصل، وممَّا لا شكَّ فيه أنَّ هذه العلاقةَ ليست واضحةً للمستخدم بشكلٍ كافٍ.

وتتمتَّعُ الشَّركةُ التي تستخدمُ البياناتِ التي تمَّ جمعُها، بمعرفةٍ وعلمٍ متعمِّقٍ بحياةِ المستهلك الشَّخصيَّةِ والمهنيَّة في كثيرٍ من الأحيان. وهذا الوعيُ لدى الأفرادِ يكونُ في أغلبِ الأحيانِ نتيجةً للفضائحِ الكبرى التي اندلعَتْ، على سبيلِ المثالِ مع مكبِّراتِ الصَّوتِ المُتَّصلة بـ "Alexa "7 أو "Google Home".

فالأشياء المُتَّصلةُ تلتقطُ البيانات، وتخزِّنها، وتعالجُها، وتنقلُها، ويمكنُها تلقِّي التَّعليماتِ وإعطاؤها، وبالتَّالي لديها القدرةُ على الاتِّصالِ بشبكةِ معلومات(٧٦). ويتمُّ

(٧٥) قريبٌ من هذا المعنى راجع: سمية محمد سعيد محمود، التَّحدياتُ القانونيَّةُ للذَّكاء الاصطناعيّ: الروبوت نموذجًا، مجلة العلوم القانونيَّة والاقتصاديَّة، مج٦٦،،ع١، جامعة عين شمس– كليَّة الحقوق، سنة ٢٠٢٤، ص١٥٧٥– ١٦٦٨.

توفيرُ هذه المعالجةِ من خلالِ خوارزميَّةِ الذَّكاء الاصطناعيّ، والتي تُسهم في ثراءِ هذه التِّكنولوجيا، وفي ذاتِ الوقتِ هي سببٌ رئيسٌ لتعقيدِها.

وجديرٌ بالذِّكر ليس الذَّكاء الاصطناعي العنصرَ المحدَّدَ الوحيدَ للشَّيءِ المتَّصل، فهي جزءٌ من بيئةٍ أكبر، وهي بيئةُ "إنترنت الأشياء"، والتي يُشار إليها عادةً بالاختصارِ "IOT"، أي "إنترنت الأشياء" في البلدانِ الأنجلوسكسونيَّة. فهو يُحدِّد النِّظامَ البيئيَّ الذي تنتمي إليه الأشياءُ المُتَّصلة؛ أي الإنترنت، وترابطه مع الأشياءِ الأخرى، وقاعدة تخزينِ الخدمةِ السحابيَّة(٧٧).

ولهذا فإن للشَّيءِ المتَّصلِ قدرةً على جمعِ البيانات، ومُعالجتها، وتحليلها من أجلِ معالجةِ الطَّلب، ووضع بياناتهِ في الشَّبكات، ومع ذلك، يكمُنُ العيبُ الرئيسُ للشَّيءِ المتَّصلِ في تشغيله، حيث يجبُ أن يجمعَ الشَّيءُ كميَّةً كبيرةً من البيانات، والتي يتمُّ تسجيلُها وتخزينُها والإشارةُ إليها بشكلٍ عامٍ من قِبل الشَّركاتِ من خلال النِّظام البيئيّ الذي تمكَّنا من وصفه. ومع التطوُّرِ الأخيرِ للذَّكاءِ الاصطناعيّ والتِّقنيَّاتِ الجديدة، فإنَّ نشاطَ الشَّركات، المتمثِّل في جمعِ البياناتِ أصبح على نطاقٍ واسعٍ، وتستحقُّ هذه الملاحظةُ الاهتمامَ؛ كونه يدعمُ القوَّةَ الاقتصاديَّةَ للبيانات، والتي يُشار إليها غالبًا باسمِ النِّفطِ الجديدِ أو "الذَّهب الأسود" "nouveau pétrole ou or noir". حيث تُعدُّ البياناتُ الشَّخصيَّةُ موضوعَ اقتصادٍ عالميٍّ حقيقيٍّ، حيث تعتمدُ سيطرةُ الشَّركاتِ

(76) «objets captent, stockent, traitent et transmettent des données, peuvent recevoir et donner des instructions et qui ont pour cela la capacité à se connecter à un réseau d'information». Arnaud de Baynast, op cit, p.212.

(77) formatique en nuage» ou «informatique dans les nuages») est, selon la définition officielle de la Commission générale de terminologie et de néologie, un «mode de traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire», […] le «nuage» représentant est un ensemble de serveurs en réseau (incluant des systèmes d'exploitation et des logiciels), installés dans un datacenter, qui exécutent les traitements et stockent les données» V. Serge Braudo, «Définition du cloud computing», en lige: https://www.dictionnaire juridique.com/definition/cloud computing.php.

(ISSN: 2537- 0758)

الرقميَّة على السُّوقِ على كميَّةِ ونوعيَّةِ البيانات التي تجمعها لملءِ قواعد بياناتها، وبالتَّالي نقومُ بتطوُّرِ استراتيجيَّاتها التجاريَّة.

ثانيا: خطرُ استغلالِ البياناتِ الشَّخصيَّة عبْرَ الأشياءِ المُتَّصلة:

Risque d'exploitation des données personnelles par l'intermédiaire des objets connectés:

إن ثورة الأشياءِ المُتَّصلةِ فضَّلت القيمةَ الاقتصاديَّةَ للبياناتِ دون تفضيلِ حقوقِ المستهلكين في حمايةِ حياتهم الخاصَّةِ بشكلٍ متناسبٍ، وفي الحقيقةِ لا تتعلَّقُ البياناتُ المجمَّعةُ بالخصائصِ الموضوعيَّةِ للأشخاص، بل تتعلَّقُ بالمعلوماتِ الشَّخصيَّة: عنوانهم، وحالتهم العائليَّة، وأذواقهم، وعادات وأسلوب حياتهم. وممَّا لا شكَّ فيه تؤدّي قدرةُ الشَّركاتِ على التَّجميعِ والوعدِ بتقديمِ خدمةٍ فعالةٍ وشخصيَّةٍ إلى مخاطرَ جديدةٍ تؤثّر على الخصوصيَّة، وهنا يثورُ التَّساؤلُ: ما هي الضَّماناتُ في حالةِ الوصولِ إلى البياناتِ الشَّخصيَّةِ والتَّلاعب بها؟

تكمُنُ المشكلةُ القانونيَّةُ الرئيسة للأشياءِ المُتَّصلة، في حمايةِ الخصوصيَّةِ واستغلالِ البياناتِ الشَّخصيَّة. وفي عام ٢٠١٤، سلَّط مجلسُ الدَّولةِ الفرنسيُّ الضَّوءَ على بعضِ الاستخداماتِ الرقميَّةِ التي تنتهكُ هذا الحقَّ، مثل: نشرِ البياناتِ الشَّخصيَّةِ خارج إرادةِ الفردِ المعنيّ، أو استخداماتها الضارة، أو استخدامها من قِبل السُّلطاتِ العامَّةِ لأغراضِ الحفاظِ على النِّظام العامّ"[٧٨]. وبشكلٍ عامّ، تتعلَّق هذه المخاطرُ بسلامةِ حياتنا الخاصَّة، والتي أصبحتْ الآن في مفترقٍ بين المجالِ الخاصّ والمجال الاقتصاديّ للشَّركات.

وعلى ذلك أدَّت التِّكنولوجيا الرقميَّةُ، وبخاصَّةٍ الأشياءُ المُتَّصلة، إلى ظهورِ الحاجةِ إلى مزيدٍ من الإشرافِ على الحقّ الأساسيّ في حمايةِ الخصوصيَّة، لا سيَّما من خلالِ حمايةِ البيانات الشَّخصيَّة. وممَّا لا شكَّ فيه يُتطلَّبُ لعملِ الشَّيء المتَّصلِ

(78) Conseil d'État, Les rapports du Conseil d'État– Le numérique et les droits fondamentaux, La documentation française, 9 septembre 2014, p.17

أن يجمعَ الكثيرَ من بياناتِ المستخدم، وهو أمرٌ مُثيرٌ للدهشةِ؛ كون أنَّ عدمَ تقييدِ جمعِ البياناتِ وَفْق معاييرَ قانونيَّةٍ يجعل خصوصيَّةَ البياناتِ في مهبِّ الرِّيح، حيث يُمكننا القولُ: إنَّ استخدامَ الشَّيءِ المتَّصل يعني التخلِّي عن جزءٍ من الحياةِ الخاصَّة للحصولِ على خدمةٍ ما.

وجديرٌ بالملاحظةِ أن الحقَّ في حمايةِ الخصوصيَّةِ لا يُمكن أن يكونَ مطلقًا، لكنَّ هذا الأمرَ لا يعني أنه يجبُ على المُستخدمِ التَّنازلُ عن هذا الحقِّ عند إعطاءِ الموافقةِ على استخدامِ بياناته، فالغرضُ الأوَّل من الموافقةِ هو مجرَّد تشغيلِ الشَّيءِ المتَّصل، وبناءً على ذلك، لم يعُدْ من الممكن في عصرِ الثَّورةِ الرقميَّةِ اعتبارُ مفهومِ الخصوصيَّةِ مفهومًا لا يُمكن المساسُ به. ومن ثمَّ فإنَّ الأمرَ يتعلَّقُ بإيجادِ توازُنٍ عادلٍ بين احترامِ الحقوقِ الأساسيَّة للمُستخدمين وحريَّة القيامِ بالمشاريع(٧٩).

ثالثًا: حدودُ التَّنظيمِ التَّقليديِّ حول الأشياءِ المُتَّصلة:

Les limites de la réglementation classique autour des objets connectés:

قبل التطرقِ لمسألةِ تنظيمِ استغلالِ البياناتِ الشَّخصيَّةِ أو الذَّكاء الاصطناعيّ أو الأشياء المرتبطة به، يجبُ أن نعيَ أن التِّكنولوجيا الرقميَّةَ أثارتْ مناقشاتٍ كبيرةً حول إطارِها القانونيّ، وهو الأمرُ الذي أدَّى في البدايةِ إلى معارضةِ فكرةِ التَّنظيمِ ذاتها. ولذلك لم تكُنْ فكرةُ التَّنظيمِ واضحةً في العالمِ الرَّقميّ.

إن عدم الاهتمام بفكرة التنظيم القانوني قد أدى إلى عدم السَّيطرةِ على هذا الفضاءِ الرَّقميّ، ولم تكن تقنيَّاتُ الرَّقابةِ التي اعتمدها المُشرّعُ المصريُّ والفرنسيُّ مناسبةً لهذا القطاع. ومع ذلك، فقد ظهرتْ مجموعاتٌ جديدةٌ من القواعد، بهدف تنظيمِ بعضِ الممارساتِ الرقميَّة، خاصَّةً بعد ظهورِ فضائحَ وإشكالياتٍ جديدةٍ للاستخدام المُسيء. ومن خلال مراقبةِ الثَّورةِ الرقميَّة، استخلص المُشرّعُ الفرنسيُّ بعضَ الاستنتاجات. وكان من الضَّروريّ إيجادُ توازُنٍ بين التَّنظيمِ الرَّقميّ في سياقِ

(79) Mathilde Bondu, Ethique et objets connectés, Maîtrise en droit, Université Laval, Québec, Canada et Université Paris-Saclay Cachan, France Mathilde Bondu, 2020, p. 4-5.

(ISSN: 2537- 0758)

استغلالِ البياناتِ، والاقتصاد العالميّ للأشياءِ المُتَّصلةِ التي يحكمُها منطقُ السُّوق(٨٠).

وفي وقتنا الحاليّ ليس لدى الشَّيءِ المتَّصلِ أو خوارزميَّةِ الذَّكاءِ الاصطناعيّ لوائحُ وقواعدُ محدَّدة، ولكن يُمكن أن تكونَ جزءًا من قوانينَ أكثر عموميَّةً مرتبطة بالتِّكنولوجيا الرقميَّة. صحيحٌ أن فرنسا اعتمدت قرارًا- على سبيل المثال- بشأن تنظيمِ الأجسامِ المُتَّصلةِ وتطوير إنترنتّ الأشياء في أوروبا في عام ٢٠١٨(٨١)، لكنَّ هذه ليست مبادرةً قادرةً على أن تُؤتي ثمارَها لفترةٍ طويلةٍ، ولم يتمَّ تنظيمُ القضايا المتعلِّقةِ بالخوارزمياتِ والبياناتِ الشَّخصيَّة(٨٢). كما أنَّ التَّشريعَ المصريَّ إذا سنَّ قوانينَ تتعلَّقُ بحماية حقوقِ الملكيَّةِ الفكريَّة، وحماية البياناتِ الشَّخصيَّةِ، فإن التَّطبيقَ الفعليَّ والعمليَّ لاستخدام الأشياءِ المُتَّصلةِ يُشير إلى وجودِ كثيرٍ من الإشكاليَّاتِ لا سيَّما القانونيَّةُ التي تحتاجُ إلى دراسةٍ متخصِّصةٍ وقواعدَ متعمِّقة؛ كون أنَّ الأضرارَ النَّاجمةَ عن استخدامِ الأشياءِ المُتَّصلة أصبحت كثيرةً ومتعدِّدةً.

ولقد كان تنظيمُ الأشياءِ المُتَّصلةِ واستخدام البياناتِ في جميعِ أنحاءِ العالم غير ملزمٍ في وقتٍ سابقٍ، إلا أنه مع ازديادِ المخاطرِ المتعلِّقةِ بممارساتِ الشَّركاتِ الرقميَّة الكبيرة، دفع المُشرِّعَ بوضعِ إطارٍ قانونيٍّ محكمٍ. فعلى سبيل المثال، في أوروبا، ظهرتْ فكرةُ توحيدِ البياناتِ الشَّخصيَّةِ تدريجيًّا، مما أدَّى إلى اعتمادِ اللَّائحةِ المتعلِّقةِ بحمايةِ البياناتِ الشَّخصيَّة- المشار إليها فيما بعدُ باللَّائحةِ العامَّةِ لحماية البيانات-.

ولقد سعى هذا الإصلاحُ إلى عدَّة أهدافٍ، "تعزيز حقوق الإنسان" و"إضفاء المصداقيَّةِ على التنظيمِ من خلال تعزيزِ التَّعاونِ بين المحترفين الرقميّين، وجعلهم مسؤولين عن مُعالجةِ البيانات". ورغم ما جاءتْ به هذه اللَّائحةُ من تنظيمٍ فإنها لم

(80) Mathilde Bondu, Ethique et objets connectés, Maîtrise en droit, op cit.,p. 5.

(81) Sénat, Résolution européenne sur la régulation des objets connectés et le développement de l'internet des objets en Europe, Session ordinaire-n°106, 22 mai 2018.

(82) Alexandra Bensamoun et Grégoire Loiseau, «L'intelligence artificielle: faut-il légiférer?», D.2017, p.581.

تضعْ حدًّا للمعالجةِ المسيئةِ للبياناتِ الشَّخصيَّة. ومع استمرار تراكُمِ الإشكاليَّاتِ والمخاطر عام ٢٠١٩، ظهر خِطابٌ جديدٌ في أوروبا وعلى السَّاحةِ الدوليَّة، يتلخَّصُ في عدمِ كفايةِ التَّنظيمِ حول الأشياءِ المرتبطة، كما ظهر عدمُ احترامِ الشَّركاتِ الدوليَّة للقواعدِ القانونيَّةِ الحاليَّةِ المتعلِّقةِ بحمايةِ البياناتِ الشَّخصيَّة(٨٣).

وفي الواقعِ زادت المناقشةُ بين مختلفِ الجهاتِ الفاعلة، العامَّةِ والخاصَّةِ، الوطنيَّةِ والدوليَّةِ، ولكلٍّ منها وجهةُ نظرٍ مختلفةٌ حول الشَّكلِ الذي ينبغي أن يكونَ عليه تنظيمُ الشَّيءِ المتَّصل، دون إغفالِ الإطارِ القانونيّ. وتُثار تعقيداتُ التَّنظيمِ، في عالمٍ تتطوَّرُ فيه التِّقنيَّاتُ الرقميَّةُ باستمرار، دون انتظارٍ لتطوُّرِ التَّشريعات. فمع الزِّيادةِ الهائلةِ في سعات التَّخزين، وتَضاعُفِ مصادرِ التَّجميع، وإنشاء أشياءَ متَّصلةٍ جديدةٍ 5G، أصبح الوضعُ الحاليُّ يقودُنا إلى الاعتقادِ بأن الجهاتِ الخاصَّةَ والعامَّةَ لا تزالُ تُواجه صعوباتٍ في التَّواصلِ لإيجادِ تنظيمٍ فعَّالٍ.

وفي وقتنا الحاليّ أصبح التَّفكيرُ أوسعَ حول طريقةِ إدارة الأشياءِ المُتَّصلةِ والتِّكنولوجيا الرقميَّة؛ لضمانِ امتثالِ سلوكِ المُحترفين الرَّقميّين للإطارِ القانونيّ المعتمد. ومع الأخذِ بعين الاعتبارِ الغموض التِّكنولوجيُّ الذي يُحيط بالتِّكنولوجيا الرقميَّة، يرى بعضهم أنه «يبدو أن الاعتمادَ على المُشرِّعِ لا علاقةَ له بالموضوع، حيث تتطلَّبُ التقنيَّةُ الرقميَّة التَّوفيقَ بين التَّنظيمِ الرقميّ والممارساتِ الجديدة، وتظلُّ الأخلاقُ أداةً أساسيَّةً(٨٤)، **وهذا ما سيُوضَّح فيما يلي:**

(83) Mathilde Bondu, Ethique et objets connectésop cit, p. 6.

(84) Luc Bégin, «Légiférer en matière d'éthique: le difficile équilibre entre éthique et déontologie», Éthique publique, Revue internationale d'éthique sociétale et gouvernementale, printemps 2011, vol.13, #1, p. 39-61, en ligne: https://journals.openedition.org/ethiquepublique/361

(ISSN: 2537- 0758)

الفرع الثاني
ظهورُ التَّفكيرِ في الأخلاقِ كمنظِّمٍ جديدٍ للأشياءِ المُتَّصلة

L'émergence d'une réflexion sur l'Ethique comme nouveau régulateur des objets connectés

إن الأخلاقَ مفهومٌ متعدِّدُ المعاني، وفي هذا الشَّأن يتحتَّمُ تعريفُه لفهم معناه القانونيّ، كما أن فهمَ هذا الأمرِ سيقودنا حتمًا إلى التَّشكيكِ في شرعيَّةِ التَّسلسلِ الهرميّ للقانونِ في المجال الرقميّ؛ لأن الأخلاقَ هي حاجةٌ سياسيَّةٌ واجتماعيَّةٌ واقتصاديَّةٌ.

أولًا: المقصودُ بالأخلاقِ كمنظِّمٍ جديدٍ للأشياءِ المُتَّصلة:

يبدو أن الحاجةَ إلى فتحِ حوارٍ بين المحترفين الرَّقميّين والهيئةِ التنظيميَّةِ للدَّولةِ ضروريَّةٌ لاستعادةِ ثقةِ المستهلك. ولذلك يتمُّ فرضُ أداةٍ معروفةٍ للجميع: الأخلاق، فهي استجابةٌ لغياب الحوكمةِ الدوليَّةِ للأشياءِ المُتَّصلة، ومع التَّغييرِ التَّنظيميّ الرقميّ كما نعرفه، ظهر معيارٌ جديدٌ.

وفي الواقعِ يُمكن أن تكونَ الأخلاقُ عنصرًا غامضًا، إذا لم يتمَّ تحديدُ إطارِها. فما المقصودُ بها؟

تعدُّ هذه الفكرةُ واسعةً جدًّا. فهي مجموعةٌ من المبادئِ الأخلاقيَّةِ التي هي أساسُ سلوكِ الشَّخص، ويرى بعضهم أنها معادلةٌ للأخلاق، حيث تتميَّزُ بالعواقبيَّةِ والأخلاقِ الواجبةِ والأخلاق الفضيلة، ومن المهمّ التَّأكيدُ أنَّ الأخلاقَ وعِلمَ الأخلاقِ يتميَّزان، من النَّاحيةِ القانونيَّةِ، حيث إنَّ القيمَ والمبادئَ تقع ضِمنَ نطاقِ الأخلاق، في حين أنَّ القواعدَ تقعُ ضِمن نطاقِ علمِ الأخلاقِ(٨٥).

وفي تقريرِ فيلاني Villani، والذي يرمي إلى تحديدِ استراتيجيَّةٍ وطنيَّةٍ مرتبطةٍ بالذَّكاءِ الاصطناعيّ، عرَّف الأخلاقَ بأنها "فرعٌ من الفلسفةِ [يُحاول] التَّمييزَ بين

(85) Luc Bégin, «Légiférer en matière d'éthique: le difficile équilibre entre éthique et déontologie», Éthique publique, Revue internationale d'éthique sociétale et gouvernementale, printemps 2011, vol.13, #1, p. 39-61, en ligne: https://journals.openedition.org/ethiquepublique/361

الخيرِ والشرِّ، والمثل الأعلى الذي نسعى لتحقيقه، والطُّرق التي تُبعدنا عنه"[٨٦]. ولكنَّها في الواقعِ تحمِلُ عدَّة معانٍ بحسَبِ السِّياقِ الذي تحدُثُ فيه. ويُمكن تعريفُها أيضًا بالفطرةِ السَّليمةِ، بمعنى التصرُّفِ بطريقةٍ عادلةٍ.

والأخلاق كما يفهمُها الفقهاءُ تتكوَّن من أخلاقيَّاتٍ مطبقةٍ في السِّياق الرقميّ، وما نَعنيه هنا بالأخلاقِ في مجالٍ معيَّنٍ، ألا وهو التِّكنولوجيا الرقميَّة، وليس في منظورٍ عامٍ.

ثانياً: الاختيار بين الأخلاقِ أم القانون؟
Un choix entre l'Ethique ou le Droit؟

عند الحديثِ عن مفهومَي الأخلاقِ والقانون، يبدو أنَّهما متعارضان تمامًا من حيث التَّنظيمُ؛ لأنَّ الأخلاقَ غير ملزمةٍ، ومبنيَّةٌ بشكلٍ مشتركٍ ومرن، لكنَّ واقعَ تنظيمِ الأشياءِ المُتَّصلة مختلفٌ تمامًا، حيث تتمتَّعُ الأخلاقُ بالقدرةِ على أن تكونَ الحليفَ الأكبرَ للقانونِ في المجالِ الرقميّ المعقد، ويُمكن أن تُصبح مرشدًا قانونيًّا «éclaireuse du droit» عظيمًا[٨٧].

ويبدو أنَّ التَّفكيرَ الجماعيَّ والمشترك، وأحيانًا الدوليَّ، والذي يُضمِّنه الإطارُ الأخلاقيُّ المرن، هو أفضلُ طريقةٍ لتوفيرِ ركيزةٍ قويةٍ ومشروعةٍ للحقِّ في تنظيمِ الأشياءِ المُتَّصلة، وفي الحقيقةِ يُمكن أن تتناغمَ كلمةُ "الأخلاق" أيضًا مع كلمة "الربح". فهي كدرعٍ لطمأنينةِ المستهلكِ بشأن الممارساتِ الاقتصاديَّةِ للشَّركة.

وهنا يثورُ التَّساؤلُ عن الدَّورِ الحقيقيّ للأخلاق والقانون في تنظيمِ الشيءِ المتَّصل. وعلى الرَّغم من أنَّ الأخلاقَ والقانونَ معياريان حقيقيَّان لتنظيمِ الشَّيءِ المتَّصل، لكنَّ صعوبةَ الإطارِ القانونيّ لهذا الأمر، يدعونا إلى التَّشكيكِ في التَّشابكِ الحقيقيّ بين هاتين الرَّكيزتين. وفي هذا الشَّأنِ نُلقي الضَّوءَ على قضيَّةِ الأخلاقِ

(86) Cédric Villani, Donner du sens à l'intelligence artificielle: pour une stratégie nationale et européenne, Paris, 28 mars 2018, p.139.

(٨٧) د. معتز محمد أبو زيد، الذَّكاءُ الاصطناعيُّ بين القانون والأخلاق: تنظيمُ أخلاقياتِ استخدامِ الذَّكاءِ الاصطناعيّ، أعمال مؤتمرِ التَّحدياتِ والآفاق القانونيَّةِ والاقتصاديَّة للذَّكاءِ الإصطناعيّ، جامعة عين شمس– كليَّة الحقوق، سنة ٢٠٢٤، ص٩٤٩–٩٦٠.

(ISSN: 2537- 0758)

باعتبارها وسيلةً للتَّنظيمِ الرقميّ، حيث تدعو هذه الفكرةُ إلى تنظيمٍ يصعب السَّيطرةَ عليه، لا سيَّما مع الاستخدامِ المتزايدِ للبياناتِ الشَّخصيَّةِ والاعتداء على الحقّ في الخصوصيَّة.

ومع ذلك، يبدو أنَّ تطويرَ أنظمةٍ مرنةٍ ومشتركةٍ هو أفضلُ طريقةٍ لتنظيم سلوكِ الشَّركاتِ في المجال الرقميّ. وهنا يثورُ التَّساؤل، هل الأخلاقُ هي الملاذُ الأخيرُ للتَّنظيمِ الفعَّالِ للأشياءِ المرتبطةِ؟ L'Ethique est-elle le dernier recours pour une régulation effective des objets connectés?

ولهذا سنُسلِّط الضَّوءَ على قدرةِ الأخلاقِ على تنظيمِ جوانبَ معيَّنةٍ من التِّقنيَّاتِ الجديدةِ، مثل: الأشياء المُتَّصلة، ومن المُمكن أن يكونَ مساعدًا للقانونِ من أجلِ التحكُّمِ والحدِّ من خطورتها.

ومن المؤكَّد أنَّ للشَّيءِ المتَّصلِ خصوصيَّةً مقارنةً بالتِّقنيَّاتِ الأخرى، والتي تعتمدُ على بُعدِها الماديّ. ومع ذلك، فإنَّ هذه الدِّراسةَ ستتعاملُ فقط مع البعدِ غير الماديّ للشَّيءِ المتَّصلِ فيما يتعلَّقُ بالبياناتِ الشَّخصيَّة، مع تناوُلِ الأخلاقياتِ المحيطةِ بتصميم هذا الشَّيءِ؛ أي "التصميم" الأخلاقيّ للأشياءِ المُتَّصلةِ والتطوير الأخلاقيّ لخوارزميَّاتِ الذَّكاءِ الاصطناعيّ، فهذه القضايا تستحقُّ تفكيرًا جديدًا ومتميِّزًا في الأخلاقِ كوسيلةٍ لتنظيمِ الأشياءِ المُتَّصلة.

ولهذا فإنَّنا نعمل على تقييمِ إمكاناتِ الأخلاقِ في مجالِ تنظيمِ الأشياءِ المُتَّصلة، وبالتالي سيتمُّ إثباتُ وجودِ نظامٍ قانونيّ ذي طابعٍ أخلاقيّ يحكم الأشياءَ المُتَّصلةَ فيما يتعلَّقُ بالبياناتِ الشَّخصيَّة، وليس المقصودُ من الأخلاقيَّاتِ أن تحلَّ محلَّ القواعدِ التنظيميَّةِ الحاليَّة، كما قد يعتقدُ بعضهم.

وفي هذا الشَّأنِ يثور عديدٌ من التَّساؤلات، نطرحُها كما يلي: هل تتناسبُ الأخلاقيَّاتُ مع الخصائصِ التقنيَّةِ للشَّيءِ المتَّصل وبيئتهِ الرقميَّةِ المتحرِّكة باستمرارٍ؟ وما مدى فائدةِ الأخلاقيَّاتِ عندما تكون الأشياءُ المُتَّصلةُ بالفعل موضوعًا لإطارٍ قانونيّ حاليّ للبيانات الشَّخصيَّة؟ وكيف أن الأخلاقيَّاتِ هي أداةٌ فعالةٌ لتنظيم الأشياءِ

المُتَّصلةِ وتُواجه في ذات الوقتِ تجاوزاتِ الموجةِ الرقميَّةِ. وكيف يتمُّ التَّعبيرُ عن الأخلاقياتِ التنظيميَّةِ للأشياءِ المُتَّصلةِ في الممارسةِ العملية؟

وفي الواقعِ لقد أصبحت الأخلاقياتُ بالفعلِ جزءًا من المشهدِ التِّكنولوجيّ، على عدَّةِ مستويات، حيث زادت السُّلطاتُ العامةُ من مبادراتِ إدخالِ الأخلاقيات، كما تطبِّق الشَّركاتُ الأخلاقَ، ولكن يجبُ عليها أيضًا التَّوفيقُ بين هذه الأداةِ وأهدافِها الاقتصاديَّةِ الخاصَّة. ويتطلَّب تنظيمُ الأشياءِ المُتَّصلة أيضًا بذلَ جهدٍ من الأفرادِ في احترامِ حقوقِهم ومبادراتِهم وسلوكِهم النَّشط.

ثالثًا: الأخلاقُ في خدمةِ تنظيمِ الأشياءِ المُتَّصلة:

l'Ethique au service de la régulation des objets connectés:

يبدو أن الأخلاق تتمتَّعُ بشرعيَّةٍ متجدِّدةٍ عندما يتعلَّقُ الأمرُ بتنظيمِ الأشياءِ المُتَّصلة، وهذه الأشياءُ الموجودةُ في السُّوق هي جزءٌ من نظامٍ تنظيميٍّ معقَّد، حيث يكملُ القانونُ والأخلاق بعضهما البعض، وممَّا لا شكَّ فيه ما زال الأمرُ غير واضحٍ؛ لأنَّ الأخلاقَ فكرةٌ غامضةٌ نسبيًّا.

ولذلك، سوف نسعى إلى دراسةِ السَّببِ الذي يجعلُ الأخلاقَ فعالةً حقًّا من أجلِ استكمالِ التَّنظيمِ المتعلِّق بالبياناتِ الشَّخصيَّة، ولقد تمَّ اتِّخاذُ قواعدِ الأخلاقِ؛ لوضع حدودٍ أخرى على استغلالِ البياناتِ الشَّخصيَّة. وسرعان ما أصبحت الأشياءُ المُتَّصلةُ موضوعًا لاضطرابٍ معياريٍّ بين القواعدِ القانونيَّةِ والمبادئ الأخلاقيَّة. وانتهى الأمرُ بالسُّوقِ إلى ظهورِ معاييرَ أخلاقيَّةٍ جديدةٍ لتنظيمِ هذه التِّكنولوجيا، بعد ملاحظةِ عدم كفايةِ القواعدِ التنظيميَّةِ الحاليَّة.

الفرع الثالث

الفجواتُ (الثَّغرات) التنظيميَّةُ للتِّكنولوجيا المتطوِّرة

Les lacunes de la réglementation d'une technologie évolutive

من المعلوم أن العالمَ الرقميَّ يقوم بطرحِ تقنيَّاتٍ جديدةٍ دون إعطاء أيّ إطارٍ قانونيٍّ مُحددٍ لها، وهذا هو الحالُ مع الكائنِ المتَّصلِ. وبالتالي تُتيحُ لنا هذه الملاحظةُ أن نشهدَ حالاتِ عدم التَّوافقِ الفنيّ بين احتياجاتِ تشغيلِ الأجهزةِ المُتَّصلة والإطار القانونيّ المنظِّم لها.

(ISSN: 2537- 0758)

أولًا: الأشياءُ المُتَّصلة، تقنيةٌ متعددةُ الأوجهِ تحت اختبارِ الأنظمة:

الأشياءُ المُتَّصلةُ تقنيَّةٌ قادرةٌ على جمعِ وتحليلِ وتنفيذِ الخدمة، فهي جزءٌ من بيئةٍ أكبر، وهي بيئةُ إنترنتّ الأشياء.

١- إشكاليَّةُ تشغيلِ الشَّيءِ المتَّصلِ المجهَّز بالذَّكاءِ الاصطناعيّ:

ممَّا لا شكَّ أن الشَّيءَ المتَّصلَ موجودٌ ومنتشرٌ في جميعِ المجالات، كالرِّياضةِ مع السَّاعةِ المُتَّصلة، ومجال التَّشغيلِ الآليّ للمنزل، والصِّحةِ مع الأساورِ المُتَّصلة، أو مِسبحةٍ متَّصلة[٨٨]. ويُصنِّف المؤلِّفُ الكنديُّ ألكسندر بلورد هذه الأشياءَ إلى خمسِ فئاتٍ رئيسةٍ: السَّياراتُ، والتِّقنيَّاتُ القابلةُ للارتداء، وأنظمةُ التَّشغيلِ الآليّ للمنزل، والأجهزةُ المنزليَّة، المساعداتُ الصوتيَّة.

ويرجع هذا النَّجاحُ أيضًا إلى سلوكِ الشَّيءِ وجمع المعلوماتِ عن مُستخدميه؛ لفهمِها، ويُمكن تعريفُ هذه التقنيَّةِ وفقًا لما قدَّمته CNIL[٨٩] "بكونِها الأشياءَ المجهزةَ بوسائلِ اتِّصالٍ سلكيَّة أو لاسلكيَّة". ومن جانبنا نؤكِّد أنَّ هذه التقنيَّةَ تُشير إلى: الأشياء التي تلتقطُ البياناتِ وتخزِّنها وتُعالجها وتنقلُها، والتي يُمكنها تلقِّي التَّعليماتِ وإعطاؤها وبالتَّالي لديها القدرةُ على الاتِّصالِ بشبكةِ معلوماتٍ[٩٠].

وتتكوَّنُ برامجُ التَّحليلِ هذه عمومًا من خوارزمياتِ الذَّكاءِ الاصطناعيّ. ويُمكن تعريفُ الخوارزميَّةِ بأنه: سلسلةٌ محدودةٌ لا لبسَ فيها من التَّعليماتِ التي تمكن من الحصولِ على نتيجةٍ من البياناتِ المقدَّمة كمُدخلات، لكنَّ الخوارزميَّةَ المجهَّزةَ بالذَّكاءِ الاصطناعيّ لها تعريفاتٌ عديدةٌ، لا سيَّما بسببِ طابعِها التقنيّ للغايةِ و"الأكثر تعقيدًا للغايةِ من الخوارزميَّةِ الكلاسيكيَّة".

---

(88) Radio Canada, "Le Vatican lance un chapelet intelligent pour encourager les jeunes à prier", Radio canada, 18 octobre 2019, en ligne: (consulté le 13/08/2020).

(89) CNIL, «Objets connectés: n'oubliez pas de les sécuriser!» (04 décembre 2017), en ligne: < https://www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser> (consulté 12/05/2020).

(90) Arnaud de Baynast, op. cit, p.212.

وإذا كان مصطلحُ الذَّكاءِ الاصطناعيّ قد تمَّت صياغتُه لأوَّل مرَّةٍ من قبل John McCarthy وMarvin Lee Minsky، فإنَّ أوَّلَ برنامجٍ للذَّكاءِ الاصطناعيّ يُنسَب إلى Alan Turing. ومنذ ذلك الحين، استمرَّ مفهومُ الذَّكاءِ الاصطناعيّ في التطوُّر(٩١)، حيث تحظى هذه التِّكنولوجيا الثوريَّةُ بشعبيَّةٍ كبيرةٍ لعدَّة سنوات، وهي تُشكِّل في الواقعِ "السَّبب في تطوُّرِ الأشياءِ المُتَّصلة".

وممَّا لا شكَّ فيه أنَّ قدرةَ الذَّكاءِ الاصطناعيّ على الاقترابِ من الذَّكاءِ البشريّ من خلالِ تقليدِ قدراتِهِ المعرفيَّة، تجعل الشّيءَ المتَّصلَ مختلفًا تمامًا عن الملحقاتِ الرقميَّةِ الكلاسيكيَّةِ الموجودة في السُّوق، كما لديه القدرةُ على جمعِ البياناتِ وتحليلها وتفسيرها، وبالتَّالي التنبُّؤ بسلوكِ المستخدمِ أو توقُّعه. وأصبحتْ هذه المجموعةُ ممكنةً بفضلِ أجهزةِ الاستشعارِ التي تمَّ تجهيزُ الأشياءِ بها، وهذا يعني أن برنامجَ الذَّكاءِ الاصطناعيّ ينفذ ويتَّخذ قرارًا بشأنِ الإجراءِ الذي طلبَهُ المستخدم.

٢- الشَّيءُ المتَّصلُ مصدرٌ لمسؤوليَّاتٍ متعدِّدة.

L'objet connecté comme source de responsabilités multiples

إن إحدى أهم القضايا المرتبطةِ بالأشياءِ المُتَّصلةِ هي تعدُّدُ أصحابِ المصلحة. وفي الواقع، يتطلَّب مجالُ الأشياءِ المُتَّصلة الجمعَ بين مجموعةٍ من المهاراتِ في قطاعاتٍ مختلفةٍ مع عددٍ وافرٍ من الجهاتِ الفاعلةِ المشاركة في إنشاءِ الأشياءِ وتطويرها وتسويقها. ومع انتشارِ التِّقنيَّاتِ المستخدمةِ والأجهزة المُتَّصلة يزيدُ من صعوبةِ تحديدِ أدوارِ كلِّ صاحبِ مصلحةٍ ومسؤوليَّات كلٍّ منهم(٩٢).

على سبيلِ التَّوضيح، بموجبِ قانونِ لوكسمبورغ، يتمتَّعُ المشتري بعديدٍ من الضَّماناتِ في حالةِ وجودِ عيبٍ أو عدم مطابقةِ المنتج. فمن ناحيةٍ، يُمكن لأيِّ مشترٍ أن يحتجَّ بالضَّماناتِ المنصوصِ عليها في القانونِ المدنيّ (ضمان التَّسليمِ طبقًا

(91) Alexandra Bensamoun et Grégoire Loiseau, «L'IA à la mode éthique», D.2017, p, p.581.

(92) Les objets connectés d'aujourd'hui: Nouveaux défis de demain, https://www.entreprisesmagazine.com/fr/articles/les-objets-connectes-d-aujourd-hui-nouveaux-defis-de-demain.

(ISSN: 2537- 0758)

للمُواصفاتِ التعاقديَّةِ، وكذلك الضَّمانُ ضدَّ العيوبِ الخفيَّة). ومن ناحيةٍ أخرى، يُمكن للمستهلكين الاحتجاجُ بضمانِ المطابقةِ المنصوصِ عليه في قانونِ المستهلكِ في حالةِ وجودِ عيبٍ في الشَّيء، وعليه سيتمكَّن المشتريُّ المستهلكُ من اتِّخاذِ إجراءٍ ضدَّ بائعِ الشَّيءِ المتَّصل. ومع ذلك، ونظرًا لتعقيدِ السِّلسلةِ التعاقديَّةِ، فمَن الذي يُمكن للبائعِ أن يلجأَ إليه؟ الإجابةُ عن هذا السُّؤالِ ليستْ بسيطةً، وستعتمد بشكلٍ أساسٍ على العقودِ المبرمةِ بين الأطرافِ المعنيَّة.

ومن المرجَّحِ أن تنتشرَ القواعدُ القانونيَّةُ المتعدِّدة عبرَ سلسلةِ الجهاتِ الفاعلة، ولكن أيضًا تعقيد التِّكنولوجياتِ المستخدمةِ يجعلُ من الصَّعبِ تحديدَ الخطأ والضَّررِ وتوزيع المسؤوليَّات. ولذلك فمِن الضروريّ تفسيرُ هذا التَّعقيدِ تعاقديًّا بطريقةٍ واضحةٍ وشاملةٍ ومُطَمئنةٍ لجميعِ أصحابِ المصلحةِ في السِّلسلةِ التعاقديَّةِ مع ضرورةِ توزيعِ المسؤوليَّات.

٣- الشَّيءُ المتَّصلُ كفاعلٍ قانونيّ:

L'objet connecté comme acteur juridique:

يكتسب الشَّيءُ- مع إنترنتّ الأشياء- تجسيدًا جديدًا: فهو يتصرَّفُ ويتفاعل، وفي بعضِ الحالات، يُصبح شبهَ مستقلٍّ. ينشأ مفهومُ الكائنِ باعتبارِه فاعلًا قانونيًّا، دون أن يمنحَه الأهليَّةَ القانونيَّةَ[٩٣].

وفي الواقعِ، نظرًا لتصميمِ وتسويقِ الأشياءِ المُتَّصلةِ المستقلَّة بشكلٍ متزايدٍ، ولأنَّ هذه الأشياءَ تتمتَّعُ بنوعٍ من "الذَّكاء"، وإن كان مصطنعًا، ستنشأُ أسئلةٌ فيما يتعلَّقُ بالمسؤوليَّةِ وكذلك بالتَّأمين، فعلى سبيلِ المثالِ في حالةِ وقوعِ حادثٍ بواسطةِ مركَّبةٍ ذاتيَّة القيادة[٩٤]. من خلال التصرُّفِ دون سيطرةٍ بشريَّةٍ دائمةٍ، ستُصبح الأشياءُ

---

[٩٣] للمزيدِ من التَّفاصيل راجع: محمد حسن عبد الرحيم حمزة، الاعترافُ بالشخصيَّةِ القانونيَّةِ لأنظمةِ الذَّكاء الاصطناعيّ، مجلة القانون والتِّكنولوجيا، مج٣، ع٢ الجامعة البريطانيَّة- كليَّة القانون، سنة ٢٠٢٣، ص٦٦٥- ٧١٥.

[٩٤] محمد حماد مرهج الهيتي، مركباتُ الذَّكاءِ الاصطناعيّ: المنافعُ والمخاطرُ وتحدياتُ المسؤوليَّةِ الجنائيَّة عمَّا تتسبَّب به من حوادث: نظرة...، ع١٣، هيئةُ التَّشريعِ والإفتاءِ القانونيّ ٢٠٢٣ ص، ١٧- ٧٦.

جهاتٍ فاعلةً وشركاء وصنَّاع قرارٍ حقيقيّين. ولكنْ مَن سيكون المسؤولَ في حالةِ حدوثِ ضررٍ بسبب كائنٍ ذكيٍّ متَّصل؟[٩٥].

في الحقيقة كلُّ شخصٍ مسؤولٌ عن الأضرارِ النَّاجمةِ عن أفعالِه، وأيضًا عن الأشياءِ التي تقعُ تحتَ حراستِه، وفي حالةِ الشَّيء المتَّصلِ الذي يفلتُ من سيطرتنا بشكلٍ مستقلٍّ: هل سيكونُ من غير المتصوَّرِ تحميلُ الشَّيءِ نفسهِ المسؤوليَّةَ، ما دام هذا الأخيرُ لا يتمتَّعُ بشخصيَّةٍ قانونيَّة؟ وهل يُمكن أن يكونَ الشَّخصُ الذي يحتفظُ بالشَّيءِ غيرَ مسؤولٍ بشكلٍ كاملٍ عن الإجراءاتِ التي تمَّ التَّخطيطُ لها؟ وهل الشَّيءُ المتَّصلُ يُمكن مقارنتُه تمامًا بشيءٍ تحت حراستنا على الرَّغم من أنَّه يتمتَّعُ باستقلاليَّةٍ خاصَّةٍ به، يُمليها ذكاؤه الاصطناعيُّ؟

٤- الشَّيءُ المتَّصل كمصدرٍ للمعلوماتِ:

L'objet connecté comme source d'informations

هناك تحدٍ قانوني رئيسي آخر يتعلق بالوصول إلى كميات هائلة من البيانات التي يمكن للأشياءِ المُتَّصلة جمعها وتخزينها، واحتمالية إساءة استخدامها. وبما أن الاتِّصالَ بالإنترنتّ أصبح وظيفةً متكاملةً للأشياءِ اليوميَّة، فمن الضَّروريّ أن يواجه مصمِّمو ومستخدمو هذه المعدَّاتِ مخاطر الهجماتِ الإلكترونيَّة.

بالإضافةِ إلى أمانِ الشَّبكةِ التي يتَّصل بها المنتجُ نفسه، سيكونُ من المستحسنِ التعرُّف على الوظائفِ المختلفةِ للمنتجِ وإعدادات السريَّةِ الخاصَّة به. ومن المهمِّ أيضًا تنفيذُ التَّدابيرِ الأمنيَّةِ القياسيَّة لتكنولوجيا المعلومات، وذلك من خلالِ تحديثِ البرامجِ بانتظامٍ، وإنشاء كلماتِ مرورٍ قويَّة، وما إلى ذلك[٩٦].

ثانيا: خصوصيَّةُ خوارزميَّةِ الذَّكاءِ الاصطناعيِّ:

إنَّ نجاحَ الشَّيءِ المتَّصلِ يعتمدُ على استقلاليَّته، وغياب التدخُّل البشريّ لتنفيذِ الخدمةِ المطلوبة. وهذه الخاصيَّةُ هي التي تجعلُ إطارَه القانونيَّ معقدًا بشكلٍ خاصّ،

(95) Les objets connectés d'aujourd'hui: Nouveaux défis de demain, https://www.entreprisesmagazine.com/fr/articles/les-objets-connectes-d-aujourd-hui-nouveaux-defis-de-demain.

(96) Les objets connectés d'aujourd'hui، op. cit.

(ISSN: 2537- 0758)

والسِّمةُ المعقَّدةُ الثانية للذَّكاء الاصطناعيّ تعتمدُ على تقنيَّاتِ التعلُّم المغروسة فيه. فالذَّكاء الاصطناعيُّ عبارةٌ عن خوارزميَّةٍ تمَّ تكوينُها من خلالِ "التَّعليماتِ التي سيتمُّ تنفيذُها، والتي لم تعُدْ مبرمجةً بشكلٍ صريحٍ من قِبل مطوِّرٍ بشريٍّ، بل يتمُّ إنشاؤُها في الواقع بواسطةِ الآلةِ نفسها، والتي "تتعلم" من البياناتِ المقدَّمة لها"، حيث تتعلَّم خوارزميات التعلُّمِ الآليّ من خلالِ التَّدريب، وبشكلٍ أكثرَ دقَّةً من خلالِ التَّكرارِ[٩٧].

ولقد تمَّ إعادةُ إطلاقِ هذه التقنيَّةِ من قِبل باحثين كنديِّين في العقدِ الأوَّل من القرن الحادي والعشرين، وأبرزُهم المتخصِّص Yoshua Bengio الذي حصل على جائزةِ تورينج من جمعيَّةِ آلاتِ الحوسبة، إلى جانب Yann Le Cun et Geoffrey Hinton في عام ٢٠١٨. ويُمكن القولُ بعباراتٍ بسيطةٍ: يسمح التعلُّم العميقُ للخوارزميَّةِ لتتعلَّم من تلقاءِ نفسِها. وفي الوقتِ الحاليّ، يعدُّ هذا نهجًا خاضعًا للإشراف، ويتطلَّب بشكلٍ خاصٍّ الكثيرَ من البياناتِ للسَّماحِ لخوارزميَّةِ الذَّكاء الاصطناعيّ بالعملِ بشكلٍ مستقلٍّ دون تدخُّلٍ بشريٍّ.

وتُثير مسألةُ تشغيلِ الشَّيءِ المتَّصلِ من خلال الذَّكاءِ الاصطناعيّ باستخدامِ طريقةِ التعلُّمِ الآليّ عديدًا من المشكلاتِ القانونيَّة. سنختارُ مسألتين تبدوان أساسيَّتين بالنِّسبةِ لنا في ضوءِ مشكلتنا العامَّة: التعلُّم الآليُّ الذي يتضمَّن تلقِّي كميَّةٍ كبيرةٍ جدًّا من البيانات، وعمليَّة الذَّكاءِ الاصطناعيّ الغامضة التي يصعُبُ تفسيرُ نتيجتها.

١- صعوبةُ إنشاءِ خوارزميَّةٍ متعلِّمةٍ تلقائيًّا، والذَّكاء الاصطناعي

أ- إمداداتٌ ضخمةٌ من البيانات:

يتمُّ جمعُ كميَّةٍ كبيرةٍ من البياناتِ من خلالِ الأشياءِ المُتَّصلة، سواءٌ كانت بياناتٍ شخصيَّةً أو غيرها، وتعدُّ هذه العمليَّةُ ضروريَّةً؛ لأنَّ إنشاءَ الارتباطاتِ بواسطةِ برنامج الذَّكاء الاصطناعيّ يتطلَّب تدريبًا كبيرًا، والذي يعتمدُ على عددِ البياناتِ المجمعة، وبدونها لن يتمكَّن الكائنُ المتَّصل من العملِ بشكلٍ صحيحٍ[٩٨]، وهذا أيضًا

(97) Mathilde Bondu, Ethique et objets connectés, Maîtrise en droit, Université Laval, Québec, Canada et Université Paris-Saclay Cachan, France Mathilde Bondu, 2020, p. 19.

(98) Alexandre Plourde, «Retour vers le futur: l'Internet des objets et la protection de la vie privée», Volume 465- Développements récents en

أحد الشُّروطِ الثلاثةِ لارتفاع قوَّة الذَّكاءِ الاصطناعيّ داخل الأجهزةِ المُتَّصلةِ وفقًا لجوسلين ماكلور وماري نويل سان بيير والتي تتمثَّل في "التعلُّم الآلي، وزيادة قوَّةِ الحوسبةِ، وتوافر البياناتِ الرقميَّة"(٩٩).

كما أنَّ تعزيزَ الذَّكاءِ الاصطناعيّ يأتي على حسابِ فائدته، كما يؤكِّد المبدأ: "إن جمعَ البياناتِ ومعالجتها على نطاقٍ واسعٍ هو جوهرُ الروبوتات الذكيَّة: فالتعلُّمُ بهذه الطَّريقةِ يتطلَّب كميَّةً كبيرةً من البياناتِ"(١٠٠)، ولكي يتمَّ تكييفُها مع المستخدمين يتحتَّمُ أن تَعرف هذه الآلاتُ مُستخدمَها، من خلال البياناتِ التي يدعمُها بها، لتكونَ قادرةً على تخصيصِ التَّبادل(١٠١). ونتيجةً لذلك، ينقل الشَّيءُ المتَّصل كميَّةً كبيرة من البيانات، سواءٌ كانت مهنيَّةً أو شخصيَّةً أو غير ذلك، والتي غالبًا ما تكونُ استخدامُاتها غير معروفةٍ، ناهيك عن أن هذه البياناتِ تحتفظُ بها الشَّركات(١٠٢).

لذلك يُمكننا أن نقارنَ ظاهرةَ البياناتِ الضَّخمة، أو المعلومات الكبيرة، التي يستقيها الويب والشَّبكات الاجتماعيَّةُ والبياناتُ التي تتلقَّاها الأجهزةُ المُتَّصلة، فهي بالفعل فكرةٌ غامضةٌ إلى حدٍّ ما، وتعدُّ بشكلٍ عامٍّ متعدِّدةَ الأشكال. وقد يكون المفهومُ البسيطُ لهذا الأمرِ هو وجود كميَّةٍ هائلةٍ من المعلوماتِ التي من المُستحيل إدارتُها

droit à la vie privée, JuriBistro eDoctrine, 2019, en ligne: <https://edoctrine.caij.qc.ca/developpements-recents/465/369051330/> (consulté le 12/05/2020).

(99) «Le machine learning, l'augmentation de la puissance de calcul, et la disponibilité des données numériques»

Jocelyn Maclure et Marie-Noëlle Saint-Pierre, «Le nouvel âge de l'intelligence artificielle: une synthèse des enjeux éthiques», Les Cahiers de propriété intellectuelle, octobre 2018, n°3, p.747.

(100) «la collecte massive et le traitement de données sont de l'essence même des robots intelligents: l'apprentissage est à ce prix […], il nécessite une grande masse de données»

Alexandra Bensamoun et Grégoire Loiseau, «L'intégration de l'intelligence artificielle dans certains droits spéciaux», Dalloz IP/IT 2017, p.295.

(101) Stéphane Grumbach et Stéphane Frénot, «Tribune- Vers un principe de précaution numérique?», Le Monde, 15 avril 2013, en ligne: (consulté le 13/07/2020).

(102) Mathilde Bondu, Ethique et objets connectéso, op cit p. 21.

(ISSN: 2537- 0758)

باستخدامِ الأدواتِ التقليديَّة، أو أن الشَّركاتِ غير قادرةٍ لإدارة كميَّةٍ هائلةٍ من البيانات. وتأخذ هذه المقارنةُ معناها الكاملَ عندما ندركُ أن كميَّةَ المعلوماتِ المتوفِّرة عن شخصٍ ما من خلالِ الاستخدامِ الوحيدِ لجهازِه هائلة، ممَّا يوفِّر قوَّةً مذهلةً للشَّركات.

ولهذا يثورُ التَّساؤلُ إلى أيّ مدى يُمكن للشَّركاتِ استغلال بياناتِ الأشخاصِ؟ ومن ناحيةٍ أخرى، هل من الممكن أن نتساءلَ عن طرقِ تدريبِ الذَّكاءِ الاصطناعيّ دون الوصولِ إلى مصدرٍ مهمٍّ للمعلوماتِ من بياناتِ الأفراد؟ وهذا ما يؤكِّده Bensamoun وLoiseau : التعلُّم من البشرِ هو في المقام الأوَّل تعلُّم عن البشر. وفي هذا السِّياق، سيُطلب من الروبوت الذكيّ أن يتغذَّى على البياناتِ الشَّخصيَّة، أو حتى البياناتِ الحساسةِ(١٠٣)، وهو ما يتردَّد صداه بشكلٍ خاصّ عندما نتحدَّثُ عن الأشياءِ المُتَّصلة، وهي التِّكنولوجيا الأقربُ للأفراد. وفي هذا الصَّددِ نُشير إلى الأزمةِ الصِّحيةِ عام ٢٠٢٠م، حيث إنَّ بعضَ الصَّحفيين أثاروا أنَّ الذَّكاء الاصطناعيَّ لا يُمكِنه العملُ على القضايا المرتبطةِ بـ COVID-19 لأنه لا توجدُ بياناتٌ كافيةٌ.

وبالتَّالي فإنَّها نفسُ المشكلةِ التي تشتركُ فيها الأشياءُ المُتَّصلةُ مع ظاهرةِ البياناتِ الضَّخمة، وفي الواقع أن التَّحدي الأولَ الذي يواجه المُشرِّعَ فيما يتعلَّق بالأشياءِ المُتَّصلةِ **هو التَّوفيقُ بين مبدأ الإشراف على البياناتِ الشَّخصيَّةِ المجمَّعة، والمبدأ المعاكس له، وهو الحاجةُ إلى البياناتِ للقيامِ بالأعمالِ التِّجاريَّة.** ويُسلِّط هذا التَّوازنُ الضَّوءَ على مفارقةِ الإطار القانونيّ للكائن المتَّصل، وهو كائنٌ تقنيٌّ، بموجب القانون، وفي هذا الشَّأن يطرحُ مكتبُ مفوضِ الخصوصيَّةِ الكنديّ تساؤلًا يدورُ حول كيفيَّةِ حمايةِ نظامٍ ذكيٍّ مجهَّزٍ بعدَّة نقاطِ اتِّصالٍ وأجهزة استشعارٍ دون التَّأثيرِ عليه في الاستخدام؟(١٠٤).

(103) «apprendre de l'humain, c'est donc d'abord apprendre l'humain. Dans ce cadre, le robot intelligent sera amené à se nourrir de données à caractère personnel, voire de données sensibles Alexandra Bensamoun et Grégoire Loiseau, op. cit, p.295.

(104) Commissariat à la protection de la vie privée du Canada, «La protection de la vie privée pour tous: Hier, c'était déjà demain… L'Internet des objets l'impératif d'un cadre approprié pour la sécurité de l'information et la protection de la vie privée; Commentaires au Rendez-vous de la sécurité de l'information (RSI) 2014» (07 mai 2014), en ligne:

وفي واقعِ الأمرِ هذه الصُّعوباتُ المرتبطةُ بحجم البياناتِ وكميَّتها لا يُعالجها قانونُ البياناتِ الشَّخصيَّة حقًّا، بل يتمُّ وضعُها في إطارِ مبادئ التَّقليلِ أو التَّناسب، والتي غالبًا ما يعتمدُ تطبيقُها على أخلاقياتٍ معينةٍ للشَّركات، والتي يُطلب منها في الوقتِ ذاتهِ الاستمرار في الابتكار. وجديرٌ بالذِّكر يركز التَّشريعُ الحاليُّ على حمايةِ الفردِ من خلالِ العملِ على تقليل وتناسب المعلومات، وهذا الفكرُ يتناقضُ مع منطقِ الذَّكاءِ الاصطناعيّ، والذي يتطلَّب استخدامَ قدرٍ كبيرٍ من المعلومات.

وفي هذا الشَّأن نشيرُ إلى وجهةِ نظرِ مكتبِ مفوِّض الخصوصيَّة الكنديّ في سياقِ إصلاحِ قوانين المعلوماتِ الشَّخصيَّةِ التي تؤكِّد وفقًا لتقييمِها الخاصّ أن قانونَ حمايةِ المعلوماتِ الشَّخصيَّة والوثائق الإلكترونيَّة التي ترتكزُ على مبدأ تقييدِ جمعِ المعلومات، قد يتعارضُ مع الوظائفِ الأساسيَّةِ لأنظمةِ الذَّكاء الاصطناعيّ، ويُمكن أن يؤدِّيَ إلى انخفاضِ جودةِ النَّتائجِ وفائدتها(١٠٥).

وهذه المفارقة الشَّديدةُ بين القانونِ والتِّكنولوجيا الرقميَّةِ ليست الوحيدةَ، كما أنَّ الذَّكاءَ الاصطناعيَّ أمامه تحدٍّ آخرُ يصعُبُ على المُشرِّعِ تحديدُه.

ب- مبدأ غموضِ الأنظمةِ الخوارزميَّة

Le principe d'opacité des systèmes algorithmiques

تتميزُ الأشياءُ المُتَّصلةُ بالخصائصِ الرئيسةِ لأنظمةِ الذَّكاء الاصطناعيّ التي تميِّزها عن أنظمةِ البرمجيَّاتِ التقليديَّةِ الأكثر بساطةً؛ نظرًا لقدرةِ الذَّكاءِ الاصطناعيّ على الاستدلال، وتُشير هذه القدرةُ على الاستدلالِ إلى عمليَّةِ الحصولِ على المخرجات، مثل التنبُّؤاتِ أو التَّوصياتِ أو القرارات، والتي يُمكن أن تؤثِّر على البيئاتِ الماديَّةِ والافتراضيَّة، فضلًا عن قدرةِ أنظمةِ الذَّكاء الاصطناعيّ على استنباطِ النَّماذج أو الخوارزميَّات، أو كليهما، من المُدخلاتِ أو البيانات. وتشملُ التِّقنيَّات التي

---

https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2014/sp-d_20140507_dc/

(105) Commissariat à la protection de la vie privée du Canada, «Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'IA», 13 mars, 2020, en ligne: < https://priv.gc.ca/fr/a-propos-ducommissariat/ce-que-nous-faisons/consultations/consultation-ai/pos_ai_202001/> (consulté le 13/07/2020).

(ISSN: 2537- 0758)

تمكن الاستدلال أثناء بناء نظام الذَّكاء الاصطناعي مناهج التعلم الآلي التي تتعلَّمُ من البياناتِ كيفيَّةَ تحقيقِ أهدافٍ معيَّنةٍ، والمناهج القائمة على المنطقِ والمعرفةِ التي تستنتجُ من المعرفةِ المشفَّرة أو التَّمثيل الرَّمزي للمهمَّةِ المراد حلُّها. كما تتجاوزُ قدرةُ أنظمةِ الذَّكاء الاصطناعيّ للعمل بمستوياتٍ متفاوتةٍ من الاستقلاليَّة، ممَّا يعني أنها تتمتَّعُ بدرجةٍ معينةٍ من الاستقلال عن التدخُّل البشريّ وقدرتها على العملِ دون تدخُّلٍ بشريٍّ.

وتُشير القدرةُ على التَّكيُّفِ التي يُمكن أن يُظهِرُها نظامُ الذَّكاء الاصطناعيّ إلى قدراتِ التعلُّم الذاتيّ، ممَّا يسمحُ للنِّظامِ بالتَّغييرِ أثناء الاستخدام، ويمكن استخدامُ أنظمةِ الذَّكاء الاصطناعيّ بشكلٍ مستقلٍّ أو كمكوّنٍ من مكوّناتِ المنتج، بغضّ النَّظرِ عما إذا كان النِّظامُ مدمجًا فعليًّا في المنتجِ (مُضمَّنًا) أو يخدم وظيفةَ المنتجِ دون دمجهِ فيه (غير مُضمَّن).

وتعتمدُ قدرةُ الأشياءِ المُتَّصلة على التعلُّمِ بنفسها بفضلِ الذَّكاءِ الاصطناعيّ باستخدامِ برنامج التعلُّم الآليّ (مبدأ غموضِ الأنظمةِ الخوارزميَّة). ومن الصَّعب، إن لم يكن من المستحيل، شرح أسباب خوارزميَّةِ التعلُّم الذاتيّ ونتائجها. دون الإشارةِ إلى أنه ليس من الممكنِ بالضَّرورة لروَّاد الأعمالِ أن يُحدِّدوا مسبقًا المعلوماتِ التي سيتمُّ معالجتها، أي التي سيتمُّ استخدامُها فعليًّا أو المعرفة التي سيتمُّ استخلاصُها منها. وتجدر الإشارةُ إلى أنه في البرمجةِ الكلاسيكيَّة، يتمُّ استنتاجُ القواعد التي تمَّ إدخالها. كون أنَّ قواعدَ التَّشغيلِ التي تحدِّد عمليَّةَ صُنعِ القرارِ يتمُّ وضعُها بشكلٍ واقعيٍّ بواسطةِ المبرمج، لكن المنطقَ مختلفٌ تمامًا بالنِّسبةِ للذَّكاءِ الاصطناعيّ الذي يستخدمُ التعلُّم الآليَّ.

ويتكوَّن التعلُّمُ الآليُّ من "تغذيةِ الآلةِ بأمثلةٍ للمهمَّة المقترحةِ لإنجازها، وهكذا يقومُ الإنسانُ بتدريبِ النِّظامِ من خلالِ تزويدِه بالبياناتِ التي سيتعلَّم منها، ويحدِّد بنفسهِ العمليَّاتِ التي سيتمُّ تنفيذُها لإنجازِ المهمَّةِ المعنيَّةِ. وسوف يقومُ الذَّكاء الاصطناعيُّ بإجراءِ الارتباطاتِ بنفسه، ويقدِّم نتيجةً، ولكن دون إعطاءِ فكرةٍ عن المنطقِ المستخدم. وهذا الأمرُ يثيرُ الجدلَ بالنِّسبةِ للمبرمجين؛ لأنهم يفقدون القدرةَ على تفسيرِ منطقِ النَّتائجِ المنتجة.

ولهذا كيف يُمكننا إذًا تفسيرُ عمل الذَّكاءِ الاصطناعيّ ونتائجه، إذا لم نتمكَّن من تفسيرِه؟ إن قابليَّةَ تفسيرِ الأنظمةِ القائمة على التعلُّمِ تُشكِّل تحدّيًا علميًّا حقيقيًّا يزيدُ من حاجتنا إلى التَّفسيرِ واهتمامنا بـ "الكفاءة".

وبالتَّالي فإنَّ هذه الصُّعوبةَ الفنيَّةَ تُثير اهتمامَ المُشرِّع، حيث تعدُّ مبادئُ الشَّفافيةِ والوضوح أساسيَّةً في سياقِ القانونِ الرقميّ، فكيف يُمكننا إذًا تلبيةُ هذه المتطلَّباتِ القانونيَّةِ إذا كانت التِّكنولوجيا لا تسمحُ بذلك؟ صحيحٌ أن هناك بعضَ الالتزاماتِ القانونيَّة التي يُمكن تحقيقُها، منها على سبيل المثال: يتعيَّن على المصمِّمين إعطاءُ معلوماتٍ عن إطارِ عملِ الخوارزميَّةِ وليس شرح أسبابِها والنَّتيجة.

كما أنَّ هذه الصُّعوبةَ تُنبِّهنا مرَّةً أخرى إلى أهميَّةِ إيجادِ طريقةٍ لتنظيمِ هذه الظَّاهرة التي تعتمدُ اليوم على الممارساتِ الأخلاقيَّةِ من قبل الشَّركاتِ أو السُّلطات العامَّة، على الرَّغم من استحالةِ ذلك من الناحيةِ الفنيَّةِ في الوقتِ الحاليّ، ودعونا نتخيَّلُ عدالةً مستقبليَّةً تُحقِّقها الرّوبوتات[١٠٦]: كيف يُمكننا أن نشرحَ للمُواطن اختيارَ القاضي الآليّ، وكما يُشير سيدريك فيلاني "إنَّ قابليَّةَ تفسيرِ هذه التِّقنيَّاتِ هي أحدُ شروطِ قبولِها اجتماعيًّا".

ويُوضِّح هذا الغموضُ في الأنظمةِ الخوارزميَّةِ أيضًا مشكلةً اقتصاديَّةً، فعلى سبيلِ المثالِ مع ظاهرةِ "تحسين محرّك البحث"، تسعى الجهاتُ الفاعلةُ الاقتصاديَّة إلى التَّأثيرِ على نتائج خوارزميَّةِ المنافس، لتكونَ قادرةً على توضيحِ أنَّ جوجل "لا تُعيد رمزَها العام". وإن جعل البرنامجُ شفافًا من شأنِهِ أن يؤدّيَ إلى إتاحةِ إمكانيَّةِ التَّأثيرِ على خوارزميَّةِ اتّخاذِ القرار.

وعلى ذلك فإنَّ الشَّيءَ المتَّصل المكون من الذَّكاءِ الاصطناعيّ يواجه تحدياتٍ تكنولوجيَّةٍ لا تزالُ من الصَّعبِ إدارتها؛ لذلك من الضَّروريّ النَّظر في دورِ

---

[١٠٦] للمزيد من التَّفاصيل في هذه المسألةِ راجع: محمد أحمد المعداوي عبد ربه مجاهد، المسؤوليَّةُ المدنيةُ عن الروبوتات ذات الذَّكاء الاصطناعي: دراسةٌ مقارنةٌ، المجلة القانونيَّة، مج٩، ع٢، جامعة القاهرة– كليَّة الحقوق– فرع الخرطوم، سنة، ص٢٨٣– ٣٩٢.

(ISSN: 2537- 0758)

الأخلاقيَّاتِ في تنظيمِها، دون أن ننسى أن الشَّيءَ المتَّصلَ يُواجه تحدياتٍ أخرى، أكثر تحديدًا على وجهِ الخصوص: إنترنت الأشياء.

٢- مدى تعقيدِ (غموض) الشَّيءِ المتَّصل: بيئة إنترنتّ الأشياء:

تتضاعفُ المخاطرُ التي يُمكن أن تسبّبها الأشياءُ المُتَّصلةُ فيما يتعلَّقُ بالبياناتِ الشَّخصيَّة؛ بسبب نشرِها داخل إنترنتّ الأشياء. ويُشكِّل هذا النِّظامُ البيئيُّ، الذي يُختصرُ غالبًا بمصطلحِ "IOT"، "إنترنت الأشياء"، تحدّيًا أساسيًّا جديدًا في الاقتصادِ الرقميّ[١٠٧] بسبب قدرتهِ على ربطِ الأشياءِ المُتَّصلة ببعضها البعض وإتاحة مشاركةِ بياناتها. وجدير بالذِّكر أنَّ إنترنتّ الأشياءِ هو مفهومٌ ناشئٌ منذ عام ٢٠١٠. وليس له بعدُ تعريفٌ رسميٌّ أو مشتركٌ. ويُمكننا تعريفُه تعريفًا واسعًا: مجموعة من الأشياءِ المُتَّصلةِ والاتِّصالات والإنترنت، التي تندمجُ مع موجاتِ السَّحابةِ والبيانات الضَّخمة، وبشكلٍ أكثر دقَّةً، هي شبكةٌ من الشَّبكاتِ التي تسمح، من خلالِ أنظمةِ تحديدِ الهويَّةِ الإلكترونيَّة الموحَّدة والأجهزة المحمولة اللاسلكيَّة، بالتعرُّف بشكلٍ مباشرٍ ودون لبسٍ على الكياناتِ الرقميَّةِ والأشياء الماديَّة، وبالتالي تكون قادرةً على الاسترجاعِ والتَّخزينِ والنَّقل والمعالجة، دون انقطاعٍ بين العالم الماديّ والافتراضيّ، والبيانات ذات الصِّلة[١٠٨].

وبالتالي فإن الشَّيءَ المتَّصلَ قادرٌ على التَّواصلِ مع البيئةِ المحيطةِ به، ويُمكن التحكُّمُ فيه عن بعدٍ عبر الجهازِ الداخليّ. وتتميَّزُ هذه البيئةُ بخاصيَّتين تُضيفان درجةً إضافيَّةً من الصُّعوبةِ للمشرِّع.

(107) Gérard Haas, Amanda Dubarry, Marie D'Auvergne, Rachel Ruimy, «Enjeux et réalités juridiques des Objets, Connectés», Dalloz IP/IT 2016, p.394.

(108) Pierre-Jean Benghozi, Sylvain Bureau et Françoise Massit-Folléa, L'internet des objets– Quels enjeux pour l'Europe, Paris, Éditions de la Maison des sciences de l'homme, 2019, p.15-24.

الخاصيَّة الأولى: الارتباطُ مع إنترنتّ الأشياء:

إن إنترنت الأشياءِ هو "تغييرٌ حقيقيٌّ في نطاقِ الأشياءِ المُتَّصلةِ"[١٠٩]، وبما أنَّ إنترنت الأشياءِ يسمحُ بربطِ الأشياءِ معًا، فإنَّ عددَ البياناتِ التي تمَّ جمعُها ومشاركتها يتضاعفُ يومًا تلو الآخر. وتَعدُّ السُّلطاتُ العامَّة هذا النِّظامَ البيئيَّ أيضًا وسيلةً لتلبيةِ توقُّعاتِ المجتمعِ والمواطنين، ويتمُّ تضمينُ جميع المعلوماتِ التي تمَّ جمْعُها بواسطةِ الأشياءِ المُتَّصلة في عمليَّةٍ أكبر، بحيث تتميَّزُ بتنوُّعِ التِّقنيَّاتِ المتبادلة مع بعضِها البعض: الأشياء المُتَّصلة، والشَّبكات، والسَّحابة، والبيانات الضَّخمة، وتجد هذه الكائناتُ نفسَها غنيَّةً بالبيانات، وبالتالي يُمكن تحسينُها بشكلٍ متزايدٍ، دون تدخُّلٍ بشريٍّ من خلال إنشاءِ تدفُّقات بياناتٍ جديدةٍ nouveaux flux de données[١١٠].

ومن خلالِ هذا التَّرابطِ ينشأ عديدٌ من المشكلاتِ المعروفةِ حول الأشياءِ المُتَّصلة، والتي تتضاعفُ بشكلٍ مستمرٍ، فكيف يُمكن حمايةُ بياناتِ المستخدم إذا تمَّت مشاركةُ البياناتِ بسهولةٍ؟ وكيف يُمكن تحقيقُ الأمن؟

وفي الشَّأن ذاته يطرحُ مكتبُ مفوّض الخصوصيَّةِ في كندا هذا السُّؤال: "مع انتشارِ إنترنتّ الأشياءِ في كلّ مكانٍ، كيف يُمكننا ضمانُ حمايةِ هذه الأنظمةِ بشكلٍ مناسبٍ؟[١١١]. وبالتَّالي فإنَّ حوكمةَ إنترنت الأشياء تمثِّل أيضًا تحدّيًا كبيرًا تصدَّت له أوروبا على وجهِ الخصوصِ من خلال المشاريعِ المختلفةِ[١١٢]، حيث تتعلَّقُ الأفكارُ

(109) Laura Marino, «To be or not to be connected: ces objets connectés qui nous espionnent, A propos des téléviseurs LG», Recueil Dalloz 2014.p.29

(110) Mathilde Bondu, Ethique et objets connectés, op. cit, 2020, p. 27.

(111) Commissariat à la protection de la vie privée du Canada, «La protection de la vie privée pour tous: Hier, c'était déjà demain… L'Internet des objets: l'impératif d'un cadre approprié pour la sécurité de l'information et la protection de la vie privée; Commentaires au Rendez-vous de la sécurité de l'information (RSI) 2014» (07 mai 2014), en ligne: < https://www.priv.gc.ca/fr/no+637uvelles-du-commissariat/allocutions/2014/sp-d_20140507_dc/> (consulté le 12/05/2020).

(112) Voir pour plus d'informations sur le projet, en ligne: https://cordis.europa.eu/about/fr.

(ISSN: 2537- 0758)

المختلفةُ لهذه المشاريعِ حول إنترنتّ الأشياءِ والقانون وكيفيَّة ضمانِ التَّكاملِ المستمرّ لهذه التِّكنولوجيا في إطارٍ قانونيٍّ متماسكٍ، بحيث يكون للأخلاقِ مكانتُها الكاملةُ لإثارةِ المناقشاتِ والمعايير.

وفي الواقعِ يتطلَّب التطوُّرُ السَّريعُ لإنترنتّ الأشياءِ مناقشاتٍ متجدّدةً حول حوكمةِ هذه التِّكنولوجيا، لا سيَّما عندما تكون تقنيَّةُ 5G على عتبةِ مُجتمعنا.

الخاصيَّة الثانية: ظهور 5G وخطرُ فقدانِ السَّيطرة:

يشهدُ مجتمعنا ثورةً كبيرةً، والتي يُسمِّيها Me Bensoussan المرحلةَ الرَّابعةَ من ثورةِ الأشياءِ المُتَّصلة، بعد ترابطِها داخلَ إنترنتّ الأشياء، وفي الحقيقةِ إنَّ مصمِّمي الكائناتِ المُتَّصلةِ مُهْتمون جدًّا بتقنيَّة 5G؛ لأنَّ هذه التقنيَّةَ ستوفِّر سرعاتٍ أقوى وأسرعَ بكثيرٍ من 4G، ممَّا سيعملُ على تسريعِ اتِّصالِ الأشياءِ وزيادة حجمِ البياناتِ المجمَّعة بشكلٍ كبيرٍ(١١٣).

وهذا الابتكارُ، اخترق السُّوقَ بشكلٍ كبيرٍ، حيث تضاعفت المخاطرُ المحيطةُ بالبيانات. وأصبحت عمليَّاتُ النقلِ بين الشَّيءِ المتَّصلِ وشبكة الإنترنتّ أكثر تعقيدًا وأكثر تنوُّعًا، إضافةً إلى ذلك زاد حجمُ البياناتِ المشتركةِ بشكلٍ هائلٍ، والتي تزايَدَ معه المخاطرُ الأَمنيَّة، وفي هذا الصَّددِ ذكر المؤلِّف الكنديُّ ألكسندر بلورد أنَّ مِن بين جميعِ القضايا المتعلِّقةِ بحمايةِ الخصوصيَّةِ التي تُثيرها إنترنت الأشياء، يظلُّ الأمنُ السيبرانيُّ هو الأكثرَ واقعيَّةً والأكثرَ إثارةً للقلق. وإذا ركَّزنا على المخاطرِ المتعلِّقةِ بكميَّةِ البيانات، فإنَّ هذا المكسبَ في الإنتاجيَّةِ يُمكن أن يُسهِّل عمليَّةَ جمعٍ أكثر تعمُّقًا للبيانات، والتي يُمكننا من خلالها استنتاجُ زيادةٍ كبيرةٍ في كميَّةِ المعلوماتِ عن المُستخدمين. وفي الشَّأن كتبت مجلة (Forbes): إنَّ القفزةَ إلى الأمامِ التي يُمثِّلها الانتقالُ إلى الجيلِ الخامس ستجبر الشَّركاتِ على تبنِّي استراتيجيَّةٍ أكثر عالميَّةً لإدارة البيانات(١١٤). وهذا سباقٌ تكنولوجيٌّ حقيقيٌّ، ينطوي على مخاطرَ هائلةٍ تتطلَّب بالضَّرورةِ تدخُّلَ الأخلاقِ قبل وأثناء وحتى بعدَ سَنِّ معاييرِ القانونِ المنظَّم.

(113) Alain Bensoussan et Frédéric Forster, Droit des objets connectés et télécoms, Edition Bruylant, 2017.

(114) Xavier Guérin, «Comment La 5G Va Affecter La Gestion Des Données», Forbes, 28 juin 2019, en ligne: <

ويُشكِّل الشَّيءُ المتَّصل تحدِّيًا تكنولوجيًا معقدًا وبشكلٍ خاصٍ للمشرِّع. كما أنَّ الاستخدامَ المشتركَ للذَّكاء الاصطناعيّ وبيئة إنترنتّ الأشياء، التي تسارعَتْ بفضلِ شبكةِ الجيل الخامس، يجعلُ مسألةَ وضعِ تشريعٍ مناسبٍ أمرًا يصعُبُ تحقيقُه نوعًا ما. ويثير مفوضيَّة حمايةِ الحياة الخاصَّةِ في كندا هذا الأمرَ بقولها: لكي يظلَّ هذا الإطارُ مناسبًا وفعَّالًا، يجبُ أن يؤخذَ بالضَّرورةِ في الاعتبارِ الجانبُ التِّكنولوجيُّ والمترابطُ والعالميُّ لإنترنت الأشياء(١١٥). ويرى جانبٌ من الفقهِ أنه ينبغي سنُّ الإطارِ القانونيّ المناسبِ على أساسِ التِّكنولوجيا الأساسيَّة، ويُفضَّل أن يكونَ ذلك من قِبل مُشرِّعٍ دوليٍّ وباستخدام الأدواتِ التي طوَّرَها القِطاعُ الخاصُّ(١١٦).

وفي هذا الصَّددِ يثور التَّساؤلُ عن مدى فائدةِ الأخلاقياتِ عندما تكون الأشياءُ المُتَّصلةُ خاضعةً بالفعل لإطارٍ قانونيّ للبياناتِ الشَّخصيَّة. وتجدر الإشارةُ إلى أنَّ جمعَ البياناتِ الشَّخصيَّة تخضع لإطارٍ قانونيّ مؤطَّرٍ بالمبادئ الأخلاقيَّة، فهل قلَّل هذا الإطارُ من تأثيرِ التِّكنولوجيا الرقميَّةِ على التَّنظيمِ الفعَّالِ للأشياءِ المُتَّصلة؟

ثالثًا: تنظيمُ الأشياءِ المُتَّصلةِ وجمعُ البياناتِ الشَّخصيَّة:

في فرنسا، تحمي النُّصوصُ القانونيَّةُ الحقَّ في احترامِ الحياةِ الخاصَّة(١١٧)، فضلًا عن الأحكامِ القضائيَّةِ الصَّادرة في هذا الشَّأن، وهو حقٌّ أساسٌ منصوصٌ عليه في

---

https://www.forbes.fr/technologie/comment-la-5g-va-affecter-votre-strategie-de-gestion-des-donnees/.

(115) Commissariat à la protection de la vie privée du Canada, «La protection de la vie privée pour tous: Hier, c'était déjà demain… L'Internet des objets: l'impératif d'un cadre approprié pour la sécurité de l'information et la protection de la vie privée; Commentaires au Rendez-vous de la sécurité de l'information (RSI) 2014» (07 mai 2014), en ligne: < https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2014/sp-d_20140507_dc/>

(116) Mathilde Bondu, Ethique et objets connectés, op, cit,p. 29.

(117) Article 9 (Code civil français); Article 8 (Convention européenne des droits de l'homme, RO1974 2151, 4 novembre 1950); ou plus récemment article 7 (Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 18 décembre 2000).

(ISSN: 2537- 0758)

ميثاقِ الحقوقِ الأساسيَّةِ للاتِّحاد الأوروبيّ[١١٨]. ومع ذلك، فإنَّ حمايةَ البياناتِ الشَّخصيَّة، والتي تعدُّ عنصرًا من عناصرِ احترامِ الحياةِ الخاصَّة، تتطلَّب قانونًا أكثرَ دقَّةً. ومع تطوُّرِ العالم الرقميّ، حيث غزى مجتمعاتنا ما يُسمَّى **بـ "اقتصاد البيانات"**، والذي يتجسَّد بشكلٍ خاصّ اليوم في استخدام الأشياءِ المُتَّصلة، والذي أسهم على وجهِ الخصوصِ في جمعِ البياناتِ المتعلِّقة بالمعلوماتِ الشَّخصيَّةِ؛ ممَّا أدَّى إلى زيادةِ مخاطر انتهاكِ الخصوصيَّة. ونتيجةً لذلك، وبعد برهةٍ بسيطةٍ، تناولت أوروبا هذه القضيَّةَ وفتحت الاتفاقيَّةَ رقم ١٠٨ لحمايةِ البياناتِ الشَّخصيَّة، والتي يُعدُّ أوَّلَ صكٍّ دوليٍّ ملزمٍ قانونًا في مجالِ حمايةِ البيانات[١١٩].

---

[118] Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 18 décembre 2000.

[١١٩] تجدر الإشارة إلى أنَّ كندا لديها إطارٌ قانونيٌّ يهدف إلى التكيُّفِ مع التقنيَّاتِ الجديدةِ، مثل: الكائنات المتَّصلة، ويعدُّ الحقُّ في الخصوصيَّةِ حقًّا أساسيًّا في كندا، تحميه المادَّة ٥ من ميثاق حقوقِ الإنسانِ والحريَّاتِ في كيبيك بما في ذلك الحقُّ في حمايةِ المعلوماتِ الشخصيَّة.

وفي الحقيقةِ نرى أن سنَّ التَّشريعاتِ في كندا يكون بشكلٍ منعزلٍ عن قريبها الأوروبيّ، صحيحٌ أن قانونَ كيبيك هو في الأساسِ قانونٌ ناطقٌ بالفرنسيَّة وأكثر قانونٍ مدنيّ، ولكنْ في هذا الشَّأن نوضِّح فقط القانونين الفيدراليَّين المخصَّصين لكندا والمتَّعلقين بالمعلوماتِ الشخصيَّة. ويتجلَّى القلقُ بشأن حمايةِ هذه المعلوماتِ في التَّقريرِ الذي أعدَّته مجموعةُ الدِّراسةِ الفيدراليَّةِ المعنيَّة بالكمبيوتر والخصوصيَّة، والذي تمَّ تقديمُه في عام ١٩٧٢.

ومع مرورِ أكثر من سنةٍ من الزَّمن، تمَّ تعديلُ القانون الكنديّ بشأن حقوقِ الإنسانِ في عام ١٩٧٧ من أجل إنشاء منصبِ مفوَّضٍ لحمايةِ الحياة الخاصَّةِ في كندا، وقبل كلّ شيءٍ، إنشاء أوَّلِ بندٍ فيدراليٍّ بشأن احترامِ الحياةِ الخاصَّة. تمامًا مثل النِّظامِ الفرنسيّ، حيث تأثَّر بمثلِ هذا الإصلاحِ القطاعُ العامُّ في بادئِ هذا الأمر.

Ministère des Communications et ministère de la Justice, L'ordinateur et la vie privée: rapport du Groupe d'étude, Information Canada, Ottawa, 1972.

عند دراسةِ القانونِ الكنديّ، يجب أن نميِّزَ بين مستويَيْن: الفيدراليّ والإقليميّ. تتعلَّق القوانينُ التي سندرسُها بالقانونين الفيدراليَّين المتعلِّقين بالمعلوماتِ الشخصيَّة: قانون حمايةِ المعلوماتِ

الفصل الثاني
نحو إمكانيَّةِ وجودِ إطارٍ قانونيٍّ خاصٍّ بالأشياءِ المُتَّصلةِ

تمهيدٌ وتقسيمٌ:

في واقعِ الأمرِ ليس هناك قانونٌ خاصٌّ للأشياءِ المُتَّصلة، لذلك يهدفُ القانونُ المدنيُّ إلى تنظيمِ هذه الأشياء. ومن النَّاحيةِ العمليَّة، يتمُّ التَّمييزُ بين نوعين من المسؤوليَّةِ المدنيَّة، وهما المسؤوليَّةُ التعاقديَّةُ والمسؤوليَّةُ التقصيريَّة، وفي هذا الشَّأن تُثير الأشياءُ المُتَّصلةُ عديدًا من التَّساؤلات؛ كون أن استخدامَ الأشياءِ المُتَّصلة لا يخلو من المخاطر، فقد يكونُ الخطأُ راجعًا إلى الشَّيء المتَّصل أثناء إرسالِ التَّعليماتِ أو حتى فشل في اتِّصالِ الشَّيءِ بالشَّبكة.

وفي واقعِ الأمرِ سيُحدث هذا السُّوقُ المزدهر ثورةً في العلاقةِ بين العالمِ المادِّيّ والعالم الرقميّ. وممَّا لا شكَّ فيه أنَّ تكاثُرَ هذه الأشياءِ المُتَّصلة يثيرُ الدَّهشةَ والتَّساؤلاتِ لا سيَّما مع خاصيَّةِ التعلُّمِ الآليّ، وقدرة الذَّكاء الاصطناعيّ على تعلُّم نفسهِ، ومن المحتملِ أن تتأثَّر جميعُ جوانبِ حياتنا بالمنتجاتِ والخدماتِ الجديدة.

وإذا كانت المسؤوليَّةُ عن الفعلِ الإنسانيّ تبدو مخفَّفةً في الشَّيءِ المتَّصلِ الذي يحلُّ محلَّه أو يكمله، فهل يُمكننا حقًّا أن نقولَ عن الشَّيءِ المتَّصلِ إنَّه "مسؤولٌ عن

الشخصيَّة للقطاعِ العامّ سنة ١٩٨٥، وقانون حمايةِ المعلوماتِ الشخصيَّة والوثائق الإلكترونيَّة للقطاعِ الخاصّ لعام ٢٠٠٠.

Loi sur la protection des renseignements personnels et les documents électroniques, LPRPDE, LC 2000

تكريس ديناميكيَّةٍ تنظيميَّةٍ جديدةٍ من قِبل اللَّائحةِ العامَّة لحمايةِ البيانات (GDPR) إدراكًا للدَّورِ المركزيّ للبيانات الشخصيَّة في الاقتصادِ الحاليّ والتقدُّم التكنولوجيّ المستمر، فإنه يُفرض على المشرِّعِ ضرورةُ توفيرِ مجموعةٍ من القواعدِ القويَّة، التي يجبُ على الشَّركاتِ إثباتُ الالتزامِ بها، كما يستندُ المشرِّعُ إلى منطقِ زيادةِ مُساءلةِ الشَّركات، التي أصبحت الآن "مسؤولةً عن المعالجة" والغرض الأساسي من اللَّائحةِ العامَّةِ لحمايةِ البيانات (GDPR) هو تعزيزُ التَّطويرِ المسؤول للتِّقنياتِ التي تتعاملُ مع البياناتِ الشخصيَّةِ التي يتمُّ جمعُها بواسطة الكائناتِ المتَّصلة.

(ISSN: 2537- 0758)

أفعاله؟ أليست الثِّقةُ في إنترنت الأشياء، بل وحتى الذَّكاء الاصطناعي، موضوعًا اجتماعيًّا قبل أن يُصبحَ نقاشًا قانونيًّا؟ فهل للشَّيءِ المتَّصل دائمًا حارس؟، l'objet connecté a-t-il toujours un «gardien»؟

ومن النَّاحية القانونيَّة، يُمكن للمضرورِ أيضًا اتِّخاذ إجراءاتٍ ضدَّ الشَّركةِ المصنِّعةِ للشَّيء. ويستندُ ذلك على أساسِ المسؤوليَّةِ عن المنتجاتِ المعيبةِ وعلى هذا النَّحو، تنصُّ المادة ١٢٤٥ من القانونِ المدنيّ الفرنسيّ على أنه: "المنتجُ مسؤولٌ عن الضَّررِ النَّاجم عن عيبٍ في منتجه، سواءٌ كان مرتبطًا بعقدٍ مع المتضرّر أم لا".

ومع ذلك، فإن الشَّيءَ المتَّصلَ يتعلَّمُ ويتكيَّف مع سلوكِ مستخدمِهِ. ولذلك قد يكونُ العيبُ نتيجة أن حالةَ المعرفةِ العلميَّة في وقتِ بيع الجهازِ لم تكُنْ تسمحُ بتوقُّعِ هذا العيبِ. وفي الحقيقةِ أن الطَّبيعةَ الجوهريَّةَ لمثل هذا الشَّيء، تجعلُ تطبيقَ نصّ المادة ١٢٤٥-١٠ من القانون المدنيّ الفرنسيّ صعبًا؛ نظرًا لأنَّ الشَّركةَ المصنِّعةَ قد تعتمدُ بسهولةٍ على المادَّة ١٢٤٥-١٠ لإعفاءِ نفسِها من كلِّ المسؤوليَّة، رغم أن طبيعةَ الشَّيءِ المتَّصلِ مختلفةٌ عن الأشياءِ الأخرى.

ووفقًا لما سبق يبدو أن مسؤوليَّةَ الشَّيءِ المتَّصلِ تفلت من المستخدمِ والشَّركةِ المصنِّعة. وممَّا لا شكَّ فيه أنَّ الغموضَ القانونيَّ حقيقيٌّ، والمشروعَ الإصلاحيَّ للمسؤوليَّةِ المدنيَّةِ لا يوضِّح هذا الغموضَ الذي يُحيط بمفاهيمِ المسؤوليَّة. وحتى لو اقترحت المفوضيَّةُ الأوروبيَّةُ في عام ٢٠١٧ إنشاء وضعٍ قانونيّ خاصّ لـ"الأشخاص الإلكترونيّين" والروبوتات[١٢٠]، فإن السُّؤالَ لم يتمَّ حلُّه بعدُ، وهو غيرُ متوافقٍ حاليًّا مع انتشارِ إنترنتّ الأشياءِ في مُجتمعاتنا.

وبطبيعةِ الحال، فإنَّ موضوعَ الأشياءِ المُتَّصلة لا يزالُ في مَهْده. وحتى الآن لم تقُمْ أيُّ دولةٍ بإنشاء إطارٍ قانونيّ واضحٍ، ربَّما حتى لا يؤدّي إلى تقييدِ الإبداع، وكأنَّه إغفالٌ متعمدٌ لحين إصدار الشَّركاتِ المصنِّعة قائمةً بمسؤوليَّتها، ولهذا فإنَّ الشَّركاتِ المصنِّعةَ هي التي تتَّخذُ أحيانًا الخطوةَ الأولى، وفي هذا الشَّأن صرَّحت Google

(120) Article du Parlement Européen (Janvier 2017): http://www.europarl.europa.eu/news/fr/press-room/20170110IPR57613/robots-vers-des-regles-europeennes.

وVolvo وMercedes، على سبيلِ المثال، بأنَّها ستوافقُ على تحمُّلِ المسؤوليَّةِ القانونيَّة في وقوعِ حادثٍ بسبب سيارتِهم ذاتيَّةِ القيادة(١٢١).

وفي هذا الشَّأن نُحاول إيجادَ نظامٍ محدَّدٍ لتنظيمِ المسائلِ المتعلِّقةِ بالأشياء المُتَّصلة، وفي سبيل تحقيقِ ذلك نقسم هذا الفصلَ مبحثين، **وذلك على النَّحو التالي:**

المبحث الأول: الحمايةُ القانونيَّةُ لاستخداماتِ الأشياءِ المُتَّصلة.

المبحث الثاني: إمكانيَّةُ ظهورِ نظامٍ جديدٍ للمسؤوليَّةِ خاصٍّ بالأشياءِ المُتَّصلة.

المبحث الأول

الحمايةُ القانونيَّةُ لاستخداماتِ الأشياءِ المُتَّصلة

تمهيدٌ وتقسيمٌ:

يستدعي الشَّيءُ المتَّصلُ في المقامِ الأوَّل أفكارًا عامَّةً حول حمايةِ البياناتِ واحترام الحياةِ الخاصَّةِ والملكيَّةِ الفكريَّة، ويتطلَّب اتِّصالُ الشَّيءِ أيضًا تحليلًا محدَّدًا في قانونِ العقودِ وقانون المستهلك. ويبرزُ في هذا الشَّأن عدَّة أسئلةٍ: كيف يتمُّ إبرامُ العقدِ متعلِّقًا باستخدام الشَّيءِ المتَّصل؟ فضلًا عن كيفيَّةِ التأكُّد من أنَّ المستخدمَ يُعطي الموافقةَ أثناء عمليَّةِ الاتِّصال؟ وما المسؤوليَّةُ في حالةِ حدوثِ عطل؟ وما الحلُّ الذي يُمكن للمستخدمِ اللُّجوءُ إليه عندما لا يلبِّي الكائن المتَّصل توقُّعاته؟(١٢٢).

وبالتالي، هل القواعدُ القانونيَّةُ التي تحكُمُ الأشياءَ التي يقتنيها المستهلكُ ويستخدمها تتكيَّف مع الشَّيءِ المتَّصل؟ أم ينبغي أن يكونَ من المناسبِ منحُ الشَّخصيَّةِ القانونيَّةِ للأشياءِ المُتَّصلة المستقلة؟ وما التطوُّراتُ المتوقَّعةُ من إصلاحِ قانونِ المسؤوليَّةِ المدنيَّة؟(١٢٣).

---

(121) http://www.autoguide.com/auto-news/2015/10/volvo-google-and-mercedes-to-accept-responsibility-in-self-driving-car-collisions.html.

(١٢٢) قريبٌ من هذا المعنى، د. رضا إبراهيم عبد الله البيومي، الحمايةُ القانونيَّةُ من مخاطرِ الذَّكاء الاصطناعيّ: دراسةٌ تحليليَّةٌ مقارنة، المجلَّة القانونيَّة، مج١٨، ع٣، جامعة القاهرة- كليَّة الحقوق- فرع الخرطوم، سنة ٢٠٢٣، ص. ١٠٢٧- ١٠٥٤.

(١٢٣) للمزيد من التَّساؤلاتِ راجع بالتَّفصيل: مها يسري عبد اللطيف عبد اللطيف نصار، الوضعُ الذاتيُّ للذَّكاء الاصطناعيّ في القانون المدنيّ، المجلة القانونيَّة، مج٢٠، ع٢، جامعة القاهرة-

(ISSN: 2537- 0758)

جديرٌ بالذِّكر أنَّ تنوُّعَ وتطوُّرَ الأشياءِ المُتَّصلة يحدُّ من وجودِ إطارٍ قانونيٍّ محدَّدٍ في هذا المجال، وإذا ظلَّ القانونُ العامُّ هو المطبَّق على الإشكاليَّاتِ المرتبطةِ بهذه الأشياء، فمن الضَّروريّ معرفة إلى أيّ مدى يُمكن الاعتمادُ على القواعدِ العامَّة، لا سيَّما فيما يتعلَّقُ بمسائل مسؤوليَّةِ الأشياءِ المُتَّصلة والمرتبطة بالتغيُّراتِ التِّكنولوجيَّة، كما تُثير مسألةُ الأشياءِ المُتَّصلة والملكيَّة الفكريَّة عديدًا من التَّساؤلاتِ حول حمايةِ التَّصميمِ ذاته، بالإضافةِ إلى حمايةِ قاعدةِ بياناتِ الأشياءِ المُتَّصلة. فضلًا عن ماهيَّةِ المبادئِ الأساسيَّةِ المتعلِّقة بتشغيلِ الأشياءِ المُتَّصلة.

إن مسألةَ مسؤوليَّةِ الأشياءِ المُتَّصلة هي أحدُ المواضيعِ المتكرِّرة، بسبب "استقلاليَّتها" المتزايدةِ وانفجار الاستخداماتِ المرتبطةِ بالتغيُّراتِ التِّكنولوجيَّة[١٢٤]. ويعدُّ الإطارُ القانونيُّ للأشياءِ المُتَّصلةِ واسعًا بشكلٍ خاصّ، ويغطِّي جميعَ مجالاتِ القانون، بدءًا من حمايةِ البيانات الشَّخصيَّةِ وحتى الأمن السيبراني، بما في ذلك مسؤوليَّةُ المنتجِ وقانون المستهلك[١٢٥].

وهنا يَثورُ التَّساؤلُ حول ما إذا كان الإطارُ التَّشريعيُّ والتنظيميُّ الحالي متكيّفًا مع هذه القضيَّةِ أم لا، أو ما إذا كانت التَّعديلاتُ ضروريَّةً أو ممكنةً على المدى الطويل[١٢٦].

وفي مواجهةِ هذه الأسئلة، من الضَّروريّ البحث عن وجودِ إطارٍ قانونيٍّ لضمان مستوى مناسبٍ من الأمنِ والسَّلامةِ للأشياءِ المُتَّصلة ولمُستخدميها وللغير لا سيَّما

كليَّة الحقوق– فرع الخرطوم ٢٠٢٤، ص. ٨٤٣– ٨٦٢؛ محمود محمد علي محمد، مدى استيعابِ نصوصِ القانون المدنيّ لوقائع الذَّكاءِ الاصطناعيّ، دراسةٌ فقهيَّةٌ مقارنة، مجلة الشَّريعةِ والقانون، ع٤٢، جامعة الأزهر – كليَّة الشَّريعةِ والقانون بالقاهرة، ٢٠٢٣، ص١٣٠٥– ١٣٦٣.

(124) Mady Delvaux, auteure du rapport Delvaux concernant les règles de droit civil sur la robotique.

(125) Quel cadre pour la responsabilité du fait des objets connectés?,11 juin 2020, https://www-cabinetderoulez-com.translate.goog/fr/blog/2020/6/10/responsabilite-objets-connectes?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

(١٢٦) للمزيد من التَّفاصيل راجع: د. محمد فتحي محمد إبراهيم، التَّنظيم التشريعيُّ لتطبيقاتِ الذَّكاء الاصطناعيّ، مجلة البحوث القانونيَّة والاقتصاديَّة، ع ٨١، جامعة المنصورة– كليَّة الحقوق، سنة ٢٠٢٢، ص١٠٢٥–١١٣٧.

في ظلِّ قواعدَ محدَّدةٍ تنطبق على الأشياءِ المُتَّصلة. ومع ذلك، ليس من الضروريِّ سنُّ تشريعاتٍ بشأن جميعِ التطوُّراتِ الجديدة، وفي هذا الشَّأن نقسم هذا المبحثَ مطلبين، **وذلك على النَّحو التَّالي:**

المطلب الأول: تطبيقُ النُّصوصِ البديلةِ على الأشياءِ المُتَّصلةِ.

المطلب الثاني: استحداثُ أدواتٍ قانونيَّةٍ خاصَّةٍ لحماية مُستخدمي الأشياءِ المُتَّصلة.

المطلب الأول
تطبيقُ النُّصوصِ البديلةِ على الأشياءِ المُتَّصلةِ
L'application de textes de substitution aux objets connectés

في ظلِّ غيابِ نصوصٍ محدَّدةٍ في القانونِ الفرنسيِّ، فهناك نصوصٌ بديلةٌ يُمكن تطبيقُها على الأشياءِ المُتَّصلةِ، ولا سيَّما بعضُ أحكامِ القانونِ المدنيِّ والقوانين ذات الصِّلة.

الفرع الأول
رقابةُ اللَّجنةِ الوطنيَّةِ لحمايةِ البياناتِ الشَّخصيَّةِ والحريَّات في فرنسا CNIL

في الولاياتِ المتَّحدة، قدَّم الكونجرس مشروعَ قانونٍ يرمي إلى تحسينِ أمانِ الأجهزةِ التي تشكِّل جزءًا من إنترنتّ الأشياءِ إلى مجلسي الشُّيوخ والنوَّابِ في مارس ٢٠١٩.، حيث يرمي هذا القانونُ إلى وضعِ معاييرَ دُنْيَا لأمنِ الأشياءِ المُتَّصلة. وعلى المستوى الأوروبيِّ، اعتمد البرلمان، في ١٦ فبراير ٢٠١٧، قرارًا يتضمَّن توصياتٍ إلى المفوضيَّةِ بشأن قواعدِ القانونِ المدنيِّ المتعلِّقة بالروبوتات. ومؤخَّرًا، اعتمد الاتِّحادُ الأوروبيُّ أيضًا قرارًا جديدًا لسياسةٍ صناعيَّةٍ أوروبيَّةٍ شاملةٍ بشأن الذَّكاءِ الاصطناعيِّ والروبوتات.

علاوةً على ذلك، فإن اللَّائحةَ العامةَ لحماية البيانات (GDPR) المؤرَّخة ٢٧ أبريل ٢٠١٦، والتي تمَّ تضمينُ مبادئها في القانونِ الفرنسيِّ بموجب قانون ٢٠ يونيو ٢٠١٨[١٢٧]، كما أطلقت الحكومةُ الفرنسيَّة، في فبراير ٢٠١٧، خطَّةً تتعلَّقُ

(127) Règlement (UE) n° 2016/679, 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOUE 4 mai, n° L 119,

(ISSN: 2537- 0758)

بالاستراتيجيَّةِ الوطنيَّةِ للذَّكاء الاصطناعيّ: "France AI". وفي عام ٢٠١٨، صدرت مراسيمُ وأوامرُ تتعلَّق بفحصِ المركباتِ ذاتيَّةِ القيادةِ على الطُّرق العامَّة[١٢٨]. ونُلاحظ أنَّ معظمَ التَّدابيرِ التي اتَّخذتها السُّلطاتُ التنظيميَّةُ والتَّشريعيَّةُ هي ذات طبيعةٍ أخلاقيَّةٍ أو إداريَّة، وتقتصرُ على وصفِ قواعدِ السُّلوك[١٢٩]، مع استثناءِ اللَّائحةِ العامَّة لحمايةِ البيانات (GDPR) التي تنصُّ على جزاءاتٍ نوعًا ما دون الإشارةِ إلى مسألةِ التَّعويضِ عن الأضرار.

وسرعان ما أخذتْ CNIL هذا الموضوعَ بعينِ الاعتبارِ. وفي عام ٢٠٠٩، نشرت مقالًا عن إنترنتّ الأشياء. في هذه المقالة، ذكَّرت CNIL التَّحدِّيَّات التي تُواجه تطويرَ هذا القطاع، لكنَّها أبرزت قبل كلِّ شيءٍ لا سيَّما الحاجةُ إلى حمايةِ خصوصيَّةِ المستخدمين دائمًا من خلالِ حمايةِ بياناتِهم الشَّخصيَّة[١٣٠].

وتخضعُ البياناتُ الشَّخصيَّةُ لقانونِ حمايةِ البياناتِ الفرنسيَّة المعدَّل في عام ٢٠١٨ ليأخذَ في الاعتبارِ اللَّوائحَ الأوروبيَّةَ العامَّة لحمايةِ البيانات. ويتمُّ تعريفُ البياناتِ الشَّخصيَّة على أنَّها "أيُّ معلوماتٍ تتعلَّق بشخصٍ طبيعيٍّ محدَّدٍ أو يُمكن التعرُّف عليه" بغضِّ النَّظر عما إذا كان من الممكن التعرُّف عليه بشكلٍ مباشرٍ أو غير مباشرٍ، وتخضع بعضُ ما يُسمَّى بالبياناتِ الحسَّاسةِ مثل البياناتِ الصِّحيَّةِ لحمايةٍ مُعززةٍ.

ومع ذلك، طالما وافَقَ المستخدمُ، فهذا يجعلُ من الممكنِ السَّماح بمعالجةِ عديدٍ من البياناتِ الشَّخصيَّة، حيث ستُصبح المعالجةُ قانونيَّةً بعد الحصولِ على موافقةِ

---

transposé en droit français par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

(128) Décret n° 2018-211 du 28 mars 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques; Arrêté du 17 avril 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques.

(129) A. Bensamoun et G. Loiseau, «La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité», JCP G 2017, I, n° 1204.

(130) http://www.village-justice.com/articles/Objets-connectes-challenge-des,17 html– http://www.lesnumeriques.com/objets-connectes-securite-donnees-a1790.html-.

الشَّخص المعنيّ. وفي بعض الأحيان، تكون المعالجةُ قانونيَّةً بسبب التَّنفيذِ السَّليم للعقد، دون الحصولِ على موافقةٍ صريحةٍ من الشَّخص. وهذا هو الحالُ بالنِّسبةِ لشبكاتِ التَّواصلِ الاجتماعيّ، فبمجرَّد التَّسجيلِ فإنَّ هناك موافقةً ضمنيَّةً على تقديمِ البياناتِ الشَّخصيَّة من أجلِ إنشاءِ حسابٍ، وفي حالةِ عدم رغبةِ المستخدمِ في جمع بياناتٍ تتعلَّقُ به، فعليه الامتناع عن التَّسجيلِ نهائيًّا(١٣١).

ومع ذلك، يجب على معالجِ البياناتِ التأكُّدُ من احترامِ مبادئ اللَّائحةِ العامَّةِ لحمايةِ البيانات (مشروعيَّة المعالجة، والأساسِ القانونيّ للمعالجة، والمدَّة، والغرض، والتَّناسُب، والملاءمة). وهنا يثورُ التَّساؤل، هل يجبُ أن نتركَ الأمرَ لإنترنتّ الأشياءِ لإدارةِ نفسهِ بنفسه؟ ألا يُشكِّل ذلك مخاطرةً بحدوث ردِّ فعلٍ غير متناسبٍ، وهو الأمرُ الذي يشكِّل خطورةً كبيرةً. وفي الواقعِ يجبُ أن يسبقَ المناقشةَ القانونيَّةَ التَّفكيرُ الاستراتيجيُّ والمجتمعيُّ.

وفي هذا الشَّأنِ تمَّ فتحُ المناقشةِ على نطاقٍ واسعٍ للبحث عن الحيّزِ الذي نريدُ أن نعطيَه للأشياءِ المُتَّصلةِ في مُجتمعاتنا. وفي هذا الصَّدد، تساءلتْ CNIL في عام ٢٠١٧ عن تحديَّاتِ الخوارزميَّاتِ والذَّكاء الاصطناعيّ(١٣٢)، فكيف نسمحُ للبشرِ بالحفاظِ على السَّيطرةِ في مجتمع، حيث من المتوقَّع أن تشغلَ التِّكنولوجيا والأشياءُ المُتَّصلةُ– بلا شكٍّ– مساحةً كبيرةً فيه.

وفي خِضمّ هذا التخوُّفِ قدم CNIL كجزءٍ من مُهمَّةِ التَّفكيرِ الأخلاقيّ التي يعهدُ بها القانون لجمهوريَّةٍ رقميَّةٍ، مقترحًا بتأطيرِ مبدأين رئيسين: **الولاء (الأمانة) واليقظة.**

ويُمكن تطبيقُ هذين المبدأين بسهولةٍ على الأشياءِ المُتَّصلة، أولًا: يجبُ ألا يخونَ الشَّيءُ المتَّصلُ مستخدمَه، وللتَّخفيفِ من المسؤوليَّةِ نتيجة استخدامِ هذه التِّقنيَّاتِ الجديدة، فمن المناسبِ التَّشكيكُ بانتظامٍ في تصنيعِ واستخدامِ الجهازِ المتَّصل لتقليلِ

(131) OBJETS CONNECTES ET DONNEES PERSONNELLES,29 Sep 2022,Murielle Cahen Cabinet d'avocats Paris, https://www-murielle--cahen-fr.translate.goog/objets-connectes-et-donnees-personnelles/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

(132) Document de la CNIL consultable sur le lien suivant: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.

(ISSN: 2537- 0758)

التحيُّزِ المعرفيّ الذي قد يدفعُ البشرَ إلى وضعِ قدرٍ كبيرٍ من الثِّقة في الخوارزميَّة. وفي الواقع، الأشياءُ المُتَّصلةُ غير معصومةٍ من الخطأ وغير كاملةٍ، ولهذا يجبُ على المُستخدم أن يكونَ على درايةٍ بذلك دائمًا.

ويسمحُ هذان المبدأين (الأمانة واليقظة) بالتَّطويرِ الخاضعِ للرَّقابةِ للأشياءِ المُتَّصلة والذَّكاء الاصطناعيّ دون الحدِّ من قدراتهما من خلالِ إطارٍ قانونيٍّ مقيدٍ للغاية. ويجب دمجُ هذه المبادئ، التي تبدو نظريَّةً جدًّا للوهلةِ الأولى، عمليًّا أثناء النَّشرِ على نطاقٍ محلِّيٍّ للمشاريعِ التي تتضمَّنُ إنترنت الأشياءِ والذَّكاء الاصطناعيَّ.

وعلى هذا النَّحو، يبدو من المناسبِ إضافة رؤيةٍ عامَّةٍ لهذا التَّفكيرِ الذي قامَتْ به CNIL: وهو **مبدأُ الاستقلال**، وذلك بدلًا من توخِّي اليقظةِ، بحيث يجبُ على البشرِ أن يسعَوْا جاهدين لتعزيزِ قدرٍ معيَّنٍ من الاستقلالِ في مُواجهةِ الأشياءِ المُتَّصلةِ والذَّكاءِ الاصطناعيّ بشكلٍ عامّ. والاستقلال ليس معناه لا مبالاة، لكن الاستقلالَ يُبقي المسؤوليَّةَ ضِمن الحظيرةِ البشريَّة. وهذا يدعمُ جهدًا تدريبيًّا كبيرًا لتنبيهِ المُستخدمين إلى المخاطرِ التي تنطوي عليها هذه الأشياءُ الذكيَّة والحفاظ على مستوى إتقانِهم. وفي الواقعِ يتطلَّب تطبيقَ هذه المبادئِ الثلاثة دعم أصحابِ المصلحةِ الرَّئيسين من القطاعين العامّ والخاصّ[١٣٣]، **وذلك على النَّحو التَّالي:**

- رفعُ مستوى الوعي بهذه المبادئِ الثَّلاثةِ في جميعِ أنحاءِ سلسلةِ الأشياءِ المُتَّصلةِ، ويتحتَّمُ دعمُ السُّلطاتِ المحليَّةِ أو الشَّركاتِ الكبيرة أو الإدارات التي ترغبُ في تنفيذِ مشروعِ إنترنتّ الأشياء من البدايةِ إلى النهايةِ على المدى الطَّويلِ ومراعاة جميعِ عواملِها الخارجيَّة.
- تعزيزُ التَّفكيرِ في مسؤوليَّةِ وأخلاقيَّاتِ الأشياء المُتَّصلة داخل الشَّركاتِ والإدارات العامَّة.
- تنفيذ عملياتِ تدقيقٍ منتظمةٍ للأشياءِ المُتَّصلةِ والخوارزميات المنفِّذة والتحقُّق المنتظم من إتقانِ ونطاقِ عملِ إنترنت الأشياء من قِبل المالك، ولا يُمكن

(133) Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsable.

للتِّكنولوجيا أن تكونَ حكرًا على الآلة، ولا على المعرفةِ الجوهريَّةِ بالموضوعِ احتكارًا للمورد. ويجب أن نضعَ في اعتبارنا أن هذه التِّكنولوجيا لا تُغنينا عن الأشياءِ العاديَّة، فمثلًا ظهورُ نظامِ تحديدِ المواقع العالميّ (GPS) لم يجعل البحارةَ غير قادرين على استخدامِ البوصلة، كما أنَّ الجرَّاحَ الآليَّ لا يستطيعُ أن يحلَّ محلَّ الطَّبيب، ولا تستطيعُ السيارةُ ذاتيَّةُ القيادة إلغاءَ مدارس تعليمِ القيادة.

وفي السِّياق ذاته أشارت CNIL في دليلٍ عمليٍّ نُشر في نوفمبر ٢٠٢٠ إلى أنَّ المُساعدين الصَّوتيين المستخدمين في سياقٍ احترافيٍّ يجبُ أن يحترموا جميعَ المبادئ التي يفرضُها القانونُ العامُّ لحمايةِ البياناتِ (GDPR) لأيّ معالجةٍ للبيانات الشَّخصيَّة.

كما تقومُ CNIL بانتظامٍ بإبلاغِ المستخدمين بالمخاطرِ التي قد يتعرَّضون لها على الإنترنتّ وبحمايةِ بياناتِهم الشَّخصيَّة، ولذلك نَشرت دليلًا في عام ٢٠١٧ لتقديمِ توصياتٍ لاستخدامِ الأشياءِ المُتَّصلة. وعلى وجهِ الخصوص، تُوصِي عمومًا بما يلي(١٣٤):

التحقُّق من الاتِّصالاتِ المختلفةِ المرتبطة بالأشياءِ المُتَّصلةِ لدى المستخدمِ للتأكُّد من عدمِ اتِّصالِ أيّ شخصٍ آخر؛ مع القيامِ بتغييرِ كلماتِ المرور أو رموز PIN الخاصَّة بأجهزتهِ بانتظامٍ، وعدم الاحتفاظِ أبدًا بتلك المقدَّمة افتراضيًّا؛ مع التأكُّدِ من أنَّ الهواتفَ والأجهزةَ اللوحيَّة الخاصَّة به تتطلَّب كلمةَ مرورٍ لفتحها، والتأكُّد من حمايةِ شبكة WIFI بشكلٍ صحيحٍ؛ إضافةً إلى ذلك يتحتَّمُ على المستخدمِ القيامُ بتعطيلِ المشاركةِ التلقائيَّةِ للبيانات بين الأشياءِ المُتَّصلةِ وشبكاته الاجتماعيَّة إذا كانت مرتبطةً؛ كما تنبه CNIL بشأن البياناتِ الصحيَّة؛ بالإضافةِ إلى التأكُّدِ من أنَّه لا يزال بالإمكانِ الوصولُ إلى البياناتِ، ويُمكن حذفُها؛ وأخيرًا، ضرورةُ إيقافِ تشغيلِ الأشياءِ المُتَّصلةِ التي لا تستخدمُها.

وتجدر الإشارةُ إلى أنَّ CNIL تقدِّم توصياتٍ أخرى للأشياءِ المُتَّصلةِ التي تتطلَّب فتحَ حسابٍ عبر الإنترنت: منها استخدام أسماءٍ مستعارةٍ حيثما أمكن ذلك،

(134) https://www.cnil.fr/fr/assistants-vocaux-les-bons-reflexes-pour-les-professionnels.

(ISSN: 2537- 0758)

وعدم تقديمِ الهويَّةِ الحقيقيَّة؛ وإعطاء أقلِّ قدرٍ مُمكنٍ من المعلومات؛ واستخدام عناوينَ بريدٍ إلكترونيٍّ مختلفةٍ للأشياءِ المُتَّصلةِ المختلفة؛ والقيام دائمًا بتأمينِ الوصولِ إلى هذه الحساباتِ بكلماتِ مرورٍ مختلفةٍ لكلِّ شيءٍ متَّصل.

الفرع الثاني

مدى فعاليَّةِ المبادئ التي أقرَّها قانون حماية البيانات الشَّخصيَّة المصري رقم ١٥١ لسنة ٢٠٢٠ في ضوءِ تطوُّر الأشياءِ المُتَّصلة

في الحقيقةِ إنَّ عديدًا من المبادئِ التي جاء بها القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حمايةِ البياناتِ الشَّخصيَّةِ المصريِّ في الآونةِ الأخيرة، قد يصعب إنفاذُها في عديدٍ من الجوانبِ القانونيَّةِ والفنيَّة، لتعارُضِها مع الفلسفةِ التي تعملُ وفقَها خدماتُ الأشياءِ المُتَّصلة، وذلك للاعتباراتِ التي سنذكرُها خلالَ هذه الدِّراسة، وإن كان هناك جانبٌ من هذه المبادئِ يتَّفق مع الطَّبيعةِ الخاصَّة للأشياءِ المُتَّصلة، وفي هذا الشَّأن نُشير إلى جانبٍ من التَّعليقاتِ التي تدلِّل على وجودِ قصورٍ في قانونِ حمايةِ البياناتِ الشَّخصيَّةِ رقم ١٥١ لسنة ٢٠٢٠:

أولًا: **فيما يتعلَّقُ بإعمالِ مبدأِ تخصيصِ استغلالِ البيانات**:

إذا كان المُشرِّعُ المصريُّ قد أقرَّ مبدأ تخصيصِ استغلالِ البياناتِ الشَّخصيَّة في قانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حمايةِ البياناتِ الشَّخصيَّةِ، وذلك في نصِّ المادَّة الثانية بند أربعة، والتي تنصُّ على أنه: ويكونُ للشَّخصِ المعنيِّ بالبياناتِ الحقوقُ الآتية "..... تخصيصُ المعالجةِ في نطاقٍ محدَّد...." وهذا أمرٌ يُحمد للمشرِّع المصريِّ بأنه قد قيَّد من نطاقِ معالجةِ البيانات، وهو ما أكَّدته المادة مادة (٣) من القانون ذاته على أنَّه يجبُ لجمعِ البياناتِ الشَّخصيَّة ومُعالجتِها والاحتفاظِ بها، توافرُ الشُّروطِ الآتية:..... أن تعالجَ بطريقةٍ مشروعةٍ وملائمةٍ للأغراضِ التي تمَّ تجميعُها من أجلها. إلا أنَّه على الجانبِ الآخرِ جعل تخصيصَ المعالجةِ في يدِ المتحكِّم، باعتبارِه هو صاحبَ الاختصاصِ في إقرارِ مدى كفايةِ البياناتِ مع الغرضِ المحدَّد لجمعِها، وهو أمرٌ لا يُحمَد عقباه، وهو ما أشارتْ إليه المادة (٤) من القانونِ ذاته: مع مراعاةِ أحكامِ المادَّة (١٢) من هذا القانون، يلتزم المتحكِّم بما يأتي:

١- الحصولُ على البياناتِ الشَّخصيَّةِ أو تلقِّيها من الحائزِ أو من الجهاتِ المختصَّةِ

بتزويده بها بحسَبِ الأحوالِ بعد موافقةِ الشَّخصِ المعنيّ بالبيانات، أو في الأحوالِ المصرَّح بها قانونًا.

٢- التأكُّد من صحَّةِ البياناتِ الشَّخصيَّة واتِّفاقها وكفايتُها مع الغرضِ المحدَّدِ لجمعِها.

٣- وضْعُ طريقةِ وأسلوبِ ومعاييرِ المعالجةِ طبقًا للغرضِ المحدَّد، ما لم يُقرَّر تفويضُ المعالجِ في ذلك بموجبِ تعاقُدٍ مكتوبٍ.

٤- التأكُّد من انطباقِ الغرضِ المحدد من جمعِ البياناتِ الشَّخصيَّةِ لأغراضِ مُعالجتها.

وتجدرُ الإشارةُ إلى أنَّ تشغيلَ الأشياءِ المُتَّصلة، يتطلَّب في أغلبِ الأحيانِ الحصولَ على عديدٍ من المعلوماتِ في مراحلِ تشغيلِهِ المختلفة، وبخاصَّةٍ الأشياءُ المُتَّصلةُ الذكيَّةُ والمستقلةُ التي قد تحصلُ بطريقةٍ أو بأخرى على معلوماتٍ وبياناتٍ عن مستخدمِها بشكلٍ تلقائيٍ كعاداته اليوميَّةِ دون علمهِ، ولذا يكونُ من الصَّعبِ جدًّا العملُ على تخصيصِ البياناتِ لا سيَّما في ظلِّ تشابُكِ أكثر من جهازٍ متَّصلٍ مع بعضهِ في ذات الوقت، والذي قد يختلفُ بطبعهِ عن الجهازِ الآخر، كما أن تخصيصَ المعالجةِ في نطاقٍ محدَّدٍ قد يحرِمُ المستخدمَ من الحصولِ على عديدٍ من المزايا التي يُقدِّمها هذا الشَّيء.

وفي الواقعِ ينظِّم قانونُ البياناتِ الشَّخصيَّة نظمَ المعلوماتيَّةِ التقليديَّة، والتي ينطبقُ فيها الغرضُ المحدَّد من جمعِ البياناتِ الشَّخصيَّةِ لأغراضِ مُعالجتها، لكنَّ النَّاظرَ بدقَّةٍ إلى طبيعةِ عملِ الأشياء المُتَّصلة يجدُ أن عمليَّةَ نشرِ البياناتِ التي تمَّ جمعُها وتخزينُها يحتاجُ إلى عنايةٍ خاصَّة، وذلك نظرًا لكونها تعتمدُ على دمجِ البياناتِ التي تمَّ جمعُها؛ لاستغلالِ خدماتٍ أخرى مجاورةٍ، غير الخدمةِ التي تمَّ تجميعُ البياناتِ بسببها. وتجدرُ الإشارةُ إلى أنَّ هناك مخاوفَ من أنَّ القانونَ قد لا يكونُ كافيًا لحمايةِ البياناتِ بشكلٍ فعَّال، خاصةً في ظلِّ التطوُّراتِ السَّريعةِ في تكنولوجيا المعلومات.

ثانيا: الإشارةُ إلى مسألةِ إخفاءِ الهويَّة، وإغفال الإشارةِ إلى استخدامِ آليَّةِ تشفيرِ البيانات.

في واقعِ الأمرِ لم يعرف المُشرِّعُ المصريُّ آليَّةَ التَّشفيرِ بغرضِ إخفاءِ البيانات، خلافًا للتَّشريعِ الإماراتيّ على سبيلِ المثالِ الذي عرفها بأنها "التقنيَّةُ التي يتمُّ من

(ISSN: 2537- 0758)

خلالها معالجةُ البياناتِ الشَّخصيَّة للمستخدمِ على نحوٍ لا يتيحُ فرصةَ التتبُّعِ والرَّبط، وتنسيب هذه البياناتِ بصاحبها، من دون استخدامِ معلوماتٍ إضافيَّةٍ وإنساب هذه البياناتِ بصاحبها، من دون استخدامِ معلوماتٍ إضافيَّة[١٣٥]".

وممَّا لا شكَّ فيه أنَّ آليَّةَ تشفير البياناتِ المعالجة التي يتمُّ إجراؤها على البياناتِ الشَّخصيَّةِ في غايةِ الأهميَّة؛ كون أنها تؤدّي بعد إتمامِ المعالجةِ إلى عدمِ إمكانيَّةِ ربطِ وتنسيبِ هذه البياناتِ بصاحبِ البياناتِ دون استخدامِ معلوماتٍ إضافيَّة، شريطةَ أن تكونَ تلك المعلوماتُ الإضافيَّةُ محفوظةً بشكلٍ مستقلٍّ وآمن، ووفقًا للتَّدابيرِ والإجراءاتِ التقنيَّةِ والتنظيميَّة المحدَّدة، وذلك لضمانِ عدمِ ارتباطِ البياناتِ الشَّخصيَّة إلى شخصٍ طبيعيٍّ محدَّدٍ أو يُمكن التعرُّف عليه من خلالِها[١٣٦].

وتجدرُ الإشارةُ إلى أنَّ آليَّةَ إخفاءِ الهويَّة يقصدُ بها المعالجةُ التي يتمُّ إجراؤها على البياناتِ الشَّخصيَّةِ بطريقةٍ تؤدّي إلى إخفاءِ هويَّةِ صاحبِ البيانات وعدم ربطِ وتنسيب هذه البياناتِ به وعدم إمكانيَّةِ التعرُّف عليه بأيِّ طريقةٍ كانت.

وإن كان المُشرِّعُ المصريُّ في القانون رقم ١٥١ لسنة ٢٠٢٠ بشأنِ حمايةِ البياناتِ الشَّخصيَّةِ قد أشار إلي مسألةِ إخفاءِ الهويَّة، وذلك في نصِّ المادة ٤ من القانون سالفِ الإشارةِ إليه[١٣٧]، إلا أنه لم يُشِر إلى آليَّةِ تشفيرِ البياناتِ، وهو أمرٌ يجعل البياناتِ المجمَّعة في نطاقِ الأشياءِ المُتَّصلة في خطرٍ دائمٍ لا سيَّما وأن تشغيلَ هذه الأشياءِ يتطلَّب عددًا ضخمًا من البياناتِ المجمَّعة، ولهذا نرى بأنه يجبُ على المُشرِّعِ المصريِّ أن يجمعَ بين آليتين، وهما آليَّةُ تشفيرِ البياناتِ، وآليَّةُ إخفاءِ

---

[١٣٥] المادة (١) من مرسوم بقانونٍ اتِّحاديٍّ رقم (٤٥) لسنة ٢٠٢١ بشأن حمايةِ البياناتِ الشخصيَّة (الإماراتي).

[١٣٦] د. بشار طلال المومني، د. معمر طرية، التَّحدياتُ القانونيَّةُ المعاصرةُ لاستخداماتِ "إنترنت الأشياء"، مرجع سابق، ص٣٠٣.

[١٣٧] المادة (٤) من القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حمايةِ البياناتِ الشخصيَّة، مع مراعاةِ أحكامِ المادَّة (١٢) من هذا القانون، يلتزمُ المتحكم بما يأتي:

١.....

٧- محو البياناتِ الشخصيَّةِ لديه فورَ انقضاءِ الغرضِ المحدَّدِ منها، أما في حال الاحتفاظِ بها لأيِّ سببٍ من الأسبابِ المشروعةِ بعد انتهاء الغرض، فيجب ألا تبقى في صورةٍ تسمحُ بتحديدِ الشَّخصِ المعنيِّ بالبيانات.....".

الهويَّة، مع ضرورةِ أن يكونَ لدى المستخدمِ صلاحية تشفيرِ البيانات، بالإضافةِ إلى الآليَّاتِ الأخرى التي نصَّ عليها المُشرِّعُ في قانونِ حمايةِ البيانات الشَّخصيَّة، وهي التَّصحيحُ أو التَّعديلُ أو المحوُ أو الإضافةُ أو التَّحديثُ للبيانات الشَّخصيَّة.

كما أنه إذا كان المُشرِّعُ المصريُّ قد ألزم المتحكِّمَ في البياناتِ بضرورةِ القيامِ باتِّخاذ جميعِ الإجراءاتِ التقنيَّةِ والتنظيميَّةِ وتطبيق المعاييرِ القياسيَّةِ اللَّازمةِ لحمايةِ البياناتِ الشَّخصيَّةِ وتأمينها، فضلًا عن حمايةِ وتأمين عمليَّةِ المعالجةِ والوسائط والأجهزة الإلكترونيَّة المستخدمة في ذلك وما عليها من بياناتٍ شخصيَّة، إلا أنَّ حمايةَ السِّريةِ تواجه إشكاليَّةً لا سيما في ظلِّ الاستخداماتِ المتطوِّرةِ للأشياءِ المُتَّصلةِ، فالتَّحدِّي الأكبرُ الذي يواجه مبدأ الحفاظِ على سريَّةِ بياناتِ المستخدم لخدماتِ الأشياءِ المُتَّصلة يتمثَّل في التَّشخيصِ الآليِّ والتلقائيِّ الذي تقوم به هذه الخدمةُ من تلقاءِ نفسها، باستخدامِ أجهزةِ الاستشعار.

ولهذا نقترحُ وضْعَ سياساتٍ تنظيميَّةٍ، وذلك فيما يتعلَّقُ بخدماتِ إنترنتّ الأشياء، بحيث يتحتَّمُ على كلِّ مُزودٍ بخدماتِ إنترنت الأشياء ضرورة استخدامِ معيارٍ تشفيريٍّ يجعل المستخدمَ هو صاحبَ القرارِ الأساسيِّ فيه، وذلك من خلالِ العملِ على تطويرِ وتحديثِ التِّكنولوجيا المستخدمة في مجال التَّشفيرِ واخفاء المعلوماتِ؛ كي تتناسبَ مع تطوُّرِ الأشياءِ المُتَّصلة.

ثالثًا: إغفالُ الإشارةِ إلى المعالجةِ المؤتمتة:

لم يُشِر المُشرِّعُ المصريُّ في قانون حمايةِ البياناتِ الشَّخصيَّة رقم ١٥١ لسنة ٢٠٢٠ إلى مسألةِ المعالجةِ المؤتمتة، وكيفيَّة حمايةِ البياناتِ الشَّخصيَّة في ظلِّ ظهورِ وتطوُّرِ هذه الآلية، وتُعرف المعالجةُ المؤتمنةُ بأنها المعالجةُ التي تتمُّ باستخدامِ برنامجٍ أو نظامٍ إلكترونيٍّ، يعمل بطريقةٍ آليَّةٍ وتلقائيَّةٍ إما بشكلٍ مستقلٍّ كليًّا دون أيِّ تدخُّلٍ بشريٍّ أو بشكلٍ جزئيٍّ بإشرافٍ وتدخُّلٍ بشريٍّ محدودٍ.

فلم تعُدْ معالجةُ البياناتِ تتمُّ بطريقةٍ تقليديَّةٍ تقتصر على مجرَّد جمعِ البياناتِ أو تخزينها في قواعد بياناتٍ أو أنظمةِ إدارةِ بياناتٍ آمنةٍ؛ لضمان سهولةِ الوصولِ إليها لاحقًا، أو تحليلها، بل أصبحت المعالجةُ تتمُّ من خلالِ أنظمةِ الحوسبةِ والتِّكنولوجيا، حيث تُستخدم البرمجياتُ والأنظمةُ الآليَّة لجمعِ وتحليلِ البيانات؛ ممَّا يُقلِّل من الحاجةِ إلى تدخُّلٍ بشريٍّ. حيث تتميَّزُ بمعالجةِ كمياتٍ ضخمةٍ من البياناتِ في وقتٍ قصيرٍ،

(ISSN: 2537- 0758)

كما أنَّ المعالجةَ المؤتمتةَ تستخدمُ أدوات تحليلٍ متقدِّمة، مثل التعلُّمِ الآليّ وتحليل البياناتِ الكبيرة، لتوفير رؤًى أكثر عمقًا بسرعة(١٣٨).

وفي الحقيقةِ إنَّ الأنظمةَ المؤتمتةَ معقَّدة، ممَّا يتطلَّبُ خبرةً فنيَّةً متخصِّصةً لتطويرها وصيانتها، كما أنَّ زيادةَ الاعتمادِ على الأنظمةِ الآليَّة يُمكن أن يجعلَ البياناتِ عرضةً للاختراقاتِ أو الهجماتِ السيبرانيَّة. بالإضافةِ إلى فقدان التحكُّمِ البشريّ، حيث إنَّ الاعتمادَ الزَّائدَ على الأنظمةِ الآليَّة قد يؤدِّي إلى فقدانِ القدرةِ على التدخُّل اليدويّ في الحالاتِ الطَّارئةِ أو غير المتوقَّعة، ولهذا سيكون من الصَّعبِ التكيفُ مع التَّغييراتِ المفاجئةِ في التَّعاملِ مع المواقفِ التي تتطلَّب فهمًا بشريًّا أو قراراتٍ معقَّدة. والأدهى من ذلك أنه في حالةِ حدوثِ أعطالٍ تقنيَّة، قد تتوقَّفُ العملياتُ بشكلٍ كاملٍ، ممَّا يؤثِّر على الإنتاجيَّة. كما قد تقومُ هذه الأشياءُ بالتَّحليل السطحيّ، فقد لا تستطيعُ الأنظمةُ المؤتمتة دائمًا فهمَ السِّياقِ أو العواطف المرتبطة بالبيانات؛ ممَّا قد يؤدِّي إلى استنتاجاتٍ غير دقيقةٍ.

وتجدر الإشارةُ إلى أن التطوُّرَ في استخداماتِ الأشياءِ المُتَّصلة أظهر لنا ما يسمَّى بالتَّنميطِ وهو شكلٌ من أشكالِ المعالجةِ المؤتمتة، بحيث تتضمَّن استخدامَ البياناتِ الشَّخصيَّة لتقييمِ جوانبَ شخصيَّةٍ معيَّنةٍ ومرتبطةٍ بصاحبِ البيانات، ومن بينها تعليلُ أو توقُّعُ الجوانبِ المتعلِّقة بأدائهِ أو وضعهِ الماليّ، أو صحَّتهِ أو تفضيلاتهِ الشَّخصيَّةِ أو اهتماماتهِ أو سلوكهِ أو مكانهِ أو تحرُّكاتهِ أو موثوقيَّته، وهو أمرٌ في غايةِ الخطورةِ لم يُشِر إليه المُشرِّعُ المصريُّ.

رابعا: صعوبةُ رقابةِ مركزِ حمايةِ البياناتِ الشَّخصيَّة المصريِّ في ظلِّ التطورِ الهائلِ للأشياءِ المُتَّصلة.

تعبِّر بعضُ الآراءِ عن قلقِها من أنَّ الرَّقابةَ الحكوميَّةَ قد تتداخلُ مع حقوقِ الأفرادِ في الخصوصيَّة، ممَّا قد يؤدِّي إلى استخدامِ البياناتِ الشَّخصيَّة لأغراضٍ غير مصرَّحٍ بها. كما قد تواجهُ الشَّركاتُ الصغيرةُ والمتوسطةُ صعوباتٍ في الامتثالِ لمتطلَّباتِ القانون؛ ممَّا قد يُؤثِّر سلبًا على نموِّها.

---

(١٣٨) د. بشار طلال المومني، د. معمر طرية، التَّحدياتُ القانونيَّةُ المعاصرةُ لاستخداماتِ "إنترنت الأشياء"، مرجع سابق، ص٣٠٤.

ولقد واجه مركزُ حمايةِ البياناتِ الشَّخصيَّةِ المصريُّ عدَّة صعوباتٍ في رقابةِ الأشياء المُتَّصلة، حيث إنه مع تتعدُّدِ الأجهزةِ والتَّطبيقاتِ المُتَّصلة لا سيَّما المزوَّدةُ بأنظمةِ الذَّكاءِ الاصطناعيّ، يجعل من الصَّعبِ تتبُّع جميعها وفهم خصائصِ كلّ جهازٍ، وهذا التنوُّعُ يعقدُ عمليَّةَ وضعِ معاييرَ موحَّدة للحماية، لا سيَّما في ظلّ قلَّةِ الوعي بأهميَّةِ حمايةِ البيانات الشَّخصيَّة لدى المستخدمين والمطورين، حيث يؤدِّي ذلك الأمرُ إلى استخدامِ أجهزةٍ غير آمنةٍ أو عدم اتِّباع بروتوكولاتِ الأمانِ المناسبة.

كما أنه يتطلَّب العملُ مع أجهزة IoT تبادلَ البياناتِ بين مختلفِ الأطراف، وبخاصَّةٍ البياناتُ عابرةُ الحدود؛ ممَّا يُصعِّب مراقبةَ كيفيَّةِ استخدامِ البياناتِ وحمايتها، وبخاصَّةٍ في ظلّ وجودِ تشريعاتٍ غير كاملةٍ للتَّعامل مع التَّحدِّيَات الجديدة التي تطرحُها التِّقنيَّاتُ الحديثةُ، والتي قد يصعب على مركزِ حمايةِ البياناتِ الشَّخصيَّة مواكبتها وتطبيق معايير فعَّالة.

الفرع الثالث
أمنُ البياناتِ الشَّخصيَّة
Sécurisation des données personnelles

في واقعِ الأمرِ إنَّ أمنَ البياناتِ هو العاملُ الآخر الذي يؤثِّر على ثقةِ المستخدمين، سواءٌ كانوا أفرادًا أو محترفين. وفي الواقع، فإن مشتري الأشياء المُتَّصلة، على الرَّغم من قلقِهم من استخدامِ بياناتِهم من قِبل المشغِّل الذي يسمحون له بجمعِ البياناتِ، إلا أنَّهم أكثرُ حذرًا تُجاه الأطرافِ الثالثةِ وخاصَّةً عندما يتعلَّقُ الأمرُ بالقرصنة. ومن ناحيةٍ أخرى، يتعلَّق الأمانُ بمسألةِ الاحتفاظِ بالبيانات، وممَّا لا شكَّ فيه تعدُّ هذه المسألةُ هي المشكلةَ الأكثرَ عموميَّةً المرتبطة بالبياناتِ الضَّخمةِ (استضافة البيانات).

أولًا: **الأمنُ النسبيُّ** (**Une sécurité relative**):

عندما نتحدَّثُ عن الأشياءِ المُتَّصلةِ، فإنَّنا نتحدَّثُ عن الأشياءِ التي تستخدم شبكاتِ الاتِّصالاتِ لتشغيلها (بما في ذلك الشَّبكاتُ اللاسلكيَّة). ومع ذلك، لا تحتوي الأشياءُ المُتَّصلةُ بالضَّرورةِ على برامج مكافحةِ فيروسات أو برامج حمايةٍ مماثلةٍ لتلك المجهَّزةِ بأجهزةِ الكمبيوتر. وبالتَّالي، فإن سوقَ الأشياءِ المُتَّصلة يُصبح ساحةً ضخمةً للمتسلِّلين أو غيرهم من مُجْرمي الإنترنت.

(ISSN: 2537- 0758)

ومن الصَّعبِ حاليًّا تحديد جميعِ الهجماتِ التي تتمُّ على الأشياءِ المُتَّصلةِ أو عبرها. ومع ذلك، فمن السَّهل أن نتصوَّرَ ما يُمكن أن تكونَ عليه الهجماتُ المستقبليَّةُ وعواقبها، وهي أمورٌ تعكِّر صفْوَ راحةِ المستخدم، فعلى سبيل المثال، قدَّمت صحيفةُ واشنطن بوست فرضيَّةً مثيرةً للاهتمام مفادُها أن غسالةَ الصُّحون مخترقةٌ، وهذا الأمر من شأنهِ أن يغمرَ الماءُ منزلَ المستخدم(١٣٩).

والنَّاظر للوهلةِ الأولى إلى فرضيَّةِ اختراقِ غسالةِ الأطباق أو الثَّلاجة، قد يرى بأنه الأمرُ ليس بالأهميَّة، ولكن عندما نفكِّر في الأمر، يُمكن أن يكونَ لهذه الأنواعِ من الهجماتِ عواقبُ وخيمةٌ على كلٍّ من المستهلكِ والشَّركةِ المصنِّعة، وفي عام ٢٠١٢، خلال مؤتمرٍ لعلماءِ الكمبيوتر، تمكَّن بارنابي جاك، خبير أمن تكنولوجيا المعلومات في شركة IO Active، من التحكُّمِ عن بعدٍ في جهاز تنظيمِ ضرباتِ القلب. وفي عام ٢٠١٣، أظهر خبراء آخرون في تكنولوجيا المعلومات أنَّه من الممكنِ إلغاءُ تنشيطِ مكابح السَّيارةِ الكهربائيَّةِ عن بُعدٍ(١٤٠).

وفي الحقيقةِ يتعرَّض المصنِّعون أيضًا لمخاطرَ يجبُ عليهم حماية أنفسِهم منها. دعُونَا نتخيَّل أنه يُمكن تحويلُ شيءٍ متَّصلٍ إلى أداةٍ حقيقيَّةٍ للمنافسةِ غير العادلة، فقد يُؤدِّي إلى خطأٍ بسيطٍ أو هجومٍ واسع النِّطاق على العناصرِ المُتَّصلةِ من نفسِ العلامةِ التِّجاريَّةِ إلى الإضرارِ بشكلٍ خطيرٍ بصورة الشَّركة. ويُمكننا بعد ذلك أن نتخيَّل هجماتٍ جديدةً تهدف إلى تحييدِ المنافسةِ.

ثانيا: المعالجةُ المتَّسقةُ للبياناتِ الشَّخصيَّة:

Un traitement conséquent des données personnelles:

تصبح الحاجةُ إلى معالجةٍ متَّسقةٍ للبياناتِ الشسخصيَّةِ أكثر وضوحًا؛ نظرًا للطَّبيعةِ التي تكتسبها هذه الأشياءُ الصَّغيرةُ التي تحسب درجةَ حرارةِ الجسم، أو معدَّلِ ضربات القلب، أو ضغط الدَّم. ووفقًا لـ CNIL، فإنَّ هذه الأشياءَ تتأرجَحُ

(139) DIANE MULLENEX, Les objets connectés: une législation déconnectée de l'avenir industriel?, 29 AVRIL 2014, https://www-lemondedudroit-fr.translate.goog/decryptages/8744-les-objets-connectes-une-legislation-deconnectee-de-lavenir-industriel.html?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

(140) DIANE MULLENEX, Les objets connectés: une législation déconnectée de l'avenir industriel?, op. cit.

بين الرَّفاهيةِ والصِّحة، وتعتمدُ على جمعِ ومعالجةِ ما يُسمَّى بالبياناتِ "الحساسة" وهنا نتساءلُ عن عواقبِ إبلاغِها لأطرافٍ ثالثة، مثل شركاتِ التَّأمين.

بالإضافةِ إلى البياناتِ السَّابقةِ، هناك بياناتٌ أخرى، حتى لو لم تكُنْ "مصنفةً على أنَّها بياناتٌ حساسة"، يجب أن تكونَ أيضًا موضعَ اهتمامٍ وثيق، ولا سيَّما البياناتُ التي تؤدِّي إلى تحديدِ الموقعِ الجغرافيّ للأفراد. وفي الواقع، فإن بعضَ التَّطبيقاتِ المدمجة في السَّياراتِ أو عدادات الكهرباءِ أو حتى فرشاة الأسنان البسيطة تجعلُ من الممكنِ معرفةَ مكانِ تواجُدِ الفرد، وخاصَّةً معرفة أنه ليس في المنزل. وقد تكونُ هذه المعلوماتُ– في حالةِ اختلاسِها– مفيدةً جدًّا لمُجرمي الإنترنتّ أو غيرهم من الأشخاصِ الضارّين[١٤١].

ثالثًا: الحمايةُ الضروريَّةُ (الأمن الضَّروريُّ):

Une nécessaire sécurisation:

يجبُ على الشَّركاتِ المصنِّعةِ بالضَّرورة النَّظر في القضايا الأمنيَّةِ لصالحِ المستخدمين ومصلحتهم الخاصَّة (حماية المُستخدمين) وتتمُّ هذه الحمايةُ من خلال المنتج، وإن كان هذا أمرًا نادرَ الحدوثِ نوعًا ما.

والواقعُ أنَّ تركيزَ الاستثماراتِ على إنتاجِ منتجٍ "استهلاكيٍّ" من المُمكن أن يدفعَ الشَّركاتِ المصنِّعةَ إلى تنحيةِ المسائلِ المتعلِّقةِ بالسَّلامةِ جانبًا. وفي حالاتٍ أخرى، قد يرتبطُ هذا الإهمالُ بنقص الوعي بالالتزاماتِ التَّنظيميَّةِ المتعلِّقة بالبياناتِ الشَّخصيَّة. ومع ذلك، فإنَّ نهجَ "الخصوصية بحسب التَّصميم" من شأنه أن يوفِّر للمصنِّعين قدرًا أكبرَ من اليقينِ القانونيّ، ويُقلِّل التَّكاليفَ التي يواجهونها. ولضمان تطويرِ هذا السُّوق، يجبُ علينا مرَّةً أخرى إيجادُ توازُنٍ عادلٍ بين أمنِ البياناتِ وتطوير التِّقنيَّاتِ الجديدة.

ويتطلَّب التَّنفيذُ العمليُّ لهذا الذَّكاء المتَّصل إطارًا أخلاقيًّا واستراتيجيًّا، دون أن يكونَ تنظيميًّا. ويظلُّ إنترنتّ الأشياء فرصةً للشَّركاتِ والجهاتِ العامَّة والأفراد طالما أنَّ الديناميكيَّةَ جزءٌ من إرادةٍ قويَّةٍ تتفهَّم أهميَّةَ الأمر. كما أنَّ الأمانةَ واليقظةَ

(141) DIANE MULLENEX, Les objets connectés: une législation déconnectée de l'avenir industriel? op. cit.

(ISSN: 2537- 0758)

والاستقلاليَّة، هي رؤيةٌ استراتيجيَّةٌ، تدعمُ قدرةَ هذه الإمكانات الجديدةِ المتمثِّلةِ في الأشياءِ المُتَّصلة بدلًا من أن تديرَ ظهرَها للابتكار(١٤٢).

والجديرُ بالذِّكر أنَّ ظهورَ أشياءَ متَّصلةٍ "ذكية" يُمكنها اتِّخاذ القراراتِ بشكلٍ مستقلٍّ، ودون اللُّجوء إلى التدخُّلِ البشريّ من المرجح، أن يثيرَ تساؤلاتٍ حول شرائع قانونِ العقودِ، ويُثير سلسلةً من الإشكاليَّات: أولًا، فيما يتعلَّقُ بشرعيَّةِ العقدِ وموافقة الأطرافِ، في حين أنَّ الشَّيءَ المتَّصلَ أو الروبوت المتَّصل ليس له شخصيَّةٌ اعتباريَّةٌ، ثانيًا: فيما يتعلَّقُ بتقديرِ المسؤوليَّاتِ في حالةِ الضَّررِ وتحديد أو توزيع حجمِ المسؤوليَّةِ المتكبَّدة، ثالثًا: بشأنِ شروطِ إصلاحِ الضَّررِ النَّاتج عن جسمٍ متَّصل.

ووفقًا للقانونِ الفرنسيّ، لا يوجد إطارٌ قانونيٌّ محدَّدٌ ينطبق على المسؤوليَّةِ الناشئةِ عن الأشياء المُتَّصلةِ أو الروبوتات المُتَّصلة، الأمرُ الذي يتطلَّب الإشارةَ إلى آليَّاتِ المسؤوليَّةِ التعاقديَّةِ وغير التعاقديَّةِ المعمول بها، ولا سيَّما من خلالِ الأحكامِ المتعلِّقةِ بالمنتجاتِ المَعيبةِ أو حراسة الأشياء، وهذا ما سيوضَّح في المبحثِ الثاني من هذه الدِّراسة.

علاوةً على ذلك، تجدُرُ الإشارةُ إلى أنه لا يوجدُ نصٌّ محدَّدٌ بشأنِ المسؤوليَّةِ عن الأشياء المُتَّصلة، وفي هذا الشَّأن فإنَّ التَّقريرَ البرلمانيَّ المقدَّم من Corinne Erhel وde Laure de la Raudière بتاريخ ١٥ يناير ٢٠١٧ لا يقترح التدخُّلَ التَّشريعيَّ(١٤٣). وهو ما يُمكن تفسيرُه كدليلٍ على أن الإطارَ القانونيَّ الفرنسيَّ لا يُشكِّل عائقًا أمام نشرِ سوقِ الأشياءِ المُتَّصلة اليوم.

وبنفس الطريقة، أكَّد قرارُ مجلسِ الشُّيوخ الفرنسيّ بشأنِ تنظيمِ الأشياءِ المُتَّصلةِ وتطوير إنترنت الأشياء في أوروبا بتاريخ ٢٢ مايو ٢٠١٨ لأوَّل مرَّةٍ على الحاجةِ إلى صناعةِ سياسةٍ أوروبيَّةٍ لدعم تطويرِ إنترنتّ الأشياء. قبل النَّظرِ في بعضِ الجوانبِ القانونيَّة. وعلى هذا النَّحو، تمَّ ذكرُ قانونِ المستهلكِ وحماية البياناتِ فقط كنقاطٍ تتطلَّب نظرةً قانونيَّةً جديدةً(١٤٤).

---

(142) Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsable.

(143) http://www.assemblee-nationale.fr/14/rap-info/i4362.asp#P586_152431.

(144) Quel cadre pour la responsabilité du fait des objets connectés?,11 juin 2020, https://www-cabinetderoulez-

الفرع الرابع
الأشياءُ المُتَّصلةُ وقانونُ حمايةِ المستهلك

من الواضحِ أن مسألةَ المسؤوليَّةِ عن الأشياءِ المُتَّصلةِ تحظى باهتمامِ قانونِ المستهلك، كما أشارت التَّقاريرُ البرلمانيَّةُ المذكورة أعلاه. وفي هذا الصَّدد، يجبُ التَّأكيدُ على أنَّ عديدًا من الأدواتِ الحاليَّةِ تجعلُ من الممكنِ بالفعلِ تلبيةَ متطلَّباتِ الحماية.

ويتطلَّبُ الالتزامُ بالمعلوماتِ قبل التَّعاقدِ من المحترفِ بموجب نصِّ المادة ١١١٢-١ من القانونِ المدنيِّ الفرنسيِّ أن ينقلَ إلى المستهلكِ سلسلةً من المعلوماتِ وخاصَّةً حول "الخصائص الأساسيَّة للسِّلعة" المشار إليها في المادَّة L. 111-1، 1° من قانونِ حمايةِ المستهلك. وبالنِّسبة لجمعيَّةِ UFC Que Choisir، تعدُّ أيُّ معالجةٍ للبياناتِ الشَّخصيَّةِ عند استخدامِ شيءٍ متَّصلٍ جزءًا لا يتجزَّأ من عملها، وبالتَّالي تشكِّل سمةً أساسيَّةً لهذا النَّوعِ من المنتجات. وعلى هذا النَّحو، رفعت هذه الجمعيَّةُ دعوى قضائيَّةً ضدَّ FNAC وأمازون لعدمِ امتثالهما الواضحِ لالتزاماتهما المتعلِّقة بالمعلوماتِ قبل التَّعاقدِ فيما يتعلَّقُ بالأشياءِ المُتَّصلة، وكذلك الإخلالُ بالالتزامِ بالمشورةِ على أساسِ ممارساتِ بعض الأمورِ التِّجاريَّةِ المضلِّلة[١٤٥].

بالإضافةِ إلى الالتزامِ بالمعلوماتِ قبل التَّعاقدِ الواقعِ على عاتقِ البائع، يتمتَّعُ المستهلكُ أيضًا بإمكانيَّةِ الدِّفاعِ عن نفسهِ ضدَّ البنودِ غير العادلةِ من خلالِ المادَّتين L.212-1 وL.212-2 من قانون المستهلكِ الفرنسيِّ اللَّتين تنصَّان على أنَّ أيَّ شرطٍ غير متوازنٍ بين حقوقِ والتزاماتِ الأطراف، في العقدِ بين محترفٍ ومستهلكٍ (أو غير محترفٍ) باطل[١٤٦].

---

com.translate.goog/fr/blog/2020/6/10/responsabilite-objets-connectes?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

(145) Connected objects, UFC-Que Choisir summons FNAC and AMAZON, Published on January 9, 2018.
https://www.quechoisir.org/action-ufc-que-choisir-objets-connectes-l-ufc-que-choisir-assigne-la-fnac-et-amazon-n50080/

(146) Article L212-1
Modification Ordonnance n°2016-131 du 10 février 2016- art. 2

(ISSN: 2537- 0758)

فعلى سبيلِ المثالِ، فإنَّ البنودَ التي بموجبها لا تحدِّد الشَّركةُ المصنِّعةُ للشَّيء المتَّصل بشكلٍ كافٍ شروطَ جمعِ ومعالجةِ البيانات أو أغراضها (فيما يتعلَّق بإيداعِ ملفَّاتِ تعريفِ الارتباطِ أو تحديد الموقعِ الجغرافيّ للمستخدمِ لأغراضِ الإعلاناتِ المستهدفة) يمكن أن تشكِّل شروطًا غير عادلةٍ وتعسفيَّة.

وينطبقُ الأمرُ نفسُه على البنودِ التي بموجبها لا تطلُبُ الشَّركةُ المصنِّعة موافقةَ مستخدمِ الشَّيءِ المتَّصل فيما يتعلَّقُ بالتَّحليلِ التلقائيّ للمحتوى لتقديمِ وظائفَ محدَّدةٍ للمستخدم. وفي الواقعِ لا يُمكن افتراضُ قبولِ شروطِ الاستخدامِ العامَّة التي من شأنها أن تنصَّ على نقلِ البياناتِ الشَّخصيَّة إلى أطرافٍ ثالثةٍ من خلالِ استخدامِ الشَّيء، حيث يجبُ إبلاغُ المستخدمِ على النَّحو اللَّازم، ويجب الحصولُ على موافقتهِ صراحةً[١٤٧]. وفي الحقيقةِ هناك الكثيرُ من الاحتياطاتِ التعاقديَّةِ التي لا ينبغي إهمالُها، والتي يجبُ أخذُها في الاعتبارِ في سياقِ الأشياءِ المُتَّصلة.

علاوةً على ذلك، يجبُ أيضًا التَّأكيدُ على أنَّ أحكامَ التَّوجيهِ المتعلِّقة بجوانبَ معيَّنةٍ تتعلَّقُ بعقودِ توريدِ المحتوى الرقميّ والخدمات الرقميَّة[١٤٨] قد دخلت حيِّزَ

Dans les contrats conclus entre professionnels et consommateurs, sont abusives les clauses qui ont pour objet ou pour effet de créer, au détriment du consommateur, un déséquilibre significatif entre les droits et obligations des parties au contrat.

Sans préjudice des règles d'interprétation prévues aux articles 1188, 1189, 1191 et 1192 du code civil, le caractère abusif d'une clause s'apprécie en se référant, au moment de la conclusion du contrat, à toutes les circonstances qui entourent sa conclusion, de même qu'à toutes les autres clauses du contrat. Il s'apprécie également au regard de celles contenues dans un autre contrat lorsque les deux contrats sont juridiquement liés dans leur conclusion ou leur exécution.

L'appréciation du caractère abusif des clauses au sens du premier alinéa ne porte ni sur la définition de l'objet principal du contrat ni sur l'adéquation du prix ou de la rémunération au bien vendu ou au service offert pour autant que les clauses soient rédigées de façon claire et compréhensible.

Un décret en Conseil d'Etat, pris après avis de la commission des clauses.

(147) Quel cadre pour la responsabilité du fait des objets connectés?, op, cit.

(148) https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32019L0770.

التَّنفيذِ في ١ يناير ٢٠٢٢ وذلك بهدفِ تنسيقِ حقوقِ المستهلك وتعزيز التزاماتِ المحترفين، وكذلك السَّماحُ للمُستهلكين بطلبِ استعادةِ الخدمةِ المعنيَّة، وفي حالةِ عدم قيامِ المورِّد بذلك يتمُّ تخفيضُ السِّعرِ أو إنهاءُ العقد. وهذا ما تُشير إليه بشكلٍ خاصٍّ قراءاتُ التَّوجيه ٧٧٠/٢٠١٩ والمادَّة ٣ منه[١٤٩]، والتي تُشير إلى أنَّه تنطبقُ أحكام قانونِ حمايةِ البيانات الشَّخصيَّة أيضًا على الأشياءِ المُتَّصلةِ عندما يرغبُ المستهلكون في ممارسةِ حقِّهم في الوصولِ أو التَّصحيح أو حقهم في النَّقل[١٥٠].

---

[١٤٩] التَّوجيه ٧٧٠/٢٠١٩ هو تشريعٌ أوروبيٌّ يتعلَّق بالعقود الخاصَّة بالبيع الرقميّ والخدمات الرقميَّة. يهدف هذا التَّوجيهُ إلى تحديثِ القواعدِ المتعلِّقة بحمايةِ المستهلك في سياقِ المعاملاتِ الرقميَّة، وهو جزءٌ من الجهودِ الأوسع للاتِّحاد الأوروبيّ لتسهيل التِّجارةِ الرقميَّةِ وتعزيز حقوقِ المُستهلكين.

[١٥٠] تجدر الإشارةُ هنا إلى أنه في إطارِ ضمانِ الحمايةِ للمستهلكين في أوروبا ذهب بعضهم إلى أنه ينبغي ذِكرُ نظام الإنذار السَّريع الأوروبي (RAPEX) للمنتجاتِ التي تُمثِّل خطرًا جسيمًا على المستهلكين وهو الأمرُ الذي يسمحُ للمفوضيَّةِ الأوروبيَّةِ بإبلاغها عبر تنبيهاتٍ من السُّلطاتِ الوطنيَّةِ في الاتِّحاد الأوروبيّ/ المنطقة الاقتصاديَّة الأوروبيَّة وفيما يتعلَّق بالمنتجاتِ الخطرةِ المكتشفة في أسواقها، والتي يُمكن استخدامُها للكائناتِ المتَّصلة. بما في ذلك المنتجاتُ الاستهلاكيَّة (باستثناء المنتجاتِ الغذائيَّةِ والأدوية والأجهزة الطبيَّة التي تستفيدُ من تنبيهاتٍ محدَّدة) والأشياء المتَّصلة أيضًا. فقد حذرت DGCCRF بالفعل من المخاطرِ التي يجبُ الانتباهُ إليها فيما يتعلَّقُ بالأشياءِ المتَّصلة، وتمكَّنت المفوضيَّةُ الأوروبيَّةُ من إصدارِ إشعار RAPEX في عام ٢٠١٩ بشأن السَّاعاتِ المتَّصلةِ للأطفال التي تشكِّل مخاطرَ جسيمةً من حيث أمنُ البيانات. ويوضِّح هذا الإشعارُ أن الالتزاماتِ المرتبطةَ بالكائناتِ المتَّصلةِ تتداخلُ مع حمايةِ المستهلكِ ومسؤوليَّة المنتجِ وحماية البياناتِ الشخصيَّة.

- http://solidarites-sante.gouv.fr/prevention-en-sante/risques-de-la-vie-courante/article/rappel-de-produits-systeme-europeen-rapex
- https://www.economie.gouv.fr/dgccrf/Publications/Vie-pratique/Fiches-pratiques/objets-connectes
- https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/0157/19&lng=en

(ISSN: 2537- 0758)

الفرع الخامس
الشُّروطُ التَّعسفيَّةُ والأشياءُ المُتَّصلةُ

يثور التَّساؤلُ- أيضًا- حولَ ضرورةِ مراعاةِ الأحكامِ المتعلّقةِ بالشُّروطِ غير العادلةِ بالمعنى المقصودِ في القانونِ الفرنسيّ، سواءٌ في قانونِ العقودِ العامّ أو في القانون التِّجاريّ أو حتى في قانونِ حمايةِ المستهلك. وفي الواقعِ يتعيَّن أخذُ هذه الأحكامِ في الاعتبارِ بطرقٍ مختلفةٍ جدًّا أثناء تصنيعِ وتسويقِ شيءٍ متَّصل. وعلى وجهِ الخصوص، عندما يُبرم المستخدمُ عقدًا مع الشَّركةِ المصنِّعة للشَّيءِ المتَّصل، ويستخدم هذا المستخدمُ الخدماتِ التي يقدّمها الشَّيءُ المتَّصل، وفي حالةِ حدوث ضررٍ أو عندما ينفذ الشَّيء المتَّصل معاملاتٍ أو عمليات نيابة عن المستخدمِ أو المستهلك.

وفي سياقِ إنترنتّ الأشياء، يبدو أن الشُّروطَ التعاقديَّةَ غير العادلةِ بموجبِ قانون العقودِ بالمعنى المقصودِ في المادة ١١٧١ من القانون المدنيّ الفرنسيّ، كلُّ شرطٍ غير قابلٍ للتَّفاوضِ في العقد، ممَّا يخلق خللًا كبيرًا في التَّوازنِ بين حقوقِ والتزاماتِ الأطراف(١٥١). وهذا هو الحالُ بالنِّسبةِ لعقد البيعِ المتعلّق بمنتجٍ متَّصل، حيث يحتفظُ البائعُ على سبيل المثال بالحقّ في تعديلِ الشُّروطِ من جانبٍ واحدٍ أو تقديم موافقةٍ ضمنيَّةٍ على معالجةِ البياناتِ الشَّخصيَّة بمجرَّدِ الاستمرارِ في التصفُّح.

كما أن إدراجَ بندٍ من شأنهِ أن يفرغ الالتزامَ الأساسيَّ للشَّركةِ المصنِّعة من مضمونهِ وجوهره سيكون بمثابةِ خللٍ واضحٍ بحسب نصّ المادة ١١٧٠ من القانون المدنيّ الفرنسيّ شأنه في ذلك شأنُ بند الإعفاءِ من المسؤوليَّةِ في حالةِ حدوثِ خرقٍ يتعلَّق بأمنِ البيانات (la sécurité des données)(١٥٢).

ويظهرُ من خلالِ مطالعةِ قانون العقودِ الفرنسيّ (الصَّادرة بموجبِ مرسوم بقانون رقم ١٣١ لسنة ٢٠١٦م، والمُصدَّق عليه وفقًا لقانونِ التَّصديقِ رقم ٢٨٧ لسنة

(151) Dans un contrat d'adhésion, toute clause non négociable, déterminée à l'avance par l'une des parties, qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite.

(152) les dispositions sont inspirées du droit spécial des clauses abusives en droit de la consommation (article L212-1 et s.).

٢٠١٨م) أن المُشرِّعَ الفرنسيَّ قد أخذ بمبدأٍ عامٍّ ومرنٍ لمفهوم الالتزامِ الرَّئيس، وهو ما يتَّضحُ في نصِّ المادة ١١٧٠ من القانون المدني الفرنسيّ– نص مُستحدث– حيث جاء النصُّ على النَّحوِ الآتي: كلُّ شرطٍ يُفرغ الالتزام الرئيس للمدين من مضمونهِ يعتبرُ غير مكتوبٍ أو كأن لم يكن(١٥٣)؛ كونه يُسبِّب خللًا واضحًا فضلًا عن كونهِ شرطًا تعسُّفيًّا غير مبرَّر.

ووفقًا لنصِّ المادَّة ١١٧٠ من القانون المدنيّ الفرنسيّ نجدُ بأن المُشرِّعَ الفرنسيَّ قد اعتبر أن كلَّ بندٍ أو شرطٍ يُفرِّغ الالتزامَ الرَّئيس l'obligation essentielle للمدين من مضمونه، غير موجودٍ وكأنْ لم يكُنْ، دون أن يُشيرَ إلى تعريفٍ واضحٍ وصريحٍ لهذه الشُّروط، فضلًا عن أنَّه لم يضعْ مؤشِّرًا يمكن الاستدلالُ به أو الاستناد إليه، وهو أمرٌ يُحمد عليه المشرِّع الفرنسيُّ؛ لأنه يبحث عن مسألةِ تحقيقِ التَّوازن العقديّ.

ولهذا يُمكننا القولُ بأن المُشرِّعَ الفرنسيَّ قد فرضَ حمايةً موسعةً، فلم يقتصرْ على الشُّروطِ المخففةِ أو شروط الإعفاءِ من المسؤوليَّةِ والتي استقرَّ عليها القضاءُ الفرنسيُّ فيما يُعرف بقرار Chronopost(١٥٤)، بل اعتبر كلَّ شرطٍ يُجرد الالتزامَ الرئيسَ للمدين من مضمونهِ كأنْ لم يكُنْ؛ أي كأنَّ المتعاقدين لم يتَّفقا عليه في مضمونِ العقدِ، ومن ثَمَّ لا يُنتج أيَّ أثرٍ.

فطبيعةُ الشُّروطِ التي تناولتها المادة ١١٧٠ من القانونِ المدنيّ الفرنسيّ تتعلَّق بجميعِ الشُّروطِ العَقْدِيةِ التي تُفرِّغ الالتزامَ الرَّئيسَ للمدين من مضمونهِ، فلا تتعلَّقُ بشرطٍ بعينهِ، بل بكافَّةِ الشُّروطِ العَقْدِيَّة المتَّفقِ عليها في محتوى العقدِ، والتي تُفرِّغ الالتزامَ الرَّئيسَ للمدين من مضمونه.

وعلى ذلك فإنَّ هذا النصَّ يستهدفُ كلَّ بندٍ أو شرطٍ le texte vise " toute clause" يُفرغ الالتزامَ الرَّئيسَ للمدين من مضمونه(١٥٥)، فضلًا عن أن نطاقَه لا

(153) Art. 1170: "Toute clause qui prive de sa substance l'obligation essentielle du débiteur est réputée non écrite" .

(154) Mekki (M.), Darrois (J.-M.), Gauvain (J.-M.), Se conformer au nouveau droit des contrats: Regards croisés sur les clauses potentiellement excessives, J.C.P. E, No 25, 23 Juin 2016, p. 23 .

(155) Ibid ،.p. 23.

(ISSN: 2537- 0758)

يقتصرُ على عقدٍ بعينهِ، بل يشمل كافَّةَ العقودِ بما فيها عقودُ تشغيلِ الأشياءِ المُتَّصلة[١٥٦].

ويُعاقب القانونُ التِّجاريُّ الفرنسيُّ–أيضًا– قيامَ أيِّ شخصٍ يعمل بأنشطةِ الإنتاجِ أو التَّوزيع أو الخدمة بالحصولِ أو محاولةِ الحصولِ على مزيَّةٍ من الطَّرفِ الآخر دون تعويضٍ أو أن تكون غير متناسبةٍ بشكلٍ واضحٍ مع قيمةِ المقابل الممنوحِ أو

---

[١٥٦] وتجدر الإشارةُ هنا إلى أنَّ نصَّ المادَّة ١١٧١ من القانون المدنيّ الفرنسيّ الوارد ذكرُه في المرسومِ بقانون عام ٢٠١٦، والذي ينصُّ على أنه "في عقد الإذعان، يُعدُّ كأن لم يكُنْ كل شرطٍ يرتِّب اختلالًا واضحًا في التَّوازنِ بين حقوقِ والتزاماتِ أطراف العقد...". يختلف عن نصِّ المادة ١١٧٠ مدني فرنسي– مستحدث– السَّالف ذكره، فطبيعةُ الشُّروطِ التي يتناولها نصُّ ١١٧١ قاصرةٌ على الشُّروطِ التي ترتِّب إخلالًا واضحًا في التَّوازنِ العقديّ بين المتعاقدين، كما أنَّ نطاقَها مقتصرٌ على عقودِ الإذعانِ لا العقود كافَّة، خلافًا لنصِّ المادة ١١٧٠ من القانون المدنيّ الفرنسيّ. راجع: د. أشرف جابر، المرجع السابق، ص٣١٢.

Art. 1171: "Dans un contrat d'adhésion, toute clause qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite….."

- وتجدر الملاحظةُ إلى أنه عند النَّظرِ في قانونِ التَّصديق على مرسوم بقانون الصَّادر في ١٠ فبراير ٢٠١٦ نجد أن المشرِّعَ الفرنسيَّ في الفقرة الأولى من المادة ١١٧١ من القانون المدنيّ الفرنسيّ قد أضاف جملةَ أو عبارةَ "غير قابلٍ للتَّفاوض يحدِّدها مسبقًا أحد الأطرافِ" بعد كلمةِ شرط، حيث أصبحَ النَّصُّ على النَّحوِ الآتي: في عقودِ الإذعان، يعدُّ كأن لم يكن كل شرطٍ غير قابلٍ للتَّفاوضِ يحدِّده مسبقًا أحدُ الأطرافِ يرتِّب اختلالًا واضحًا في التَّوازن بين حقوقِ والتزاماتِ أطراف العقد.

Art. 1171: "Dans un contrat d'adhésion, toute clause non négociable, déterminée à l'avance par l'une des parties qui crée un déséquilibre significatif entre les droits et obligations des parties au contrat est réputée non écrite….. ".

فطبيعةُ الشُّروطِ التي تتناولها المادة ١١٧١ من القانونِ المدنيّ الفرنسيّ مقتصرة على الشُّروطِ غير القابلةِ للتَّفاوض والمحدَّدة مسبقًا من جانبِ أحدِ الأطراف، والتي تؤدِّي إلى اختلالِ التَّوازنِ في العلاقةِ العقديَّة، خلافًا للشُّروطِ التي تتناولها المادَّة ١١٧٠ من القانون المدنيّ الفرنسيّ التي تشملُ كافَّةَ الشُّروطِ العقديَّة.

إخضاع أو محاولة إخضاعِ الطَّرفِ الآخر لالتزاماتٍ تؤدّي إلى خللٍ كبيرٍ في حقوقِ والتزاماتِ الأطراف، فعلى سبيلِ المثال عندما يُعفي موردُ البرامجِ الشَّركة المصنِّعة للشَّيءِ المُتَّصلة من طلبِ الإصلاحِ الفنيّ للبرامج التي تُعاني من خللٍ من قِبل هذا المورِّد(١٥٧).

المطلب الثاني
استحداثُ أدواتٍ قانونيَّةٍ خاصَّةٍ لحمايةِ مُستخدمي الأشياءِ المُتَّصلةِ

تمهيدٌ وتقسيم:

أصبحت الأشياءُ المُتَّصلةُ جزءًا كبيرًا ومتزايدًا في الحياةِ اليوميَّةِ للمستهلكين. ويجبُ تمييزُ هذه الأشياء، التي يعتمدُ عملُها على الاتِّصالِ بالإنترنت، عن الأشياءِ الذكيَّةِ التي لا تحتاجُ إلى اتِّصالٍ لتعملَ وتنفِّذ الذَّكاءَ الاصطناعيَّ. وفي الحقيقةِ تمثِّل كلُّ هذه الأشياءِ خطرًا على خصوصيَّةِ الأفراد، سواءٌ كانت هذه الأشياءُ ذكيَّةً أم لا، وسواءٌ كانت تنتمي إلى المجالِ الخاصّ أم لا.

فمثلًا حتى وقتٍ قريبٍ، كان الجميعُ يستيقظون بفضِل المنبّه الخاصّ بهم، وينهضون لفتحِ أبوابِ منازلهم، وتشغيل الرَّاديو أو التِّلفزيون لمعرفةِ الأخبار، أما الآن بفضلِ سيري أو أليكسا أو جوجل هوم- على سبيلِ المثالِ لا الحصر- فقد أصبح الأمرُ مختلفًا، حيث غزَت الأشياءُ المُتَّصلةُ حياتنا.

وهذا المشهدُ من الحياةِ اليوميَّة، مهْمَا كان غيرَ ضارٍّ، يتضمَّن معالجةَ عددٍ كبيرٍ من البياناتِ الشَّخصيَّةِ المتمركزة بواسطةِ شيءٍ: المساعدة الشَّخصيَّة، حيث تتيحُ المساعداتُ الشَّخصيَّة، والتي تشملُ أيضًا مكبّراتِ صوتٍ متَّصلة، التحكُّم في الأشياءِ عن طريقِ الصَّوت، بالإضافةِ إلى التحكُّم المركزيّ في عديدٍ من الكائنات الأخرى؛

---

(١٥٧) شهدت المادة L.442-1 من القانونِ التِّجاريّ توسيع شروطِ تطبيقِها منذ صدورِ المرسومِ الصَّادر في ٢٦ أبريل ٢٠١٩، ممَّا يسمحُ لأيّ تاجرٍ بالدِّفاعِ عن نفسهِ إذا تمَّ النصُّ على شروطٍ غير عادلةٍ في العقد، ولا سيَّما توريدُ مكوّناتِ إنترنتّ الأشياء أو التَّوزيع.
https://www.legifrance.gouv.fr/affichTexteArticle.do;jsessionid=CF1C5F85FB8B3CC2B19862E3345DE8D8.tplgfr26s_1?cidTexte=JORFTEXT000038410002&idArticle=LEGIARTI000038410748&dateTexte= 20200417 &categorieLink=id#LEGIARTI000038410748.

(ISSN: 2537- 0758)

ممَّا يجعل بعضَ الإجراءاتِ اليوميَّة أسهل، ويُمكن ربطُ جميعِ المعلوماتِ النَّاتجة، مثل البياناتِ المتعلِّقة بالنِّظام الغذائيّ أو عادات النَّوم أو حتى الاهتمامات، بفضلِ الصَّوتِ الذي يأتي من خلالِ الأفرادِ، وتتمُّ معالجتُها بواسطةِ وحدةِ التَّحكُّم في البياناتِ حتى يعمل الشَّيء. ويُطلق على المحترفِ الذي يستخدمُ البيانات بعد ذلك اسم معالجِ البياناتِ، ويجبُ عليه، نظرًا للمخاطرِ التي تمثِّلها هذه الكائناتُ على الخصوصيَّة، احترام عديدٍ من الالتزامات(١٥٨)، والتي سنناقشُ مدى فعاليَّتها خلالَ هذه الدِّراسة.

وإذا كان كل جهازٍ (شيء) في السَّابق مستقلًّا، ويتمُّ تشغيلُه دون اتِّصالٍ بالإنترنت، فإن الأشياءَ المُتَّصلة- وبشكلٍ أكثر دقَّةً المساعدون الشَّخصيُّون الموجودون على الهواتفِ الذكيَّةِ أو مكبِّرات الصَّوتِ المُتَّصلة- تستردُّ باستمرارٍ وتحلّل وتنتجُ كميةً كبيرةً من البيانات. وقد تكون البياناتُ التي تمُّ جمعُها بياناتٍ ضروريَّةً لتشغيل الشَّيء، والتي وافق المستخدمُ على مُعالجتها. ولكن قد يتمُّ جمعُ بياناتٍ أخرى أقلَّ أهميَّةً دون علمِ المستخدمِ بذلك منها، عادات الأكل، والتَّفضيلات الموسيقيَّة أو ببساطةٍ الموسيقى التصويريَّة المنزليَّة....إلخ. وهنا يثورُ التَّساؤلُ حول حمايةِ الخصوصيَّةِ الفرديَّة. وفي هذا الشَّأن يعتقدُ الفيلسوفُ إيريك سادين في عام (٢٠١٥) أنَّ العالمَ أصبح الآن قاعدةَ بياناتٍ هائلة، وينبِّه الأفرادُ إلى مخاطر رقمنةِ الحياةِ اليوميَّةِ les dangers de numérisation du quotidien(١٥٩).

ولقد أدَّت جهودُ المُشرِّعِ الكنديّ إلى زيادةِ ثقةِ المستهلكين عبر التِّجارةِ الإلكترونيَّةِ بلا حدودٍ للحدِّ من التوسُّع في الأسواقِ الجديدة، وجديرٌ بالذِّكر أن كندا تفضِّل عبارة "المعلومات الشَّخصيَّة" على "البيانات الشَّخصيَّة"، على الرَّغمِ من تعريفِها بموجبِ المادَّة ٢ (١) من قانون PIPEDA على أنَّها "أيُّ بياناتٍ تتعلَّقُ بفردٍ يُمكن تحديد هويته"، وعلى الجانب الآخر فإنَّ اللَّائحةَ العامَّةَ لحمايةِ البيانات، تعتمدُ على السَّوابقِ القضائيَّةِ الكثيرة لتحديدِ مضمونِ هذا المصطلح.

(158) Gwenaëlle DONADIEU, Le RGPD et la protection de la vie privée face à l'essor des objets connectés, Vol. 15, N° 2-3 | 2021- 2022, p.221..
Objets connectés: enjeux technologiques, enjeux de sociétép https://doi.org/10.4000/ticetsociete.6720.
(159) Gwenaëlle DONADIEU, op. cit.

وفي الواقع لم تتغيَّر التَّشريعاتُ المتعلِّقةُ بالتِّكنولوجيا الرقميَّةِ والمعلومات الشَّخصيَّة منذ عامي ١٩٨٥ و٢٠٠٠، ولكن خصوصيَّة قانونِ المعلوماتِ الشَّخصيَّة في كندا تعتمدُ على الدَّورِ الأساسيِّ للسَّوابقِ القضائيَّةِ وسُلطتها الإشرافيَّةِ المستقلَّة: مكتب مفوِّض حمايةِ الخصوصيَّةِ في كندا[١٦٠]. وتظلُّ صلاحياتُ هذه الهيئةِ محدودةً للغايةِ مقارنةً بالسُّلطاتِ الإشرافيَّةِ للاتِّحاد الأوروبيِّ.

وتجدرُ الإشارةُ إلى أنَّ ما يُثير المخاوفَ في هذا الصَّددِ هو أن أمنَ الأشياءِ المُتَّصلة قد لا يتناسبُ مع النَّهجِ الكلاسيكيِّ لأمن الأنظمةِ المعلوماتيَّةِ المعمول به في السَّنواتِ الماضية؛ فضلًا عن مدى جوازِ تمريرِ البياناتِ المُجمَّعةِ لاستغلالِ خدماتٍ أخرى، ولهذا لا بدَّ من البحثِ عن مواءمةِ النُّصوصِ العامَّةِ التي تهدفُ إلى حمايةِ بياناتِ الأفراد من خلال شبكةِ الإنترنت، سواءٌ في نصوصِ القانونِ المدنيِّ أو قانون العقوبات، أو القوانين الخاصَّةِ بالتِّكنولوجيا المعلوماتيَّة، وذلك من أجل إقرار بعض القواعد والمبادئ التي تحمي مستخدمي الأشياء المُتَّصلة. حيث تلاحظ عدم

---

[١٦٠] مكتب مفوِّض حمايةِ الخصوصيَّةِ في كندا (Office of the Privacy Commissioner of Canada) هو هيئةٌ مستقلةٌ مسؤولةٌ عن حمايةِ حقوقِ الأفرادِ فيما يتعلَّق بالخصوصيَّةِ وحماية البيانات، حيث يقومُ المكتبُ بتعزيزِ الوعي حولَ قضايا الخصوصيَّةِ وضمان امتثالِ المؤسَّساتِ للقوانين المعمول بها.

المسؤوليَّات الرئيسيَّة:

- مراقبة الامتثال: يراقب المكتبُ التزامَ المؤسَّساتِ بالقوانين الفيدراليَّةِ المتعلقة بحمايةِ الخصوصيَّة، مثل قانون حمايةِ المعلوماتِ الشخصيَّة والوثائق الإلكترونيَّة (PIPEDA).
- التَّحقيق في الشَّكاوى: يستقبل المكتبُ الشَّكاوى من الأفرادِ حول انتهاكاتٍ محتملةٍ للخصوصيَّةِ، ويقوم بإجراءِ التَّحقيقاتِ اللَّازمة.
- تقديم الإرشادات: يوفِّر المكتبُ إرشاداتٍ ونصائحَ للمؤسَّساتِ حول كيفيَّةِ إدارةِ وحمايةِ البيانات الشخصيَّة.
- التَّوعية والتَّعليم: يعمل على زيادةِ الوعي بقضايا الخصوصيَّةِ من خلال نشرِ المعلوماتِ والموارد التي تُساعد الأفرادَ على فهمِ حقوقهم.
- تقديم التَّوصيات: يرفعُ المكتبُ توصياتٍ إلى الحكومةِ لتحسين إطارِ حمايةِ الخصوصيَّة في كندا.

وتجدر الإشارةُ إلى أنه يعتبر المكتبُ حلقةَ وصلٍ مهمَّة بين الأفرادِ والحكومة، حيث يسعى لحمايةِ الحقوقِ الفرديَّةِ وتعزيز الثقةِ في كيفيَّةِ تعامُلِ المؤسَّساتِ مع البياناتِ الشخصيَّة.

(ISSN: 2537- 0758)

كفاية النصوص العامة لحماية الخصوصية؛ لتطبيقها بشكل سليم على الأشياء المُتَّصلة، وذلك في ظلِّ غيابِ تشريعٍ خاصٍ ومحدَّدٍ لتنظيمِ مسائلِ الأشياءِ المُتَّصلة.

وفي هذا الشَّأن نبيّن دورَ اللائحةِ العامَّةِ لحمايةِ البيانات (GDPR) في إدارةِ الأشياءِ المُتَّصلة مع الإشارةِ إلى بعضِ المبادئ والأدواتِ المُستحدَثةِ لحمايةِ مستخدمي الأشياءِ المُتَّصلة، في ضوء لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ بشأن تنظيمِ الذَّكاءِ الاصطناعيّ، **وذلك على النَّحو التالي:**

الفرع الأول: حمايةُ الخصوصيَّةِ من خلالِ التَّغييرِ في طبيعةِ البياناتِ التي تتمُّ معالجتُها بواسطةِ الأشياءِ المُتَّصلة.

الفرع الثاني: حمايةُ الخصوصيَّةِ من خلال الوفاءِ بالتزامِ المعلوماتِ وجمع الموافقةِ المستنيرة.

الفرع الثالث: مبدأُ تقريرِ المصيرِ المعلوماتيّ.

الفرع الرابع: مبدأ التَّنظيمِ الذاتيّ للبياناتِ من قِبل الشَّركات.

الفرع الخامس: استحداث هيئةٍ مستقلَّةٍ لرقابةِ أنظمةِ الذَّكاء الاصطناعيّ. (الهيئةُ العامَّةُ لرقابةِ تقنيَّاتِ الأشياءِ المُتَّصلة والأمن الرَّقميّ).

الفرع الأول

حمايةُ الخصوصيَّةِ من خلال التَّغييرِ في طبيعةِ البياناتِ التي تتمُّ معالجتُها بواسطةِ الأشياءِ المُتَّصلة

La protection de la vie privée par le changement de nature des données traitées par les objets connectés

يعمل الشَّيءُ المتَّصلُ على جمعِ ومعالجةِ البيانات وخاصَّةً البياناتِ الشَّخصيَّة. وإذا كان قانونُ حماية البياناتِ الصَّادر في ٦ يناير ١٩٧٨ يشكِّل إطارًا حقيقيًّا لحمايةِ البياناتِ الشَّخصيَّة، فإن اللَّائحة ٦٧٩/٢٠١٦ الصَّادرة عن البرلمانِ الأوروبيّ فيما يتعلَّقُ بحمايةِ الأفرادِ تشكِّل معالجةً حقيقيَّةً للبياناتِ الشَّخصيَّةِ وحريَّة حركة هذه البيانات، وفي الحقيقةِ لكي تكونَ الأشياءُ المُتَّصلةُ قادرةً على العمل بشكلٍ مثاليّ، تقوم بجمعِ بياناتنا الشَّخصيَّة، وهو الأمرُ الذي لا يخلو من عواقب[١٦١].

(161) GALICHET C., «Les grands principes du Règlement européen sur la protection des données personnelles.», op. cit.

وتعتمدُ الأشياءُ المُتَّصلةُ على جلبِ أكبرِ قدرٍ من البيانات التي تخصُّ الأفراد، وممَّا لا شكَّ فيه أصبح اختراقُ الكياناتِ المُتَّصلة أمرًا سهلًا؛ كون أنَّ هذه الأشياءَ تعتمدُ على دمجِ البياناتِ التي تمَّ جمعها؛ لاستغلالِ خدماتٍ أخرى منبثَّةِ الصِّلةِ عن الخدماتِ المقصودةِ والمعنيَّة في الأساس، وهذا الأمرُ يجعلنا أمامَ صعوبةٍ في التحكُّم في هذه العمليَّات، بل يجعل التحكُّم في بعضِ الأحيانِ مستحيلًا، وهذا ما أظهرتْه الدِّراساتُ بأن ٨٠% من الأشياءِ المُتَّصلةِ تتخلَّلها ثغراتٌ في نظامِ تأمينها؛ إما بسبب عدم كفايةِ سياسةِ كلمةِ المرور، وإما لعدمِ تشفيرِ البياناتِ بشكلٍ كافٍ(١٦٢).

وفي الواقع، تُشير بعضُ الدِّراسات إلى أنَّ ٧٨% ممَّن تمَّ استجوابهم يقولون إنَّهم قلقون بشأنِ انتهاكِ الخصوصيَّةِ وغالبًا ما تكونُ هذه الأشياءُ هدفًا للقرصنة. وعلى الرَّغم من أنَّ هذه اللَّائحةَ لا تتعلَّقُ بشكلٍ مباشرٍ بالأشياءِ المُتَّصلة، فإنها في الواقعِ تتأثَّر بهذه الحمايةِ الجديدةِ للبيانات الشَّخصيَّة(١٦٣).

ولقد قام واضعو اللَّائحةِ العامَّةِ لحمايةِ البيانات، من أجل الحدِّ من المخاطرِ المرتبطةِ بسرقةِ أو تسرُّب البيانات الشَّخصيَّة، بوضعِ عددٍ معيَّنٍ من المبادئ من أجلِ حمايةِ البياناتِ الشَّخصيَّةِ على النَّحو الأمثل، حيث تكرِّس المادة ٢٥ من اللَّائحةِ العامَّة لحمايةِ البياناتِ مبدأَ حمايةِ الخصوصيَّةِ أثناء مرحلةِ تصميمِ الخدمةِ ومبدأ الخصوصيَّةِ افتراضيًّا. ويعني مبدأ الخصوصيَّةِ خلال مرحلةِ تصميم الخدمة، أن حمايةَ خصوصيَّةِ البياناتِ الشَّخصيَّة يجب أن يتمَّ حمايتُها "منذ البدايةِ في بنيةِ الشَّيء المتَّصل". ولذلك فإنَّ مُعالج البياناتِ أو حتى الشَّركةِ المصنِّعة للشَّيء يجبُ أن تكونَ منتبهةً لمختلفِ التَّدابيرِ الأمنيَّة. وعلى سبيل المثال، سيتعيَّن عليهم "على وجهِ الخُصوصِ تبريرُ كميَّةِ ونوعيَّةِ البيانات المطلوبة، ومدى المعالجةِ (الجمع

(162) Myriam, Quéméner Internet, des objets et cybercriminalité et cybersécurité Revue Banque, revue. banque- (19.04.2022.

(163) Manon Delaby, L'ENCADREMENT JURIDIQUE DES OBJETS CONNECTÉS: VERS LA POSSIBILITÉ D'UN ENCADREMENT SPÉCIFIQUE, Publié le 26 décembre 2017 dans Données numériques, https://iredic.fr/2017/12/26/lencadrement-juridique-des-objets-connectes-vers-la-possibilite-dun-encadrement-specifique/.

(ISSN: 2537- 0758)

والتَّخزين والإدارة collecte, stockage, gestion)، وفترة الاحتفاظ، وإمكانية الوصولِ إلى هذه البياناتِ بما يتوافَقُ مع الوصولِ المقيّد لعددٍ معيَّنٍ من الناس(١٦٤).

ويرتبطُ مبدأُ الخصوصيَّةِ افتراضيًّا Le principe de privacy by default ارتباطًا وثيقًا بمبدأ حمايةِ الخصوصيَّةِ أثناء مرحلةِ تصميمِ الخدمة. ويسمحُ هذا المبدأ "للأشخاصِ الذين يتمُّ جمعُ بياناتِهم بالحصولِ على أعلى مستوًى ممكنٍ من الحماية، شأنُه في ذلك شأنُ مبدأِ حمايةِ الخصوصيَّة أثناء مرحلةِ تصميمِ الخدمة". ويتطلَّب تحقيقُ هذا المبدأ في سياقِ الأشياءِ المُتَّصلة إنشاء آليَّةٍ للحصولِ على موافقةِ مستخدمِ الشَّيء لمُعالجة البيانات.

وفي الواقع، يجب على الشَّركةِ المصنِّعة للشَّيء المتَّصل أن تكونَ قادرةً على إثباتِ حصولِها على موافقةٍ صريحةٍ من المستخدم. ومع ذلك، ما هي نقطةُ البدايةِ لمعالجة البياناتِ الشَّخصيَّةِ بواسطةِ شيءٍ متَّصل؟، وبالتَّالي متى يجبُ الحصولُ على موافقةِ المستخدم؟ منطقيًّا، يبدو أن بدءَ تشغيلِ الكائنِ الذكيّ هي اللَّحظةُ المناسبةُ للحصول على موافقةِ المستخدم، ولكن يبدو أن لحظةَ شراء الشَّيءِ المتَّصل هي أيضًا اللَّحظة المناسبة لجمعِ موافقةِ المستخدم من خلالِ نموذجٍ محدَّدٍ يتمُّ إملاؤه.

وفي هذه الشَّأن، نبيّن مدى فعاليَّةِ بعضِ أحكامِ اللَّائحةِ العامَّة لحمايةِ البيانات لمنعِ خطرِ انتهاكِ خصوصيَّةِ المستخدمين عند استخدامِ الأشياءِ المُتَّصلة، حيث نستهدفُ كلًّا من الأشياءِ المُتَّصلةِ التي تمَّ الحصولُ عليها طوعًا، مثل المساعدين الشَّخصيين، والأشياء المُتَّصلة في الفضاءِ العامّ، مثل لوحاتِ الإعلاناتِ المُتَّصلة.

سنقومُ بعد ذلك بتقسيمِ مناقشتنا من خلالِ متابعةِ تشغيل عديدٍ من الأشياءِ المُتَّصلةِ والمراحل الرئيسة لبدءِ تشغيلِ كائنٍ متَّصلٍ، ولا سيَّما المساعدُ الشخصيُّ على وجهِ الخصوص؛ لأنه وفقًا للمقياسِ الرقميّ الذي وضعتْه هيئةُ تنظيمِ

(164) DEVEZEAUD C., «Objets connectés & Protection des données à caractère personnel: un mariage nécessaire pour la confiance des utilisateurs», dpo-consulting.fr, mis en ligne le 27 mars 2017< http://www.dpo-consulting.fr/single-post/2017/03/27/Objets-connect%25C3%25A9s-Protection-des-donn%25C3%25A9es-%25C3%25A0-caract%25C3%25A8re-personnel-un-mariage-n%25C3%25A9cessaire-pour-la-confiance-des-utilisateurs.

الاتِّصالاتِ الإلكترونيَّة والبريد والتَّوزيع الصَّحفي (ARCEP عام ٢٠١٩)، والمجلس العام لاقتصادِ الصِّناعةِ والطَّاقة والتِّقنيَّات الرقميَّة مُهمَّة المجتمع، فهي واحدةٌ من أكثرِ الأشياءِ المُتَّصلة ارتباطًا (ARCEP, 2019). ومن ثمَّ، سنُحدِّد طبيعةَ البياناتِ التي ستتمُّ مُعالجتها ونظامها العامُّ، وذلك قبل تحديدِ الالتزاماتِ الملقاة على عاتقِ معالجِ البياناتِ (مشغل النِّظام) وقت إبرامِ العقدِ من خلال تحليلِ أشياءَ متَّصلةٍ مختلفة، مثل المساعدين الشَّخصيِّين أو لوحاتِ الإعلاناتِ المُتَّصلة أو حتى المكانس الكهربائيَّةِ الروبوتيَّة، بما في ذلك تقنيَّةُ ChatGPT باعتبارِها نموذجًا حديثًا للذَّكاءِ الاصطناعيّ.

وكما هو واضحٌ وفق معيارِ الاستخداماتِ الرقميَّة الذي نشره ARCEP والمجلس الأعلى للسَّمعياتِ والبصرياتِ (CSA) في عام ٢٠٢١، فإن الأشياءَ المُتَّصلةَ حاضرةٌ بشكلٍ متزايدٍ في الحياةِ اليوميَّةِ للمستهلكين، إلا أنَّها لا تمثِّل جميعُها خطرًا على حياتِهم الخاصَّة. فهناك بعضُ الأشياءِ المُتَّصلة لا تجمعُ بياناتٍ شخصيَّة، وهو الأمرُ الذي سيؤدِّي إلى عدمِ تطلُّبِ التزاماتٍ فيما يتعلَّقُ بالمعلوماتِ والموافقة. ومن أجل معرفةِ النِّظام القانونيّ المطبق على كلِّ جهازٍ متَّصل، يتحتَّمُ التَّحديدُ المسبق للطَّبيعةِ القانونيَّةِ للبيانات المعالجة، سواء تمَّ تعديلُها أم لا.

أولًا: التَّمييزُ بين الأشياءِ المُتَّصلة وأنواع البيانات المجمعة:

La distinction entre les types d'objets connectés et de données collectées:

هنا يثور التَّساؤل، ما المقصودُ بالبيانات؟ عندما يتمُّ استخدامُ مصطلحِ "البيانات" في اللُّغة اليوميَّة، فإنه يُشير إلى "التَّمثيلِ التقليديّ للمعلوماتِ بهدف مُعالجتِها بواسطةِ الكمبيوتر"[١٦٥]، ولذلك فهي عنصرٌ من عناصرِ التَّرميز الذي سيربطُ بين الواقعِ الحقيقيّ والواقع الرقميّ. بالإضافةِ إلى جودتِها باعتبارِها ملكيَّةً شخصيَّةً ملموسة، فالبياناتُ هي معلوماتٌ مختلفةٌ.

وفي الحقيقةِ البياناتُ التي يتمُّ جمعُها بواسطةِ الأشياءِ المُتَّصلة هي في الواقعِ إما بياناتٌ شخصيَّةٌ أو بياناتٌ غير شخصيَّة، وليس هناك تعريفٌ قانونيٌّ للبياناتِ غير

(165) Définition du Larousse, édition 2017.

(ISSN: 2537- 0758)

الشَّخصيَّة، خلافًا للبيانات الشَّخصيَّةِ، والتي يُمكن تعريفُها وفق قانونِ حمايةِ البيانات الشَّخصيَّة **رقم ١٥١ لسنة ٢٠٢٠** بأنها أيُّ بياناتٍ متعلِّقةٍ بشخصٍ طبيعيّ محدَّد، أو يُمكن تحديدُه بشكلٍ مباشرٍ أو غير مباشرٍ عن طريقِ الرَّبط بين هذه البياناتِ، وأي بياناتٍ أخرى كالاسم، أو الصَّوت، أو الصُّورة، أو رقمٍ تعريفيّ، أو محدِّد للهويَّةِ عبر الإنترنت، أو أي بياناتٍ تُحدِّد الهويَّةَ النفسيَّة، أو الصحيَّة، أو الاقتصاديَّة، أو الثقافيَّة، أو الاجتماعيَّة.

وجديرٌ بالذِّكر تُشير البياناتُ غير الشَّخصيَّةِ- على سبيلِ المثالِ- إلى بياناتِ الأرصادِ الجويَّة أو الغلافِ الجويّ أو البياناتِ الهيدرومتريَّة التي يُمكن مُعالجتُها بواسطةِ أيّ نوعٍ من الأشياءِ المُتَّصلة، بما في ذلك بعضُ السَّماعات المُتَّصلة.

وتُعرف المادة ٤ من اللَّائحةِ العامَّة لحمايةِ البيانات، المقصودَ بالبياناتِ الشَّخصيَّةِ بأنها "أيُّ معلوماتٍ تتعلَّق بشخصٍ طبيعيٍّ محدَّدٍ أو يُمكن تحديدُ هويَّته". وإذا بدا التَّعريفُ بسيطًا بداهةً، فقد يكون من الصَّعبِ تطبيقُه في بعضِ الفرضيَّات، كما هو الحالُ فيما يتعلَّقُ بتحديدِ طبيعةِ عناوين IP. وبما أن النُّصوصَ لا تتضمَّن في الواقعِ أيَّ قائمةٍ شاملةٍ للبيانات الشَّخصيَّة، فإن تأهيلَها غالبًا ما ينتجُ عن التَّقييمِ الفنيّ لقدرةِ تحديدِ الهويَّةِ أو إعادة تحديدِ الهويَّةِ المتاحةِ لمعالج البيانات le responsable de traitement.

ومما لا شكَّ فيه أن مسألةَ طبيعةِ عناوين IP تسمحُ لنا بفهمِ الطَّبيعةِ المتطوِّرة لهذا الشَّيء. وفي هذا الشَّأنِ تنصُّ المادة ٣٠ من اللَّائحةِ العامَّة لحمايةِ البياناتِ على أنه "قد يرتبطُ الأفرادُ، من خلالِ الأجهزةِ والتَّطبيقات والأدواتِ والبروتوكولات التي يستخدمونها، بمعرفاتٍ عبر الإنترنت مثل عناوين IP وملفات تعريفِ الارتباطِ أو معرفات أخرى، وقد تتركُ هذه المعرفاتُ آثارًا، خاصَّةً عند دمجِها مع المعرفاتِ الفريدةِ والمعلومات الأخرى التي تتلقَّاها الخوادمُ، والتي يُمكن استخدامُها لإنشاء ملفاتِ تعريفٍ للأشخاصِ الطَّبيعيِّين والتعرُّف على هؤلاءِ الأشخاص[١٦٦].

(166) Le considérant 30 du RGPD précise: «Les personnes physiques peuvent se voir associer, par les appareils, applications, outils et protocoles qu'elles utilisent, des identifiants en ligne tels que des adresses IP et des témoins de connexion («cookies») ou d'autres identifiants, par exemple

ولقد اعتمدت المحاكمُ الفرنسيَّةُ في الواقعِ مواقفَ مختلفةً إلى أنْ صدَرَ قرارٌ غير واضحٍ من محكمةِ النَّقض بتاريخ ١٣ يناير ٢٠٠٩ يوضِّح أن عناوين IP ليست بياناتٍ شخصيَّةً(١٦٧). هو ما ذهبتْ إليه محكمةُ العدلِ التَّابعةُ للاتِّحاد الأوروبيّ أيضًا في الاتِّجاه المعاكسِ في عام ٢٠١١(١٦٨) وكذلك ما حكمَتْ به ١٩ أكتوبر عام ٢٠١٦(١٦٩).

مع الأخذِ في الاعتبارِ أنه إذا كانت المعلوماتُ تتعلَّقُ بشخصٍ طبيعيٍّ يُمكن تحديدُ هويَّته، وكانت هناك وسائلُ قانونيَّةٌ تسمح له بالاتِّصالِ بالسُّلطاتِ المختصَّةِ لتحديد الهويَّة، فهي بالفعلِ بياناتٌ شخصيَّةٌ. وفي ٣ نوفمبر ٢٠١٦ ذهبت محكمةُ النَّقضِ الفرنسيَّة إلى الأخذِ بالموقفِ الأوروبيّ، حيث اعتبرت صراحةً أنَّ عنوان IP هو بياناتٌ شخصيَّةٌ، بحسَبِ ما هو واردٌ في المادة ٣٠ من اللَّائحةِ العامَّةِ لحمايةِ البيانات(١٧٠).

وتجدرُ الإشارةُ إلى أن لائحةَ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤، لم تفرِّق بين البياناتِ الشَّخصيَّةِ وغير الشَّخصيَّةِ في توفيرِ الحمايةِ اللَّازمةِ لا سيَّما فيما يتعلَّقُ بتوفيرِ الشُّروطِ اللَّازمةِ لتخزينِ أيّ بياناتٍ شخصيَّةٍ وغير شخصيَّةٍ في أجهزةٍ طرفيَّةٍ، والوصول إليها من خلالها. كما توفِّر هذه اللَّائحة الحمايةَ عند معالجةِ البياناتِ عندما تتضمَّن مجموعات البياناتِ مزيجًا من البياناتِ الشَّخصيَّة وغير الشَّخصيَّة(١٧١).

---

des étiquettes d'identification par radiofréquence. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes».

(167) (Cass. Crim., 13 janv. 2009, n°08-84.088).

(168) La Cour de justice de l'Union européenne s'était également prononcée en sens inverse en 2011 (CJUE, 24 nov. 2011, aff. C-70/10).

(169) CJUE, 19 oct. 2016, aff. C-582/14).

(170) (Cass. Civ. 1ère, 3 novembre 2016, pourvoi n°15 22595).

(171) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

(ISSN: 2537- 0758)

وعلى الجانبِ الآخرِ قد وضعت اللَّائحةُ سالفة الذِّكر بعضَ القيودِ الفنيَّة لحمايةِ الفئاتِ الخاصَّة من البياناتِ الشَّخصيَّةِ عند إعادةِ استخدامِ البياناتِ الشَّخصيَّة، فضلًا عن اتِّخاذِ بعضِ التَّدابيرِ الأمنيَّةِ والحديثة للحفاظِ على الخصوصيَّة، بما في ذلك إخفاءُ الهويَّة، بالإضافةِ إلى ضمانِ تأمينِ البيانات الشَّخصيَّةِ المُعالجة وحمايتها، وخضوعها للضَّماناتِ المُناسبة، بما في ذلك الضَّوابطُ الصَّارمةُ وتوثيق الوصول؛ لتجنُّبِ سُوءِ الاستخدامِ وضمان وصولِ الأشخاصِ المصرَّح لهم فقط إلى تلك البياناتِ الشَّخصيَّةِ مع التزاماتِ السريَّةِ المناسبة. كما أنه لا يجوزُ نقلُها أو الوصولُ إليها بأيِّ طريقةٍ أخرى من قِبل أطرافٍ أخرى(١٧٢).

وإلى جانب التَّمييزِ بين البياناتِ الشَّخصيَّةِ وغير الشَّخصيَّة، من المُمكن التَّمييزُ داخلَ البياناتِ الشَّخصيَّة بين البياناتِ الحسَّاسة les données sensibles وغير الحسَّاسة. فهناك بعضُ البياناتِ مصنَّفةٌ على أنها "بياناتٌ حساسةٌ" حيث تمثِّل في الواقعِ خطرًا أكبر لانتهاكِ الخصوصيَّة؛ ممَّا يبرِّر منحها نظامَ حمايةٍ أكثر صرامةً، لا سيَّما في ظلِّ ظهورِ جيلٍ جديدٍ من الأشياء، والتي تعملُ على التَّقييمِ الذاتيّ لعاداتِ مُستخدميها، حيث يُطلق عليها البعضُ بأجهزةِ التَّقديرِ الذاتيّ للصِّحةِ، مثل:

(172) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art.10 …….. the bias detection and correction cannot be effectively fulfilled by processing other data, including synthetic or anonymised data؛

the special categories of personal data are subject to technical limitations on the re-use of the personal data, and state-of-the-art security and privacy-preserving measures, including pseudonymisation؛

the special categories of personal data are subject to measures to ensure that the personal data processed are secured, protected, subject to suitable safeguards, including strict controls and documentation of the access, to avoid misuse and ensure that only authorised persons have access to those personal data with appropriate confidentiality obligations؛

the special categories of personal data are not to be transmitted, transferred or otherwise accessed by other partie.

the special categories of personal data are deleted once the bias has been corrected or the personal data has reached the end of its retention period, whichever comes first;

السَّاعاتِ الذكيَّةِ أو أجهزة تتبُّعِ اللياقةِ البدنيَّة، وتستخدم الرَّقائق لمراقبةِ مجموعةٍ متنوّعةٍ من المؤشّرات الصحيَّة، مثل معدَّل ضرباتِ القلب، وعدد الخطوات، وجودة النَّوم، وغيرها. وهذه الأجهزةُ تجمعُ بياناتٍ عن نشاطِ المستخدمين وتقدِّم تقاريرَ وملاحظاتٍ لمساعدتهم في تحسينِ صحَّتهم ورفاهيتهم. لكنْ هناك قضايا تتعلَّق بالخصوصيَّة، حيث تجمعُ هذه البياناتُ بشكلٍ مستمرٍ؛ ممَّا يُثير تساؤلاتٍ حول كيفيَّةِ استخدامِها وحمايتها.

ويُقصد بالبياناتِ الحسَّاسةِ البياناتُ التي تُفصح عن الصِّحةِ النفسيَّةِ أو العقليَّةِ أو البدنيَّةِ أو الجينيَّة، أو بيانات القياساتِ الحيويَّةِ "البيومترية" أو البياناتِ الماليَّةِ أو المعتقداتِ الدينيَّةِ أو الآراء السياسيَّةِ أو الحالةِ الأمنيَّة، وفي جميعِ الأحوالِ تعدُّ بياناتُ الأطفالِ من البياناتِ الشَّخصيَّةِ الحساسة[١٧٣]. ووفقًا للمادة ٨ من قانونِ عام ١٩٧٨ والمادَّة ٩ من اللَّائحةِ العامَّةِ لحماية البيانات، تلك البياناتُ التي تكشفُ عن "الأصل العنصريّ أو الآراءِ السياسيَّةِ أو المعتقداتِ الدينيَّةِ أو الفلسفيَّةِ أو..."، وتشملُ أيضًا "البياناتِ الجينيَّةَ والبياناتِ البيومتريَّة[١٧٤]". وكذلك البياناتُ لأغراضِ

---

[١٧٣] راجع المادَّة الأولى من قانونِ حمايةِ البيانات الشخصيَّة رقم ١٥١ لسنة ٢٠٢٠.

[١٧٤] التعرُّف على الأشخاصِ عبر البياناتِ البيومتريَّة هو "التعرف الآليُّ على الأفرادِ استنادًا إلى سماتِهم البيولوجيَّة والسلوكيَّة". وهذا يعني أن البياناتِ البيومتريَّة بمثابةِ توقيعاتٍ بشريَّةٍ فريدةٍ يُمكن قياسها، وقد تشملُ بصماتِ الأصابعِ ومسح قزحيَّةِ العين أو طريقة الفردِ في فعلِ شيءٍ ما (مثل الطَّريقة التي يسيرُ أو يكتب بها). وهي إحدى أكثرِ الوسائلِ الموثوقةِ لإثبات الهويَّةِ المتاحة في حوزتنا، فمن الصعَّب للغايةِ تزييفُها.

وفي هذا الشَّأن عرفت المادة ١٥ من لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤: "التَّعريف البيومتريُّ هو التعرُّف الآليُّ على السِّماتِ البشريَّةِ الجسديَّةِ والفسيولوجيَّة والسلوكيَّة، مثل الوجهِ وحركةِ العين وشكلِ الجسمِ والصَّوت والنطقِ والمشيةِ والوضعيَّةِ ومعدَّل ضرباتِ القلب وضغط الدَّم، لغرضِ تحديدِ هويَّةِ الفرد من خلالِ مقارنةِ البياناتِ البيومتريَّة لذلك الفردِ بالبياناتِ البيومترية المخزَّنةِ للأفرادِ في قاعدةِ بياناتٍ مرجعيَّة، بغضِّ النَّظرِ عما إذا كان الفردُ قد أعطى موافقتَه أم لا. وهذا يستثني أنظمةَ الذَّكاءِ الاصطناعيّ المقصود استخدامُها للتحقُّقِ البيومتري، والتي تشملُ المصادقة، والغرض الوحيدُ منها هو التأكُّدُ من أن الشَّخصَ الطبيعيَّ المحدَّد هو

(ISSN: 2537- 0758)

تحديدِ هويَّةِ الشَّخصِ الطبيعيّ بشكلٍ فريدٍ، أو البيانات المتعلِّقة بالصِّحةِ أو البياناتِ المتعلِّقة بالحياةِ الجنسيَّةِ أو التوجُّه الجنسيّ لشخصٍ طبيعيٍّ". والبيانات سالفة الذِّكر هي فقط البياناتُ الحسَّاسةُ التي تستحقُّ حمايةً إضافيَّةً؛ نظرًا لخطورةِ انتهاكِ الخصوصيَّة إذا ما تمَّ الكشفُ عنها. ومع ذلك، يجبُ توضيحُ الوضعِ القانونيّ للبياناتِ الحسَّاسة؛ لأن هناك أيضًا بياناتٍ يُمكن اعتبارُها حسَّاسةً بالنِّسبة لمهنةٍ ما، ولكنَّها لا تخضعُ بالضَّرورةِ لهذا الاهتمامِ على المستوى القانونيّ.

فإذا ما نظرْنا على سبيلِ المثالِ على البياناتِ المتعلِّقة بالمعاملات، كالتي تُشير إلى المعلوماتِ المتعلِّقة بالمعاملاتِ المصرفيَّة. فهذه بياناتٌ شخصيَّةٌ؛ لأنها تسمحُ بتحديدِ هويَّةِ الفرد من خلالِ رقمِهِ البنكيّ، ولكن من وجهةِ النَّظرِ القانونيَّة، فهي ليست بياناتٍ حسَّاسة. ومع ذلك، تستخدم البنوكُ هذه المصطلحاتِ باعتبارِها حساسةً؛ لأنها تنقلُ معلوماتٍ مهمَّة عن العملاء.

وبنفسِ الطَّريقة، تعدُّ بياناتُ الدَّفع الخاصَّة بالمستهلكِ العاديّ أيضًا بياناتٍ حسَّاسة؛ لأنَّ توصيلَها إلى أطرافٍ ثالثةٍ بنوايا خبيثةٍ يُمكن أن يسبِّبَ ضررًا كبيرًا على الرَّغم من أنَّ بياناتِ المعاملاتِ ليست بياناتٍ حسَّاسة، إلا أنَّها تستفيدُ أيضًا من تشريعاتِ حمايةِ البيانات الشَّخصيَّة، بالإضافةِ إلى الحمايةِ وفق الآليَّاتِ القانونيَّةِ الأخرى مثل السريَّةِ المصرفيَّة.

الشَّخصُ الذي يدَّعي أنه هو والتأكُّد من هويَّةِ الشَّخصِ الطبيعيّ لغرضٍ وحيدٍ هو الوصول إلى خدمةٍ أو فتح قفلِ جهازٍ أو الوصول الأمنيّ إلى المباني".

The notion of 'biometric identification' referred to in this Regulation should be defined as the automated recognition of physical, physiological and behavioural human features such as the face, eye movement, body shape, voice, prosody, gait, posture, heart rate, blood pressure, odour, keystrokes characteristics, for the purpose of establishing an individual's identity by comparing biometric data of that individual to stored biometric data of individuals in a reference database, irrespective of whether the individual has given its consent or not. This excludes AI systems intended to be used for biometric verification, which includes authentication, whose sole purpose is to confirm that a specific natural person is the person he or she claims to be and to confirm the identity of a natural person for the sole purpose of having access to a service, unlocking a device or having security access to premises.

ويعدُّ تحديدُ البياناتِ التي تتمُّ مُعالجتُها بواسطةِ الأشياء المُتَّصلة أمرًا ضروريًّا لتحديدِ النِّظام القانونيّ وشروط الاستخدام، وتخضع البياناتُ الشَّخصيَّةُ في الواقعِ للائحةِ العامَّة لحمايةِ البيانات، وهذا لا ينطبقُ على البياناتِ غير الشَّخصيَّة، التي لا تشكِّل معالجتُها ونشرُها أيَّ خطرٍ على الأفراد، حيث يجبُ على هذه الأشياءِ المُتَّصلة، على سبيلِ المثال، أن تطلبَ من المستخدمِ موافقته على معالجةِ البياناتِ وتزويده بالمعلوماتِ الكافية. ومع ذلك، من المُمكن لمعالجِ البياناتِ تعديل طبيعةِ البياناتِ عن طريقِ تحويلِ البياناتِ الشَّخصيَّة إلى بياناتٍ مجهولةِ المصدرِ أو مستعارة.

ثانيا: تعديلُ طبيعةِ البيانات للحدِّ من انتهاك الخصوصيَّة:

Les données dont la nature a été modifiée pour minimiser l'atteinte à la vie privée:

تنص المادَّة العاشرة من لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ على طبيعةِ البياناتِ وحوكمتها من خلالِ إجراءٍ سابقٍ لممارسةِ الأشياء المُتَّصلة، والتي تتضمَّن خوازمياتِ الذَّكاءِ الاصطناعيّ، بالاستعانةِ ببياناتٍ بغرضِ الفحصِ والاختبار، حيث يجبُ أن تخضعَ هذه البياناتُ لممارساتِ حوكمةِ البيانات وإدارتها المناسبة للغرضِ المقصودِ من نظام الذَّكاءِ الاصطناعيّ عالي المخاطر. **وتتعلَّقُ هذه الممارساتُ على وجهِ الخصوصِ بما يلي**[١٧٥]:

---

(175) Article 10 Regulation (EU) 2024/1689.

data and data governance.....2. Training, validation and testing data sets shall be subject to data governance and management practices appropriate for the intended purpose of the high-risk AI system. Those practices shall concern in particular:

(a) the relevant design choices؛

(b) data collection processes and the origin of data, and in the case of personal data, the original purpose of the data collection؛

(c) relevant data-preparation processing operations, such as annotation, labelling, cleaning, updating, enrichment and aggregation؛

(d) the formulation of assumptions, in particular with respect to the information that the data are supposed to measure and represent؛

(e) an assessment of the availability, quantity and suitability of the data sets that are needed؛

(ISSN: 2537- 0758)

(أ) الالتزامُ بخياراتِ التَّصميمِ ذات الصِّلة.
(ب) عمليَّاتُ جمعِ البياناتِ وأصل البيانات، وفي حالةِ البياناتِ الشَّخصيَّة، يجبُ تحديدُ الغرضِ الأصليّ من جمع البيانات.
(ج) عمليَّات معالجةِ إعدادِ البيانات ذات الصِّلة، مثل التَّعليقِ والتَّصنيفِ والتَّنظيفِ والتَّحديث والإثراء والتَّجميع.
(د) صياغةُ الافتراضات، وخاصَّةً فيما يتعلَّقُ بالمعلوماتِ التي من المفترضِ أن تقيسَها البياناتُ وتمثِّلها.
(هـ) تقييم مدى توافُقِ وملاءمةِ البياناتِ التي تمَّ جمعُها مع مجموعاتِ البياناتِ المطلوبة.
(و) الفحصُ في ضوءِ النَّتائجِ المحتملة التي مِن المرجَّح أن تؤثِّر على صحَّةِ وسلامةِ الأشخاص، أو يكون لها تأثيرٌ سلبيٌّ على الحقوقِ الأساسيَّةِ خاصَّةً عندما تؤثِّر مخرجات البياناتِ على المدخلاتِ للعمليَّاتِ المستقبليَّة.
(ز) تحديد التَّدابيرِ المناسبةِ للكشفِ عن النتائجِ المحتملةِ ومنعها أوتخفيفها.
(ح) تحديد فجواتِ البياناتِ أو أوجه القصورِ ذات الصِّلة وكيفيَّة معالجةِ هذه الفجوات والعيوب.

في الواقعِ، من المُمكن لوحدةِ التحكُّم في البياناتِ تعديل طبيعةِ البياناتِ التي تتمُّ مُعالجتها بواسطةِ الأشياءِ المُتَّصلة، وذلك بفضلِ الأجهزةِ التي تسمح بتحويلِ البياناتِ الشَّخصيَّةِ إلى بياناتٍ مجهولةٍ. وجديرٌ بالذِّكر تمَّ تعريفُ البياناتِ المجهولة في البدايةِ بموجبِ التَّوجيهِ الأوروبيّ لعام ١٩٩٥ (التَّوجيه EC/٤٦/٩٥)، وهو تعريفٌ لم يتمَّ تضمينُه في المادة ٤ من اللَّائحةِ العامَّةِ لحمايةِ البيانات، حيث تُشير هذه البياناتُ

(f) examination in view of possible biases that are likely to affect the health and safety of persons, have a negative impact on fundamental rights or lead to discrimination prohibited under Union law, especially where data outputs influence inputs for future operations؛
(g) appropriate measures to detect, prevent and mitigate possible biases identified according to point (f)؛
(h) the identification of relevant data gaps or shortcomings that prevent compliance with this Regulation, and how those gaps and shortcomings can be addressed.

التي أصبحتْ مجهولةَ المصدرِ إلى أنه لم يعُدْ من المُمكن التعرُّف على الشَّخصِ المعنيّ. كما أنَّ النِّظامَ المرتبطَ بها أكثر مرونةً، فلم يعُدْ من الممكنِ تحديدُ هويَّةِ الفرد الذي تمَّ جمعُ بياناته. وبالتالي فإنَّ المسؤولين عن معالجةِ البياناتِ مجهولةِ المصدرِ لم يعودوا يُخاطرون بانتهاكِ خصوصيَّةِ الأفرادِ الذين تنشأ منهم البياناتُ.

وفي وقتِنا الحاليّ يظلُّ ضمانُ الطَّبيعةِ التي لا رجعةَ فيها لإخفاءِ الهويَّةِ أمرًا معقَّدًا؛ لأن التِّكنولوجيا تتطوَّرُ بسرعةٍ، وأصبح من السَّهلِ العثورُ على وسائل عكس عمليَّاتِ إخفاءِ الهويَّة. وهذا ما يفسِّر تكريسَ المادة ٤ من اللَّائحةِ العامَّةِ لحمايةِ البيانات لنوعٍ جديدٍ من البيانات: البيانات ذات الأسماءِ المستعارة. ويُمكن تعريفُ "الأسماء المستعارة" على النَّحو التَّالي:

"مُعالجةُ البياناتِ الشَّخصيَّة بطريقةٍ لا يُمكن فيها نسبُ البياناتِ الشَّخصيَّة إلى شخصٍ معيَّنٍ أو محدَّد دون استخدامِ معلوماتٍ إضافيَّة، بشرطِ أن يتمَّ الاحتفاظُ بهذه المعلوماتِ الإضافيَّةِ بشكلٍ منفصلٍ، حيث تخضعُ لإجراءاتٍ فنيَّةٍ وتنظيميَّةٍ لضمان ألا تُنسب البياناتُ الشَّخصيَّةُ إلى شخصٍ طبيعيٍّ محدَّدٍ أو يُمكن تحديدُ هويَّته"(١٧٦).

ولذلك تمَّ تحويلُ البياناتِ المعنيَّة، بحيث لم يعُدْ من الممكنِ التعرُّف على الشَّخصِ بشكلٍ مباشرٍ، ولكن بشكلٍ غير مباشرٍ فقط. ويتمثَّل معيارُ التَّمييزِ بين البياناتِ مجهولةِ المصدرِ والبيانات ذات الأسماءِ المستعارةِ من خلال تمييزِ الأسماءِ المستعارة عندما يصعبُ إخفاءُ الهويَّة، فمن المُمكن تخصيصُ شخصٍ ما، ثم السَّماح بالتَّداخلِ والارتباط بين مجموعاتٍ مختلفةٍ من البيانات، حيث تتمُّ حمايةُ البياناتِ بشكلٍ أفضلَ في نهايةِ المطاف، لكنَّ هذا لا يغيّر من طابعِها الشخصيّ(١٧٧).

---

(176) «traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable».

(177) Gwenaëlle DONADIEU, Le RGPD et la protection de la vie privée face à l'essor des objets connectés, Vol. 15, N° 2-3 | 2021- 2022, p.226.

Objets connectés: enjeux technologiques, enjeux de sociétép https://doi.org/10.4000/ticetsociete.6720

(ISSN: 2537- 0758)

وفيما يلي نوضِّحُ مثالًا لكيفيَّةِ التَّمييزِ بين البياناتِ مجهولة المصدرِ والبيانات المستعارة في الممارسةِ العمليَّة، في ظلِّ وجودِ أشياءَ متَّصلةٍ على الطُّرقِ العامَّة. وفي هذا الشَّأن نشيرُ إلى قضيَّةِ شركةِ JCDecaux[١٧٨]، واللَّوحات الإعلانيَّة المُتَّصلة التي أرادتْ هذه الشَّركةُ وضعَها، حيث أرادت شركةُ JCDecaux تجربةَ جهازٍ يهدف إلى توفيرِ منهجيَّةٍ للتَّقديرِ الكميّ لتدفُّقاتِ المشاةِ على لوحِ La Défense في باريس. وهذه الأشياءُ المُتَّصلة، على الرَّغم من أنها غير مرئيَّةٍ لمعظمِ الأفراد، فإنها تُمثِّل خطرًا حقيقيًّا على الخصوصيَّةِ بشكلٍ ملموسٍ، وقد تضمَّن ذلك تجهيزَ اللَّوحاتِ الإعلانيَّة بأجهزةِ استشعارٍ قادرةٍ على جمعِ عناوين MAC (Media Access Control) للمارَّة على مسافةِ ٢٥ مترًا حول كلِّ لوحةٍ[١٧٩]، والجديرُ بالذِّكر تعملُ عناوين MAC على نفسِ مبدأ عناوين IP التي تمَّت مناقشتُها أعلاه، ولكن بدلًا من تحديدِ أجهزةِ الكمبيوتر المُتَّصلة بالإنترنت، فإنها تحدِّد جميع الأجهزةِ (مثل الهواتف الذكيَّة) التي تسعى إلى الاتِّصالِ بشبكةِ Wi-Fi، وبالتَّالي فهي تتبعثُ من هواتفِ المارَّة دون علمِهم.

وبالإشارةِ إلى الهيئةِ الوطنيَّةِ لحمايةِ البيانات والحريَّات (CNIL)، باعتبارِها هيئةً وطنيَّةً مستقلَّةً لحمايةِ البيانات، ووفقًا للمادة L.581-9 من قانونِ البيئة، فقد وضع قانونًا خاصًّا لنظامِ التَّرخيصِ المتعلِّق بالألواحِ الضوئيَّة. ولهذا وجب على CNIL بالفعلِ أن تتحكَّم في صحَّةِ عمليَّةِ إخفاءِ الهويَّةِ لأجهزة الاستشعارِ الأخرى الموجودة على أثاثِ الشَّوارعِ كالأجهزةِ الإعلانيَّةِ المجهَّزة بأجهزة استشعارٍ تسمح بقياسِ تدفُّقِ المشاةِ في مترو باريس[١٨٠]؛ حيث رأتْ أنَّ البياناتِ لم تكُنْ مجهولةَ المصدرِ بشكلٍ

---

(178) Conseil d'État, 8 février 2017, pourvoi n° 393714.

(١٧٩) عنوان MAC (Media Access Control) هو معرفٌ فريدٌ يُستخدم لتحديدِ الأجهزةِ في الشَّبكات. يتكوَّن من سلسلةٍ من الأرقامِ والحروف، ويُستخدم في الشَّبكاتِ المحليَّة لتحديدِ الأجهزةِ التي تتواصلُ مع بعضِها البعض. يعمل عنوان MAC على مستوى الطبقةِ الثانيةِ في نموذج OSI، ويكون عادةً ثابتًا للأجهزة؛ ممَّا يُساعد في تسهيلِ عملياتِ التَّواصلِ وتبادل البياناتِ في الشَّبكة.

(180) CNIL, 29e rapport d'activité 2008: Doc. Fr., 2009, p. 50.

كافٍ، وأنه يجبُ الحصولُ على موافقةِ المستخدمين. وفي هذا الشَّأن أقرَّت CNIL أيضًا أنَّ النِّظامَ المطبَّق على أجهزةِ الاستشعارِ، والتي يتمُّ من خلالها قياسُ معدَّلِ عودةِ المستهلكين في المتاجرِ في مركزِ التَّسوُّق(١٨١)، لم يتمَّ إخفاءُ هويَّةِ البياناتِ بشكلٍ كافٍ، واعتبرت CNIL أنه يجبُ إبلاغُ المستهلكين بجمعِ البياناتِ وحقهم في الاعتراضِ على المُعالجة(١٨٢).

وتُظهرُ هذه القراراتُ رغبةَ CNIL في حمايةِ خصوصيَّةِ الأفراد، سواءٌ كمستخدمين لوسائلِ النَّقلِ أو كمستهلكين في مركزِ تسوُّقٍ أو مقيمين في منازلهم، من خلال منعِ استخدامِ البياناتِ المتعلِّقة بسلوكِهم دون علمِهم. ويُمكن أن يتجلَّى هذا الاستخدامُ من خلالِ إرسالِ إشعاراتٍ أو رسائلَ نصيَّةٍ قصيرةٍ لإعلامهم بالخصوماتِ من أجلِ جذبهم إلى متاجرَ معيَّنةٍ وتشجيعهم على الاستهلاك، وهذا يُمثِّل تدخلًا في حياتِهم الخاصَّةِ لا يُمكنهم محاربته ولا يعرفون عنه في أغلبِ الأحيان. ولقد قامت CNIL بالسَّيطرةِ على هذا الوضعِ من خلالِ منعِ هذه الأنواعِ من الأجهزةِ من الازدهارِ تحت غطاءِ إخفاءِ الهويَّةِ الجزئيّ للتَّحايل في نهايةِ المطافِ على التَّشريعاتِ المتعلِّقة بالبياناتِ الشَّخصيَّة.

ثم أجرت CNIL فحصًا فنيًّا لعمليَّةِ إخفاءِ الهويَّةِ من أجل التحقُّقِ من طبيعتِها التي لا رجعةَ فيها، حيث تمَّت عمليَّةُ التحكُّمِ على مرحلتين: قامت أولًا بدراسةِ المنهجيَّةِ المتَّبعةِ لإخفاء الهويَّةِ قبل دراسةِ التحكُّم في تأثيراتِ التَّشفير. وفيما يتعلَّقُ بالمنهجيَّةِ المتَّبعة، أشارتْ إلى أنَّ عمليَّةَ إخفاء الهويَّةِ التي تستخدمها شركة JCDecaux، اقتطعت عنوان MAC بمقدارِ نصفِ بايت وإضافة أحرفٍ أو بياناتٍ أخرى، حيث أدَّى هذا في النِّهايةِ إلى إزالةِ بعضِ العناصر المحدَّدةِ للهويَّةِ وتحويلها، بحيث لم يعُدْ من الممكنِ التعرُّفُ على الفردِ. كما أشارت CNIL في مداولاتها إلى أنَّ العمليَّةَ تُمثِّل إشكاليَّةً؛ لأنها استندتْ إلى بياناتٍ مكَّنت بشكلٍ غير مباشرٍ، من رؤيةِ شخصٍ ما، يتجسَّد هنا في سلسلةٍ من الأرقام، قد مرَّ عدَّة مراتٍ أمام اللَّوحات.

(181) CNIL, Mesure de fréquentation et analyse du comportement des consommateurs dans les magasins, 19 août 2014.
(182) (CNIL, délib. n° 2015-255 du 16 juillet 2015).

(ISSN: 2537- 0758)

لذلك، أشارت CNIL إلى أنه لكي يكونَ حلُّ إخفاءِ الهوية فعالًا، يجبُ أن يمنعَ جميع الأطرافِ من عزلِ فردٍ في مجموعةِ بيانات، أو ربط سجلَّين معًا في مجموعةِ بياناتٍ (أو في مجموعتين منفصلتين من البيانات) واستنتاج المعلوماتِ من مجموعةِ البيانات، وهنا، لم تكنْ هذه المعاييرُ متوافقةً، ويعدُّ ذلك أحدَ أسبابِ عدمِ سماح CNIL بهذه المعالجة. ولذلك لا يكفي إثباتُ استخدامِ عمليَّاتِ التَّشفير التي لا رجعةَ فيها لاعتبارِ أن البياناتِ الناتجةَ مجهولة المصدر.

ومع ذلك، إذا كانت البياناتُ التي تجمعُها هذه اللَّوحاتُ تتضمَّن المعرفَ الرقميَّ للفرد، أو وقت مرورِه الأول أو حتى وقت عودتهِ أمام اللَّوحةِ المعنيَّة، إلا أنَّه يعدُّ تدخُّلًا حقيقيًّا في الحياةِ الخاصَّة لهذا الفرد، وهو اقتحامٌ لم يكن على علمٍ به، كذلك لا يعلمُ المارَّة أنه تمَّ التقاطُ هذه البياناتِ على الرَّغم من أنها تكشفُ عن معلوماتٍ مهمَّةٍ حول نشاطه، وهي معلوماتٌ يُمكن استخدامُها لاحقًا لصالحه.

والبياناتُ هنا كانت ببساطةٍ مستعارةً، ولذلك يجبُ أن يتوافقَ جميعُها مع التَّشريعاتِ المتعلِّقةِ بالبياناتِ الشَّخصيَّة. ولقد حدَّدت CNIL أيضًا أنه يجبُ على شركةِ JCDecaux الحصول على موافقةِ الأفرادِ الذين يتمُّ جمعُ بياناتهم، ولا يُمكن أن يتمَّ هذا التَّجميعُ باستخدام أوراق A4 الموضوعة على اللَّوحات؛ لأنَّ طريقةَ التَّجميعِ هذه لم تضمن المعلومات الكاملة للمارَّة الذين يُمكن جمعُ بياناتِهم على مسافةٍ تصل إلى ٢٥ مترًا من اللَّوحات، ومن خلالِ هذا التَّقييمِ الدَّقيق لطريقةِ المعلومات وجمع الموافقة، سعت CNIL إلى حمايةِ الأفراد.

وتجدر الإشارةُ إلى أنَّ الشَّركةَ قد أحالت الأمرَ إلى مجلسِ الدَّولةِ باعتبارِه سلطةَ الاستئنافِ لمداولات CNIL، حيث تمَّ الطَّعنُ في عدَّة نقاطٍ فيما يتعلَّقُ بالمعلوماتِ التي قدَّمتها CNIL أثناء التَّحقيقِ في الملفِّ، وفيما يتعلَّقُ بالقرارِ نفسه. ويرى مجلسُ الدَّولةِ أن CNIL قد نفذت تطبيقًا صارمًا للمادَّة ٢ من قانونِ حمايةِ البيانات، التي تفرق بين البياناتِ وفقًا "للوسائل" من أجلِ السَّماحِ بتحديدِ الهويَّة، ولذلك، فقد تحقَّقت من صحَّةِ مداولاتِ CNIL، وكذلك دوافعها واعتبرتْ أن المعالجةَ المصمَّمة، والتي كانت تهدفُ إلى تحديدِ تحرُّكاتِ الأشخاصِ على لوحِ المشاة LaDéfense والأهداف ذاتها لجمعِ البياناتِ من قبل الشَّركةِ كانت غير متوافقةٍ مع إخفاءِ الهويَّةِ،

وبالتالي عندما يكون من الممكنِ تخصيصُ شخصٍ ما أو ربط البياناتِ الناتجةِ عن سجلَّين يتعلَّقان به، فلا يُمكن اعتبارُ البياناتِ الشَّخصيَّة مجهولةَ المصدر.

واعتبر جانبٌ من الفقهِ بعد هذا القرارِ أن فكرةَ البياناتِ المجهولة هي في النِّهايةِ مجرَّد فكرةٍ مثاليةٍ لا يُمكن تحقيقُها(١٨٣)، وأنه في أحسنِ الأحوالِ، تكون البياناتُ مستعارةً. وهذا يعني بالتالي تنفيذَ اللَّائحةِ العامَّة لحمايةِ البيانات وتطبيق قانونِ حمايةِ البيانات على المعالجةِ المتوخَّاة(١٨٤).

وفي الواقع، لا تبدو أيُّ عمليَّةٍ لإخفاءِ الهويَّة بعيدةً عن الاختراقِ على المدى الطَّويل. فمن الممكن أن تكونَ عمليَّةُ إخفاءِ الهويَّةِ فعالةً في وقتِ تنفيذِها، ولكنها قد تصبحُ قديمةً بعد عدَّة سنواتٍ إذا أتاحت التطوُّراتُ التِّكنولوجيَّةُ إمكانيَّة التَّشفير(١٨٥).

وقد يبدو أن حلَّ مجلسِ الدَّولةِ قاسيًا بالنِّسبةِ لمعالجِ البيانات؛ لأن البيانات في هذا المثال– حتى لو أثبتت الشَّركةُ أن مخاطرَ إعادةِ تحديدِ الهويَّة كانت في حدِّها الأدنى– لم تعتبر مجهولةَ المصدرِ بما فيه الكفاية؛ ممَّا يُثير التَّساؤلَ حول الاستعانةِ بأطرافٍ ثالثةٍ موثوقةٍ، والتي يُمكن من خلالها ضمانُ إخفاءِ الهويَّة.

ومع ذلك، ليست كلُّ البياناتِ الصَّادرة عن الأفرادِ والتي تتمُّ معالجتُها عبر أجهزةٍ متَّصلةٍ هي بياناتٌ شخصيَّة. وبالتالي فإنَّ معالجتها (سواءٌ كان الأمرُ يتعلَّق بجمعِ البياناتِ أو العمليَّة التي سيتمُّ تنفيذُها لاحقًا على البيانات) يخضعُ لموافقةِ الأفراد، حيث يحقُّ للأفرادِ إمكانيَّة ممارسةِ صلاحياتهم المختلفة على هذه البيانات(١٨٦). وهذا

(183) Pastor, P.-M. L'anonymisation d'une donnée doit rendre l'identification impossible: Conseil d'État 8 février 2017, Actualité Juridique Droit Administratif, (2017), p.325.

Metallinos, N. «Unique dans la foule»: l'impossible anonymisation de l'analyse des flux piétons. Communication Commerce électronique, 6, (2016) p. 36-41.

(184) Gwenaëlle DONADIEU, Le RGPD et la protection de la vie privée face à l'essor des objets connectés, Vol. 15, N° 2-3 | 2021- 2022, p.229, Objets connectés: enjeux technologiques, enjeux de sociétép https://doi.org/10.4000/ticetsociete.6720

(185) Perray, R. et Uzan-Naulin, J. Existe-t-il encore des données non personnelles? Dalloz IP/IT, 5,(2017), 286-289.

(186) Gwenaëlle DONADIEU, op. cit., p.229-230.

(ISSN: 2537- 0758)

التطوُّر لم يتطرَّق له المُشرِّعُ المصريُّ في قانونِ حمايةِ البيانات الشَّخصيَّة **رقم ١٥١ لسنة ٢٠٢٠.**

وتمثِّل هذه الأشياءُ المُتَّصلة تحدّيًا خاصًّا فيما يتعلَّقُ باستخداماتِ الأفراد، حيث أصبحَ من الممكنِ التعرُّف على الشَّخصِ من خلال عنوان MAC الخاص به(١٨٧)، وكذلك معرفة عددِ المرَّات التي مرَّ فيها أمامَ هذه العلامة، وفي الحقيقةِ فالشَّخصُ الذي يعلمُ أنه مراقبٌ، لن يتصرَّفَ بنفسِ الطَّريقةِ إذا كان لا يعرفُ أنه مراقَبٌ. وهذا على وجهِ الخصوصِ أحد التَّحدّيَّاتِ المتعلّقةِ بتحديدِ الموقعِ الجغرافيّ للأفراد أثناء الوباء. وفي هذا الشَّأن تمَّ اقتراحُ أجهزةِ تحديدِ الموقع الجغرافيّ وتنفيذها في بعضِ الولاياتِ لمحاولةِ تقييم الامتثالِ للتَّدابيرِ الوقائيَّة. ومن المؤكَّد أن هذه الإجراءاتِ سيكون لها عواقبُ تتجاوزُ المستوى القانونيَّ والأخلاقيَّ على سلوكِ الأفرادِ واستخداماتهم. ومن المحتملِ أن تكون هناك أيضًا مجموعةٌ من الهواتفِ تعمل كمرحلاتٍ لتحديدِ الموقع الجغرافيّ(١٨٨).

وفي هذا الإطارِ فإنَّ الأفرادَ الذين لا يحترمون التَّدابيرَ الاحترازيَّة، ولا يرغبون في الكشفِ عن هويَّتِهم خوفًا من الجزاءاتِ القانونيَّة، سوف يميلون إلى السَّفرِ بدون هواتفِهم؛ ممَّا يثيرُ الشُّكوكَ حول موثوقيَّةِ البياناتِ التي يتمُّ جمعُها بواسطة هذا النَّوعِ من التَّطبيقات.

Objets connectés: enjeux technologiques, enjeux de sociétép https://doi.org/10.4000/ticetsociete.6720

(١٨٧) يُعد الـ Mac Address هو أحدَ الأرقامِ الأساسيَّة لاتصالِ أيّ جهازٍ ذكيّ بشبكةِ الإنترنت، وهو اختصارٌ لكلمة Media Access Control، وهو وسيلةٌ تسمح بالتحكُّم في الكثيرِ من الأمورِ أهمها إمكانيَّة الدُّخولِ على الإنترنت في الشَّبكةِ الخاصَّةِ بالأفرادِ، وتتبع الأنشطة الخاصَّة بكلّ مستخدمٍ ومكانه بشكلٍ مستمرٍ.

ولعل خطورة الـ Mac Address تتعلَّق بكونه يُمكن من خلاله أن يتحكَّم مديرُ الشَّبكة في الكثيرِ من الأمورِ ويتتبع جميع أنشطةِ المستخدمين على الإنترنت ومنها بالطَّبعِ أنشطةُ التسوُّق واستخدام البطاقاتِ المدفوعةِ مسبقًا.

(188) Pour quelques illustrations:
https://www.francesoir.fr/politique-societe-economieenvironnement/ confinenent-surveillance-par-smartphone-la-realite-rattrape;
https://www.lebigdata.fr/google-donnees-geolocalisation-confinement.

وممَّا لا شكَّ فيه كانت دراسةُ الأنواعِ المختلفة من البياناتِ الموجودة شرطًا أساسًا لفهم سببِ ضرورةِ حمايةِ خصوصيَّةِ الأفراد وكيف يُمكن للتَّغييرِ في طبيعةِ البيانات أن يكونَ له تأثيرٌ في حمايةِ البيانات. ومع ذلك، ليست كلُّ الأشياء المُتَّصلة تمثِّل نفسَ الخطر، في حين تقومُ اللَّوحاتُ الإعلانيَّة بجمعِ عناوين MAC فقط، بينما يقومُ المساعدون الشخصيُّون بتجميعِ البياناتِ من عدَّة أشياءَ في ذاتِ المنزل، بما في ذلك البياناتُ المصنفةُ على أنها بياناتٌ حسَّاسةٌ، حيث يُشكِّل هذا الخطرُ انتهاكًا كبيرًا للخصوصيَّة، وفي هذا الشَّأن يتعيَّن على المهنيِّين احترام عديدٍ من الالتزامات، بما في ذلك الالتزامُ بتقديمِ المعلوماتِ وجمع موافقةٍ واضحةٍ[١٨٩].

الفرع الثاني

حمايةُ الخصوصيَّةِ من خلالِ الوفاءِ بالتزامِ المعلوماتِ وجمع الموافقةِ المستنيرة.

La protection de la vie privée par l'exécution de l'obligation d'information et la collecte d'un consentement éclairé

يصاحب ظهورُ الأشياءِ المُتَّصلة التي تُعالج البياناتِ الشَّخصيَّة عديدًا من الالتزاماتِ على معالجِ البيانات، والتي يُمكننا دراسةُ مظاهرِها من خلالِ مثالِ المساعد الشخصيّ، قبل أن يتمكَّن المستهلكُ من استخدامِ مساعدِه الشَّخصيّ، فإنه في الواقعِ مدعوٌّ لقراءةِ الشُّروطِ العامَّةِ للاستخدام، وقبولها قبل أن يتمكَّن من استخدامِ الشَّيء. ومع ذلك، فإن أحكامَ اللَّائحةِ العامَّة لحمايةِ البياناتِ المتعلِّقة بالمعلوماتِ والموافقة لا تجعلُ من الممكنِ دائمًا حماية الأفراد، خاصَّةً عند استخدامِ الأشياءِ المُتَّصلة، لأن طرقَ التَّنفيذِ المختارة يُمكن أن تنشطَ التحيُّزاتِ المعرفيَّةَ لدى المستخدم؛ ممَّا يضرُّ بفعاليَّةِ هذه الأحكام.

أولًا: حمايةُ الخصوصيَّةِ من خلالِ إرساءِ التزامِ المعلوماتِ والشَّفافية:

تفرض الموادُّ ١٢ و١٣ و١٤ من اللَّائحةِ العامَّة لحمايةِ البياناتِ التزامًا بالمعلوماتِ والشَّفافيةِ على معالجِ البيانات[١٩٠]. ولذلك يجبُ أن يكونَ الأفرادُ الذين

(189) Fabre-Magnan, M. De l'obligation d'information dans les contrats: essai d'une théorie. Paris, France, Librairie générale de droit et de jurisprudence. (1992).

(190) Article 13 EU RGPD "Informations à fournir lorsque des données à caractère personnel sont collectées auprès de la personne concernée" 1.

(ISSN: 2537- 0758)

تتمُّ معالجةُ بياناتهم قادرين على معرفةِ أسبابِ وأغراضِ المعالجة التي تتمُّ، حتى يتمكَّنوا من تحديدِ معالجِ البيانات، ومعرفة الحقوقِ التي يتمتَّع بها الأخيرُ على البياناتِ التي تتمُّ مُعالجتها.

ومع ذلك، لم يتمَّ تحديدُ أيّ معلوماتٍ بشأنِ شروطِ تنفيذِ هذا الالتزام، وفي هذا الشَّأن يُفضِّل معالجو البياناتِ بعد ذلك تنفيذَ شروطِ الاستخدامِ العامَّة، والتي يجبُ على المستخدمِ قبولُها قبلَ أن يتمكَّنَ من استخدامِ كائنٍ أو تطبيقٍ متَّصلٍ.

وفي هذا الشَّأن لم يُشِر المُشرِّعُ المصريُّ في قانون حمايةِ البياناتِ الشَّخصيَّة رقم ١٥١ لسنة ٢٠٢٠م إلى أحقيَّةِ المستخدمِ في معرفةِ أسبابِ وأغراض المعالجة، حيث ذكر المُشرِّعُ المصريُّ في نصّ المادَّة الثانية حقوق الشَّخصِ المعنيّ بالبياناتِ دون التطرُّق إلى أنه يحقُّ لهذا الشَّخصِ معرفة ما هو الغرضُ من المعالجة، حيث تنصُّ على أنه "لا يجوزُ جمعُ البياناتِ الشَّخصيَّة أو معالجتها أو الإفصاح عنها أو إفشاؤها بأيّ وسيلةٍ من الوسائلِ إلا بموافقةٍ صريحةٍ من الشَّخصِ المعنيّ بالبيانات، أو في الأحوالِ المصرَّحِ بها قانونًا. **ويكون للشَّخصِ المعنيّ بالبياناتِ الحقوقُ الآتية:**

Lorsque des données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne, le responsable du traitement lui fournit, au moment où les données en question sont obtenues, toutes les informations suivantes:

a) l'identité et les coordonnées du responsable du traitement et, le cas échéant, du représentant du responsable du traitement
b) le cas échéant, les coordonnées du délégué à la protection des données؛
c) les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que la base juridique du traitement؛
d) lorsque le traitement est fondé sur l'article 6, paragraphe 1, point f), les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers؛
e) les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent; et
f) le cas échéant, le fait que le responsable du traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, dans le cas des transferts visés à l'article 46 ou 47, ou à l'article 49, paragraphe 1, deuxième alinéa, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition;

١- العلمُ بالبياناتِ الشَّخصيَّةِ الخاصَّة به الموجودة لدى أيِّ حائزٍ أو متحكِّمٍ أو معالجٍ والاطِّلاع عليها والوصول إليها أو الحصول عليها.
٢- العدولُ عن الموافقةِ المسبقةِ على الاحتفاظِ ببياناتهِ الشَّخصيَّة أو معالجتها.
٣- التَّصحيحُ أو التَّعديلُ أو المحوُ أو الإضافةُ أو التَّحديثُ للبياناتِ الشَّخصيَّة.
٤- تخصيصُ المعالجةِ في نطاقٍ محدَّد.
٥- العلمُ والمعرفةُ بأيِّ خرقٍ أو انتهاكٍ لبياناتهِ الشَّخصيَّة.

وفي الواقع إنَّ الشُّروطَ العامَّة للبيعِ أو الاستخدام هي عقودُ إذعانٍ؛ أي العقودُ المبرمةُ بين المستهلكِ والمهنيِّ، والتي لا يُمكن التَّفاوضُ على شروطها، وإذا كان محتوى البنودِ المجمَّعة في هذه الشُّروط له أهميَّةٌ معيَّنةٌ، فسوف نركِّز هنا على الشَّكلِ العامِّ لهذه الوثائق، وتتجسَّد الشُّروطُ العامَّة في الواقعِ من خلالِ سلسلةٍ طويلةٍ من المقالات، مكتوبة بمصطلحاتٍ قانونيَّةٍ تقنيَّة، وعلى الرَّغم من وجودِ المعلومات، فإنه من الصَّعبِ على المستخدمِ فهمُها واستيعابُها.

وبالتَّالي فإنَّ فعاليةَ هذه الأحكامِ في حمايةِ خصوصيَّةِ الأفراد المستخدمين لأشياءَ متَّصلةٍ بشكلٍ خاصٍّ أمرٌ مشكوكٌ فيه. فمسألة فهمِ وقراءةِ واستيعابِ جميع المعلوماتِ المرسلةِ من قِبل معالجِ البياناتِ يكاد يكون مستحيلًا، كما أوضحتْ لاجارد عام (٢٠١٦). وبهذا المعنى، أظهَرَ الباحثون في الاقتصادِ السلوكيِّ أن المنفعةَ أو الفائدةَ العمليَّة للمعلوماتِ تميلُ إلى الانخفاضِ مع كثرةِ كميَّتها"[١٩١]؛ ممَّا يُفسِّرعدمَ كفاءةِ نقلِ المعلوماتِ من خلال شروطِ الاستخدامِ العامَّة.

ولقد استشهدت البروفيسور موريل فابر ماجنان في أطروحتِها عام ١٩٩٢[١٩٢]، بما أشارَ إليهِ بيرليوز والذي يعودُ تاريخُه إلى عام ١٩٨٥ والذي أفادَ بأنه يتخوَّف دائمًا من قراءةِ عقودٍ قام بالتَّوقيع عليها؛ كونها عقودًا مفروضةً، وليس أمامَه سوى التَّوقيعِ والانضمامِ، بالإضافةِ إلى أن التفاوضَ مستحيلٌ، فليس لدى المستخدمين

(191) «l'utilité marginale de l'information tend en effet à décroître à mesure que la quantité de celle-ci augmente»
Briard, A. et Faure, M. Ce que l'économie comportementale peut apporter aux juristes: illustrations européennes. Revue Trimestrielle de Droit Européen, 4, (2015). P. 715-736.

(192) Fabre-Magnan, M. (1992). De l'obligation d'information dans les contrats: essai d'une théorie. Paris, France, Librairie générale de droit et de jurisprudence.

(ISSN: 2537- 0758)

الوقتُ لقراءةِ هذه النُّصوص. وفي الشَّأن ذهبَ بعضهم إلى القولِ بأنَّ الأمرَ قد سيستغرقُ وقتًا طويلًا حتى يقرأ المستهلكُ مجملَ الشُّروطِ العامَّةِ التي يوافق عليها خلالَ حياته(١٩٣)، وتُضيف التِّكنولوجيا الرقميَّةُ والأشياء المُتَّصلة أيضًا بُعدًا جديدًا لهذه الملاحظات. ففي الواقع، أصبح مألوفًا أن يوافقَ المستهلكُ على المجموعةِ الكاملةِ من ملفَّاتِ تعريفِ الارتباط؛ بسبب الملل أو ببساطةٍ لأسبابٍ تتعلَّقُ بالسُّرعةِ، ولحاجتهِ الملحَّةِ على استخدامِ الشَّيء المتَّصل، على سبيل المثال(١٩٤).

ولقد أظهرت دراسةٌ أُجريَتْ على ٨٠ ألف شخصٍ أن المستخدمين ينقرُونَ على "أوافق" بمجرَّد أن تظهرَ على النافذةِ أيكونةُ موافق على الشُّروطِ العامَّة للاستخدام؛ ممَّا يدلُّ على أنَّ المستهلكين لا يقرأون الشُّروط المذكورة(١٩٥)، ومع ذلك، فإن "الموافقة بالنَّقر" مطلوبةٌ اليوم عدَّة مرَّاتٍ يوميًّا في حياةِ المستهلك، خاصَّةً عندما يرغبُ هؤلاء بالاتِّصالِ بهذه الأشياءِ؛ ممَّا يُثير التَّساؤلَ حول طبيعةِ الموافقةِ الحرَّة والمستنيرة حقًّا(١٩٦).

ويبدو من التطوُّراتِ السَّابقةِ أنه إذا فَرضت اللَّائحةُ العامَّةُ لحمايةِ البياناتِ (GDPR) على معالجِ البياناتِ التزامًا بتوفيرِ المعلوماتِ والشَّفافية، فإن شروطَ تنفيذِها يضرُّ بفعاليَّتها، وفي الوقتِ ذاته لا تمنعُ حدوثَ هجماتٍ خطيرةٍ على خصوصيَّةِ المستهلكين، كما أنه من المُمكن في الواقع، أن تدفَعَ طريقةُ عرضِ الشُّروطِ العامَّة، المُستهلكين إلى قبولِها دونَ قراءتِها؛ ممَّا يُثير مسألةَ الامتثالِ لالتزامٍ آخر: جمع موافقةِ المُستخدمين بفعلٍ إيجابيٍّ واضحٍ.

(193) Mac Donald, A. et Cranor, L. (2008). The cost of reading privacy policies. Journal of law and policy for the information society, 4(3), 331-354.

(194) Depincé, M. Du consommateur fidèle au consommateur captif: Analyse de droit du marché. Revue Lamy Droit des affaires, 150, (2019). 341-365.

(195) Bhöme, R. et Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. Proceedings of the SIGCHI Congerence on human factors in computing systems (p. 2403-2406). Association for Computing Machinery. Repéré à https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.8938&rep=rep1&type=pdf.

(196) Bordais, P., juin). Le consentement en Droit privé à l'épreuve des sciences cognitives. ***Actes du colloque de l'école doctorale***. Université de Montpellier. ***461***, (2017, 15-35. Université de Montpellier.

والمطَّلع على لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ يجدُ أنها قد أقرَّت آليَّةً تتمركزُ في أنه يجبُ على مزوِّدي أنظمةِ الذَّكاءِ الاصطناعيّ، وبخاصَّةٍ الأنظمةُ عاليةُ الخطورةِ في حالةِ إذا كان نظامُ الذَّكاءِ الاصطناعيّ الذي وضعوه في السُّوق أو وضعوه في الخدمةِ غير متوافقٍ مع ما ورَدَ في اللائحةِ سالفةِ الذِّكر لا بدَّ من إعادةِ النَّظر في هذه الأنظمةِ مع ضرورةِ اتِّخاذ إجراءاتٍ تصحيحيَّةٍ لازمةٍ على الفورِ لجعل هذا النِّظام متوافقًا، أو سحبه، أو تعطيله، بحسب الاقتضاء. ويجبُ عليهم إبلاغُ موزِّعي الأجهزةِ المُتَّصلةِ المدعومة بنظام الذَّكاءِ الاصطناعيّ عالي الخطورةِ وكذلك، الناشرون والمستوردون بالإضافةِ إلى المستخدمين(١٩٧).

وفي ذات الإطارِ يقعُ على عاتقِ المزوِّد بمجرَّدِ عِلمهِ بوجودِ خطرٍ في نظامِ الذَّكاءِ الاصطناعيّ يجب عليه التَّحقيقُ فورًا في الأسبابِ، بالتَّعاون مع النَّاشرِ المبلغ، عند الاقتضاءِ، وإبلاغ سلطاتِ مراقبةِ السُّوق المختصَّة بنظامِ الذَّكاءِ الاصطناعيّ عالي الخطورةِ المعني.

ثانياً: حمايةُ المستهلكِ من خلالِ اشتراطِ وجودِ فعلٍ إيجابيٍّ واضحٍ يجسد الموافقة:

La protection du consommateur par l'exigence d'un acte positif clair matérialisant le consentement:

في الأصلِ، أعطى قانونُ حمايةِ البياناتِ أهميَّةً قليلةً للموافقةِ(١٩٨)، حيث تمَّت إضافةُ اللَّائحةِ العامَّة لحمايةِ البياناتِ كأساسٍ لتبريرِ معالجةِ البيانات في توجيهِ عام ١٩٩٥، وعزَّزت مكانة الموافقةِ من خلالِ جعلها "شرطًا أساسًا لنظامِ معالجةِ

(197) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, Article 20 " Corrective actions and duty of information

1. Providers of high-risk AI systems which consider or have reason to consider that a high-risk AI system that they have placed on the market or put into service is not in conformity with this Regulation shall immediately take the necessary corrective actions to bring that system into conformity, to withdraw it, to disable it, or to recall it, as appropriate. They shall inform the distributors of the high-risk AI system concerned and, where applicable, the deployers, the authorised representative and importers accordingly.

(198) Rogue, F. Capacité et consentement au traitement de données à caractère personnel et au contrat. AJ Contrats, (2019). 370-372.

(ISSN: 2537- 0758)

البيانات"[١٩٩]، وهو أحدُ الابتكاراتِ الرئيسة في اللَّائحة العامَّة لحمايةِ البياناتِ هو على وجهِ التَّحديد التَّعريف الدَّقيق لمفهومِ الموافقة. وتعرف المادة ٤ من اللَّائحةِ موافقة الشَّخصِ بأنها "أيُّ مظهرٍ من مظاهرِ الإرادةِ الحرَّة والمحدَّدة والمستنيرة وغير الغامضةِ التي يقبلُ من خلالها الشَّخصُ المعنيُّ، بإعلانٍ أو بفعلٍ إيجابيٍّ واضحٍ[٢٠٠]، وهذا التَّعريفُ مهمٌّ لأنَّه يشيرُ إلى أنَّ الموافقةَ يجب أن تكونَ عملًا إيجابيًّا. وهذا يعني أنه لا يمكنُ استنتاجُه من الصَّمتِ أو عدم الفعل. وهنا يثورُ التَّساؤلُ هل تجوزُ الموافقةُ الضمنيَّةُ لاستخدامِ البياناتِ الشَّخصيَّةِ لتشغيلِ الأشياءِ المُتَّصلة؟

في الحقيقةِ تعترفُ القوانينُ الكنديَّةُ بإمكانيَّةِ الموافقةِ الضِّمنيَّة وذلك خلاف اللَّائحةِ العامَّةِ لحمايةِ البيانات، ولقد أصبحت الموافقةُ الآن صريحةً بالضَّرورةِ دون أن ننسى الإشارةَ إلى أن القانونَ الكنديَّ لا يتطلَّب بشكلٍ منهجيٍّ الموافقةَ على جمعِ المعلوماتِ الشَّخصيَّة[٢٠١].

وتجدرُ الإشارةُ إلى أن قانونَ حمايةِ البياناتِ الشَّخصيَّة رقم ١٥١ لسنة ٢٠٢٠م نصَّ على أنه **لا يجوزُ جمعُ البياناتِ الشَّخصيَّةِ أو معالجتها أو الإفصاحُ عنها أو إفشاؤها بأيّ وسيلةٍ من الوسائلِ إلا بموافقةٍ صريحةٍ من الشَّخص المعنيّ بالبيانات، كما ألزم المتحكِّمَ بضرورةِ** الحصولِ على البياناتِ الشَّخصيَّةِ أو تلقِّيها من الحائزِ أو من الجهاتِ المختصَّة بتزويدِه بها بحسَبِ الأحوالِ بعد موافقةِ الشَّخصِ المعنيّ بالبيانات، ورغم أن المُشرِّعَ المصريَّ قد أكَّد ضرورةَ الحصولِ على موافقةٍ صريحةٍ من صاحبِ البياناتِ إلا أنه **يُؤخَذ عليه أنه لم يحدِّد طرقًا معيَّنةً للموافقةِ الصَّريحةِ وهو الأمرُ الذي يفتحُ المجالَ على مصراعيه لتمريرِ عديدٍ من الموافقاتِ بمجرَّد النقرِ عليها، باعتبار أن هذه الموافقةَ أصبحتْ موافقةً صريحةً، وهذا ما يتمُّ**

(199) Castets-Renard, C. (2016). Brève analyse du règlement général de la protection des données. Dalloz IP/IT, 7-8, 331-334.

(200) toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement»

(201) Article 8, Loi sur la protection des renseignements personnels (L.R.C. (1985).

استخدامُه في أغلبِ الأحيانِ عند استخدام أيّ كائنٍ متَّصل، بحيث تأخُذُ الموافقة الصَّريحةَ من المستخدمِ بمجرَّد النَّقرِ على موافق "الموافقةُ بالنَّقرِ"، وهو أمرٌ لا يُحمد عُقباه.

وفي هذا الشَّأن يُحدِّد القانونُ العامُّ لحمايةِ البياناتِ (GDPR) أيضًا شروطَ تنفيذِ متطلَّباتِ الموافقة، حيث تنصُّ الفقرة ٢ من المادة ٧ على سبيلِ المثالِ على أنه "إذا تمَّ إعطاءُ موافقةِ صاحبِ البياناتِ في سياقِ إعلانٍ كتابيٍّ يتعلَّق أيضًا بمسائلَ أخرى، فيجبُ تقديمُ طلبِ الموافقةِ في شكلٍ يُميِّزه بوضوحٍ عن الأسئلةِ الأخرى المطروحة، في شكلٍ مفهومٍ ويُمكن الوصولُ إليه بسهولةٍ، وصياغته بعباراتٍ واضحةٍ وبسيطةٍ[٢٠٢].

ولقد تمَّ تحديدُ عناصرَ أخرى، مثل إمكانيَّةِ أن يكونَ إعلانًا إلكترونيًّا أو كتابيًّا أو شفهيًّا وأنه يجبُ حظرُ بعضِ السُّلوكيَّات، مثل المربعاتِ المحدَّدة افتراضيًّا، حيث تسمحُ هذه العناصرُ لمعالجي البياناتِ بمعرفةِ كيفيَّةِ جمعِ الموافقة، ومما لا شكَّ فيه تعدُّ هذه الطَّرائقُ حاسمةً ومهمَّةً بالنِّسبة للمهنيِّين؛ لأنه يتعيَّن عليهم تقديمُ دليلٍ على هذه الموافقة.

وهناك طرقٌ معينةٌ أخرى للحصولِ على الموافقةِ، ومن بينها نجدُ حقيقةً إضافةَ بندٍ ينصُّ على أن "استخدام الخدمةِ يُشكِّل قبولًا لجمعِ البياناتِ التي ستنجمُ عنها" في الشُّروطِ العامَّةِ لبيعِ منتجٍ أو في الشُّروطِ العامَّة لاستخدامِه. وقد يكونُ أيضًا من خلالِ إضافةِ بندٍ من شأنِه إبلاغ المشتري أو المستخدم بأنه يتمُّ جمعُ بياناتِه ونقلها إلى أطرافٍ ثالثة، وسواءٌ تمَّت صياغةُ هذا البندِ على نطاقٍ واسعٍ أو ضيّق، فسيتمُّ حظرُه بنفسِ الطَّريقة، وبالمثل، لا يُمكن أيضًا أن يقومَ الشَّخصُ الذي يتمُّ جمعُ بياناتِه بإكمالِ نموذجٍ يحتوي على خاناتٍ محدَّدةٍ مسبقًا.

وفي الواقعِ إنَّ فعلَ تحديدِ الصُّندوق هو مظهرٌ من مظاهرِ الموافقة؛ لأنه عملٌ إيجابيٌّ، في حين أنَّه إذا تمَّ تحديدُ الصُّندوقِ بالفعل، فقد يقبلُ الشَّخصُ الجمعَ والمعالجةَ دون أن يكونَ على علمٍ بذلك فعليًّا.

---

(202) «si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples».

(ISSN: 2537- 0758)

الفرع الثالث
مبدأ تقرير المصير المعلوماتي
le principe d'autodétermination informationnelle

في الحقيقة إنَّ المفهومَ الأوروبيَّ لحمايةِ البياناتِ الشَّخصيَّة، بما في ذلك القانونُ الكنديُّ يُشير إلى بعضِ المبادئ، حيث يعتمدُ في البدايةِ على فكرةٍ سيطرةٍ معيَّنةٍ للمُستخدم على بياناته، لكن لو نظرنا في الواقعِ نجدُ بأنَّ هذه الفكرةَ لا تؤتي ثمارَها، ولهذا فقد حرصت اللَّائحةُ العامَّةُ لحمايةِ البياناتِ على إنشاءِ منطقِ التَّنظيمِ الذاتيّ للشَّركاتِ من خلالِ مبادئِ المساءلة، ولكن ثبت أن إطارَها أقلُّ فعاليةً ممَّا توقعه المُشرِّع.

ولقد استندت هذه الأفكارُ إلى تعزيزِ ثقةِ المستخدمِ في هذا الموضوعِ بالشَّيءِ المتَّصل، وضمان موثوقيَّةِ نظامهِ من خلال احترامِ الحقِّ في الخصوصيَّة. وهو ما يتَّضحُ من خلالِ تعريفِ مبدأ تقريرِ المصيرِ المعلوماتيّ[٢٠٣]، حيث يتمُّ تعريفُه بشكلٍ خاصٍّ في المادة (١) من قانونِ حمايةِ البيانات (١٩٧٨)، في صيغتهِ الجديدةِ منذ ١ يونيو ٢٠١٩ بأنه "حقُّ الأفرادِ في تحديدِ ومراقبة استخداماتِ البياناتِ الشَّخصيَّةِ المتعلِّقة بهم مع مراعاةِ الالتزاماتِ الواقعة على عاتقِ الأشخاصِ الذين يقومون بمعالجةِ هذه البيانات. ولهذا نرى بأنه يُمكن إضافةُ حقِّ المستخدمِ في تحديدِ ومراقبة البياناتِ الشَّخصيَّةِ عند استخدامِ كائنٍ متَّصل، وهو ما يجعلنا نقترحُ تعديلَ نصِّ المادة ٢ من قانون حمايةِ البياناتِ الشَّخصيَّةِ رقم ١٥١ لسنة ٢٠٢٠ بإضافةِ إمكانيَّةِ المستخدمِ في تحديدِ ومراقبةِ البيانات الشَّخصيَّةِ ليُصبحَ نصُّ المادة كالآتي:..... ويكون للشَّخصِ المعنيّ بالبياناتِ الحقوقُ الآتية: التَّصحيح أو التَّعديلُ أو المحوُ أو الإضافةُ أو التَّحديثُ للبياناتِ الشَّخصيَّة، مع إمكانيَّةِ تحديدِ ومراقبة استخداماتِ البياناتِ الشَّخصيَّة.

وبمقتضى مبدأ تقريرِ المصيرِ المعلوماتيّ يحقُّ للأفرادِ التحكُّم في بياناتِهم الشَّخصيَّةِ وتحديد كيفيَّةِ جمعِ تلك البياناتِ واستخدامها ومشاركتها، وممَّا لا شكَّ فيه

(203) Cour constitutionnelle fédérale Allemande, 16 février 1983, «BVerfGE».

أنَّ هذا المفهومَ له أهميَّةٌ خاصَّةٌ في سياقِ حمايةِ البياناتِ والخصوصيَّة في العصرِ الرقميّ.

ويُشير هذا المبدأُ إلى إمكانيَّةِ إعادةِ التَّأكيد على الموافقةِ على جمعِ البياناتِ الشَّخصيَّةِ و"صندوق الأدوات" المقدّم للفرد، والذي يُمكن أن يمكِّنه بشكلٍ ملموسٍ من القيامِ بذلك والقدرةِ على التحكُّمِ في البياناتِ التي تستخدمُها الشَّركات.

أولًا: الإعادةُ المتكررة على الموافقةِ على جمعِ البيانات:

تتطلَّبُ المعالجةُ القانونيَّةُ للبيانات الشَّخصيَّةِ موافقةَ صاحبِ البيانات بموجبِ القانونِ الكنديّ والفرنسيّ والمصريّ. وقد تمَّ تعريفُها من قبلِ اللَّائحةِ العامَّة لحمايةِ البياناتِ في المادة ٤ بأنها "أيُّ تعبيرٍ عن الإرادة، حر ومحدَّد ومستنير ولا لبْسَ فيه يقبلُ من خلالهِ صاحبُ البيانات، من خلالِ إعلانٍ أو بموجبِ عملٍ إيجابيٍّ واضحٍ، يفيد بأنَّ البياناتِ الشَّخصيَّةَ المتعلِّقة به تخضعُ للمعالجة"، وهذا تعريفٌ قويٌّ، يضعُ أسسَ استقلاليَّةِ الفرد في التحكُّم في بياناته.

ومن الواضحِ أنَّ من يمنحُ الموافقةَ يُمكنه في الوقتِ ذاته سحبُها في أيِّ وقتٍ من خلال حقِّ المعارضة، وهو مبدأ لم ينصَّ عليه بعد في القوانين الكنديَّةِ المتعلِّقة بالمعلوماتِ الشَّخصيَّة، خلافًا للقانونِ المصريّ الذي يسمحُ بالعدولِ عن الموافقةِ المسبقة على الاحتفاظِ ببياناتهِ الشَّخصيَّة أو معالجتها.

وفي الواقع تُواجه الموافقةُ تحدياتٍ معيَّنةً، فتجريدُ الموافقةِ من النَّاحيةِ الماديَّة له تأثيرٌ على قبولِ الفرد، ناهيك عن أساليبِ التَّنبيهِ التي تسهِّل الموافقةَ التي ليست بالضَّرورةِ مستنيرةً أو حرَّة حقًّا. ولهذا يثورُ التَّساؤلاتُ بشأنِ كيفيَّةِ اعتبارِ الموافقةِ حقيقيَّةً إذا لم يكُنْ لدى المستخدمِ خياراتٌ أخرى؟ حيث إن الرَّفضَ يمنع المستخدمَ من استخدامِ الشَّيء المتَّصل.

والنَّاظرُ إلى المادة ٤٢ من اللَّائحةِ العامَّةِ لحمايةِ البياناتِ يجدُ بأنها تضعُ الأساسَ القويَّ لاحترامِ الموافقة، "لا ينبغي اعتبارُ الموافقةِ مُنحت بحريَّةٍ إذا لم يكُنْ لدى الشَّخصِ المعنيّ حريَّةُ اختيارٍ حقيقيَّة أو لم يكنْ قادرًا على رفضِ الموافقةِ أو سحبها دون التعرُّضِ للأذى".

بيْدَ أن واقعَ الموافقةِ مختلفٌ تمامًا، حيث لا توفِّر الموافقةُ المسبقةُ سوى حمايةٍ أقلَّ إذا وافق الشَّخصُ على كافَّةِ مجموعاتِ البيانات. وفي هذا الشَّأن لاحظ

(ISSN: 2537- 0758)

مستخدمو الإنترنتّ اليوم، على سبيل المثال، أنه يجبُ عليهم الموافقةُ بانتظامٍ على جمعِ بياناتِهم من خلال النَّقرِ على "أقرأ وأوافق" حتى يتمكنوا من الوصولِ إلى الموقعِ الذي يهمُّهم.

وفي الواقع، يستمرُّ المستخدمون في استخدامِ الأشياءِ المُتَّصلةِ ونقل المعلوماتِ الشَّخصيَّة؛ لأنَّ الرَّغبةَ في استخدامِ الخدمةِ تحلُّ محلَّ الرَّغبةِ في حمايةِ بياناتهم الخاصَّة. وفي هذا السِّياق يُشير مدير INRIA، دانييل لو ميتاير، إلى قول: "يبدو أنَّ التطوُّراتِ التِّكنولوجيَّةَ في السَّنواتِ الأخيرة وكذلك الممارساتُ الاجتماعيَّة التي تولِّدها تقوض قدرةَ الأفراد، بل وحتى إرادتُهم، على ممارسةِ سيطرةٍ حقيقيَّةٍ على بياناتِهم الشَّخصيَّة"(٢٠٤).

وتشكِّل التطوُّراتُ التِّكنولوجيَّةُ مثل إنترنت الأشياءِ أو الذَّكاء الاصطناعيّ تحدياتٍ خطيرةً للأطرافِ المشاركةِ في المعاملة، وممَّا لا شكَّ فيه أنَّه لا يُمكن تحديدُ أو توقُّع جميعِ الأسبابِ التي قد تؤدِّي إلى استخدام المعلوماتِ الشَّخصيَّةِ أو الكشف عنها في سوق اليوم سريع الخُطَى، والمُعتمِد على البيانات.

ويبدو أن مبدأَ الموافقةِ كحامٍ حقيقيٍّ لخصوصيَّةِ مستخدمي الأشياءِ المُتَّصلة يمرُّ بأزمةٍ قانونيَّةٍ، ولا يزالُ في قلبِ المناقشاتِ حول استخدامِ الأفرادِ وسيطرتهم الحقيقيَّةِ على بياناتهم، ناهيك عن مبدأ الموافقةِ المقيَّد باستثناءاتٍ عديدةٍ.

ثانيا: ربطُ المعلومات: «Le paquet informationnel»

يعتمد أحد الابتكاراتِ الرئيسة البارزة في نصِّ اللَّائحةِ العامَّة لحمايةِ البياناتِ على مجموعةٍ من الحقوقِ المقدَّمةِ للمستهلكين لإضفاءِ مضمونٍ على حقِّهم في التحكُّمِ في بياناتِهم التي تستخدمُها الشركات، بحيث توفِّر المبادئُ مثل الوصولِ أو التَّصحيح أو التَّحديد أو النَّقل أو حتى المحو فرصةً كبيرةً للفردِ الذي يرغبُ في فهمِ استخدامِ ومدى جمعِ المعلوماتِ المتعلِّقة به(٢٠٥).

(204) Daniel Le Metayer, Christophe Lazaro, «Le consentement au traitement des données personnelles: une perspective comparative sur l'autonomie du sujet», Revue juridique Themis, 43(3), 768-815, 2015.

(205) Voir la définition à l'article 13 du Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la

ثالثًا: الإقرارُ بحقِّ مستخدم الأشياءِ المُتَّصلةِ في تعطيلِ خاصيَّةِ الاتِّصالِ بالشَّبكة:

يتحتَّمُ أن يراعيَ في تصميمِ أو تصنيعِ الشَّيء المتَّصل لا سيَّما المزوَّدة بأنظمةِ الذَّكاءِ الاصطناعيّ عالي المخاطر، وذلك من أجلِ الحمايةِ المقررة للخصوصيَّة، وهو ما يُشير إليه بالحقّ في صمتِ الرقاقة (الشَّريحة) (Right to Silence the Chip) هو مفهومٌ يتعلَّق بالأجهزةِ المُتَّصلةِ والرَّقائق الذكيَّة، ويُشير إلى حقّ المستخدمين في إيقافِ تشغيلِ أو تعطيلِ وظائفِ الاتِّصالِ أو جمع البياناتِ من هذه الأجهزةِ عندما يرغبون في ذلك، هذا الحقُّ يعكسُ أهميَّةَ الخصوصيَّةِ والتَّمكين الرقميّ للأفراد.

ويهدفُ هذا الإجراءُ إلى جعلِ مستخدمِ الأشياءِ المُتَّصلة متحكِّمًا في الشَّيءِ المتَّصل، وذلك من خلال العودةِ إلى الاستخدامِ العاديّ للكائنِ، دون تفاعُلٍ إلكترونيٍّ، بواسطةِ الاحتفاظِ بحقّ المستهلكِ في تعطيلِ اتِّصالِ الجهازِ ومشاركة البياناتِ[٢٠٦]، ويتعيَّن على الشَّركاتِ المصنِّعة إدراجُ هذه الخاصيَّةِ منذ مرحلةِ تصميمِ الشَّيء المتَّصل (الجهاز).

وفي هذا الشَّأن نتَّفق مع الرَّأي الذي يدعو دائمًا إلى الرَّقابةِ البشريَّةِ على الأشياءِ المُتَّصلةِ وبخاصَّةٍ الذَّكيَّة منها والمتوقَّع منها حدوثُ مخاطرَ كبيرةٍ، حيث يتحتَّمُ على مصمِّم هذه الأشياءِ ضرورةُ تصميمِ الجهازِ بما يتَّفق مع حقّ المستخدمِ في الرَّقابةِ والإشرافِ في أيّ مرحلةٍ يتمُّ فيها تشغيلُ النِّظام.

وهذا ما ذهبت إليه لائحةُ الاتِّحادِ الأوروبيّ ١٦٨٩/٢٠٢٤ في نصّ المادة ١٤ منها، حيث تنصُّ على مسألةِ الرَّقابةِ البشريَّة على أنظمةِ الذَّكاءِ الاصطناعيّ، بحيث يجب تصميمُ وتطويرُ أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطرِ من خلالِ استخدامِ

---

directive 95/46/CE. (UE(2016/679 du Parlement européen et du Conseil du 27 avril 2016.

[٢٠٦] د. بشار طلال المومني، د. معمر طرية، التَّحدياتُ القانونيَّةُ المعاصرةُ لاستخداماتِ "إنترنت الأشياء" دراسةٌ في النِّظام القانونيّ الإماراتيّ والمقارن، مجلة كليَّة القانون الكويتيَّة– السَّنة العاشرة– العدد ٤ العدد التَّسلسليُّ ٤٠، سبتمبر ٢٠٢٢، ص٣٠٩.

(ISSN: 2537- 0758)

أدواتٍ معيَّنة، بحيث يُمكن للأشخاصِ الطبيعيّين الإشرافُ عليها بشكلٍ فعَّالٍ أثناء الفترةِ التي تكونُ قيدَ الاستخدامِ. كما تهدفُ الرَّقابةُ البشريَّة إلى منعِ أو تقليلِ المخاطرِ على الصِّحةِ أو السَّلامةِ أو الحقوق الأساسيَّة التي قد تنشأُ عند استخدام نظامِ الذَّكاءِ الاصطناعيّ، وفقًا للغرضِ المقصودِ منه أو في ظلِّ ظروفِ سوءِ الاستخدامِ المتوقَّعة بشكلٍ معقولٍ(٢٠٧).

وفي هذا الصَّددِ يتحتَّم أن تكونَ تدابيرُ الرَّقابةِ متناسبةً مع المخاطرِ ومستوى الاستقلالِ وسياق استخدام نظامِ الذَّكاءِ الاصطناعيّ، ويجب ضمانُها من خلال أحدِ أو كِلَا النَّوعين التَّاليين من التَّدابير:

أولًا: التَّدابيرُ التي تمَّ تحديدُها وبناؤها، عندما تكونُ ممكنةً من النَّاحيةِ الفنيَّة، في نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ من قِبل المزوِّد قبل طرحهِ في السُّوقِ أو وضعهِ في الخدمة.

(207) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Article 14, Human oversight

1 .High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can be effectively overseen by natural persons during the period in which they are in use.

2 .Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular where such risks persist despite the application of other requirements set out in this Section.

3 .The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured through either one or both of the following types of measures:

(a) measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service؛

(b) measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer.

ثانيًا: التَّدابيرُ التي حدَّدها المزوِّد قبل طرحِ نظامِ الذَّكاء الاصطناعيّ عالي المخاطرِ في السُّوق أو وضعه في الخدمةِ، والتي من المناسبِ أن ينفِّذها النَّاشر.

وفي هذا الشَّأن يثورُ التَّساؤلُ: كيف يُمكن للأشخاصِ الطبيعيِّين التمكُّنُ من رقابةِ الشَّيء المتَّصلِ بشكلٍ فعالٍ؟

كي يتمكَّن الأشخاصُ الطبيعيُّون من رقابةِ الشَّيءِ المتَّصلِ وبخاصَّةٍ الأشياءُ عاليةُ المخاطرِ يجب فهمُ القدراتِ والقيودِ ذات الصِّلة بنظامِ الذَّكاء الاصطناعيّ عالي المخاطرِ بشكلٍ صحيحٍ والقدرة على مراقبةِ تشغيلِهِ بشكلٍ صحيحٍ، بما في ذلك الكشفُ عن الشُّذوذِ والاختلالات والأداء غير المتوقَّع ومُعالجتها؛ بالإضافةِ إلى الدِّرايةِ بالميلِ المحتملِ للاعتماد تلقائيًّا أو الاعتماد المفرط على نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ (تحيُّز الأتمتة)؛ لتوفيرِ المعلوماتِ أو التَّوصيةِ ببعض القراراتِ التي يتعيَّن على الأشخاصِ الطبيعيِّين اتِّخاذها؛ كما أنه لا بدَّ وأن يكونَ لديهم تفسيرٌ عن مُخرجاتِ نظامِ الذَّكاء الاصطناعيّ عالي الخطورةِ بشكلٍ صحيحٍ، مع الأخذِ في الاعتبارِ، على سبيل المثال، أدوات وأساليب التَّفسيرِ المُتاحة؛ فضلًا عن أساليبِ اتِّخاذ القرارِ، في أيّ موقفٍ معيَّن. كما يتحتَّم أن يكونَ لدى الأشخاصِ الطبيعيِّين مكنةُ التَّدخلِ في تشغيلِ نظامِ الذَّكاء الاصطناعيّ عالي الخطورة أو مقاطعة النِّظامِ من خلالِ زرّ "إيقاف" أو إجراءٍ مماثلٍ يسمحُ للنِّظامِ بالتوقُّفِ في حالةٍ آمنة[٢٠٨].

---

[٢٠٨] في ذات المعنى راجع:

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Article 14,..... 4. For the purpose of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:

(a) to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance؛

(b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide

(ISSN: 2537- 0758)

كما أنَّه بالنِّسبةِ للأشياءِ المُتَّصلةِ المجهَّزة بأنظمةِ الذَّكاء الاصطناعيّ عاليةِ الخطورة يجبُ أن تتضمَّن التَّدابيرُ عدمَ اتِّخاذ أيّ إجراءٍ أو قرارٍ من قِبل المستخدمِ على أساسِ التَّعريفِ النَّاتج عن النِّظام ما لم يتمَّ التحقُّق من هذا التَّعريفِ بشكلٍ منفصلٍ وتأكيده من قِبل شخصين طبيعيّين على الأقلّ يتمتَّعان بالكفاءةِ والتَّدريب والسُّلطة اللَّازمة[٢٠٩].

الفرع الرَّابع
مبدأ التَّنظيمِ الذاتي للبياناتِ من قبلِ الشَّركات
le principe d'autorégulation

كانت المناقشاتُ في هذا الأمرِ مدفوعةً بالحاجةِ إلى التَّوفيقِ بين مبدأ تداولِ البياناتِ واحترام الحريَّاتِ الفرديَّة. وهكذا تمَّ فرضُ مبدأِ المساءلةِ على جميعِ المشاركين في معالجةِ البيانات، ومعالجي البياناتِ والمتعاقدين من الباطن، وتجدرُ الإشارةُ إلى أنَّ الالتزاماتِ المحدَّدة المخصَّصة للمتعاقدين من الباطنِ ليست موجودةً

information or recommendations for decisions to be taken by natural persons؛

(c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;(d)to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system؛

(e) to intervene in the operation of the high-risk AI system or interrupt the system through a 'stop' button or a similar procedure that allows the system to come to a halt in a safe state.

[٢٠٩] نصَّت لائحةُ الاتِّحاد الأوروبيّ على أنه لا ينطبقُ شرطُ التحقُّقِ المنفصل من قِبل شخصيْنِ طبيعيَّين على الأقلّ على أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطرِ المستخدمةِ لأغراضِ إنفاذِ القانونِ أو الهجرة أو مراقبةِ الحدودِ أو اللُّجوء، حيث يَعدُّ قانونُ الاتِّحادِ أو القانونُ الوطنيُّ أن تطبيقَ هذا الشَّرطِ غيرُ متناسبٍ.

- The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.

بعدُ في قوانين المعلومات الشَّخصيَّةِ في كندا، وهو ما يُمثِّل استقلالًا ذاتيًّا جديدًا للشَّركات، ولهذا يتحتَّم على الجهاتِ الفاعلةِ في معالجةِ البيانات وضعُ تدابيرَ فنيَّةٍ وتنظيميَّة، يتمُّ تحديثُها وتوثيقُها دائمًا(٢١٠).

ويُمكننا التَّمييزُ بين ثلاثِ فئاتٍ من الالتزامات: **مبدأ الشَّفافية، ومبدأ التَّناسب، ومبدأ الأمن.** وفي هذا الشَّأن نبيّن المبادئَ المتعلِّقة بمعالجةِ البياناتِ الشَّخصيَّة، حيث يتحتَّمُ أن تكونَ البياناتُ الشَّخصيَّة(٢١١):

أ- قد تمَّ معالجتُها بطريقةٍ قانونيَّةٍ وعادلةٍ وشفَّافة (الشرعيَّة والأمانة والشَّفافية).

ب-تمَّ جمعُها لأغراضٍ محدَّدةٍ وصريحةٍ ومشروعة.

ج-كافية وذات صلةٍ ومحدودةٌ بما هو ضروريٌّ فيما يتعلَّق بالأغراضِ التي تتمُّ معالجتُها من أجلها (تقليل البيانات).

د- دقيقةٌ وحديثةٌ عند الضَّرورة؛ يجب اتِّخاذ جميع التَّدابيرِ المعقولةِ لضمان مسحِ أو تصحيحِ البياناتِ الشَّخصيَّة غير الدَّقيقة، مع مراعاةِ الأغراضِ التي تتمُّ معالجتُها من أجلها، دون تأخير (الدِّقة).

هـ-يتمُّ الاحتفاظُ بها في نموذجٍ يسمحُ بتحديدِ أصحابِ البياناتِ لفترةٍ لا تتجاوزُ الفترة اللَّازمة للأغراضِ التي تتمُّ معالجتُها من أجلها؛ ويجوزُ الاحتفاظُ بالبياناتِ الشَّخصيَّةِ لفتراتٍ أطول إلى الحدِّ الذي ستتمُّ معالجتُه حصريًّا لأغراضِ الأرشفةِ للمصلحةِ العامَّة، أو لأغراضِ البحثِ العلميّ أو التاريخيّ أو لأغراضٍ إحصائيَّة، مع اتِّخاذ التَّدابيرِ التنظيميَّةِ من أجلِ ضمانِ حقوقِ وحريَّاتِ صاحبِ البيانات (تقييد الاحتفاظ).

---

(210) Mathilde Bondu, Ethique et objets connectés, op. cit.,p. 45.

(٢١١) تجدرُ الإشارةُ إلى أنَّ **مادة (٣) من قانون حمايةِ البياناتِ الشخصيَّةِ المصريّ رقم ١٥١ لسنة ٢٠٢٠، تحدِّد ضوابطَ جمعِ البياناتِ الشخصيَّة، حيث تنصُّ على أنه: "يجبُ لجمعِ البياناتِ الشخصيَّةِ ومعالجتها والاحتفاظ بها، توافر الشُّروط الآتية:**

١- أن تجمعَ البياناتُ الشخصيَّةُ لأغراضٍ مشروعةٍ ومحدَّدةٍ ومعلنةٍ للشَّخص المعنيّ.

٢- أن تكون صحيحةً وسليمةً ومؤمنةً. ٣- أن تعالجَ بطريقةٍ مشروعةٍ وملائمةٍ الأغراضَ التي تمَّ تجميعُها من أجلها ٤- ألا يتمَّ الاحتفاظُ بها لمدَّةٍ أطولَ من المدَّة اللَّازمةِ للوفاءِ بالغرضِ المحدَّد لها....".

(ISSN: 2537- 0758)

و- معالجتها بطريقةٍ تضمَن الأمانَ المناسبَ للبياناتِ الشَّخصيَّة، بما في ذلك الحمايةُ من المعالجةِ غير المصرَّح بها أو غير القانونيَّةِ وضدَّ الفقدانِ العرضيّ أو التَّدمير أو الضَّرر، باستخدامِ التَّدابيرِ الفنيَّةِ أو التنظيميَّةِ المناسبة (النَّزاهة والسريَّة).

أولًا: مبدأ الشَّفافية:

في الحقيقةِ مبدأ الشَّفافيةِ في معالجةِ البياناتِ هو مبدأٌ دوليٌّ، إلا أنَّه قد يبدو في بعضِ الأحيانِ غامضًا للغايةِ؛ نظرًا لواقعِ تطبيقهِ من قِبل الشَّركات. والنَّاظرُ إلى اللَّائحةِ العامَّة لحمايةِ البياناتِ يجد بأنها تنصُّ على أنَّ البياناتِ الشَّخصيَّةَ المتعلِّقة بالأشخاصِ الطَّبيعيّين يتمُّ جمعُها أو استخدامُها أو معالجتها...، بحيث يُمكن الوصولُ بسهولةٍ إلى جميعِ المعلوماتِ والاتِّصالات المتعلِّقة بمعالجةِ هذه البياناتِ الشَّخصيَّة، فضلًا عن سهولةِ الفهم، وصياغتها بعباراتٍ واضحةٍ وبسيطةٍ. كما تُسهم عمليَّةُ الشَّفافيةِ في سيطرة الأفرادِ على بياناتِهم مع شرطِ المعلومات الشَّاملةِ التي تقدِّمها الشَّركات، والتي تمَّ تحديدُ طرقِ تنفيذِها على سبيل المثالِ في الحيثيَّةِ رقم ٥٨ من اللَّائحةِ العامَّة لحمايةِ البيانات: "يتطلَّب مبدأ الشَّفافيةِ أن تكونَ أيُّ معلوماتٍ موجَّهةٍ إلى العامَّةِ أو الشَّخصِ المعنيّ موجزةً وسهلةَ الوصولِ إليها وسهلةَ الفهم، ومصاغةً بعباراتٍ واضحةٍ وبسيطة، بالإضافةِ إلى توضيحِها باستخدامِ العناصرِ المرئيَّةِ عند الاقتضاء.

ومما لا شكَّ فيه أن مبدأَ الشَّفافيةِ يغذِّي مبدأ المسؤوليَّة؛ لأنه يُتيح تسليطَ الضَّوءِ على الإجراءاتِ التي يتَّخذها معالجو البياناتِ لاحترامِ الالتزاماتِ الملقاةِ على عاتقهم[٢١٢].

(212) Observatoire international sur les impacts sociétaux de l'IA et du numér: ique et le Laboratoire de cyberjustice du Canada, «Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA- Document de réponse aux questions posées par la Commission d'accès à l'information du Québec dans le cadre de la consultation sur l'intelligence artificielle», avril 2020, p.39, en ligne: <http://collections.banq.qc.ca/ark:/52327/bs4067010> (consulté le 03/06/2020).

ومع ذلك، تكشف الممارساتُ العمليَّةُ عن صعوبةِ ترجمةِ هذه الالتزامات، وضمان الموافقةِ المستنيرةِ من مستخدمي الأشياءِ المُتَّصلةِ في كثيرٍ من الأحيان، فضلًا عن ضمانِ السريَّةِ أو الخصوصيَّة، ويُمكننا القول: إنَّ هذه الالتزاماتِ قد تكونُ معقَّدةً وطويلةً جدًّا، ووفقًا للواقعِ لا يتمُّ تفعيلُ كافَّةِ هذه الالتزاماتِ عند استخدامِ الشَّيءِ المتَّصلِ لأوَّل مرَّةٍ.

ولضمانِ الشَّفافيةِ يقعُ على عاتقِ الشَّركةِ المصممة للأشياءِ المُتَّصلةِ ضرورةُ الأخذِ بما يُسمَّى "**بنظامِ مراقبةِ ما بعد التَّسويق**" حيث تتمُّ من خلالِ جمعِ ومراجعةِ الخبرةِ المكتسبةِ من استخدامِ هذه الأنظمةِ في السُّوق ومدى تحقيقِها للغرضِ المصنعة من أجلهِ من أجلِ اتِّخاذِ أيِّ إجراءاتٍ تصحيحيَّةٍ أو وقائيَّةٍ ضروريَّةٍ على الفور إذا لزمَ الأمرُ، وهذا ما ذهبتْ إليه لائحةُ (الاتِّحاد الأوروبيّ) ١٦٨٩/٢٠٢٤[٢١٣].

علاوةً على ذلك، فإن منطقَ المساءلةِ لا يُؤتي ثمارَه بالضَّرورة؛ لأنه على الرَّغمِ من الالتزامِ بالشَّفافية، استمرَّت فضائحُ الاستماعِ إلى المتحدِّثين المتَّصلين بالشَّبكةِ في الظُّهور: Google home، أو Alexa، أو حتى Siri...

إلا أنه مع صدورِ لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ فقد تمَّ النصُّ بشكلٍ صريحٍ على الشَّفافية وتوفير المعلوماتِ للمُستخدمين، حيث تنصُّ المادة ١٣ من اللَّائحةِ سالفة الذِّكر بأنه يجبُ تصميمُ وتطويرُ أنظمةِ الذَّكاء الاصطناعيّ وبخاصَّةٍ عاليةُ المخاطرِ بطريقةٍ تضمَن أن يكونَ تشغيلها شفافًا بدرجةٍ كافيةٍ لتمكين المُستخدمين من تفسيرِ مخرجاتِ النِّظام واستخدامه بشكلٍ مناسبٍ، يجب ضمانُ نوعٍ ودرجةٍ مناسبين من الشَّفافيةِ بهدف تحقيقِ الامتثالِ للالتزاماتِ ذات الصِّلة للمزوِّد والمُستخدم. كما يجبُ أن تكونَ الأشياءُ المُتَّصلةُ المدعومة بأنظمةِ الذَّكاءِ

(213) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art. 25) 'post-market monitoring system' means all activities carried out by providers of AI systems to collect and review experience gained from the use of AI systems they place on the market or put into service for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions;

(ISSN: 2537- 0758)

الاصطناعيّ عالية المخاطرِ مصحوبة بتعليماتٍ للاستخدامِ بتنسيقٍ رقميٍّ مناسبٍ تتضمَّن معلوماتٍ موجزةً وكاملةً وصحيحةً وواضحةً وذات صلةٍ، ويُمكن الوصولُ إليها وفهمُها من قِبل المُستخدمين(٢١٤).

وفي الحقيقةِ أنَّ علمَ المستخدمِ بتفسيرِ مُخرجاتِ النِّظام في الشَّيءِ المتَّصلِ وكيفيَّة استخدامهِ بشكلٍ مناسبٍ، أمرٌ في غايةِ الأهميَّة، حيث إنَّ العلمَ المسبقَ لدى المستخدمِ بتعليماتِ الجهازِ المتَّصل بصورةٍ صحيحةٍ وموجزةٍ جعل استخدامَ وتشغيلَ الشَّيء المتَّصل واضحًا وشفافًا لدى المستخدمين.

والسُّؤال الذي يطرحُ نفسَه في هذا الشَّأن، ما هي تعليماتُ الاستخدامِ التي يتحقَّق معها شفافيةُ الاستخدامِ لدى المستخدم؟

في هذا الشَّأن بيَّنَ نصُّ المادة ١٣ من لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ أنه يجبُ أن تحويَ تعليماتُ الاستخدامِ المعلوماتِ التَّاليةَ على الأقلّ:

(أ) هويَّةُ وتفاصيلُ الاتِّصالِ الخاصَّة بالمُستخدم. (ب) خصائصُ وقدراتُ وقيودُ أداءِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر، بما في ذلك: الغرضُ المقصودُ منه؛ ومستوى الدِّقة، بما في ذلك مقاييسُه وقوَّته وأمنُه السيبرانيُّ، والذي تمَّ اختبار نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ والتحقُّق من صحَّتهِ على أساسهِ والذي يُمكن توقُّعه، وأيُّ ظروفٍ معروفةٍ ومتوقَّعةٍ قد تؤثّر على هذا المستوى المتوقَّع من الدقَّةِ

(214) Article 13, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

Transparency and provision of information to deployers

1. High-risk AI systems shall be designed and developed in such a way as to ensure that their operation is sufficiently transparent to enable deployers to interpret a system's output and use it appropriately. An appropriate type and degree of transparency shall be ensured with a view to achieving compliance with the relevant obligations of the provider and deployer set out in Section 3.
2. High-risk AI systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to deployers.

والمتانةِ والأمن السيبرانيّ؛ فضلًا عن أيّ ظرفٍ معروفٍ أو متوقَّع، يتعلَّقُ باستخدامِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ وفقًا للغرضِ المقصودِ منه أو في ظلِّ ظروفِ إساءةِ الاستخدامِ المتوقَّعة بشكلٍ معقولٍ، والتي قد تؤدِّي إلى مخاطرَ على الصِّحةِ والسَّلامةِ أو الحقوق الأساسية[٢١٥].

كما بيَّنت المادة ١٣ المذكورة آنفًا ذلك عند الاقتضاءِ بحسَب الشَّيءِ المتَّصلِ ذاته، حيث يُمكن إضافةُ بعضِ التَّعليماتِ الأخرى للاستخدامِ، مثل أدائهِ فيما يتعلَّق بأشخاصٍ أو مجموعاتٍ محدَّدةٍ من الأشخاصِ الذين من المفترضِ عليهم استخدام الشَّيءِ المتَّصل، فضلًا عن مواصفاتِ بياناتِ الإدخال، أو أي معلوماتٍ أخرى ذات صلةٍ من حيث مجموعاتُ بياناتِ التَّدريبِ والتحقُّق والاختبار المستخدمة، كما أنه عند الاقتضاء، يجبُ على مصمِّم الجهازِ المتَّصلِ إضافةُ معلوماتٍ لتمكين المستخدمين من تفسيرِ مُخرجاتِ نظامِ الذَّكاء الاصطناعيّ عالي المخاطرِ واستخدامها بشكلٍ مناسبٍ؛ فضلًا عن بيانِ التَّغييراتِ التي تطرأُ على نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ وأدائهِ، والتي تمَّ تحديدُها مسبقًا من قِبل المزوِّد في لحظةِ تقييمِ المطابقةِ الأوَّليّ، إن وُجدت[٢١٦].

---

(215) Article 13, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

....."3The instructions for use shall contain at least the following information:

(a) the identity and the contact details of the provider and, where applicable, of its authorised representative؛

(b) the characteristics, capabilities and limitations of performance of the high-risk AI system, including:

(i) its intended purpose؛

(ii) the level of accuracy, including its metrics, robustness and cybersecurity referred to in Article 15 against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;

(216) Article 13, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

(ISSN: 2537- 0758)

كما أن مزوِّد الشَّيءِ المتَّصل ملتزمٌ ببيانِ التَّدابيرِ الفنيَّةِ الموضوعة لتسهيلِ تفسيرِ مخرجاتِ أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطرِ من قِبل المستخدمين؛ والموارد الحاسوبيَّةِ والأجهزةِ اللَّازمة، والعمر المتوقَّع لنظامِ الشَّيءِ المتَّصل، وأي تدابير صيانةٍ ورعايةٍ ضروريَّة؛ لضمانِ الأداءِ السَّليم لنظامِ الذَّكاءِ الاصطناعيّ، بما في ذلك تحديثاتُ البرامج(٢١٧).

وفي السِّياق ذاته تنصُّ المادة ٥٠ من لائحةِ الاتِّحاد الأوروبيّ رقم ١٦٨٩/٢٠٢٤ على التزاماتِ الشَّفافيةِ لمقدِّمي ومشغِّلي أنظمةِ الذَّكاء الاصطناعيّ، حيث يقع على عاتقِ مقدِّمي أومشغِّلي عديدٍ من التزاماتِ الشفاقية(٢١٨)، حيث يجبُ

(v) when appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used؛
(vi)when appropriate, specifications for the input data, or any other relevant information in terms of the training, validation and testing data sets used, taking into account the intended purpose of the high-risk AI system؛
(vii)where applicable, information to enable deployers to interpret the output of the high-risk AI system and use it appropriately؛
(c) the changes to the high-risk AI system and its performance which have been pre-determined by the provider at the moment of the initial conformity assessment, if any;.."

(217) Article 13, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

(d) the human oversight measures referred to in Article 14, including the technical measures put in place to facilitate the interpretation of the outputs of the high-risk AI systems by the deployers؛
(e) the computational and hardware resources needed, the expected lifetime of the high-risk AI system and any necessary maintenance and care measures, including their frequency, to ensure the proper functioning of that AI system, including as regards software updates؛
(f) where relevant, a description of the mechanisms included within the high-risk AI system that allows deployers to properly collect, store and interpret the logs in accordance

(٢١٨) راجع:

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art. (5٠).

على مقدِّمي الخدماتِ ضمان تصميمِ وتطويرِ أنظمة الذَّكاء الاصطناعيّ المخصَّصة للتَّفاعلِ المباشرِ مع الأشخاصِ الطَّبيعيّين بطريقةٍ تجعلُ الأشخاصَ الطبيعيّين المعنيّين على علمٍ بأنهم يتفاعلون مع نظامِ الذَّكاءِ الاصطناعيّ، ما لم يكنْ ذلك واضحًا من وجهةِ نظرِ شخصٍ طبيعيٍّ يتمتَّعُ بقدرٍ معقولٍ من المعرفةِ والملاحظةِ والحذر، مع مُراعاةِ الظُّروفِ وسياق الاستخدام.

وفي هذا الشَّأن وضع الاتِّحادُ الأوروبيُّ استثناءً يتمثَّل في عدمِ انطباقِ هذا الالتزامِ على أنظمةِ الذَّكاء الاصطناعيّ المصرَّح بها قانونًا للكشفِ عن الجرائمِ الجنائيَّةِ أو منعها أو التَّحقيق فيها أو مقاضاة مرتكبيها، مع مراعاةِ الضَّماناتِ المناسبةِ لحقوق وحريَّاتِ الأطرافِ الأخرى، ما لم تكُنْ هذه الأنظمةُ متاحةً للجمهورِ للإبلاغِ عن جريمةٍ جنائيَّةٍ.

كما يقعُ على عاتقِ مقدِّمي الأشياءِ المُتَّصلةِ المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ،- بما في ذلك أنظمةُ الذَّكاءِ الاصطناعيّ للأغراضِ العامَّة، التي تولِّد محتوًى صوتيًّا أو صوريًّا أو فيديو أو نصيًّا اصطناعيًّا-، التزامٌ بضمانِ تمييزِ مخرجاتِ نظامِ الذَّكاء الاصطناعيّ بتنسيقٍ قابلٍ للقراءة آليًّا واكتشاف ما إذا تمَّ التَّلاعبُ بها بشكلٍ مصطنعٍ. ويتعيَّن على مقدِّمي خدماتِ الذَّكاء الاصطناعيّ ضمان فعاليَّةِ حلولهم التقنيَّة وقابليتها للتَّشغيلِ المتبادلِ وقوَّتها وموثوقيَّتها بقدرِ ما هو ممكنٌ من النَّاحيةِ التقنيَّة، مع مراعاةِ خصوصيَّات، وقيودِ أنواعٍ مختلفةٍ من المحتوى وتكاليف التَّنفيذِ والحالة الفنيَّة المعترف بها عمومًا، كما قد تنعكسُ في المعاييرِ التقنيَّةِ ذات الصِّلة.

ثانيا: **مبدأ التَّناسب**:

يُشير هذا المبدأُ إلى تقليلِ البياناتِ والالتزامِ بالغرض، والنَّاظر إلى اللَّائحةِ العامَّةِ لحمايةِ البيانات، يجدُ بأنها تؤكِّدُ أنه يجبُ أن تكونَ الأغراضُ المحدَّدةُ لمعالجةِ البياناتِ الشَّخصيَّةِ صريحةً ومشروعةً، ويتمُّ تحديدُها عند جمعِ البياناتِ الشَّخصيَّة. ويجب أن تكونَ البياناتُ الشَّخصيَّةُ كافيةً وذات صلةٍ ومقتصرةً على ما هو ضروريٌّ للأغراضِ التي تتمُّ معالجتُها من أجلها، ولذلك فرض المُشرِّعُ مبدأَ التَّناسبِ في جمعِ

(ISSN: 2537- 0758)

البيانات. وهو ما ذهبَ إليه أيضًا المُشرّعُ المصريُّ في قانونِ حمايةِ البياناتِ الشَّخصيَّة رقم ١٥١ لسنة ٢٠٢٠م[٢١٩].

وعلى ذلك يقعُ على عاتقِ الشَّركاتِ احترامُ تقليلِ البياناتِ إلى الحدِّ الأدنى، وذلك تحقيقًا لمبدأ التَّناسبِ من أجلِ تحقيقِ توازنٍ عادلٍ بين حمايةِ الحياةِ الخاصَّة وحريَّة الأعمال، كون أنَّ البياناتِ تلعبُ دورًا مهمًّا في التَّنميةِ الاقتصاديَّةِ.

وتُمثِّل هذه المبادئُ مشكلةً خاصَّةً فيما يتعلَّق بالأشياءِ المُتَّصلةِ المجهزة بالذَّكاءِ الاصطناعيّ. وكما ذكرنا سلفًا يتطلَّب الذَّكاءُ الاصطناعيُّ تغذيةَ كميَّةٍ كبيرةٍ من البيانات، وقد يكون من الصَّعبِ أحيانًا شرحُ تشغيله، لا سيَّما فيما يتعلَّقُ بالنتائجِ التي يقدِّمها. وبالتالي، فإنَّ التَّوفيقَ بين مبدأِ التَّقليل والتَّناسبِ مع الشيءِ المتَّصلِ هو مسألةٌ تتمُّ مناقشتُها باستمرارٍ، فإلى أيّ مدًى تكونُ البياناتُ ضروريَّةً للغايةِ ولأيّ أغراضٍ؟، مع العلمِ أنَّ الشَّيءَ المتَّصلَ قد أصبحَ مثاليًّا بفضلِ حجمِ البياناتِ المهمَّة التي تمَّ جمعُها.

ولهذا السَّببِ لا يبدو أن مبدأَ التَّناسبِ في معالجة البياناتِ الشَّخصيَّةِ هو الأسهلُ في التَّنفيذِ والتحكُّم، ولهذا يثيرُ التَّساؤلُ عما إذا كان هذا المبدأُ كافيًا لحمايةِ خصوصيَّةِ مستخدمي الأشياءِ المُتَّصلة. وفي هذا الشَّأن تثيرُ ملاحظةُ الأستاذين السيِّدة بنسون والسيد لوازو الانتباهَ، فهل من الواقعيّ أن نضمَن افتراضيًّا، أن المعالجةَ تقتصرُ على ما هو ضروريٌّ للغايةِ فيما يتعلَّقُ بالغرضِ المحدَّد للمعالجةِ في مجالٍ يكون فيه التراكمُ والمدى والمدَّةُ على وجهِ التَّحديدِ هم أساس وجودِه وتطوُّره؟[٢٢٠].

وفي هذا الشَّأن نُشير إلى السِّياسةِ التَّشريعيَّةِ الأوروبيَّة، في مجالِ حمايةِ الخصوصيَّةِ فيما يتعلَّق بالأشياءِ المُتَّصلة، والتي تعدُّ نموذجًا يُمكن الاهتداءُ به للحدِّ من انتهاكاتِ الخصوصيَّةِ التي تُشكِّلها الأشياءُ المُتَّصلة، حيث أفردت الحمايةُ طوال فترةِ استخدامِ هذه الأشياء، بل امتدَّت إلى مرحلةِ الصُّنع والتَّصميم بموجبِ توجيهِ

---

[٢١٩] **مادة (٣): يجبُ لجمعِ البياناتِ الشخصيَّة ومعالجتها والاحتفاظ بها، توافرُ الشُّروطِ الآتية:**....." أن تعالجَ بطريقةٍ مشروعةٍ وملائمةٍ للأغراضِ التي تمَّ تجميعُها من أجلِها".

[220] Mathilde Bondu, Ethique et objets connectés, op. cit,p. 47.

الاتِّحاد الأوروبيّ رقم ٢٠١٦-٦٧٩ في ٢٧ أبريل ٢٠١٦ بشأن حمايةِ البياناتِ الشَّخصيَّة.

ثالثاً: حمايةُ الخصوصيَّةِ بحسَبِ التَّصميمِ وحماية الخصوصيَّة بشكلٍ افتراضي:

Protection des données dès la conception et protection des données par défaut

يختصُّ توجيهُ الاتِّحاد الأوروبيّ رقم ٢٠١٦-٦٧٩ في ٢٧ أبريل ٢٠١٦ بحمايةِ الخصوصيَّة، في ظلِّ استخدامِ الأشياءِ المُتَّصلة، من خلال تكريسِ نهجي حمايةِ الخصوصيَّةِ بحسَبِ التَّصميم وحمايةِ الخصوصيَّة بشكلٍ افتراضيٍّ، ويعدُّ هذان المبدآن بمثابةِ أداةٍ لإدارةِ مخاطرِ حمايةِ المعلومات المستخدمة لتشغيلِ الأشياءِ المُتَّصلة، وذلك من خلالِ العملِ على حظرِ المساسِ بخصوصيَّةِ المُستخدمين ومراقبة مدى التزامِ المصمم، وكذلك المنتجُ بالالتزامِ بحمايةِ الخصوصيَّةِ بدءًا من مرحلةِ تصميمِ النِّظام، وحتى أثناء المعالجةِ، ومرورًا بمراحلِ تطويرِهِ وتحديثِهِ[٢٢١].

ولقد تمَّ الإشارةُ لمفهومِ الخصوصيَّةِ بحسَبِ التَّصميمِ في المادَّتين ٧٨ و١٠٨ من اللَّائحةِ العامَّةِ لحمايةِ البيانات[٢٢٢]، حيث تنصُّ المادة ٧٨ من اللَّائحةِ العامَّةِ لحمايةِ البياناتِ على أنه "تتطلَّب حمايةُ حقوقِ وحرياتِ الأشخاصِ الطبيعيّين فيما يتعلَّق بمعالجةِ البياناتِ الشَّخصيَّة اعتمادَ التَّدابيرِ الفنيَّةِ والتنظيميَّةِ المناسبةِ لضمان

---

[٢٢١] د. بشار طلال المومني، د. معمر طرية، التَّحدياتُ القانونيَّةُ المعاصرةُ لاستخداماتِ "إنترنت الأشياء" دراسةٌ في النِّظام القانونيّ الإماراتيّ والمقارن، مجلة كليَّة القانون الكويتيَّة- السَّنة العاشرة- العدد ٤ العدد التَّسلسلي ٤٠، سبتمبر ٢٠٢٢، ص٣٠٧.

[٢٢٢] المادة ١٠٨ من اللَّائحةِ العامَّة لحمايةِ البيانات ".....ويجبُ أن تتعلَّقَ هذه الضَّماناتُ، على وجه الخصوص، بالامتثالِ للمبادئ العامَّة المتعلِّقة بمعالجةِ البياناتِ الشخصيَّةِ ومبادئ حمايةِ البيانات بحسَبِ التَّصميمِ وحماية البياناتِ افتراضيًّا.

Ces garanties devraient porter, en particulier, sur le respect des principes généraux concernant le traitement des données à caractère personnel et des principes de protection des données dès la conception et de protection des données par défaut.

(ISSN: 2537- 0758)

احترامِ متطلباتِ هذه اللَّائحة. لكي يكونَ قادرًا على إثباتِ الامتثالِ لهذه اللَّائحة، يجبُ على المراقبِ اعتمادُ قواعدَ داخليَّةٍ وتنفيذ التَّدابيرِ التي تَحترم، على وجهِ الخصوص، مبادئ حمايةِ البياناتِ بحسَبِ التَّصميمِ وحماية البياناتِ الافتراضيَّة. يُمكن أن تشملَ هذه التَّدابير، في جملةِ أمورٍ، تقليل معالجةِ البياناتِ الشَّخصيَّة إلى الحدِّ الأدنى، وإعطاء أسماءٍ مستعارةٍ للبياناتِ الشَّخصيَّةِ حيثما أمكن ذلك، وضمان الشَّفافيةِ فيما يتعلَّقُ بوظائفِ ومعالجةِ البياناتِ الشَّخصيَّة، للسَّماحِ لصاحبِ البيانات بالتحكُّم في معالجةِ البيانات، للسَّماحِ لمراقبِ البياناتِ لتنفيذِ التَّدابيرِ الأمنيَّةِ أو تحسينها. عند تطويرِ وتصميمِ واختيارِ واستخدامِ التَّطبيقات والخدمات والمنتجاتِ التي تعتمدُ على معالجةِ البياناتِ الشَّخصيَّةِ أو معالجة البياناتِ الشَّخصيَّةِ للوفاء بوظائفها، يجب تشجيعُ مصنِّعي المنتجات ومقدِّمي الخدماتِ ومنتجي التَّطبيقاتِ على أخذِ الحقِّ في حمايةِ البياناتِ في الاعتبار. مع مراعاةِ–عند تطويرِ وتصميمِ مثل هذه المنتجاتِ والخدماتِ والتَّطبيقات– حالةِ المعرفة؛ للتأكُّد من أنَّ مراقبي البياناتِ والمقاولين من الباطنِ قادرون على الوفاءِ بالتزاماتهم المتعلِّقة بحمايةِ البيانات. وينبغي أيضًا أن تؤخَذ في الاعتبارِ مبادئ حمايةِ البياناتِ بحسب التَّصميمِ وحماية البياناتِ افتراضيًّا في المشترياتِ العامَّة[٢٢٣]، ولكنْ بشكلٍ خاصٍّ في المادة ٢٥،

(223) La protection des droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel exige l'adoption de mesures techniques et organisationnelles appropriées pour garantir que les exigences du présent règlement sont respectées. Afin d'être en mesure de démontrer qu'il respecte le présent règlement, le responsable du traitement devrait adopter des règles internes et mettre en œuvre des mesures qui respectent, en particulier, les principes de protection des données dès la conception et de protection des données par défaut. Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer. Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits qui reposent sur le

حيث يحدِّد المُشرِّعُ على سبيلِ المثالِ أنه يعني ضمنًا أن تتَّخذَ الشَّركاتُ التَّدابيرِ الفنيَّةِ والتنظيميَّة المناسبة، التي تهدفُ إلى تنفيذِ المبادئ المتعلِّقة بحمايةِ البيانات، والتي سبق وأن نوَّهنا عنها سابقًا مثل تقليلِ البياناتِ أو شفافيتها. ولذلك يهدفُ هذا المبدأُ إلى ضمانِ احترامِ حقوقِ الأشخاصِ المتأثِّرين بالمعالجة، وقد تمَّ تصميمُه كمبدأٍ توجيهيٍ يؤثِّر على سلوكِ الشَّركات.

وفي هذا الشَّأن تنصُّ المادة ٢٥ من اللَّائحةِ العامَّةِ لحمايةِ البيانات **RGPD** على حمايةِ الخصوصيَّةِ بحسَبِ التَّصميمِ، حيث تنصُّ على أنه: مع الأخذِ في الاعتبارِ حالة المعرفةِ وتكاليف التَّنفيذِ وطبيعة المعالجةِ ونطاقها وسياقها وأغراضها، فضلًا عن المخاطرِ، التي تختلفُ في درجةِ احتمالها وخطورتِها، التي تمثِّلها المعالجةُ فيما يتعلَّق بحقوقِ وحرياتِ الأشخاصِ الطبيعيِّين، ينفذ معالج البيانات، سواءٌ عند تحديدِ وسائلِ المعالجةِ أو أثناء المعالجةِ نفسها، التَّدابير الفنيَّة والتنظيميَّة المناسبة، مثل الأسماءِ المستعارة، والتي تهدفُ إلى تنفيذِ المبادئِ المتعلِّقة بحمايةِ البيانات، على سبيل المثال تقليل البيانات، بشكلٍ فعالٍ وتوفير المعالجةِ مع الضَّماناتِ اللَّازمةِ لتلبيةِ متطلَّباتِ هذه اللَّائحةِ ولحمايةِ حقوقِ صاحبِ البيانات[٢٢٤].

---

traitement de données à caractère personnel ou traitent des données à caractère personnel pour remplir leurs fonctions, il convient d'inciter les fabricants de produits, les prestataires de services et les producteurs d'applications à prendre en compte le droit à la protection des données lors de l'élaboration et de la conception de tels produits, services et applications et, compte dûment tenu de l'état des connaissances, à s'assurer que les responsables du traitement et les soustraitants sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de proection des données par défaut devraient également être pris en considération dans le cadre des marchés publics.

(224) Article 25- Protection des données dès la conception et protection des données par défaut Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et

(ISSN: 2537- 0758)

ربَّما من أجلِ منعِ التطوُّراتِ التِّكنولوجيَّة وعدم إضفاءِ المثاليَّةِ على "مبدأ التَّنظيمِ الذاتيّ للشَّركات"، أدرجت اللَّائحةُ العامَّةُ لحمايةِ البياناتِ مفهوم "الخصوصيَّة خلالَ مرحلةِ تصميمِ الخدمةِ Design by Privacy،" ويتطلَّب هذا المبدأُ دمجَ حمايةِ البياناتِ من تصميمِ أدواتِ جمعِ البياناتِ ومعالجتها واستغلالها من خلالِ التوصيةِ بنهجٍ استباقيٍّ من قِبل معالجِ البياناتِ من أجلِ منعِ مخاطر انتهاكِ الخصوصيَّةِ مسبقًا، والتي يجبُ أن تستمرَّ طوالَ فترةِ الاحتفاظِ بالبيانات(٢٢٥).

كما تُشير المادَّة ٢٥ أيضًا إلى مبدأِ حمايةِ الخصوصيَّةِ بشكلٍ افتراضيٍّ، حيث تنصُّ على أنه يقعُ على عاتقِ وحدةِ التحكُّم اتِّخاذ التَّدابيرِ الفنيَّةِ والتنظيميَّةِ المناسبةِ لضمان معالجةِ البيانات الشَّخصيَّةِ الضروريَّة لكلِّ غرضٍ محدَّد من المعالجة، بشكلٍ افتراضيٍّ. وينطبقُ هذا على كميَّةِ البياناتِ الشَّخصيَّة التي تمَّ جمعُها، ومدى معالجتِها، وفترة الاحتفاظِ بها، وإمكانيَّة الوصولِ إليها. وعلى وجهِ الخصوصِ، تضمن هذه التَّدابير عدم إتاحةِ البياناتِ الشَّخصيَّة، افتراضيًّا، لعددٍ غير محدَّدٍ من الأشخاصِ الطَّبيعيّين دون تدخُّلِ الشَّخصِ الطَّبيعيّ المعنيّ(٢٢٦).

---

organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigencesdu présent règlement et de protéger les droits de la personne concernée.

(225) Célia Zolinsky, «La Privacy by Design appliquée aux Objets Connectés: vers une régulation efficiente du risque informationnel?», Dalloz IP/IT 2016. p.404.

(226) Article 25- Protection des données dès la conception et protection des données par défaut.

Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données àcaractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

ومبدأ الخصوصيَّة بحسَبِ التَّصميمِ (Privacy by Design) هو إطارُ عملٍ يهدفُ إلى دمجِ الخصوصيَّةِ في جميعِ مراحلِ تصميمِ وتطويرِ الأنظمةِ والعمليَّات، بما في ذلك حمايةُ الخصوصيَّةِ بشكلٍ افتراضيٍ ويعتمدُ هذان المبدآن على عدَّة أسسٍ، **منها:**

- **الاستباقيَّة:** يتمُّ اتِّخاذُ تدابيرَ لحماية الخصوصيَّةِ قبل حدوثِ المشكلاتِ بدلًا من التَّعاملِ معها بعد وقوعِها.
- **الافتراض بالخصوصيَّة:** يجبُ أن تكونَ الخصوصيَّةُ هي الوضعَ الافتراضيَّ؛ ممَّا يعني أن البياناتِ الشَّخصيَّةَ يجبُ أن تكونَ محميَّةً بشكلٍ تلقائيٍ.
- **الحدُ من البيانات:** يجبُ أن يكونَ جمعُ البياناتِ محدودًا فقط لما هو ضروريٌّ لتحقيقِ الأغراضِ المحدَّدة.
- **الحماية الشَّاملة:** يجب أن تتضمَّن الأنظمةُ تدابيرَ أمنيَّةً قويَّةً لحمايةِ البياناتِ الشَّخصيَّة.
- **الشَّفافية:** يجبُ أن يكون لدى الأفرادِ معلوماتٌ واضحةٌ حول كيفيَّةِ استخدامِ بياناتهم، ويجب أن تكونَ العمليَّاتُ سهلةَ الفهم.
- **احترامُ حقوقِ الأفراد:** يجبُ أن يتمكَّن الأفرادُ من التحكُّم في بياناتِهم الشَّخصيَّة، بما في ذلك القدرةُ على الوصولِ إليها وتعديلها وحذفها.

وبتطبيقِ هذا المبدأ، يُمكن تعزيزُ الثِّقةِ بين الأفرادِ والجهات التي تتعاملُ مع بياناتهم؛ ممَّا يُسهم في تحسينِ الأمانِ وحماية الخصوصيَّة.

وفي السِّياق ذاته من أجلِ حمايةِ مستخدمي الأشياءِ المُتَّصلةِ يتحتَّم أن تراعي الشَّركاتُ المصمِّمة عند تصميمِ أيِّ نظامٍ من أنظمةِ الذَّكاء الاصطناعيِّ في الجهازِ المتَّصلِ الدقَّةَ والمتانةَ والأمنَ السيبرانيَّ، فضلًا عن وضعِ آليَّةٍ تسمحُ بالحفظِ التلقائيِّ للأحداث.

وفيما يتعلقُ بمسألةِ الدِّقةِ والمتانةِ والأمنِ السيبرانيِّ فقد نصَّت المادة ١٥ من لائحةِ الاتِّحاد الأوروبيِّ ١٦٨٩/٢٠٢٤ على أنه يجبُ تصميمُ وتطويرُ أنظمةِ الذَّكاء الاصطناعيِّ، وبخاصَّةٍ الأجهزةُ عاليةُ المخاطرِ بطريقةٍ تضمَن تحقيقَ مستوًى مناسبٍ من الدقَّةِ والمتانةِ والأمن السيبرانيِّ، وأن تعملَ بشكلٍ متَّسقٍ في هذه النَّواحي طوالَ

(ISSN: 2537- 0758)

دورةِ حياتها. ليس هذا فحسْب، بل لا بدَّ من الإعلانِ عن مستوياتِ ومقاييسِ الدقَّةِ ذات الصِّلةِ لأنظمةِ الذَّكاء الاصطناعيّ عاليةِ المخاطرِ في تعليماتِ الاستخدامِ المصاحبة(٢٢٧).

وفي السِّياق ذاته يجبُ أن تكونَ الأشياءُ المُتَّصلةُ المدعومة بأنظمةِ الذَّكاءِ الاصطناعيّ مرنة قدرَ الإمكانِ فيما يتعلَّق بالأخطاءِ أو الأعطال أو التَّناقضاتِ التي قد تحدثُ داخلَ النِّظامِ أو البيئةِ التي يعملُ فيها النِّظام، وخاصَّةً بسببِ تفاعلها مع الأشخاصِ الطَّبيعيّين أو الأنظمة الأخرى. كما يجبُ اتِّخاذُ التَّدابيرِ الفنيَّةِ والتنظيميَّة في هذا الصَّدد. ولتحقيقِ قوَّةٍ في أنظمةِ الذَّكاءِ الاصطناعيّ يُمكن الاستفادةُ من خلالِ حلولِ التَّكرار الفنيّ، والتي قد تشملُ خططَ النَّسخِ الاحتياطيّ أو خططَ الأمانِ من الفشل.

كما يتحتَّمُ على المصمِّم تطويرُ الأشياءِ المُتَّصلةِ المدعوَّة بأنظمةِ الذَّكاءِ الاصطناعيّ التي تستمرُّ في التعلُّم بعد طرحِها في السُّوقِ أو وضعها في الخدمةِ بطريقةٍ تقضي على أو تقلِّل قدرَ الإمكانِ من خطرِ تأثيرِ المخرجاتِ المتحيِّزة المحتملة على المدخلاتِ للعمليَّاتِ المستقبليَّة (حلقات التَّغذية الرَّاجعة)، ولضمانِ معالجةِ أيّ حلقاتِ تغذيةٍ مرتدةٍ على النَّحوِ اللَّائقِ بتدابيرِ التَّخفيفِ المناسبة.

---

(227) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, Article 15. High-risk AI systems shall be designed and developed in such a way that they achieve an appropriate level of accuracy, robustness, and cybersecurity, and that they perform consistently in those respects throughout their lifecycle.

2. To address the technical aspects of how to measure the appropriate levels of accuracy and robustness set out in paragraph 1 and any other relevant performance metrics, the Commission shall, in cooperation with relevant stakeholders and organisations such as metrology and benchmarking authorities, encourage, as appropriate, the development of benchmarks and measurement methodologies.

3. The levels of accuracy and the relevant accuracy metrics of high-risk AI systems shall be declared in the accompanying instructions of use.

ونرى من وجهةِ نظرنا أنه يقعُ على عاتقِ مصمِّم الجهازِ المتَّصلِ لا سيَّما المزوَّدُ بأنظمةِ الذَّكاءِ الاصطناعيّ عاليةِ المخاطرِ تصميم آليَّةٍ مرنةٍ ضدَّ محاولاتِ الغير غير المسموحِ لهم باستخدامِ الشَّيء المتَّصل باستغلالِ نقاطِ ضَعفِ النِّظام. مع التزامِ مصمِّم الجهازِ بتقديمِ الحلولِ الفنيَّةِ التي تهدف إلى ضمانِ الأمنِ السيبرانيّ لأنظمةِ الذَّكاء الاصطناعيّ عاليةِ المخاطر، بحيث تكون مناسبةً للظُّروفِ والمخاطرِ ذات الصِّلة.

وعلى الجانبِ الآخر نصَّت المادة ١٢ لائحة الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ على آليَّةِ الحفظِ التلقائيّ للأحداث، والتي تنصُّ على أنه يتحتَّم أن تتضمَّن أنظمةُ الذَّكاءِ الاصطناعيّ عند تصميمِها لا سيما الأجهزةُ عاليةُ المخاطرِ آليَّةً لحفظِ السِّجلات[٢٢٨]، **وذلك وفقًا لما يلي:**

١. يجب أن تسمَحَ أنظمةُ الذَّكاءِ الاصطناعيّ عالية المخاطرِ من الناحيةِ الفنيَّةِ بالتَّسجيلِ التلقائيّ للأحداثِ (السِّجلات) طوال عمرِ النِّظام.

---

[228] Article 12 Record-keeping

1. High-risk AI systems shall technically allow for the automatic recording of events (logs) over the lifetime of the system.
2. In order to ensure a level of traceability of the functioning of a high-risk AI system that is appropriate to the intended purpose of the system, logging capabilities shall enable the recording of events relevant for:

(a) identifying situations that may result in the high-risk AI system presenting a risk within the meaning of Article 79(1) or in a substantial modification؛

(b) facilitating the post-market monitoring referred to in Article 72; and (c) monitoring the operation of high-risk AI systems referred to in Article 26.(٥)

3. For high-risk AI systems referred to in point 1 (a), of Annex III, the logging capabilities shall provide, at a minimum:

(a) recording of the period of each use of the system (start date and time and end date and time of each use)؛

(b) the reference database against which input data has been checked by the system ؛

(c) the input data for which the search has led to a match؛

(d) the identification of the natural persons involved in the verification of the results, as referred to in Article 14(5).

(ISSN: 2537- 0758)

٢. من أجل ضمانِ مستوى إمكانيَّةِ تتبُّع عملِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ مناسبٍ للغرضِ المقصودِ من النِّظام، يجبُ أن تمكن أنظمة التَّسجيلِ من تسجيلِ الأحداثِ ذات الصِّلة ب: (أ) تحديد المواقفِ التي قد تؤدّي إلى أن يشكِّل نظامُ الذَّكاءِ الاصطناعيّ عالي المخاطر خطرًا أو في تعديلٍ كبيرٍ. ب) مراقبة تشغيلِ أنظمةِ الذَّكاءِ الاصطناعيّ عالية المخاطر لحمايةِ مُستخدميه.

٣. بالنِّسبةِ لأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر، يجب أن توفِّر قدراتُ التَّسجيل، على الأقلّ: (أ) تسجيل فترةِ كلّ استخدامٍ للنِّظام (تاريخ ووقت البدءِ وتاريخ ووقت الانتهاءِ لكلّ استخدام)؛ (ب) قاعدة البياناتِ المرجعيَّة التي تمَّ التحقُّقُ من بياناتِ الإدخالِ من خلالها بواسطةِ النِّظام؛ (ج) بيانات الإدخالِ التي أدَّى البحثُ إلى مطابقتها؛ (د) تحديد الأشخاصِ الطبيعيّين المشاركين في التحقُّق من النَّتائج.

وفي الإطارِ ذاته تنصُّ المادة ١٩ من لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ على أنه يجبُ على مزوّدي الأشياءِ المُتَّصلةِ المرتبطة بأنظمةِ الذَّكاءِ الاصطناعيّ عاليةِ المخاطرِ الاحتفاظ بالسِّجلاتِ، والتي يتمُّ إنشاؤها تلقائيًّا بواسطةِ أنظمةِ الذَّكاء الاصطناعيّ، إلى الحدِّ الذي تخضعُ فيه هذه السِّجلاتُ لسيطرتهم لفترةٍ مناسبةٍ للغرضِ المقصودِ من نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر، لا تقلُّ عن ستَّة أشهرٍ، ما لم ينصّ على خلافِ ذلك في قانونِ الاتِّحاد أو القانونِ الوطنيّ المعمول به، وخاصَّةً في قانونِ الاتِّحاد بشأنِ حمايةِ البياناتِ الشَّخصيَّة[٢٢٩].

---

(229) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, Article 19.

1. Providers of high-risk AI systems shall keep the logs referred to in Article 12(1), automatically generated by their high-risk AI systems, to the extent such logs are under their control. Without prejudice to applicable Union or national law, the logs shall be kept for a period appropriate to the intended purpose of the high-risk AI system, of at least six months, unless provided otherwise in the applicable Union or national law, in particular in Union law on the protection of personal data.

بالإضافة إلى هذه المبادئ، يتمُّ العملُ المستمرُّ والحاسم في فرنسا وكندا في مجالِ الأخلاقِ والتِكنولوجيا الرقميَّة. فعلى سبيلِ المثال، أنشأ قانونُ الجمهوريَّةِ الرقميَّة المعتمد في عام ٢٠١٦ مهمَّة التَّفكيرِ الأخلاقيّ الموكلة إلى CNIL[٢٣٠]، ويعزِّز قانونُ البياناتِ الشَّخصيَّة الصَّادر في ٢٠ يونيو ٢٠١٨ سلطة CNIL من أجلِ سنِّ معايير القانونِ غير الملزم. وفي كندا، يتمُّ العملُ الحاليُّ بشأنِ إصلاحِ القانونين المتعلِّقين بالمعلوماتِ الشَّخصيَّة، حيث تتيحُ هذه المبادئُ الأخلاقيَّة تجاوزَ التَّنظيمِ الذي يتمحورُ بشكلٍ رئيسٍ حول الفرد، إلا أنَّ الواقعَ مختلفٌ تمامًا، ويبدو أنَّ المبدأ يسلِّط الضَّوءَ على عدمِ كفايةِ التَّنظيم، حتى مع المبادئِ الأخلاقيَّة، في مواجهةِ القوَّة السوقيَّةِ للشَّركاتِ الرقميَّة.

ومع ذلك، فمن الواضحِ أنه على الرَّغمِ من هذا الإطارِ الأخلاقيّ بالإضافةِ إلى النُّصوصِ المتعلِّقة بالبياناتِ الشَّخصيَّة، فإننا لا نزالُ نرى أوجهَ قصورٍ في الحمايةِ الفعَّالةِ لخصوصيَّةِ الأفراد وبياناتهم، خاصَّةً في سياقِ الأشياءِ المُتَّصلة التي ليس لها قانونٌ قانونيٌّ محدَّد.

كما أنه غالبًا ما تتمُّ الإشارةُ في فرنسا وكندا إلى الامتثالِ للائحةِ العامَّةِ لحمايةِ البيانات وتنفيذها تُجاه الشَّركات، وفي هذا الصَّددِ أشار البعضُ إلى أنَّ "التَّنظيم المفرط وغير الواقعيّ يؤدِّي عمومًا إلى سوءِ تطبيقِ القانون" وفي هذا الشَّأن ذهب معهدُ مونتين الفرنسيّ إلى القولِ بأنه بدُونِ الابتكاراتِ التِّكنولوجيَّةِ الجذريَّة، ستظلُّ مجتمعاتنا مجمَّدةً[٢٣١].

رابعاً: تقييمُ تأثيرِ المخاطرِ المحتملةِ على الخصوصيَّة:

تقييمُ تأثيرِ الخصوصيَّةِ (Privacy Impact Assessment- PIA): أداةٌ مهمَّةٌ تستخدمُ لتقييم المخاطرِ المحتملةِ التي قد تؤثِّر على خصوصيَّةِ الأفرادِ عند معالجةِ

---

[٢٣٠] اللَّجنـةُ الوطنيَّـةُ للمعلوماتيَّـةِ والحريَّـات (بالفرنسيَّة: Commission nationale de l'informatique et des libertés) أو (CNIL) هي سلطةٌ إداريَّةٌ مستقلةٌ فرنسيَّة، مسؤولةٌ عن التأكُّد من أن تكنولوجيا المعلومات موضوعةٌ في خدمةِ المواطن وأنها لا تشكِّل ضررًا لا لهويَّـةِ الإنسان، أو حقوقِ الإنسانِ ولا في الخصوصيَّة، أو الحريَّاتِ الفرديَّةِ والعامَّة. وتمارسُ مهامَّها وفقًا للقانون رقم ٧٨-١٧ في ٦ يناير ١٩٧٨ المعدَّل في ٦ أغسطس ٢٠٠٤.

[231] «sans innovations technologiques radicales, nos sociétés resteraient figées»,

(ISSN: 2537- 0758)

بياناتهم الشَّخصيَّة، وذلك من خلالِ تحليلِ البيانات، ومعرفة مدى تأثيرِ معالجةِ البياناتِ على خصوصيَّةِ الأفراد، مع تحديدِ المخاطرِ المحتملةِ، مثل التَّسريباتِ، الوصولِ غير المصرَّحِ به، أو استخدامِ البياناتِ لأغراضٍ غير متَّفقٍ عليها. فضلًا عن اتِّخاذِ كافَّةِ تدابيرِ التَّخفيفِ لتقليلِ المخاطرِ المحتملة، مثل تحسينِ الأمان، وضع سياساتٍ واضحةٍ للخصوصيَّة.

وفي هذا الشَّأن يقعُ على عاتقِ الشَّركاتِ المسوِّقة لأيِّ تكنولوجيا متَّصلةٍ التزامٌ بإجراءِ دراسةٍ بشأنِ تأثيرِ معالجةِ البياناتِ الشَّخصيَّة على الخصوصيَّة، وذلك تحت مسمَّى تقييمِ تأثيرِ الخصوصيَّة؛ قبل طرحِ الشَّيء المتَّصلِ في السُّوق.

وفي هذا الصَّددِ يتحتَّمُ على الشَّركاتِ المنتجةِ ضرورة وضعِ دراسةٍ حقيقيَّةٍ حول مدى التَّفاعلِ بين هذه الأشياءِ ومُستخدميها، للتأكُّد من كسْبِ ثقةِ المستخدمين في الخدماتِ المقدَّمة، حيث فرض التَّنظيمُ الأوربيُّ عقوبةً شديدةً على في حالِ مخالفةِ الالتزامات، فمن أجلِ ضمانِ الأمنِ ومنع أيِّ معالجةٍ تشكِّل انتهاكًا للخصوصيَّة، يقعُ على عاتقِ جهازِ التحكُّم أو المعالج بتقييمِ المخاطرِ الكامنةِ في المعالجةِ وتنفيذ تدابيرَ للتَّخفيفِ منها، مثل التَّشفير. ويجبُ أن تضمن هذه التَّدابيرُ مستوًى مناسبًا من الأمانِ، بما في ذلك السريَّةُ، مع الأخذِ في الاعتبارِ حالة المعرفةِ وتكاليفِ التَّنفيذِ فيما يتعلَّقُ بالمخاطرِ وطبيعةِ البياناتِ الشَّخصيَّة المطلوب حمايتها. وعند تقييمِ مخاطرِ أمنِ البيانات، ينبغي النَّظرُ في المخاطرِ التي تشكِّلها معالجةُ البياناتِ الشَّخصيَّة، مثل التَّدميرِ أو الخسارةِ أو التَّغيير، أو الكشف غير المصرَّحِ به عن البياناتِ الشَّخصيَّةِ المنقولة أو المخزَّنة أو المعالجة بطريقةٍ أخرى أو الوصول غير القانونيِّ إلى هذه البيانات، عن طريقِ الخطأ أو بشكلٍ غير قانونيٍّ ممَّا قد يترتَّبُ عليه ضررٌ جسديٌّ أو ماديٌّ أو معنويٌّ[٢٣٢].

---

(232) Afin de garantir la sécurité et de prévenir tout traitement effectué en violation du présent règlement, il importe que le responsable du traitement ou le sous-traitant évalue les risques inhérents au traitement et mette en œuvre des mesures pour les atténuer, telles que le chiffrement. Ces mesures devraient assurer un niveau de sécurité approprié, y compris la confidentialité, compte tenu de l'état des connaissances et des coûts de mise en œuvre par rapport aux risques et à la nature des données à caractère personnel à protéger. Dans le cadre de

ونرى بأنه يقعُ على عاتقِ المزوِّدين والمصمِّيمين وجميعِ المهنيِّين الذين لهم دورٌ في طرحِ الأشياءِ المُتَّصلة (الذكيَّة) فورَ عِلمِهم باكتشافِ عيبٍ قد يضرُّ بمستخدمي هذه الأشياء، ضرورة إبلاغِ السُّلطاتِ المختصَّة مع العملِ على نشرِ وإعلامِ جميعِ المستخدمين ببيانِ كيفيَّةِ الوقايةِ منها، مع سحْبِ هذه الأشياءِ من السُّوق إذا دعت الضَّرورةُ إلى ذلك.

كما يقعُ على عاتقِ الشَّركةِ المصنِّعة التأكُّدُ من وجود "مكوِّن السَّلامة" وهو ما ذكرتْه لائحةُ (الاتِّحاد الأوروبي) ١٦٨٩/٢٠٢٤ بتاريخ ١٣ يونيو ٢٠٢٤ في نصِّ المادة ٣ /٢٣ منها باعتبارِ أن مكوِّن السَّلامةِ أحد مكوِّناتِ المنتجِ أو نظام الذَّكاءِ الاصطناعيِّ الذي يفي بوظيفةِ السَّلامة، حيث يتحتَّم أن يكونَ لأيِّ منتجٍ وبخاصَّةٍ المنتجاتُ المُتَّصلةُ إلكترونيًّا مكونٌ يسمَّى بمكوِّنِ السَّلامة، في حالة إذا أدَّى فشلُه أو عُطلُه إلى تعريضِ صحَّةِ وسلامةِ الأشخاصِ أو الممتلكات للخطر(٢٣٣).

لكنْ في بعضِ الأحيانِ قد تُواجه أنظمةُ الأشياءِ المُتَّصلة بعض التَّعديلاتِ الجوهريَّة التي لم تكُنْ في الحسبان، فيقعُ على عاتقِ الموزِّع أو المستخدمِ إبلاغ مزوِّد النِّظامِ بكافَّةِ تفاصيلِ التَّعديلات، ويُقصد بالتَّعديلِ الجوهريِّ وفقًا للائحةِ (الاتِّحاد الأوروبي) ١٦٨٩/٢٠٢٤ ذلك التَّغيير الذي يطرأُ على نظامِ الذَّكاءِ الاصطناعيِّ بعد طرحِهِ في السُّوق أو وضعه في الخدمةِ، والذي لم يكُنْ متوقَّعًا أو مخطَّطًا له في تقييمِ المطابقةِ الأولى الذي أجراها المزوِّد(٢٣٤).

---

l'évaluation des risques pour la sécurité des données, il convient de prendre en compte les risques que présente le traitement de données à caractère personnel, tels que la destruction, la perte ou l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite, qui sont susceptibles d'entraîner des dommages physiques, matériels ou un préjudice moral.

(233) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art. (14) ‘safety component’ means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property;

(234) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial

(ISSN: 2537- 0758)

وفي هذا الشَّأنِ لضبطِ مسألةِ تقييمِ المخاطرِ المحتملة وتحديد المسؤوليَّاتِ النَّاجمةِ عن استخدامِ الأشياءِ المُتَّصلةِ المزوَّدة بأنظمةِ الذَّكاءِ الاصطناعيّ، فإنَّ هناك عدَّة التزاماتٍ تقعُ على عاتقِ كلٍّ من الممثِّلين المعتمدين لمقدِّمي الأشياءِ المُتَّصلةِ المزوَّدة بأنظمةِ الذَّكاءِ الاصطناعيّ شديدة الخطورةِ في الدُّول المختلفة، وكذلك المستوردون والموزِّعون، وهذا ما أوضحتْه لائحةُ الاتِّحادِ الأوروبيّ ١٦٨٩/٢٠٢٤، وفي هذا الصَّددِ نُشير إلى جانبٍ من هذه الالتزاماتِ مع بيانِ إمكانيَّةِ تطبيقِ مثل هذه القواعدِ في مصر قبل استيرادِ الأشياءِ المُتَّصلة المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر.

١- التزاماتُ الممثِّلين المعتمدين لمقدِّمي أنظمةِ الذَّكاءِ الاصطناعيّ عاليةِ المخاطر:

المُطَّلع على لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ يجدُ بأنها أوجبتْ قبلَ إتاحةِ أنظمةِ الذَّكاء الاصطناعيّ وبخاصَّةٍ الأنظمةُ شديدةُ الخطورةِ في سوقِ الاتِّحاد الأوروبيّ، على مقدِّمي الخدماتِ الموجودين في بلدان ثالثة، تعيين ممثِّلٍ معتمدٍ مقيم في الاتِّحاد، حيث يقعُ على عاتقهِ أداءُ المهامِّ المحدَّدة في التَّفويضِ الذي تلقَّاه من مقدِّم الخدمة. **ومن هذه المهامِّ**[٢٣٥]:

---

intelligence" Art. (23) 'substantial modification' means a change to an AI system after its placing on the market or putting into service which is not foreseen or planned in the initial conformity assessment carried out by the provider.

(235) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Article 22.....

3. The authorised representative shall perform the tasks specified in the mandate received from the provider. It shall provide a copy of the mandate to the market surveillance authorities upon request, in one of the official languages of the institutions of the Union, as indicated by the competent authority. For the purposes of this Regulation, the mandate shall empower the authorised representative to carry out the following tasks:

(a)verify that the EU declaration of conformity referred to in Article 47 and the technical documentation referred to in Article 11 have been drawn

(أ) التحقُّقُ من إعدادِ إعلانِ المطابقةِ للاتِّحادِ الأوروبيّ أو الوثائق الفنيَّة، ومن قيامِ المزوِّد بإجراءِ تقييمِ المطابقةِ المناسب.

(ب) الاحتفاظُ تحت تصرُّفِ السُّلطاتِ المختصَّة والسُّلطاتِ أو الهيئاتِ الوطنيَّةِ، لمدة ١٠ سنواتٍ بعد طرحِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ في السُّوقِ أو تشغيله، بتفاصيلِ الاتِّصالِ بالمزوِّد.

(ج) تزويدُ السُّلطةِ المختصَّة، بناءً على طلبٍ مسبَّب، بجميعِ المعلوماتِ والوثائق، اللَّازمة لإثباتِ توافقِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ مع المتطلَّباتِ المنصوصِ عليها، بما في ذلك الوصولُ إلى السِّجلات، وبخاصَّةٍ التي يتمُّ إنشاؤها تلقائيًّا بواسطةِ نظامِ الذَّكاء الاصطناعيّ عالي المخاطر، إلى الحدِّ الذي تخضعُ فيه هذه السِّجلاتُ لسيطرةِ المزوِّد.

(د) التَّعاونُ مع السُّلطاتِ المختصَّة، بناءً على طلبٍ مسبَّب، في أيِّ إجراءٍ تتَّخذه الأخيرةُ فيما يتعلَّق بنظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر، وخاصَّةً للحدِّ من المخاطرِ التي يفرضُها نظامُ الذَّكاءِ الاصطناعيّ عالي المخاطرِ والتَّخفيف منها.

---

up and that an appropriate conformity assessment procedure has been carried out by the provider؛

(b) keep at the disposal of the competent authorities and national authorities or bodies referred to in Article 74(10), for a period of 10 years after the high-risk AI system has been placed on the market or put into service, the contact details of the provider that appointed the authorised representative, a copy of the EU declaration of conformity referred to in Article 47, the technical documentation and, if applicable, the certificate issued by the notified body؛

(c) provide a competent authority, upon a reasoned request, with all the information and documentation, including that referred to in point (b) of this subparagraph, necessary to demonstrate the conformity of a high-risk AI system with the requirements set out in Section 2, including access to the logs, as referred to in Article 12(1), automatically generated by the high-risk AI system, to the extent such logs are under the control of the provider؛

(d) cooperate with competent authorities, upon a reasoned request, in any action the latter take in relation to the high-risk AI system, in particular to reduce and mitigate the risks posed by the high-risk AI system;

(ISSN: 2537- 0758)

وفي هذا الإطارِ نقترح على المُشرِّعِ المصريّ ضرورة سنّ بعضِ القواعدِ الحاكمة التي تمنعُ استيرادَ أشياءَ متَّصلةٍ، وبخاصَّةٍ المزوَّدةُ بأنظمةِ الذَّكاءِ الاصطناعيّ عالية المخاطرِ قبل قيامِ مقدِّمي الخدماتِ الموجودين في بلدان أخرى، بموجبِ تفويضٍ مكتوبٍ، بتعيين ممثِّلٍ معتمدٍ يقعُ على عاتقهِ عديدٌ من الالتزاماتِ، **والتي من أهمِّها:** (أ) التحقُّقُ من إعدادِ إعلانِ المطابقةِ والوثائق الفنيَّة، فضلًا عن التأكُّد من قيامِ مقدِّم الخدمةِ بإجراءِ تقييمِ شروطِ المُطابقةِ المناسب؛ والتحقُّق من قيامِ مقدِّمِ الخدمةِ بإجراءِ تقييمِ شروطِ المطابقةِ المناسب؛ إضافةً إلى مدِّ السُّلطةِ المختصَّةِ والمقترح أن تكونَ هيئةً مستقلةً تحت مسمَّى "الهيئة العامَّة لرقابةِ تقنياتِ الأشياءِ المُتَّصلةِ والأمن الرَّقمي"– والتي سنُشير إليها لاحقًا–، بناءً على طلبٍ مسبَّب، بجميعِ المعلوماتِ والوثائق، اللَّازمة لإثباتِ توافُقِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ مع المتطلَّباتِ المنصوصِ عليها وفقًا لقوانين الدَّولة، بما في ذلك الوصولُ إلى السِّجلات، وبخاصَّةٍ التي يتمُّ إنشاؤها تلقائيًّا بواسطةِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر.

٢– التزاماتُ المستوردين لأشياءَ متَّصلةٍ مزوَّدةٍ بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر:

عند استيرادِ أشياءَ متَّصلةٍ مزوَّدةٍ بأنظمةِ الذَّكاءِ الاصطناعيّ عالية المخاطرِ إلى دولِ الاتِّحادِ الأوروبيّ (مثل الأجهزةِ الذكيَّةِ أو الأنظمةِ التي تعتمدُ على الإنترنتّ للأشياءِ)، هناك مجموعةٌ من الالتزاماتِ التي يجبُ على المستوردين الالتزامُ بها، وفي هذا الشَّأن نُشير إلى هذه الالتزاماتِ بحسب ما وردَتْ في المادة ٢٣ من لائحة (الاتِّحاد الأوروبي) ١٦٨٩/٢٠٢٤، والتي تنصُّ على عدَّةِ التزاماتٍ تقع على عاتقِ المستوردين[٢٣٦]، **نذكُرُ منها:**

---

(236) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Article 23

Obligations of importers

1. Before placing a high-risk AI system on the market, importers shall ensure that the system is in conformity with this Regulation by verifying that:

(a) the relevant conformity assessment procedure referred to in Article 43 has been carried out by the provider of the high-risk AI system؛

أ- قبل طرحِ نظامِ الذَّكاء الاصطناعيّ عالي الخطورةِ في السُّوق، يجبُ على المستوردين التأكُّد من أنَّ النِّظامَ متوافقٌ مع هذه اللَّائحةِ من خلالِ التحقُّق من أنه تمَّ تنفيذُ إجراءِ تقييمِ المطابقةِ ذي الصِّلة من قِبل مزوِّد نظامِ الذَّكاءِ الاصطناعيّ عالي الخطورة؛ مع التأكُّد من قيامِ المزوِّد بإعدادِ الوثائقِ الفنيَّةِ وقيامه أيضًا بتعيينِ ممثِّل مفوَّضٍ.

ب- إذا كان لدى المستوردِ سببٌ كافٍ للاعتقادِ بأنَّ نظامَ الذَّكاءِ الاصطناعيّ عالي الخطورةِ غير متوافقٍ مع شروطِ السَّلامة، أو مزوَّر، أو مصحوبٍ بوثائقَ مزوَّرة، فلا يجوزُ له طرحُ النِّظام في السُّوق حتى يتمَّ جعلُه متوافقًا، وإذا كان نظامُ الذَّكاءِ الاصطناعيّ عالي الخطورة يُشكِّل خطرًا، فيجبُ على المستوردِ إبلاغُ مزوِّد النِّظامِ والممثلِ المعتمدِ وسلطاتِ مراقبةِ السُّوق بهذا الخطر.

ج- يجب على المستوردين التأكُّد من مسألةِ التَّخزينِ أو النَّقل بشكلٍ صحيحٍ أثناء وجودِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ تحت مسؤوليَّتهم.

د- يتعيَّن على المستوردين تزويدُ السُّلطاتِ المختصَّة ذات الصِّلة، بناءً على طلبٍ مسبَّب، بجميعِ المعلوماتِ والوثائق اللَّازمة، فضلًا عن التَّعاونِ مع السُّلطاتِ المختصَّة ذات الصِّلة في أيّ إجراءٍ تتَّخذه تلك السُّلطاتُ فيما يتعلَّق بنظام الذَّكاءِ الاصطناعيّ عالي المخاطرِ الذي يطرحُه المستوردون في السُّوق، وخاصَّةً للحدِّ من المخاطرِ التي يفرضُها ذلك النِّظامُ والتَّخفيف منها.

وبناءً على ما سبق نجدُ أنَّ الاتِّحادَ الأوروبيَّ قد قيَّد المستوردين ببعضِ القيودِ التي تحدُّ نوعًا ما من خطورةِ الأشياءِ المُتَّصلةِ المزوَّدة بأنظمةِ الذَّكاءِ الاصطناعيّ عاليةِ الخطورة، حيث وضع على عاتقِهم عديدًا من الالتزامات، وفي هذا الشَّأن نرى بأنه ما جاءتْ به لائحةُ الاتِّحاد الأوروربيّ ١٦٨٩/٢٠٢٤ بشأن التزاماتِ المستوردين

(b) the provider has drawn up the technical documentation in accordance with Article 11 and Annex IV؛
(c) the system bears the required CE marking and is accompanied by the EU declaration of conformity referred to in Article 47 and instructions for use؛
(d) the provider has appointed an authorised representative in accordance with Article 22(1).

(ISSN: 2537- 0758)

هو أمرٌ في غايةِ الأهميَّة، كما هو الحالُ بالنِّسبةِ للممثلين المعتمدين لمقدِّمي أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر. ولهذا نُوصِي المُشرِّعَ المصريَّ بضرورةِ التَّشديدِ في التزاماتِ المستوردين لأشياءَ متَّصلةٍ مزودةٍ بأنظمةِ ذكاءٍ اصطناعيٍّ شديدةِ الخطورة.

وتجدر الإشارةُ في هذا الصَّدد إلى أنَّ الاتِّحادَ الأوروبيَّ في قانون ١٦٨٩/٢٠٢٤ قد نصَّ في المادة ٢٤ على بعضِ التزاماتِ الموزِّعين، والتي لا تختلفُ كثيرًا عن التزاماتِ المستوردين(٢٣٧).

(237) Obligations of distributors:

1. Before making a high-risk AI system available on the market, distributors shall verify that it bears the required CE marking, that it is accompanied by a copy of the EU declaration of conformity referred to in Article 47 and instructions for use, and that the provider and the importer of that system, as applicable, have complied with their respective obligations as laid down in Article 16, points (b) and (c) and Article 23.(٣)
2. Where a distributor considers or has reason to consider, on the basis of the information in its possession, that a high-risk AI system is not in conformity with the requirements set out in Section 2, it shall not make the high-risk AI system available on the market until the system has been brought into conformity with those requirements. Furthermore, where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall inform the provider or the importer of the system, as applicable, to that effect.
3. Distributors shall ensure that, while a high-risk AI system is under their responsibility, storage or transport conditions, where applicable, do not jeopardise the compliance of the system with the requirements set out in Section 2.
4. A distributor that considers or has reason to consider, on the basis of the information in its possession, a high-risk AI system which it has made available on the market not to be in conformity with the requirements set out in Section 2, shall take the corrective actions necessary to bring that system into conformity with those requirements, to withdraw it or recall it, or shall ensure that the provider, the importer or any relevant operator, as appropriate, takes those corrective actions. Where the high-risk AI system presents a risk within the meaning of Article 79(1), the distributor shall immediately inform the provider or importer of the system and the authorities competent for the high-risk AI system

خامساً: حظر بعضِ أنظمةِ الأشياءِ المُتَّصلةِ الذكيَّة:

تنصُّ لائحةُ الاتِّحادِ الأوروبيّ ١٦٨٩/٢٠٢٤ بتاريخ ١٣ يونيو ٢٠٢٤- والتي تضعُ قواعدَ منسجمةً بشأنِ الذَّكاءِ الاصطناعيّ- على بعضِ ممارساتِ الذَّكاء الاصطناعيّ المحظورة[٢٣٨]، التي يتوجَّب على الشَّركاتِ المصنِّعة الالتزام بها، **نذكرُ منها ما يلي:**

---

concerned, giving details, in particular, of the non-compliance and of any corrective actions taken.

5. Upon a reasoned request from a relevant competent authority, distributors of a high-risk AI system shall provide that authority with all the information and documentation regarding their actions pursuant to paragraphs 1 to 4 necessary to demonstrate the conformity of that system with the requirements set out in Section 2.

(238) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art 5 The following AI practices shall be prohibited:

the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm؛

the placing on the market, the putting into service or the use of an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability or a specific social or economic situation, with the objective, or the effect, of materially distorting the behaviour of that person or a person belonging to that group in a manner that causes or is reasonably likely to cause that person or another person significant harm؛

the placing on the market, the putting into service or the use of AI systems for the evaluation or classification of natural persons or groups of persons over a certain period of time based on their social behaviour or known, inferred or predicted personal or personality characteristics, with the social score leading to either or both of the following:

(ISSN: 2537- 0758)

أ- لا يجوزُ طرحُ نظامِ ذكاءٍ اصطناعيٍّ في السُّوق أو تشغيلُه أو استخدامُهِ، طالما يعمل على استخدام تقنيَّاتٍ خفيَّةٍ تتجاوزُ وعي الشَّخصِ أو تقنيَّات تتَّصفُ بالخداعِ المتعمَّد، بهدف تشويهِ سلوكِ شخصٍ أو مجموعةٍ من الأشخاصِ بشكلٍ ملموسٍ من خلال إضعافِ قدرتهم على اتِّخاذ قرارٍ مستنيرٍ، وبالتالي دفعهم إلى اتِّخاذ قرارٍ لم يكونوا ليتَّخذوه لولا ذلك بطريقةٍ تسبِّب أو من المحتملِ أن تسبِّب بشكلٍ معقولٍ ضررًا كبيرًا لذلك الشَّخص أو شخصٍ آخرَ أو مجموعةٍ من الأشخاص.

ب-يحظرُ على الشَّركاتِ المصنِّعة استغلال الحاجةِ من خلالِ طرحِ شيءٍ متَّصلٍ أو خدمةٍ باستغلالِ أيِّ من نقاطِ الضَّعفِ لدى شخصٍ طبيعيٍّ أو مجموعةٍ محدَّدة من الأشخاصِ بسببِ سنِّهم أو إعاقتِهم أو وضعٍ اجتماعيٍّ أو اقتصاديٍّ محدَّد، وذلك بغرضِ تشويهِ سلوكِ ذلك الشَّخصِ أو شخصٍ ينتمي إلى تلك المجموعةِ بشكلٍ مادِّيٍّ أو من المحتملِ أن يتسبَّب في إلحاقِ ضررٍ كبيرٍ بذلك الشَّخص أو شخصٍ آخر.

ج- لا يجوزُ طرحُ شيءٍ متَّصلٍ ذكيٍّ في السُّوق بغرضِ تقييمِ أو تصنيفِ الأشخاصِ الطَّبيعيين أو مجموعاتِ الأشخاصِ خلال مدَّةٍ زمنيَّةٍ معيَّنةٍ بناءً على سلوكِهم الاجتماعيِّ أو خصائصهم الشَّخصيَّةِ أو الشَّخصيَّةِ المعروفةِ أو المستنتجةِ أو المتوقَّعة، مع النتيجةِ الاجتماعيَّةِ التي تؤدِّي إلى أيٍّ ممَّا يلي أو كليهما:

- المعاملةُ الضارَّة أو غير المواتيةِ لبعضِ الأشخاصِ الطبيعيِّين أو مجموعات الأشخاصِ في سياقاتٍ اجتماعيَّةٍ غير مرتبطةٍ بالسِّياقاتِ التي تمَّ فيها إنشاءُ البيانات أو جمعها في الأصل.
- المعاملة الضارَّة أو غير المواتيةِ لبعضِ الأشخاصِ الطبيعيِّين أو مجموعاتٍ من الأشخاصِ والتي لا مبرِّر لها أو غير متناسبةٍ مع سلوكهم الاجتماعيِّ أو خطورته.

د- يحظرُ طرحُ شيءٍ متَّصلٍ في السُّوق، أو تشغيلُه أو استخدامُ نظامِ الذَّكاءِ الاصطناعيِّ لإجراءِ تقييمات مخاطرِ الأشخاصِ الطبيعيِّين من أجل تقييمِ أو التنبُّؤ بخطرِ ارتكابِ شخصٍ طبيعيٍّ لجريمةٍ جنائيَّة، بناءً على تحديدِ ملفِّ تعريفِ الشَّخصِ الطبيعيِّ أو تقييم سماتِ شخصيَّتِهِ وخصائصه فقط.

وتجدرُ الإشارةُ في هذا الصَّدد إلى أنَّ لائحةَ الاتِّحادِ الأوروبيّ ١٦٨٩/٢٠٢٤ في نصِّ المادة الخامسة تَستثني من هذا الحظرِ أنظمةَ الذَّكاءِ الاصطناعيّ المستخدمة لدعم التَّقييمِ البشريّ لتورُّط شخصٍ ما في نشاطٍ إجراميٍّ، والذي يستندُ بالفعلِ إلى حقائقَ موضوعيَّةٍ وقابلةٍ للتحقُّق مرتبطةٍ مباشرةً بنشاطٍ إجراميٍّ[٢٣٩].

هـ- يحظرُ طرح أشياءَ متَّصلةٍ في السُّوق، أو تشغيلُها، أو استخدامُ أنظمةِ الذَّكاء الاصطناعيّ والتي تنشئ أو توسِّع قواعد بياناتِ التعرُّف على الوجهِ من خلالِ الكشطِ غير المستهدفِ لصورِ الوجهِ من الإنترنتّ أو لقطات كاميراتِ المراقبة.

و- يحظرُ استخدامُ الأشياءِ المُتَّصلةِ المدعومة بأنظمةِ الذَّكاء الاصطناعيّ لاستنتاجِ مشاعر شخصٍ طبيعيٍّ في مجالاتِ مكانِ العملِ والمؤسَّسات التعليميَّة، باستثناء الحالاتِ التي يُقصد فيها استخدامُ نظامِ الذَّكاء الاصطناعيّ لوضعهِ في السُّوق أو طرحهِ في السُّوقِ لأسبابٍ طبيَّةٍ أو أمنيَّة.

ز- يحظرُ استخدامُ أنظمةٍ أو أشياءَ متَّصلةٍ تعمل على التَّصنيفِ البيومتريَّة، والتي تصنِّف الأشخاصَ الطَّبيعيّين بشكلٍ فرديٍّ على أساسِ بياناتهم البيومتريَّة لاستنتاجِ عرقِهم أو آرائِهم السياسيَّةِ أو عضويَّتهم في النقاباتِ العماليَّةِ أو معتقداتهم الدينيَّةِ أو الفلسفيَّةِ أو حياتهم الجنسيَّةِ أو توجُّههم الجنسيّ.

وفي الواقعِ لا يشملُ هذا الحظرُ أيَّ تصنيفٍ أو تصفيةٍ لمجموعاتِ البياناتِ البيومترية المكتسبة بشكلٍ قانونيٍّ، مثل الصُّور، بناءً على البياناتِ البيومتريَّة أو تصنيف البياناتِ البيومتريَّة في مجالِ إنفاذِ القانون[٢٤٠].

---

(239) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art. (5)..... this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity;

(٢٤٠) وجديرٌ بالذِّكر تنصُّ اللائحةُ (الاتِّحاد الأوروبي) ١٦٨٩/٢٠٢٤ على ما يلي "استخدامُ أنظمةِ التَّعريفِ البيومترية عن بُعد "في الوقتِ الفعليّ" في الأماكنِ التي يُمكن الوصولُ إليها للعامَّة لأغراضِ إنفاذِ القانون، ما لم يكنْ هذا الاستخدامُ ضروريًّا تمامًا لأحدِ الأهدافِ التَّالية:

- البحث المستهدفُ عن ضحايا محدَّدين للاختطافِ أو الاتِّجار بالبشرِ أو الاستغلالِ الجنسيّ للبشر، فضلًا عن البحثِ عن الأشخاصِ المفقودين.

(ISSN: 2537- 0758)

الفرع الخامس
استحداثُ هيئةٍ مستقلَّةٍ لرقابةِ أنظمةِ الذَّكاءِ الاصطناعيِّ
(الهيئةُ العامَّةُ لرقابةِ تقنياتِ الأشياءِ المُتَّصلة والأمن الرقمي)

تنصُّ المادة ٧ من لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ على أنَّه "عند تقييم بإضافة أو تعديل حالاتِ استخدامِ أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطرِ تأخذُ المفوضيَّةُ في الاعتبارِ المعايير التَّالية[٢٤١]:

(أ) الغرضُ المقصودُ من نظامِ الذَّكاءِ الاصطناعيّ.

- منع تهديدٍ محدَّدٍ وجوهريّ ووشيكٍ لحياة الأشخاصِ الطبيعيّين أو سلامتهم الجسديَّةِ أو تهديدٍ حقيقيّ وحاضرٍ أو حقيقيّ ومتوقَّعٍ بهجومٍ إرهابيّ.
- تحديد موقعٍ أو تحديدِ هويَّةِ شخصٍ يُشتبه في ارتكابهِ جريمةً جنائيَّةً، لغرضِ إجراءِ تحقيقٍ جنائيّ أو مقاضاة أو تنفيذ عقوبةٍ جنائيَّةٍ عن الجرائمِ المشار إليها في الملحقِ الثاني، والتي يُعاقب عليها في الدَّولةِ العضو المعنيَّةِ بعقوبةِ سجنٍ أو أمر احتجازٍ لمدَّةٍ أقصاها أربع سنواتٍ على الأقلّ.

[241] Article 7
Amendments to Annex III
1. The Commission is empowered to adopt delegated acts in accordance with Article 97 to amend Annex III by adding or modifying use-cases of high-risk AI systems where both of the following conditions are fulfilled:
(a) the AI systems are intended to be used in any of the areas listed in Annex III؛
(b) the AI systems pose a risk of harm to health and safety, or an adverse impact on fundamental rights, and that risk is equivalent to, or greater than, the risk of harm or of adverse impact posed by the high-risk AI systems already referred to in Annex III.
2. When assessing the condition under paragraph 1, point (b), the Commission shall take into account the following criteria:
(a) the intended purpose of the AI system؛
(b) the extent to which an AI system has been used or is likely to be used؛
(c) the nature and amount of the data processed and used by the AI system, in particular whether special categories of personal data are processed؛
(d)the extent to which the AI system acts autonomously and the possibility for a human to override a decision or recommendations that may lead to potential harm;

(ب) المدى الذي تمَّ فيه استخدامُ نظامِ الذَّكاء الاصطناعيّ أو من المرجَّحِ أن يتمَّ استخدامُه.

(ج) طبيعةُ وكميَّةُ البياناتِ التي تتمُّ معالجتُها واستخدامُها بواسطةِ نظامِ الذَّكاء الاصطناعيّ، وخاصَّةً ما إذا كانت تتمُّ معالجةُ فئاتٍ خاصَّةٍ من البياناتِ الشَّخصيَّة.

(د) المدى الذي يعملُ فيه نظامُ الذَّكاءِ الاصطناعيّ بشكلٍ مستقلٍ وإمكانيَّة تجاوزِ الإنسانِ لقرارٍ أو توصياتٍ قد تؤدِّي إلى ضررٍ محتمل.

(هـ) المدى الذي تسبَّب فيه استخدام نظامِ الذَّكاءِ الاصطناعيّ بالفعل في إلحاقِ الضَّررِ بالصِّحةِ والسَّلامة، أو كان له تأثيرٌ سلبيٌّ على الحقوقِ الأساسيَّة أو أثار مخاوفَ كبيرةً فيما يتعلَّقُ باحتماليَّةِ حدوثِ مثل هذا الضَّررِ أو التَّأثير السلبيّ، كما يتَّضح، على سبيلِ المثال، من خلالِ التَّقاريرِ أو الادِّعاءات الموثقة المقدَّمة إلى السُّلطاتِ الوطنيَّةِ المختصَّة أو من خلال تقاريرَ أخرى، بحسب الاقتضاء.

(و) المدى المحتملُ لمثلِ هذا الضَّررِ أو هذا التَّأثير السلبيّ، وخاصَّةً من حيث شدَّتُه وقدرتُه على التَّأثير على أشخاصٍ متعدِّدين أو التأثير بشكلٍ غير متناسبٍ على مجموعةٍ معيَّنةٍ من الأشخاص.

(ز) المدى الذي يعتمدُ فيه الأشخاصُ الذين يحتملُ أن يتضرَّرُوا أو يعانوا من تأثيرٍ سلبيّ على النتيجةِ النَّاتجةِ عن نظامِ الذَّكاءِ الاصطناعيّ.

(ح) المدى الذي يوجدُ فيه خللٌ في التَّوازنِ في القوَّة، أو الأشخاص الذين يحتملُ أن يتضرَّرُوا أو يعانوا من تأثيرٍ سلبيّ في وضعٍ ضعيفٍ فيما يتعلَّق بمستخدمِ نظامِ الذَّكاء الاصطناعيّ، وخاصَّةً بسببِ المكانةِ أو السُّلطةِ أو المعرفة أو الظُّروف الاقتصاديَّة أو الاجتماعيَّة أو العمر.

(ط) المدى الذي تكونُ فيه النَّتيجةُ الناتجةُ عن نظامِ الذَّكاءِ الاصطناعيّ قابلةً للإصلاح أو العكس بسهولة، مع مراعاةِ الحلولِ التقنيَّةِ المتاحةِ لتصحيحها أو عكسها، حيث لا تعتبرُ النَّتائجُ التي لها تأثيرٌ سلبيٌّ على الصِّحةِ أو السَّلامةِ أو الحقوقِ الأساسيَّةِ قابلة للإصلاحِ أو العكس بسهولةٍ.

(ي) حجم واحتمالُ الاستفادةِ من نشرِ نظامِ الذَّكاء الاصطناعيّ للأفرادِ أو

(ISSN: 2537- 0758)

المجموعات أو المجتمع ككلٍّ، بما في ذلك التَّحسيناتُ المحتملةُ في سلامةِ المنتج.

وهديًا على ما قدَّمتْه لائحةُ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤، ووفقًا لما سبق نقترحُ في هذا الشَّأن بإنشاء هيئةٍ تكون مسؤولةً عن مراقبةِ تقنياتِ الأشياءِ المُتَّصلة والأمن الرقميّ، وذلك تحت مسمَّى "الهيئة العامَّة لرقابةِ تقنيَّاتِ الأشياءِ المُتَّصلة والأمنِ الرقميّ" باعتبارِها هيئةً تكونُ مسؤولةً عن تنظيمِ ومراقبةِ تكنولوجيا الإنترنتّ للأشياءِ (IoT) وضمان الأمنِ الرقميّ في البنيةِ التحتيَّةِ الرقميَّةِ المرتبطة بالأجهزةِ المُتَّصلة. حيث إنَّ تأسيسَ مثل هذه الهيئةِ يعكسُ اهتمامَ الدَّولةِ بتطوير تقنيَّاتٍ ذكيَّةٍ وآمنةٍ من أجلِ حمايةِ البياناتِ الشَّخصيَّة والأمن السيبرانيّ في عالمٍ مليءٍ بالأجهزةِ المُتَّصلةِ والشَّبكات الذكيَّة.

وفي هذا الشَّأن نقترحُ بعضَ المهامِّ الرئيسة للهيئةِ العامَّة لرقابةِ تقنيَّاتِ الأشياءِ المُتَّصلة والأمن الرقمي:

أولًا: مراقبةُ الأجهزةِ المُتَّصلة: من خلالِ التأكُّد من توافُقِ الأجهزةِ المُتَّصلةِ مع المعاييرِ التقنيَّةِ والقانونيَّة للأمان، مثل التحقُّقِ من أنَّ هذه الأجهزةَ لا تحتوي على ثغراتٍ أمنيَّةٍ قد تعرض الشَّبكاتِ لتهديداتٍ. بالإضافةِ إلى الرَّقابةِ على التَّطبيقاتِ المدمجة في الأجهزةِ مثل الأجهزةِ المنزليَّةِ الذكيَّة، السيَّاراتِ الذاتيَّةِ القيادة، الأجهزة الطبيَّة، وأدواتِ الذَّكاءِ الاصطناعيّ...إلخ.

ثانيًا: حماية البيانات الشَّخصيَّة: التأكد من أن الأجهزة المُتَّصلة تحترم خصوصيَّة بيانات المستخدمين التي يتم جمعها عبر الأجهزة المُتَّصلة ومنع إساءة استخدامها.

ثالثًا: تنظيمُ الأمانِ الرقميّ: العمل على تحقيقِ معاييرِ الأمانِ السيبرانيّ للأجهزة المُتَّصلة، بما في ذلك التحقُّق من الطَّبقاتِ الأمنيَّةِ في الشَّبكاتِ والتِّقنيَّاتِ المستخدمة في الأجهزة. مع الإشرافِ على تطبيقِ التَّحديثاتِ الأمنيَّةِ بانتظامٍ للأجهزةِ المُتَّصلة.

رابعًا: وضعُ السّياساتِ والمعايير: تطويرُ إطارٍ تنظيميٍّ يتضمَّن معاييرَ الأمانِ والإجراءات القانونيَّة للأشياءِ المُتَّصلةِ بهدفِ الحفاظِ على الشَّفافيةِ والاستدامة، مع وضعِ سياساتٍ لحمايةِ المستهلكين وضمان عدمِ وجودِ انتهاكٍ لحقوق الأفرادِ أو الشَّركات في استخدامِ الأجهزةِ المُتَّصلة. وتقديم مشورةٍ وإرشاداتٍ للمطوّرين والشَّركات

المصنِّعة حول كيفيَّةِ تحسينِ الأمانِ في الأجهزةِ المُتَّصلة. فضلًا عن إجراءِ فحوصاتٍ دوريَّةٍ للأجهزة المُتَّصلة للتحقُّق من الامتثالِ للمعاييرِ، ومن هذه المعايير: تحديدُ الغرضِ المقصودِ من نظام الشيءِ المتَّصل، المدى الذي تمَّ فيه استخدامُ الشَّيءِ المتَّصلِ أو من المرجَّحِ أن يتمَّ استخدامُه مع تحديدِ طبيعةِ وكميَّةِ البياناتِ التي تتمُّ معالجتُها واستخدامها بواسطةِ نظامِ الذَّكاء الاصطناعيّ، وخاصَّةً ما إذا كانت تتمُّ معالجةُ فئاتٍ خاصَّةٍ من البيانات الشَّخصيَّة؛ مع التأكُّد من المدَى الذي يعملُ فيه نظامُ الذَّكاءِ الاصطناعيّ بشكلٍ مستقلّ وإمكانيَّة تجاوُزِ الإنسانِ لقرارٍ أو توصياتٍ قد تؤدِّي إلى ضررٍ محتمل؛ المدى الذي تسبَّب فيه استخدامُ الشَّيء المتَّصل بالفعلِ في إلحاقِ الضَّررِ بالصِّحة والسَّلامة.

خامساً: وضعُ نظامٍ لإدارةِ المخاطرِ:

Risk management system:

تعدُّ إدارةُ المخاطرِ النَّاجمة عن تقنياتِ الأشياءِ المُتَّصلة أمرًا بالغَ الأهميَّةِ؛ نظرًا للنموِّ السَّريعِ لهذه التِّكنولوجيا، واستخدامها في مجموعةٍ واسعةٍ من التَّطبيقات، من المنازلِ الذكيَّةِ إلى الرِّعايةِ الصِّحيةِ، والصِّناعة، والنَّقل. كما أنَّ الأجهزةَ المُتَّصلةَ بالإنترنتّ تعرِّض الأفرادَ والمنظَّماتِ لمجموعةٍ متنوِّعةٍ من المخاطرِ التي يجبُ مُعالجتها من خلال **إدارةِ المخاطرِ** الفعَّالة. ومن ثمَّ يقعُ على عاتقِ الهيئةِ المقترحةِ **(الهيئة العامَّة لرقابةِ تقنيَّات الأشياءِ المُتَّصلةِ والأمن الرَّقمي)** مهامَّ وضعِ نظامٍ لإدارةِ مخاطرِ الأشياء المُتَّصلة، فضلًا عن متابعةِ تنفيذِه، وفي هذا الصَّددِ تنصُّ المادة ٩ لائحة الاتِّحاد الأوروبي ١٦٨٩/٢٠٢٤ على نظامِ إدارةِ المخاطرِ، حيث يتطلَّب الآتي:

١. يجب إنشاءُ نظامٍ لإدارةِ المخاطرِ وتنفيذه وتوثيقه وصيانته فيما يتعلَّقُ بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر.
٢. يُفهم نظامُ إدارة المخاطرِ على أنه عمليَّةٌ تكراريَّةٌ مستمرَّةٌ يتمُّ التَّخطيطُ لها وتنفيذُها طوال دورةِ حياةِ نظامِ الذَّكاءِ الاصطناعيّ عالية المخاطر بالكامل، وتتطلَّبُ مراجعةً وتحديثًا منتظمين ومنهجيَّين. **ويتألَّف من الخطواتِ التالية**[٢٤٢]:

(242) Article 9 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, Risk management system

(ISSN: 2537- 0758)

(أ) تحديد وتحليلُ المخاطرِ المعروفةِ والمتوقَّعةِ بشكلٍ معقولٍ، والتي يُمكن أن يشكِّلها نظامُ الذَّكاءِ الاصطناعيّ عالي المخاطرِ على الصِّحةِ أو السَّلامةِ أو الحقوق الأساسيَّة عندما يتمُّ استخدامُ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ وفقًا للغرضِ المقصودِ منه.

(ب) تقدير وتقييمُ المخاطرِ التي قد تنشأُ عند استخدامِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ وفقًا للغرضِ المقصودِ منه، وفي ظلِّ ظروفِ إساءة الاستخدامِ المتوقَّعة بشكلٍ معقولٍ.

(ج) تقييم المخاطر الأخرى التي قد تنشأ، استنادًا إلى تحليل البيانات المجمعة من نظام مراقبة ما بعد التَّسويق.

(د) اعتماد تدابير إدارةِ المخاطرِ المناسبةِ والمستهدفةِ والمصمَّمةِ لمعالجةِ المخاطرِ سالفةِ الذِّكر في بند (أ).

٣. يجب إجراءُ اختبارِ أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر، بحسب الاقتضاء، في أيّ وقتٍ طوال عمليَّةِ التَّطوير، وفي أيّ حال، قبل طرحِها في السُّوقِ أو وضعها في الخدمة. يجبُ إجراءُ الاختبارِ وفقًا لمقاييسَ محدَّدةٍ مسبقًا.

---

1. A risk management system shall be established, implemented, documented and maintained in relation to high-risk AI systems.
2. The risk management system shall be understood as a continuous iterative process planned and run throughout the entire lifecycle of a high-risk AI system, requiring regular systematic review and updating. It shall comprise the following steps:

(a) the identification and analysis of the known and the reasonably foreseeable risks that the high-risk AI system can pose to health, safety or fundamental rights when the high-risk AI system is used in accordance with its intended purpose؛

(b) the estimation and evaluation of the risks that may emerge when the high-risk AI system is used in accordance with its intended purpose, and under conditions of reasonably foreseeable misuse ؛

(c) the evaluation of other risks possibly arising, based on the analysis of data gathered from the post-market monitoring system referred to in Article 72 ؛

(d) the adoption of appropriate and targeted risk management measures designed to address the risks

٤. عند تنفيذِ نظامِ إدارةِ المخاطر، يجبُ على المزوِّدين مراعاةُ ما إذا كان من المرجَّح أن يكونَ لنظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ تأثيرٌ سلبيٌّ على الأشخاصِ الذين تقلُّ أعمارُهم عن ١٨ عامًا، وبحسب الاقتضاء، على الفئاتِ الضَّعيفةِ الأخرى(٢٤٣).

كما أن لائحةَ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ قد أشارتْ إلى أنه عند تحديدِ تدابيرِ إدارةِ المخاطرِ الأكثر ملاءمةً، **يجبُ ضمانُ ما يلي:**

(أ) القضاءُ على المخاطرِ أو الحدُّ منها والتي تمَّ تحديدُها وتقييمُها بقدرِ الإمكانِ من النَّاحيةِ الفنيَّة من خلالِ التَّصميمِ والتَّطويرِ المناسبين لنظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر.

(ب) حيثما كان ذلك مناسبًا، تنفيذُ تدابيرِ التَّخفيفِ والسَّيطرةِ الكافية لمعالجةِ المخاطرِ التي لا يُمكن القضاءُ عليها، وفي هذا الشَّأن نرى أن لائحةَ الاتِّحادِ الأوروبيّ قد وَضعت في حسبانها أن هناك مخاطرَ يصعُبُ القضاءُ عليها، بل قد يستحيلُ في الوقتِ الحاليّ القضاء عليها؛ لذا يتوجَّب أخذُ بعضِ التَّدابيرِ التي تخفِّف من وطأةِ المخاطر.

(ج) توفيرُ المعلوماتِ المطلوبةِ حيثما كان ذلك مناسبًا، لتدريبِ وتوعيةِ المستخدمين؛ بهدف القضاءِ على المخاطرِ المتعلِّقة باستخدامِ نظامِ الذَّكاء الاصطناعيّ عالي المخاطرِ أو الحدِّ منها، بحيث يقعُ على عاتقِ الشَّركةِ المصطنعة منحُ المستخدمِ المعرفةَ الفنيَّةَ والخبرةَ والتَّعليمَ والتدريبَ والافتراضاتِ المختلفةَ لاستخدامِ النِّظام.

(243) Article 9 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024,……. When implementing the risk management system as provided for in paragraphs 1 to 7, providers shall give consideration to whether in view of its intended purpose the high-risk AI system is likely to have an adverse impact on persons under the age of 18 and, as appropriate, other vulnerable groups.

(ISSN: 2537- 0758)

المبحث الثاني
إمكانيَّةُ ظهورِ نظامٍ جديدٍ للمسؤوليَّةِ خاصٍّ بالأشياءِ المُتَّصلةِ

تمهيدٌ وتقسيمٌ:

يُمثِّل ربطُ الأشياءِ عبر الإنترنتّ بدايةَ مرحلةٍ جديدةٍ من الثَّورة الرقميَّة. كما أنَّ مجالاتِ التَّطبيقِ عديدةٌ وتستمرُّ في النموّ (الروبوتات، السيَّارات، الصِّحة، تخطيط المدن، التأمين، إلخ). ويتطلَّب هذا الوضعُ دراسةَ موقفِ القانونِ الوضعيّ فيما يتعلَّقُ بهذا التطوُّر، وبشكلٍ أكثرَ دقَّةً فيما يتعلَّق بمسائلِ المسؤوليَّةِ المدنيَّةِ التي قد تنشأ عنه أثناء استخدامها، فمن المُحتملِ أن تتسبَّبَ الأشياءُ المُتَّصلةُ المستقلَّةُ والمزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ عالية الخطورةِ في حدوثِ ضررٍ، سواء لمالكِها أو لأطرافٍ ثالثةٍ[٢٤٤].

وبقدر ما كانت أنظمةُ المسؤوليَّةِ المدنيَّةِ الحاليَّة قد وُضعت قبل ظهورِ هذه الأشياءِ، فيثور التَّساؤل التالي: هل قانونُ المسؤوليَّةِ المدنيَّةِ المعمول به مناسبٌ للتَّعويضِ عن الضَّررِ النَّاتجِ عن الأشياءِ المُتَّصلةِ المستقلة؟ ولتحقيقِ ذلك، بعد تحليلِ ما إذا كانت أنظمةُ المسؤوليَّةِ المدنيَّةِ المعمول بها يُمكن تطبيقُها للتَّعويضِ عن الأضرارِ النَّاجمةِ عن الأشياءِ المرتبطة، فإنَّنا نتعاملُ مع إمكانيَّةِ تطبيقِ نظامِ مسؤوليَّةٍ خاصٍّ بهذه الأشياء.

ويُمثل ربطُ الأشياءِ عبر الإنترنتّ بدايةَ مرحلةٍ جديدةٍ من الثَّورةِ الرقميَّة[٢٤٥] التي بدأتْ في نهايةِ السبعينيَّاتِ مع ظهورِ الكمبيوتر الشخصيّ والهواتفِ المحمولةِ، وفي عام ٢٠٢٠، هناك ما يقرُبُ من ٧ أشياءَ متَّصلةٍ لكلّ شخصٍ في العالم[٢٤٦].

كما أنَّ إنترنتّ الأشياءِ (IoT)، هي الشَّبكةُ التي ترتبطُ بها هذه الأشياء، وتجعلُ ما كان يعتبرُ خيالًا لفترةٍ طويلةٍ أصبح الآن حقيقةً مسلَّمًا بها. فعلى سبيلِ المثالِ،

---

[٢٤٤] محمد المبطول، المسؤوليَّةُ المدنيَّةُ عن الذَّكاءِ الاصطناعيّ، مجلَّة عدالة للدِّراساتِ القانونيَّةِ والقضائية، ع٣٤- ٢٠٢٣، ص. ٥٦- ٦٩.

[245] Soriano, Préface du livre de F. Forster et A. Bensoussan, Droit des objets connectés et télécom, Bruxelles, Editions Bruylant, 2017, p.147.

[246] https://www.pwc.co.uk/issues/megatrends/technological-breakthroughs.html#4.

مع التَّشغيل الآليّ للمنزلِ الذي يُشكِّل أحدَ الرُّسومِ التوضيحيَّةِ لهذه الثَّورة، كلُّ ما يتطلَّبهُ الأمرُ هو كلمةٌ بسيطةٌ لرؤيةِ بابِ منزلك مفتوحًا، أو مصباح كهربائيٍّ يُضيء، أو تشغيل الميكروويف، وما إلى ذلك، حيث تتواصلُ الأشياءُ المُتَّصلةُ مع البشرِ ومع بعضِهم البعض! ومع تجهيزِهم بشكلٍ متزايدٍ بنظامِ الذَّكاءِ الاصطناعيّ (AI)، وبشكلٍ أكثر تحديدًا التعلُّم الآلي، يُمكنهم اتِّخاذُ قراراتٍ مستقلَّة، والاختيار بين عديدٍ من الحلولِ الممكنةِ لاختيار الحلِّ الأنسب، وأحيانًا يكون هذا الحلُّ أفضلَ ممَّا يختارُه الإنسانُ الأفضل.

وهكذا، بدءًا من الحياةِ اليوميَّةِ للإنسانِ وحتى القطاعاتِ المهنيَّةِ والمؤسسيَّة، يُعدِّل إنترنت الأشياءِ عديدًا من النَّماذج الرَّاسخة. ففي قطاعِ الرُّوبوتات–على سبيلِ المثال– ظهر مفهومٌ جديدٌ: الروبوتات السحابيَّة، وهو مجالٌ مستمدٌّ من الحوسبةِ السحابيَّة[٢٤٧] والتَّخزينِ السَّحابيّ[٢٤٨] وتقنياتِ الإنترنتّ الأخرى التي تركِّز على الاستفادةِ من البنى التحتيَّةِ المتقاربةِ والخدماتِ المشتركة. ويعدُّ ذلك شكلًا ناشئًا من الذَّكاءِ الاصطناعيّ للروبوتات[٢٤٩] والذي يتكوَّن من "ربط الرُّوبوتات بالإنترنت، إما لمشاركةِ المعلوماتِ مع الروبوتاتِ الأخرى المُتَّصلة، أو للاستفادةِ من قوَّة الحوسبةِ أو مساحة التَّخزين الإضافيَّة[٢٥٠]. وبالتالي تسمحُ هذه التقنيَّةُ بإنشاءِ روبوتات متَّصلة. وهكذا، في الخطَّةِ المتعلِّقةِ بالحلولِ العشرة لفرنسا الصناعيَّةِ الجديدة (NFI) في مايو ٢٠١٥، تمَّ تصنيفُ الروبوتات في فئةِ الأشياءِ المُتَّصلة.

إن مجالاتِ تطبيقِ إنترنتّ الأشياءِ عديدةٌ ومتناميةٌ باستمرارٍ. ويتطلَّب هذا الوضعُ دراسةَ موقفِ القانونِ الوضعيّ فيما يتعلَّقُ بهذا التطوُّر، وبشكلٍ أكثرَ دقَّةً فيما

(247) Stockage et l'accès aux données par l'intermédiaire d'internet plutôt que via le disque dur d'un ordinateur», in Cloud Computing: Définition, avantages et exemples d'utilisation, https://www.lebigdata.fr/definition-cloud-computing.

(248) Offre aux utilisateurs finaux et aux applications une architecture de stockage virtuel évolutive en fonction des besoins des applications», https://www.techopedia.com/definition/26535/cloud-storage.

(249) N. Nevejans, Traité de droit de la robotique civile, LEH Edition, Bordeaux 2017, n°135.

(250) «What is cloud robotics?», RoboEarth, http://roboearth.ethz.ch/cloud_robotics/index.html.

(ISSN: 2537- 0758)

يتعلَّق بمسائلِ المسؤوليَّةِ المدنيَّة التي قد تنشأ عنه. ومع ذلك، فقد تمَّ تحديدُ أن مسائلَ المسؤوليَّةِ المدنيَّةِ التعاقديَّةِ التي تتعلَّقُ بشكل خاصّ بالعلاقاتِ بين البائعِ والمشتري والمؤجِّر أو المالكِ والمستأجرِ للشَّيءِ المتَّصلِ لن يتمَّ تناولُها في هذه الدِّراسة. ومن هنا يثورُ التَّساؤل، هل قانونُ المسؤوليَّةِ المدنيَّة النافذ يصلحُ لإصلاحِ الضَّررِ النَّاتجِ عن الأجسامِ المُتَّصلةِ المستقلَّة والمزوَّد بأنظمةِ الذَّكاء الاصطناعيّ؟[٢٥١]، وسيتمُّ تركيزُ الاهتمامِ على قانون المسؤوليَّةِ المدنيَّة خارج نطاقِ التَّعاقدِ بالإضافةِ إلى بعضِ الأنظمةِ الخاصَّة.

وفي الحقيقةِ هذا السُّؤالُ مثيرٌ للاهتمامِ؛ لعدَّة أسبابٍ، **أولًا:** على المستوى القانونيّ، من المسلَّمِ به أن التطوُّر التِّكنولوجيَّ كان دائمًا متقدِّمًا على القانون، ستسمحُ لنا القضايا التي يُثيرها هذا البحثُ بمعرفةِ ما إذا كان من الممكنِ أو الضَّروريّ إعادةُ التَّفكيرِ في قانونِ المسؤوليَّةِ المدنيَّةِ الحالي لتكييفهِ مع الأشياءِ المُتَّصلة. **وثانيًا:** على مستوى التَّأمين، يُمكن أن يكونَ للأشياءِ المُتَّصلةِ تأثيرٌ فيما يتعلَّق ببعضِ القطاعاتِ الرئيسةِ التي يُغطِّيها التَّأمين، وهي: الصِّحةُ والمنزلُ والسيارات....إلخ. وهذا يُثير تساؤلاتٍ عديدةً تتعلَّق على وجهِ الخصوص: بطبيعةِ الخطرِ المضمون، وتقديره، ومدى الضَّمان، وشروط التَّعويض. **وثالثًا:** على المستوى السياسيّ والاقتصاديّ، تعدُّ الأشياءُ المُتَّصلةُ بمثابة أدواتٍ للتَّحولِ الرقميّ للشَّركات، وخاصَّةً الشَّركاتِ الصَّغيرة جدًّا (VSEs) والشَّركاتِ الصَّغيرةَ والمتوسِّطةَ الحجم (SMEs)، حيث يحتلُّون مكانًا مهمًّا في القدرةِ التنافسيَّةِ الدوليَّة. ورابعًا على المستوى الاجتماعيّ، يطرحُ إنترنتّ الأشياءِ مشكلاتٍ أمنيَّةً إلى حدٍّ كبيرٍ.

---

[٢٥١] للمزيد من التَّفاصيل راجع: فؤاد الشعيبى، المسؤوليَّةُ المدنيَّةُ عن أضرارِ روبوتات الذَّكاء الاصطناعيّ مجلة المعيار، ع٨، كليَّة الإمام مالك للشَّريعةِ والقانون، ص١٦١– ٢٠٠؛ محمد عرفان الخطيب، المسؤوليَّةُ المدنيَّةُ والذَّكاءُ الاصطناعيُّ– إمكانيَّةُ المساءلة؟: دراسةٌ تحليليَّةٌ معمَّقةٌ لقواعدِ المسؤوليَّةِ المدنيَّة، مجلَّة كليَّة القانون الكويتيَّة العالميَّة، مج٨، ع٢٩، كليَّة القانون الكويتيَّة العالميَّة سنة ٢٠٢٠، ص١٠٧– ١٥٢؛ د. محمد أحمد الشرايري، المسؤوليَّةُ المدنيَّةُ الذكيَّة عن أضرارِ الذَّكاء الاصطناعيّ: دراسةٌ مسحيَّةٌ مقارنةٌ، مجلَّة كليَّة القانون الكويتيَّة العالميَّة، مج١٠، ع٣٨، كليَّة القانونِ الكويتيَّة العالميَّة، سنة ٢٠٢٢، ص٣٥٧– ٤٠٨.

ستكون هذه الدِّراسةُ فرصةً للتَّفكيرِ في الحلولِ الممكنةِ التي سيتمُّ تنفيذُها في حالةِ حدوث أضرارٍ ومخاطرَ ناتجةٍ عن استخدامِ الأشياءِ المُتَّصلة المزوَّدة بأنظمةِ الذَّكاءِ الاصطناعيّ. ولتحقيق ذلك، بعد تحليلِ ما إذا كانت أنظمةُ المسؤوليَّةِ المدنيَّة المعمول بها (أنظمةُ المسؤوليَّةِ المدنيَّةِ خارج العقدِ والأنظمة الخاصَّة) يُمكن تطبيقُها للتَّعويضِ عن الأضرارِ النَّاجمةِ عن الأشياءِ المُتَّصلةِ سالفة الذِّكر، وهذا ما يوضَّح في (المطلب الأول)، كما أنَّه سيتمُّ التَّركيزُ على إمكانيَّةِ تنفيذِ نظام المسؤوليَّةِ الخاصّ بهذه الأشياء في (المطلب الثاني).

المطلب الأول: نظامُ المسؤوليَّةِ المدنيَّةِ المعمولُ به للتَّعويضِ عن الأضرارِ النَّاجمةِ عن الأجسامِ المُتَّصلةِ المستقلَّة.

المطلب الثاني: النِّظام الخاصُّ للمسؤوليَّةِ عن المنتجاتِ المَعيبة.

المطلب الأول
نظامُ المسؤوليَّةِ المدنيَّةِ المعمولُ به
للتَّعويضِ عن الأضرارِ النَّاجمةِ عن الأشياءِ المُتَّصلة

من المعلومِ أن علاقةَ السببيَّةِ هي علاقةٌ بين الحدثِ المُسبّبِ والضَّرر. ومن ثمَّ لا تعتبرُ المسؤوليَّةُ المدنيَّةُ للشَّخصِ عادلةً إلا بقدرِ ما يُمكن أن يُعزَى إليه الضَّررُ الذي يطلب التَّعويضَ عنه مباشرة، بسبب الخطأ الذي ارتكبَه، أو بشكلٍ غير مباشرٍ، عندما يكونُ هذا الضَّررُ ناجمًا عن خطأ ارتكبه الشَّيء ذاته أو الأشخاص الذين تحت سيطرته[٢٥٢]. وبالتَّالي فإنَّ الحاجةَ إلى وجودِ علاقةٍ سببيَّةٍ هي عنصرٌ جوهريٌّ مع المسؤوليَّة[٢٥٣]. ولهذا يوجدُ مبدأٌ يقضي بعدمِ قبولِ المسؤوليَّةِ في حالة الشكِّ في العلاقةِ السببيَّة. كما أدَّت العلاقةُ السببيَّةُ إلى خلقِ عديدٍ من النظريَّاتِ الفقهيَّة، بما في ذلك نظريَّةُ تكافؤ الأسبابِ (تعادل الأسباب) والسببيَّة الكافية (السبب الكافي)[٢٥٤].

---

(252) Ph. Brun, Responsabilité civile extracontractuelle, 4ème Edition, LexisNexis, 2016, Paris, p. 1 .

[٢٥٣] للمزيد من التَّفاصيلِ بشأنِ المسؤوليَّةِ التقصيريَّة، راجع: د. سليمان مرقص، النظريَّةُ العامَّةُ للالتزام، ديوان المطبوعات الجامعيَّة، ج١، ط ٥، سنة ١٩٩٢، ص١٢٧.

[٢٥٤] للمزيدِ من التَّفاصيل راجع: أحمد علي حسن عثمان، انعكاساتُ الذَّكاء الاصطناعيّ على القانونِ المدنيّ: دراسةٌ مقارنةٌ، مجلة البحوثِ القانونيَّةِ والاقتصادية، ع٧٦، جامعة المنصورة–

(ISSN: 2537- 0758)

ومما لا شكَّ فيه أن تكافؤَ الظُّروفِ (مبدأ تعادل الأسباب principe de l'équivalence des causes) يجعلُ جميعَ الظُّروفِ التي أسهمت في حدوثِ الضَّررِ في مرتبةٍ واحدةٍ؛ لأنه بدونها جميعًا لم يحدُثْ الضَّرر. بمعنًى آخر، إنَّ كلَّ سببٍ اشترك في إحداثِ ضررٍ بحيث لولاه لما حدَثَ، بحيث يعدُّ وحدَه سببًا له[٢٥٥] وبالتَّالي، يُمكن للمضرورِ أن يرجعَ على أحدِ المسؤولين للمطالبةِ بالتَّعويضِ عن جميعِ الأضرارِ التي لحقَتْ به، وللأخيرِ أن يرجعَ على الشُّركاءِ الآخرين. أما السببيَّةُ الكافيةُ، فهي على العكسِ من ذلك تهدفُ إلى تعيينِ مَا هو السَّببُ الفعَّالُ من بين

كليَّـة الحقـوق سـنة ٢٠٢١، ص١٥١٦– ١٦٣٠؛ مُصـعب ثـائر عبـد السـتار، المسـؤوليَّةُ التقصيريَّةُ المتعلِّقة بالذَّكاء الاصطناعيّ، مجلة العلوم القانونيَّةِ والسياسيَّة، مج١٠، ع٢، جامعة ديالى– كليَّة القانون والعلوم السياسيَّة سنة ٢٠٢١، ص. ٣٨٥– ٤١٢؛ محمد محمد عبد اللطيف، المسؤوليَّةُ عن الذَّكاء الاصطناعيّ بين القانونِ الخاصّ والقانون العامّ، مجلة البحوثِ القانونيَّةِ والاقتصاديَّة، عددٌ خاصٌّ، جامعة المنصورة– كليَّة الحقوق ٢٠٢١، ص٢– ٥٢.

[٢٥٥] ونحيلُ التَّفاصيلَ للمراجعِ العامَّة، د. سعيد سعد عبد السلام، مصادرُ الالتزامِ المدنيّ، الطَّبعة الأولى، دار النَّهضـة العربيَّـة، القاهرة، سنة٢٠٠٣، ص٣٩٠؛ د. أحمـد شـرف الـدين، نظريَّـةُ الالتـزامِ، الجـزء الأول، مصـادرُ الالتـزام، الكتـاب الأول: المصـادر الإراديَّـة (العقـد– والإرادة المنفردة) بـدون ناشـر، سـنة ٢٠٠٣؛ د. أنـور سـلطان، المـوجز فـي النظريَّـةِ العامَّـة للالتـزام، مصادرُ الالتزام، دار المطبوعات الجامعيَّة، سنة ١٩٩٨؛ د. أيمن سعد سليم، مصـادرُ الالتزام، دراسةٌ مقارنةٌ بين القانونِ المدنيّ المصريّ ومشروعٍ مقترحٍ للقانونِ المدنيّ المصريّ طبقًا لأحكام الشَّريعة الإسـلاميَّة، الطبعـة الثانيـة، دار النَّهضـة العربيَّـة، القـاهرة، سـنة ٢٠١٧؛ د. إسـماعيل غانم، النظريَّةُ العامَّة للالتزام، مصادر الالتزام، مكتبة عبد الله وهبة، بدون سنة نشر. د. حسام الدين كامل الأهواني، الجزء الأول، مصادر الالتزام، الطبعة الثانية، بدون ناشر، سنة ١٩٩٥، ص٤٢؛ د. حمـدي عبـد الـرحمن، الوسـيطُ فـي النظريَّـةِ العامَّـة للالتزامـات، الكتـاب الأول، المصادرُ الإراديَّةُ للالتزام، العقدُ والإرادةُ المنفردة، الطَّبعة الأولى، دار النَّهضـة العربيَّة، القاهرة، سنة ١٩٩٩؛ د. رمضان أبو السعود، مصـادرُ الالتزام، دار الجامعةِ الجديدة، الإسكندريَّة، سنة ٢٠١٨؛ د. رضا عبد الحليم عبد المجيد عبد الباري، مصادرُ الالتزام، الكتاب الأول، المصـادر الإراديَّـة للالتـزام (العقـد– الإرادةُ المنفردة)، الطَّبعـة الأولـى، دار النَّهضـة العربيَّـة، القـاهرة، سـنة ٢٠١٢.

مختلفِ فاعلي الضَّرر، وبالتالي، سيتعيَّن على المضرورِ أن يطالبَ بالمسؤوليَّةِ من الشَّخصِ الذي أدَّى فعلُه عادةً أو قد يؤدِّي إلى حدوث الضَّرر.

وجدير بالذِّكر أنَّ تعادُلَ الظُّروفِ أو الأسبابِ أكثر فائدةً للمضرور، وحتى لو لم يُشِرْ إليها صراحةً، فإنَّ السَّوابقَ القضائيَّةَ تطبِّق في كثيرٍ من الأحيانِ نظريَّةَ تعادلِ الأسبابِ أو الظُّروف[٢٥٦]. وفيما يتعلَّقُ بالحدثِ المسبب، يستنتجُ من الموادِّ ١٢٤٠ وما يليها أن الحدثَ المسبِّبَ للمسؤوليَّةِ يُمكن أن يكونَ فعلًا شخصيًّا (خطأ)، أو فعلَ أشياء، أو فعلَ شخصٍ آخر. وسنقتصرُ في هذه الدِّراسةِ على فهْمِ الأشياءِ المُتَّصلةِ من خلالِ نظامِ المسؤوليَّةِ عن الفعلِ الشخصيِّ والمسؤوليَّة عن الأشياء.

الفرع الأول
المسؤوليَّةُ عن الفعلِ الشَّخصيِّ

تنصُّ المادة ١٦٣ من القانونِ المدنيِّ المصريِّ على أنه "كلُّ خطأٍ يُسبِّب ضررًا للغير يلتزمُ من ارتكبَهُ بالتَّعويض"، وجديرٌ بالذِّكر أنه قد يكونُ من المفاجئِ اللُّجوءُ إلى قواعدِ المسؤوليَّةِ الشَّخصيَّة[٢٥٧] فيما يتعلَّقُ بالأشياءِ المُتَّصلة؛ لأنَّه من البدهيِّ

---

(256) Cass. civ. 2e, 27 janvier 2000, RCA, avril 2000, n°109, p.8; Cass. civ. 2e, 12 octobre 2000, RCA, janvier 2001, n°7, p.13; Cass. civ. 2e, 27 mars 2003, pourvoi n°01-13858.

[٢٥٧] للمزيد من التَّفاصيلِ بشأنِ المسؤوليَّةِ عن الفعل الشخصيِّ، راجع شروحَ الفقه: د. سمير عبد السيد تناغو، مصادرُ الالتزامِ (العقد– الإرادة المنفردة– العمل غير المشروع– الإثراء بلا سبب– القانون)، مصدران جديدان (الحكم– القرارُ الإداريُّ)، الطَّبعة الأولى، مكتبة الوفاء القانونيَّة، الإسكندريَّة، سنة ٢٠٠٩؛ د. عبد الحي حجازي، النظريَّةُ العامَّةُ للالتزام، الجزء الثاني، مصادر الالتزام، مكتبة عبد الله وهبة، بدون سنة نشر؛ د. عبد الرزاق أحمد السنهوري، الوسيطُ في شرح القانونِ المدنيِّ، الجزء الأول: نظريَّةُ الالتزامِ بوجهٍ عامٍّ، مصادر الالتزام، منشأة المعارف، الإسكندريَّة، سنة ٢٠٠٤؛ د. عبد العزيز المرسي ود. محمد محمد أبو زيد، مصادر الالتزام، العقدُ والإرادةُ المنفردة، كليَّة الحقوق، جامعة المنوفيَّة، (بدون تاريخ نشر)؛ د. عبد المنعم فرج الصدة، مصادر الالتزام، دار النَّهضة العربيَّة، القاهرة، سنة ١٩٩٢؛ د. علي نجيدة، النظريَّة العامَّة للالتزام، الكتاب الأول، مصادر الالتزام، دار النَّهضة العربيَّة، سنة ٢٠٠٤–٢٠٠٥؛ د. محمد حسام لطفي، النظريَّةُ العامَّة للالتزام، مصادرُ الالتزام، دار النَّهضة العربيَّة، القاهرة، سنة ٢٠١٧–٢٠١٨؛ د. محمد حسن عبد الرحمن، مصادرُ الالتزام، دراسةٌ مقارنةٌ، الطَّبعة الثانية، دار النَّهضة العربيَّة– القاهرة، سنة ٢٠١٠؛ د. محمد حسن قاسم،– الوجيزُ في نظريَّةِ الالتزام، المصادرُ– الأحكام، دار الجامعة الجديدة، سنة ١٩٩٤، القانون المدنيُّ، الالتزاماتُ، المصادرُ،

(ISSN: 2537- 0758)

أن يكون نظامُ المسؤوليَّةِ عن الأشياءِ هو الأكثرَ ملاءمة. ولكن، دون الخوضِ في تفاصيلِ هذه المسألةِ في الوقتِ الرَّاهن، سنرى أنَّ نظامَ المسؤوليَّة عن الأشياءِ المعمول به يُمكن أن يعيقَ دعوى المسؤوليَّةِ عن الأشياءِ المُتَّصلة. ولهذا السَّبب تساءلنا عن إمكانيَّةِ التَّطابقِ بين نظامِ المسؤوليَّةِ الشَّخصيَّة واستخدام الأشياءِ المُتَّصلة. وبالفعل، وبناءً على المادَّتين ١٢٤٠ و١٢٤١ من القانونِ المدنيّ الفرنسيّ، فإن المسؤوليَّةَ عن الفعلِ الشخصيّ هي المسؤوليَّةُ عن الخطأِ المثبت. وقد يكون هذا عملًا أو امتناعًا عن عملٍ[٢٥٨]. لكن هذا المفهومَ يتلاشى مع ظهورِ خططِ التَّعويضِ المستقلَّة، وتطوُّر نظمِ المسؤوليات. وفي هذا الشَّأن نحلِّل مدى إمكانيَّةِ تطبيقِ نظامِ المسؤوليَّةِ عن الخطأ المثبتِ على الأشياءِ المُتَّصلة. ولتوضيحِ ذلك، سيتمُّ النَّظرُ من ناحيةٍ إلى تحديدِ الأطرافِ التي يحتملُ مسؤوليتها، ومن ناحيةٍ أخرى، طرائق تنفيذِ المسؤوليَّة.

وبالنِّسبةِ لتحديدِ الأطرافِ المحتمل مسؤوليَّتها، على الرَّغمِ من التدخُّل بدرجاتٍ مختلفةٍ وفي مراحلَ مختلفة، فمن المحتملِ أن تكونَ المسؤوليَّةُ عن الفعل الشخصيّ بين عدَّة جهاتٍ فاعلة: المصمِّم، الشَّركة المصنِّعة، أو مطوِّر البرمجيات، أو حتى المستخدم ذاته.

أولًا: الصُّعوباتُ المتعلِّقةُ بإثباتِ الخطأ:

Difficultés relatives à la preuve de la faute:

إن إثبات أن الضَّررَ الذي لحِقَ بالمضرورِ ناتجٌ عن خطأٍ يختلفُ عن عيبِ سلامةِ المنتج المعني[٢٥٩]. ومع ذلك، ونظرًا للصُّعوباتِ المتعلِّقةِ بإثباتِ الخطأ والعلاقة السببيَّة، فإنَّ تنفيذَ المسؤوليَّةِ عن الخطأ يُمكن أن يكونَ معقدًا في سياقِ

العقد، تعريفُ العقدِ وتقسيماته– تكوين العقد، دراسةٌ فقهيَّةٌ قضائيَّةٌ مقارنةٌ في ضوء التَّوجيهاتِ التشريعيَّةِ والقضائيَّةِ الحديثة وقانون العقودِ الفرنسي الجديد (٢٠١٦)، المجلد الأول، دار الجامعة الجديدة، سنة ٢٠١٧.

(258) Civ. 27 févr. 1951 (arrêt Branly): D. 1951. 329, note Desbois; JCP 1951. Cf. Viney G. et Jourdain P., Traité de droit civil. Les conditions de la responsabilité, Ghestin J. (sous la dir.), 4e édition, LGDJ, Paris, 2013, pp. 463-467.

(259) Civ. 1ère, 10 décembre 2014, n° 13-14.14; Civ. 1ère, 17 mars 2016, n° 13-18.876, Dalloz 2017, 24, obs. Brun, Gout et Quézel-Ambrunaz.

الضَّررِ النَّاجم عن الأشياءِ المُتَّصلة. ويُمكننا أن نتساءلَ عن طبيعةِ الفعلِ الماديّ المعنيّ في سياقِ الشَّيءِ المتَّصل. هل سيكونُ هذا خطأً إغفالٍ أو خطأً في التَّصنيع (خطأ في جهازيَّةِ الخدمةِ) une faute de commission؟

في الحقيقةِ إنَّ معظمَ الأخطاءِ التي تُرتكب في سياقِ الأشياءِ المُتَّصلة ستكون أخطاءَ امتناعٍ، مثل خطأ الشَّركةِ المصنِّعة التي لم تستخدم العبوةَ الموصى بها من قِبل المصمِّم، وكذلك خطأُ مطوِّر البرمجيَّاتِ الذي لم ينفِّذ أماكنَ نظامٍ تعليميّ متوافقٍ أو خطأ المستخدمِ الذي لم يحترمْ قواعدَ استخدام الشَّيء المتَّصل. ومع ذلك، فمن الصَّعب إثباتُ الفعلِ السلبيّ وهذا يجعلُ مهمَّةَ المضرورِ أكثر صعوبةً. ومع ذلك، فإن السَّوابقَ القضائيَّةَ تعترفُ بإمكانيَّةِ العثورِ على خطأِ الامتناعِ عندما لا يتصرَّف الوكيلُ وفقًا لالتزامٍ قانونيّ. وبالتالي فإنَّ السُّؤالَ هو معرفةُ ما إذا كان هناك معيارٌ أو نصٌّ قانونيٌّ، فيما يتعلَّق بالأشياءِ المُتَّصلة، يُلزم المنتجين بالامتثالِ لالتزاماتٍ معيَّنةٍ.

يُمكننا أولًا أن نفكِّر في المبدأِ العامِّ للوقايةِ والاحتراز والذي يُمكن تطبيقُه فيما يتعلَّق بالأشياءِ المُتَّصلة، على مختلفِ المشاركين في سلسلةِ إنتاج الشَّيءِ من أجلِ تعزيزِ التزامِهم باليقظة. لكن الطَّبيعةَ القانونيَّةَ الدَّقيقة لهذه المبادئِ ونطاقها في قانونِ المسؤوليَّةِ المدنيَّة لا تزالُ في طورِ التَّطوير.

وبالإضافةِ إلى ذلك، فإن تعدُّدَ المشاركين في سلسلةِ الإنتاج يجعلُ المهمَّةَ صعبةً على المضرور[٢٦٠]. وتتضمَّن اللَّائحةُ الأوروبيةُ الصَّادرة في ٢٧ أبريل ٢٠١٦ والمتعلِّقة بحمايةِ الأفرادِ فيما يتعلَّق بمعالجةِ البياناتِ الشَّخصيَّة وحريَّة حركةِ هذه البيانات (55 GDPR) أيضًا بعض الأحكامِ التي يُمكن تطبيقُها على الأشياءِ ذات

---

[٢٦٠] في هذا الشَّأن راجع: محمد منصور خليل خزيمية، المسؤوليَّةُ المدنيَّةُ عن أضرارِ الذَّكاء الاصطناعيّ: دراسة مقارنة، رسالة ماجستير، الجامعة العربيَّة الأمريكيَّة، جنين ٢٠٢٣؛ نور خالد العبد الرزاق، المسؤوليَّةُ المدنيَّةُ الناشئةُ عن استخدامِ الذَّكاء الاصطناعيّ، أعمال مؤتمر التحدِّياتِ والآفاقِ القانونيَّة والاقتصاديَّة للذَّكاءِ الاصطناعيّ، جامعة عين شمس– كليَّة الحقوق،٢٠٢٤، ص١– ٢٨؛ مها رمضان محمد بطيخ، المسؤوليَّةُ المدنيَّةُ عن أضرارِ أنظمةِ الذَّكاء الاصطناعيّ: دراسةٌ تحليليَّةٌ مقارنةٌ، المجلة القانونيَّة، مج٩، ع٥، جامعة القاهرة– كليَّة الحقوق– فرع الخرطوم ٢٠٢١، ص١٥١٣– ١٦١٦.

(ISSN: 2537- 0758)

الصِّلة. وفي الواقع، حتى لو لم يستهدفْ بشكلٍ مباشرٍ الأشياء المُتَّصلة، فإن اللَّائحةَ العامَّةَ لحمايةِ البياناتِ تنصُّ في المادة ٢٥ على مبدأِ الخصوصيَّةِ بحسَب التَّصميم.

ومع ذلك، فإن الضَّررَ النَّاجمَ عن الأشياءِ المُتَّصلةِ لا يرتبطُ دائمًا بخطأ، حيث يُمكن أن ينتجَ عن استقلاليَّةِ اتِّخاذ القرارِ التي يتمتَّعُ بها هذا الشَّيء. وهذا يعني أن الجهازَ المتَّصلَ لا ينفذ برنامجًا؛ ولهذا يجبُ أن نضعَ هذه الصُّعوباتِ في الاعتبارِ عند تنفيذِ إجراءِ المسؤوليَّة. ويُضاف إلى الصُّعوباتِ السَّابقة الصُّعوباتُ المتعلِّقةُ بإثباتِ العلاقةِ السببيَّة.

ثانيا: صعوبةُ إثبات علاقة السببيَّة لتعدُّد أخطاءِ الفاعلين:

Difficultésquant à la preuve du lien de causalité en raison de la multiplicit é de fautes des acteurs:

إن المسؤوليَّة المنصوصَ عليها في المادَّتين ١٤٠ و١٢٤١ من القانونِ المدنيّ الفرنسيّ تفترضُ وجودَ علاقةٍ معيَّنةٍ بين الخطأ والضَّرر: وهي علاقةُ السببيَّة. وتسترشدُ هذه العلاقةُ السببيَّة بالمبدأ التالي: في حالةِ الشكِّ في العلاقةِ السببيَّةِ لا توجدُ مسؤوليَّة. ولكن، على الرَّغم من ندرتِها بالتَّأكيد، يُمكن افتراضُ العلاقةِ السببيَّة في بعضِ الحالاتِ من حيث الموضوع.

وقد يكون من الصَّعبِ على المضرورِ تقديم دليلٍ على هذه العلاقةِ السببيَّة، خاصَّةً في حالةِ وجودِ أخطاءٍ متعدِّدةٍ من جانبِ الفاعلين. كما أن يقينَ العلاقةِ السببيَّةِ ليس واضحًا دائمًا. وفي الواقع، فإن تعدُّد الجهاتِ الفاعلةِ المشاركة في سلسلةِ تصنيعِ الأشياءِ المُتَّصلة يمكن أن يؤدِّيَ إلى تعدُّدِ الأخطاء. فعلى سبيلِ المثال، إذا تعطَّلت غسالةٌ متَّصلةٌ في شقَّةٍ وتسبَّبت في تلفِ المبنى بسببِ المياه، فيجب على الجيرانِ أو المستأجرين وصفُ الخللِ الذي تسبَّب في الضَّررِ، وقد يتبيَّنُ أن عديدًا من الأخطاءِ هي سبب الضَّرر[٢٦١].

(261) Laura Jounda Sonkwa, Responsabilité civile du fait des objets connectés autonomes Master, Droit des assurances Formation en apprentissage RESPONSABILITE CIVILE DU FAIT DES OBJETS CONNECTES AUTONOMES Mémoire de recherche Par Sous la direction de Monsieur le professeur Louis Perdrix Année: 2018– 2019.

ولحلِّ هذه الصعوبة، يُمكننا تطبيقُ النَّظريَّتين المذكورتين سابقًا: السببيَّة الكافية (السبب الكافي) أو نظريَّة تعادلِ السَّببِ التي فضَّلتها السَّوابقُ القضائيَّة، والتي تقدِّم علاوةً على ذلك مزايا للمضرورِ، وبالتالي–في مثالنا السابق– سيتمكَّن المضرورون من الاقترابِ من أيِّ حلقةٍ في السِّلسلةِ للمطالبةِ بالتَّعويضِ عن الأضرارِ التي لحقَتْ بهم.

ومع ذلك، قد تنشأ صعوبةٌ أخرى. فليس من السَّهل دائمًا إثباتُ وجودِ علاقةٍ سببيَّةٍ على وجهِ اليقينِ والتَّأكيد. ولقد رأينا أن الأشياءَ المُتَّصلةَ تشكِّل نظامًا بيئيًّا واسعًا. بحيث قد يكون الضَّررُ ناتجًا عن معلوماتٍ غير صحيحةٍ تمَّ إرسالها إلى الجهازِ المتَّصل الذي تسبَّب في الضَّرر. وبالتَّالي، حتى لو ارتكبَ المضرور– على سبيل المثال– فعلًا خطأً أثناء استخدامِ ممتلكاته، فسيظلُّ من الضَّروريِّ إثبات أنَّ هذا الخطأ هو من سبَّبَ الضَّرر. وكذلك ينطبقُ الشَّيءُ نفسُه في حالةِ وجودِ شيءٍ متَّصلٍ تمَّ برمجةُ نظام التعلُّمِ الخاصِّ به بشكلٍ سيِّئ. سيتعيَّن على المضرورِ إثباتُ أن هذه البرمجةَ السيِّئةَ هي سببُ الضَّررِ الذي لحِقَ به. وممَّا لا شكَّ فيه أن هذا الدَّليلَ غير مؤكَّد.

وإزاء عدم اليقين، يمكننا أن نستمدَّ الإلهامَ من السَّوابقِ القضائيَّة المعمول بها في المسائلِ الطبيَّة. ومن المتصوَّر أيضًا إيجادُ حلٍّ للحالةِ المحدَّدةِ للمركباتِ ذاتيَّةِ القيادة. وهكذا، في المجال الطبيّ، هناك حالاتٌ استَخدمت فيها محكمةُ النَّقضِ مفهومَ فواتِ الفرصةِ للتَّعويضِ عن عدمِ اليقين بشأنِ العلاقةِ السببيَّة. وفي الحالاتِ التي يوجدُ فيها شكٌّ في العلاقةِ السببيَّة بين خطأ الطَّبيبِ ووقوع الضَّرر، فإن هذا الشكَّ يعوِّضه في الغالبِ مفهومُ فواتِ الفرصة، ففي إحدى الحالات، اختار طبيبٌ، بناءً على تفسيرٍ خطأٍ أن تلدَ امرأةٌ بالوسائل الطبيعيَّة، على الرَّغمِ من أنَّ العمليَّةَ القيصريَّةَ كانت ضروريَّةً[٢٦٢]. وبما أنَّ الطِّفل وُلد معاقًا، رفعت والدتُه دعوى قضائيَّةً ضدَّ الطَّبيبِ للحصولِ على تعويضٍ عن الضَّررِ الذي لحِقَ بهما وبطفلهما القاصر، بما في ذلك فقدانُ الفرصة. وقد لقي هذا الإجراءُ استحسانًا من قبل محكمةِ الاستئناف، على الرَّغم من أن الخبراءَ لم يتمكنوا من تحديدِ ما إذا كانت ممارسةُ عمليَّةٍ قيصريَّةٍ مبكرة ستجعلُ من الممكنِ تجنُّب الآفات، فقد خلصت مع ذلك إلى أنَّ

(262) CJUE, 21 juin 2017, semaine juridique, Ed. gén., 2017, note 908.

(ISSN: 2537- 0758)

الخطأ التَّشخيصيَّ وكان الامتناعُ العلاجيُّ النَّاتج عن ذلك سببًا في فواتِ فرصةِ ولادةِ الطِّفل خاليًا من جميعِ الآفاتِ، وقد أيَّدت محكمةُ النَّقضِ الفرنسيَّة هذا الحكمَ[٢٦٣].

وعند تطبيقِ هذا الحلِّ على الضَّرر الذي يلحق بأطرافٍ ثالثةٍ بسبب أشياءَ متَّصلة، فإن هذا الحلَّ، على الرَّغم من انتقاده، يُمكن أن يعزِّز إصلاحَ هذا الضَّرر؛ لأنه يُسهل إثباتَ العلاقةِ السببيَّة. ولكن نظرًا لكونهِ مبنيًّا على فواتِ الفرصة، فإن هذا التَّعويضَ سيقتصرُ على الفرصةِ الضَّائعة ولا يُمكن أن يكونَ مساويًا للمزيَّةِ التي كانت ستوفِّرها هذه الفرصةُ لو تحقَّقت. وبالتَّالي لن يتمكَّنَ المضرورُ من الحصولِ على تعويضٍ كاملٍ عن الضَّررِ الذي لحِقَه على هذا الأساس.

وفيما يتعلَّق بالمركباتِ ذاتيَّة القيادة، فإن إدخالَ صناديق تسجيل سوداء، في نماذجِ الطَّائرات، من أجل الحصولِ على رؤيةٍ أفضلَ لأسبابِ الضَّرر، يُمكن أن يبسطَ إثباتَ العلاقةِ السببيَّة.

وعلى الرَّغم من صعوباتِ التَّنفيذ، تظلُّ الحقيقةُ أن المسؤوليَّةَ الشَّخصيَّةَ أساسٌ متكررٌ للمسؤوليَّة التي يُمكن لأطرافٍ ثالثةٍ الاحتجاج بها، للتَّعويضِ عن الأضرارِ التي لحقَتْ بهم نتيجةً لأشياء متَّصلةٍ. ومع ذلك، يبدو أن نظامَ المسؤوليَّةِ المشتركة هو الأكثرُ ملاءمة. ونظام المسؤوليَّةِ عن الأشياءِ يُمكن اعتباره بداهةً أنسبَ نظامٍ للقانونِ العامِّ لطلبِ التَّعويضِ عن الضَّررِ الذي لحِقَ بأطرافٍ ثالثةٍ بسببِ الأشياءِ المُتَّصلة.

الفرع الثاني
المسؤوليَّةُ عن الأشياءِ

على عكسِ المسؤوليَّةِ عن الأفعالِ الشَّخصيَّة، فإنَّ المسؤوليَّةَ عن الأشياءِ هي مسؤوليَّةٌ موضوعيَّةٌ "غير مباشرةٍ"؛ لأنها مبنيَّةٌ على المخاطرِ وليس على الخطأ (التَّقييم الذَّاتي). بحيث لا يكونُ الشَّخصُ المسؤولُ مسؤولًا عن الضَّررِ الذي سبَّبه بفعلته، ولكن عن الضَّررِ الذي تسبِّبه الأشياء التي تحت سيطرتهِ أو حراسته، وعلى

[٢٦٣] للمزيد من التَّفاصيل بشأنِ فواتِ الفرصةِ راجع: د. أيمن إبراهيم العشماوي، تفويت الفرصة، دراسةٌ مقارنةٌ، دار النَّهضة العربيَّة، سنة ٢٠٠٤، ص١٤-٨٨؛ د. أيمن مصطفى أحمد البقلي، التَّعويضُ عن فواتِ الفرصةِ في إطار المسؤوليَّة المدنيَّة للأطباء، مجلة الدِّراسات القانونيَّة، كليَّة الحقوق- جامعة أسيوط، ٢٠١٣.

النَّحوِ المنصوصِ عليه في الفقرة (١ من المادة ١٢٤٢)، (الفقرة ١، ١٣٨٤) سابقًا من القانونِ المدنيّ الفرنسيّ، وقد تمكَّن الفقهُ من أن يستنتجَ من هذه المادة مبدأً عامًّا للمسؤوليَّةِ دون خطأ، وتجدر الإشارةُ إلى أنه رغمَ تكريسِ المسؤوليَّةِ دون خطأ عن وقائعِ الأشياء، فقد أبقى المُشرّع على نفاذِ النُّصوصِ الخاصَّة المنطبقة على الحيواناتِ والمباني (المادَّتان ١٢٤٣ و١٢٤٤ من القانونِ المدنيّ الفرنسيّ).

وفي هذا الشَّأن نبيّن مدى إمكانيَّةِ تنفيذِ نظام المسؤوليَّةِ عن الأشياءِ في سياقِ الأشياءِ المُتَّصلة، ولتحقيق ذلك، سيتمُّ تناولُ الأسئلةِ المتعلِّقة بتطبيقِ "حقيقة الأشياء"، من حيث الأشياءُ المُتَّصلةُ وإن كانت غير متوافقةٍ مع الاستقلاليَّةِ الممنوحةِ للأشياءِ المُتَّصلة.

وتُشير "حقيقةُ الشَّيء" في مسائلِ الأشياءِ المُتَّصلة إلى الدَّورِ السببيّ الذي تلعبُه في إحداثِ الضَّرر(٢٦٤). وبعبارةٍ أخرى، هو أن يكونَ الشَّيءُ أداةً للضَّرر، ويقع عبءُ إثباتِ هذه الحقيقةِ على عاتقِ المضرورِ(٢٦٥).

وقد يحدث الضررُ أثناء استخدامِ هذه الأشياءِ، أو نتيجة القرصنة، فما المقصودُ بالشَّيءِ الذي يُسبِّب الضَّرر؟ الشَّيء الملموس أم نظام الذَّكاءِ الاصطناعيّ؟ (أ) علاوةً على ذلك، إذا كان تنفيذُ المسؤوليَّةِ مشروطًا بإثباتِ شذوذِ الشَّيء، فكيف يُمكن وصفُ ذلك بوجودِ شيءٍ متَّصل؟ (ب).

أولًا: تحديدُ الشَّيءِ المسبِّب للضَّرر:

L'identification de la chose dont le fait est à l'origine du dommage:

جدير بالذكر أن الأشياءَ المُتَّصلةَ المستقلَّة مزوَّدةٌ بنظامِ ذكاءٍ اصطناعيٍّ يسمحُ لها باتِّخاذ القرارات، ويُمكن أن يكونَ نظامُ الذَّكاءِ الاصطناعيّ هذا برنامجًا أو

(264) Cf. Civ. 9 juin 1939, DH 1939, 2, p. 283; 19 février 1941, DC, 1941, p. 85, note J. Flour.Notons aussi que pour appliquer le régime de responsabilité du fait des choses, la jurisprudence ne distingue pas suivant que la chose a été ou non mise en mouvement par la main de l'homme.

(265) (Civ. 2e, 28 novembre 1984, JCP 1985, II, 20477, 2e esp., note N. Dejean de la Bâtie; pour une chute dans un escalator, Civ. 2e, 2 avril 1997, Bull. civ. II, n°109, 2e arrêt).

(ISSN: 2537- 0758)

خوارزميَّة. وفي حالةِ حدوثِ ضررٍ بسببِ هذه الأشياء، يُمكن تصنيفُ الشَّيء الذي سبَّب الضَّررَ. بمعنًى آخر يجبُ فصلُ نظامِ الذَّكاءِ الاصطناعيّ عن الكائنِ نفسهِ بالمعنى المقصودِ في المادة ١٢٤٢ من القانون المدنيّ الفرنسيّ.

وفي الحقيقةِ يُمكن أن يكونَ الشَّيءُ منقولًا أو غير منقول، ملموسًا أو غير ملموس. وفي الحالةِ الأخيرة، قبِلَ الفقهُ حتى الآن تطبيقَ المادةِ السابقةِ ١٣٨٤من القانون المدنيّ للصُّور، جزيئات الاسبستوس، الجزيئات، الدُّخان، البخار، الكهرباء[٢٦٦]. وإذا قُمْنا بفصلِ نظامِ الذَّكاءِ الاصطناعيّ عن الشَّيء، فيُمكننا، على أساسِ هذه السَّوابق القضائيَّة، النَّظر في المسؤوليَّةِ المستحقَّةِ على الذَّكاء الاصطناعيّ[٢٦٧].

ومع ذلك، فإن الذَّكاءَ الاصطناعيَّ هو شيءٌ غير ملموس، وهو الأمرُ الذي من شأنهِ أن يصلَ إلى توسيعِ المادة ١٢٤٢ بالنِّسبةِ للأشياءِ الماديَّة. وقد تقدَّم بهذا الاقتراحِ جانبٌ من الفقه، خاصَّةً فيما يتعلَّق بالإعلام. ولكنَّه تعرَّض لانتقاداتٍ شديدةٍ؛ لأنه يتمثَّل في إخضاعِ الأشياءِ من نوعٍ معيَّنٍ لنظامٍ قانونيٍّ لا يتكيَّف مع خصوصيَّتها؛ ممَّا يؤدِّي بلا شكٍّ إلى زيادةِ الشَّيءِ والضَّرر، وينفي الفقهُ أيَّ قرينةٍ سببيَّةٍ لصالحِ المضرور، ولكن دونَ دحضِ إمكانيَّةِ تنفيذِ المسؤوليَّة، بشرطِ أن يقدِّم المضرورُ دليلًا على الدَّور السببيّ.

وفي هذا الصَّدد، يقترحُ مشروعُ إصلاحِ المسؤوليَّةِ المدنيَّة الصَّادر في ١٣ مارس ٢٠١٧ حصْرَ مبدأِ المسؤوليَّةِ المدنيَّةِ في الأشياءِ الماديَّة فقط (المادة ١٢٤٣) والتي

---

(266) Caen, 20 novembre 2001: JCP 2003. II. 10045, note Trébulle, Civ. 2e, 27 septembre 2012, n° 11-11.762. Civ. 2e, 11 juin 1975, Bull. II n° 173. 69 Civ. 2e, 10 février 1967, Bull. II, n°66.

[٢٦٧] محمد إبراهيم حسانين، الذَّكاء الاصطناعيُّ والمسؤوليَّةُ المدنيَّةُ عن أضرارِ تطبيقه، دراسةٌ تحليليَّةٌ تأصيليَّة، المجلة القانونيَّة مج١٥، ع١، جامعة القاهرة– كليَّة الحقوق– فرع الخرطوم، سنة ٢٠٢٣– ١٧٧– ٢٧٠؛ محمد عماد فلاح العتوم، المسؤوليَّةُ المدنيَّةُ لتطبيقاتِ الذَّكاء الاصطناعيّ بين الواقعِ والحاجةِ للتَّجديد: دراسةٌ تحليليَّةٌ في القانون، رسالة ماجستير، جامعة اليرموك ٢٠٢٢؛ محمد شاكر محمود محمد، دورُ الذَّكاءِ الاصطناعيّ في تطويرِ قواعدِ المسؤوليَّة المدنيَّة: دراسةٌ تحليليَّةٌ، مجلة كليَّة القانون للعلومِ القانونيَّةِ والسياسيَّة، مج١١، ع٤٢ جامعة كركوك– كليَّة القانون والعلوم السياسيَّة، سنة ٢٠٢٢، ٦١٦– ٦٣٩.

تنصُّ على أن الشَّخصَ مسؤولٌ قانونًا عن الأضرارِ النَّاجمةِ عن الأشياءِ الماديَّة الموجودة في حوزتهِ وتحت سيطرتهِ وحراسته[٢٦٨]. ولذلك فمن المحتملِ جدًّا ألا تتطوَّر فكرةُ توسيعِ نطاقِ المسؤوليَّة عن الأشياءِ لتشملَ الذَّكاء الاصطناعيَّ؛ كون ذلك الأخيرِ شيئًا غير ماديٍّ. وكلُّ ما تبقَّى هو اللُّجوءُ إلى الدَّعم الماديّ للذَّكاء الاصطناعيّ (الروبوت، الجهاز، الآلة، إلخ) للنَّظر في المسؤوليَّةِ المحتملةِ عن حقيقةِ الأمور. وهذا الحلُّ هو الأرجحُ لتبريرِ تطبيقِ المادة ١٢٤٢-١ على الأشياءِ المُتَّصلة[٢٦٩]. لكنَّ المضرورَ قد يُواجه صعوباتٍ أخرى، خاصَّةً إذا كانَ عليه تقديمُ دليلٍ على خللٍ في الشَّيء.

أ- إثبات انحرافِ الشَّيء المتَّصل من خلالِ المسؤوليَّةِ عن الأشياء:

La preuve de l'anormalité de l'objet connecté En matière de responsabilité du fait des choses:

يتحتمُ على المضرورِ تقديمُ ما يثبتُ انحراف الشَّيءِ لإثباتِ وجودِ علاقةٍ سببيَّة. وهذا هو الحالُ بالتَّحديدِ عندما يكونُ الضَّررُ ناجمًا عن شيءٍ متحركٍ دون أيّ اتِّصالٍ من قِبل المضرور، أو عن طريقِ شيءٍ خاملٍ غير متحرِّك، لكنَّ البحثَ على إثباتِ هذه الحالةِ سيكون معقَّدًا بالنِّسبةِ للمضرور[٢٧٠]؛ كون الأشياءِ المُتَّصلةِ تمثِّل نظامًا معقَّدًا يتطلَّب تدخُّلَ خبيرٍ. لكنَّ الصُّعوبةَ الكبرى تتعلَّق بتطبيقِ نظامِ المادة ١٢٤٢- ١ من القانون المدنيّ الفرنسيّ الجديدِ على الأشياءِ المُتَّصلة لا سيَّما مسألةُ التَّوافقِ بين السَّيطرة (الحراسة) والاستقلالِ الذاتيّ للأشياءِ المُتَّصلة، ووفقًا للمادة ١٢٤٢ الفقرة ١ الجديدة من القانونِ المدنيّ، لكي تكونَ مسؤولًا عن شيءٍ ما، يجبُ

---

(268) Art. 1243: «On est responsable de plein droit des dommages causés par le fait des choses corporelles que l'on a sous sa garde».

(269) J.-S. Borghetti, «L'accident généré par l'intelligence artificielle autonome», in Le droit civil à l'ère du numérique. Acte du colloque du Master 2 droit privé général et du Laboratoire de droit civil, 21 avril 2017, JCP G 2017, numéro spécial, décembre 2017, p. 26.

1- J.-S. Borghetti, «L'accident généré par l'intelligence artificielle autonome», in Le droit civil à l'ère du numérique. Acte du colloque du Master 2 droit privé général et du Laboratoire de droit civil, 21 avril 2017, JCP G 2017, numéro spécial, décembre 2017, p. 27

(ISSN: 2537- 0758)

أن تكونَ حارسًا عليه. وبالتَّالي فإنَّ الحراسةَ تشكِّل شرطًا أساسًا لتنفيذِ المسؤوليَّةِ عن حقيقةِ الأشياء. وقد حدَّد معاييرها الحُكمُ الشَّهيرُ الصَّادرُ عن الغرفِ المشتركةِ لمحكمةِ النَّقضِ الصَّادر في ٢ ديسمبر ١٩٤١ (حكم فرانك) الذي أرسى المبدأ التالي: الحارسُ هو من يملكُ استعمالَ الشَّيءِ وتوجيهه والسَّيطرةَ عليه.

الحراسةُ تعني: تمثيلَ المالكِ لحراسةِ الشَّيء. وفي هذا الشَّأن إنَّ حكمَ فرانك الصَّادرَ عن الغرفِ المشتركةِ يُخالف هذا المفهوم، من خلال منحِ الحارسِ ليس فقط سلطةً قانونيَّةً، بل سلطةً فعليَّة (المفهوم المادِّي)[٢٧١]. لكنَّ هذا الانفصالَ لم يكتملْ؛ لأنه- بعدَ حكمِ فرانك- أَدخلت السَّوابقُ القضائيَّة افتراضًا بسيطًا للحراسةِ على حسابِ المالك. ويجوزُ للأخيرِ أن يبرِّئ نفسَه بتقديمِ ما يُثبت نقل الحراسة. ومع ذلك، فإن تطبيقَ المبادئِ النَّاتجة عن حكمِ فرانك يطرحُ صعوباتٍ، في حالة الحراسةِ الجماعيَّة.

ب- صعوبةُ إثباتِ انحرافِ الشَّيء المتَّصل في ضوءِ المسؤوليَّةِ عن الأشياء:

إن الأشياء المُتَّصلة، بطبيعتها، من المرجَّح أن تؤدِّيَ إلى تعدُّدِ الحراسِ أو ما يسمَّى بالحراسةِ الجماعيَّة. كما أن معاييرَ الحراسةِ على النَّحو المحدَّدِ في حكمِ فرانك أيضًا قد تكونُ غير متوافقةٍ مع استقلاليَّةِ الأشياءِ المُتَّصلة.

بادئ ذي بَدءٍ فإن تطبيقَ معاييرِ الحراسةِ على الأشياءِ المُتَّصلة وفقًا لحكم فرانك، سالف الإشارة إليه، فالحراسةُ بالمعنى المقصودِ في المادة ١٣٨٤ والمادة ١٢٤٢ من القانونِ المدنيّ الفرنسيّ الجديد، هو من يملكُ توجيهَ الشَّيءِ واستعماله والسَّيطرة عليه، ويتطلَّبُ هذا المعيارُ الأخيرُ فيما يتعلَّق باستقلاليَّةِ الشَّيء المتَّصلِ رفضَ تحميلِ المدَّعى عليه المسؤوليَّةَ في الإجراءات؛ لأنه بعد مصادرةِ سيارتهِ نتيجةَ السَّرقة، وُجد أنه من المستحيلِ مراقبتُها والتَّحكمُ فيها.

---

[٢٧١] من ناحيةٍ أخرى، فقد نصَّت السَّوابقُ القضائيَّةُ بوضوحٍ في عديدٍ من الأحكام على أنَّ وضعَ الحارسِ لا يُمكن أن يتوافقَ مع وضعِ المرافق؛ لأنَّه يعملُ تحت أوامرِ وتعليماتِ صاحبِ العمل.

Cass. civ., 27 février 1929, DP 1929, 1, 129; Ass., Plén., 25 février 2000, n°97-17.378 97-20.152, Bull: 2000 A. P. N° 2 (arrêt Costedoat).

وعلى ذلك، قُضِي بحرمانِ صاحبِ السيارة من استخدامِها وتوجيهِها والسَّيطرة عليها، لم يعدْ يحتفظ بها، وبالتالي لم يعدْ يخضعُ لقيرينةِ المسؤوليَّةِ المنصوص عليها في الفقرة ١ من المادة ١٣٨٤ من القانون المدنيّ.

وفي الواقع، التحكُّم يعني "السَّيطرة على شيءٍ ما avoir la maîtrise de quelque chose"، "أو ممارسة السُّلطةِ على شيءٍ ما"[٢٧٢]. وفي سياقِ الأشياءِ المُتَّصلة، سيكونُ السُّؤالُ الرئيسُ هو معرفة مَن المسؤول عن التحكُّم في الجهاز. وهل من الممكنِ أيضًا ممارسةُ السَّيطرةِ على شيءٍ مستقلٍّ؟ وقد لا يكونُ للأشياءِ المُتَّصلةِ حارسٌ.

ووفقًا لجانِ سيباستيان بورغيتي: "الطَّريقةُ البسيطةُ للتغلُّب على هذه الصُّعوبةِ هي إما اعتبار أن مالك الشَّيءِ الذي يحرّكه الذَّكاءُ الاصطناعيُّ لا يُمكن أن يفقدَ الحراسةَ على الشَّيءِ إلا عن طريقِ نقلهِ إلى شخصٍ آخر، أو تكييف تعريفِ الحراسةِ واعتبار أنَّ الحارسَ على الشَّيءِ المتحرّك هو مَن يبادرُ إلى تشغيله، حتى لو فَقَد السَّيطرةَ عليه فيما بعدُ[٢٧٣].

وفي الحقيقة لن يكونَ الحلُّ الأول الذي اقترحَه هذا المؤلِّف ممكنًا، إذا قبِلْنا فكرةَ أنَّ استقلاليَّةَ الأشياءِ المُتَّصلة التي يمنحُها الذَّكاءُ الاصطناعيُّ تجعل مفهومَ الحراسةِ يختفي، وبهذا المنطق، فإن المالكَ الذي لا يكونُ حارسًا في المقامِ الأول، بسبب عدمِ وجودِ سيطرةٍ، لا يُمكنه نقلُ الحراسةِ التي لم تكنْ لديه من قبلُ. ويبدو أنَّ الحلَّ الثاني هو الأرجحُ.

وقد يكون الحلُّ الآخرُ هو اللُّجوءَ إلى التَّمييزِ بين الحراسةِ الهيكليَّة la garde de la structure والحراسة السلوكيَّة la garde du comportement؛ ممَّا يسمحُ

(272) Laura Jounda Sonkwa, Responsabilité civile du fait des objets connectés autonomes Master, Droit des assurances Formation en apprentissage RESPONSABILITE CIVILE DU FAIT DES OBJETS CONNECTES AUTONOMES Mémoire de recherche Par Sous la direction de Monsieur le professeur Louis Perdrix Année: 2018– 2019.

(273) J.-S. Borghetti, «L'accident généré par l'intelligence artificielle autonome», in Le droit civil à l'ère du numérique. Acte du colloque du Master 2 droit privé général et du Laboratoire de droit civil, 21 avril 2017, JCP G 2017, numéro spécial, décembre 2017, p. 26-30.

(ISSN: 2537- 0758)

للمضرورِ بتحميل الشَّركةِ المصنِّعةِ المسؤوليَّةَ على أساسِ المادة ١٢٤٢ من القانون المدنيّ الفرنسيّ، وذلك إذا كان الضَّررُ بسببِ عيبٍ داخليٍّ في الكائن، أو مسؤوليَّة المستخدم، إذا كان الضَّررُ بسببِ الاستخدامِ غير السَّليم للكائن.

وفي واقعِ الأمرِ ليس فقط أنه سيكونُ من الصَّعبِ تقديمُ الدَّليلِ في هاتين الحالتين، ولكن أيضًا التَّمييزُ بين حراسةِ الهيكل وحراسةِ السُّلوك هو موضوع عديدٍ من الشُّكوك الفقهيَّة.

وفي هذا الشَّأن يُمكننا القول بأن الشَّيءَ المتَّصلَ شيءٌ متفردٌ Une chose singulière حيث يثور عديدٌ من التَّساؤلاتِ التي قد يصعبُ تحديدُها، فإذا كان القانون المدنيُّ الفرنسيُّ ينصُّ في المادة ١٢٤٢ من القانون المدنيّ الفرنسيّ الجديدِ **(**بعد تعديلات عام ٢٠١٦**)** على أنَّ الشَّخصَ مسؤولٌ عن الضَّررِ النَّاجم عن أفعالهِ أو عن الأشخاصِ الذين يجب أن يتحمَّل المسؤوليَّةَ عنهم، ولكن أيضًا عن الأشياءِ التي تقعُ تحت حوزتهِ وحراستهِ. ونظرًا لأنَّ الشَّيءَ المتَّصلَ لا يتمتَّعُ بعد بحالةٍ مستقلةٍ، فمن غيرِ المتصوَّرِ تحميلُ الشَّيءِ نفسهِ مسؤوليَّةَ "فعلهِ الخاصّ" أو اعتباره "شخصًا" يجبُ على مستخدمهِ الإجابةُ عمَّا يحدثُ منه[٢٧٤].

فهل يُمكن مقارنةُ الشَّيء المتَّصل بشيءٍ في حوزتنا؟ للوهلةِ الأولى، يُمكن للمرءِ– في الواقع– أن يفترضَ أن مستخدمَ الشَّيءِ المتَّصل، مثل أيّ شيءٍ آخر، يُمكن أن يتحمَّل المسؤوليَّةَ في حالةِ وقوعِ كارثةٍ ناجمةٍ عن هذا الشَّيء.

وتكمُنُ المشكلة– حقًّا– في أن خصوصيَّة الشَّيءِ المتَّصلِ المزوَّد بأنظمةِ الذَّكاء الاصطناعيّ والتي تتمركزُ في استقلاليَّتهِ وذكائه الاصطناعيّ، فكيف يُمكننا إذن أن

---

[٢٧٤] قريبٌ من هذا المعنى راجع: فتيحة قندوز، الجوانبُ القانونيَّةُ لاستخدام الذَّكاء الاصطناعيّ، المجلة الجزائريَّة للحقوق والعلوم السياسيَّة، مج٩، ع١، المركز الجامعيُّ أحمد بن يحيى الونشريسي تيسمسيلت– معهد العلوم القانونيَّة والإداريَّة، ٢٠٢٤، ص١١٨٠– ١١٩٠، كريم علي سالم، الجوانبُ القانونيَّةُ للذَّكاء الاصطناعيّ، مجلة جيل الأبحاثِ القانونيَّةِ المعمَّقة، ع٥، مركز جيل البحث العلميّ ٢٠٢٢ ص٥٣– ٦٦، عماد عبد الرحيم الدحيات، نحو تنظيمِ قانونٍ للذَّكاءِ الاصطناعيّ في حياتنا: إشكاليَّة العلاقةِ بين البشرِ والآلة، مجلَّة الاجتهاد للدِّراساتِ القانونيَّةِ والاقتصادية، مج٨، ع٥ ٢٠١٩، ص١٤– ٣٥.

نتصوَّرَ أن مستخدمَ الشَّيءِ المتَّصل الذي حُرِم من قدرتهِ على التحكُّمِ والتَّوجيهِ–ولو جزئيًّا– يُمكن أن يكونَ مسؤولًا عن فشله؟ في هذه الفرضيَّة، سيكونُ من المناسبِ الإشارةِ إلى التَّمييزِ بين رعايةِ البنيةِ (الشَّيء الماديّ) ومراقبة السُلوك. وبالتَّالي، يتعيَّنُ علينا أن نناقشَ مسألة معرفةٍ من مصمِّم البرنامج، أو مطوِّر الخوارزميَّة، أو حتى المستخدم الذي كان من المفترضِ أن يتعلَّم منه الشَّيء الذي كان يتولَّى بالفعلِ مسؤوليَّةَ السُلوكِ وقتَ وقوعِ الكارثة.

لذلك نرى أنه إذا كانت نزاعاتُ المسؤوليَّةِ المتعلِّقةِ بالأشياءِ المُتَّصلة ستتوافقُ بأفضلَ ما يُمكن مع القانونِ العامِّ للمسؤوليَّة، فستكون النِّزاعاتُ طويلةً ومعقَّدةً، ما لم يتمَّ تحديدُ ضامنٍ للشَّيء مسبقًا، يكون مسؤولًا قانونًا عن الضَّررِ النَّاجمِ عنه، والمؤمِّن له من هذا الخطرِ.

ثانيا: تحديدُ الحارسِ في مواجهةِ اتِّصالِ الشَّيءِ الذَّكي:

La détermination du gardien face à la connectivité de l'objet:

نقصدُ باتِّصال الشيءِ في هذا الشَّأن قدرتَه على الارتباطِ بالشَّبكةِ وعلى وجهِ التَّحديدِ مسألة اتِّصالِ الشَّيءِ بالإنترنت. وفي الواقعِ، فإن اتِّصالَ الشَّيءِ بالإنترنتّ يعرِّضه لعديدٍ من المخاطر السيبرانيَّةِ، مثل: القرصنة. ويُمكن تسليطُ الضَّوءِ على فرضيَّتين: إما أن يقومَ طرفٌ ثالثٌ خبيثٌ باختراقِ الشَّيءِ المتَّصلِ؛ ليجعلَه أداةً للضَّرر (على سبيل المثال، غسالة أطباقٍ متَّصلةٌ؛ ممَّا قد يتسبَّب في تلفِ المياه)، أو أنَّ الشَّيءَ المتَّصلَ هو مجرَّد ناقلٍ غير مباشرٍ للضَّرر (القفل الإلكترونيُّ تمَّ اختراقُه من قِبل طرفٍ ثالثٍ؛ لارتكابِ السَّرقة).

وفي هاتين الحالتين، سيكون لدى المتسلِّل القدرةُ على استخدامِ الشَّيءِ وتوجيههِ والتحكُّم فيه، وهو ما يتوافقُ مع خصائصِ الحارسِ. ولذلك فإنَّ السُؤالَ الذي يطرحُ نفسَه هو ما يلي: في حالة الضَّرر النَّاجمِ عن شيءٍ متَّصلٍ تحت سيطرةِ القرصان، هل يُمكن أن تنجَحَ دعوى المضرورِ ضدَّ مالكِ الشَّيء– الحارسِ المفترضِ– على أساسِ المادة ١٢٤٢؟

فيما يتعلَّقُ بمالكِ الشَّيء، يبدو من التَّحليلِ السَّابق أنه سيكونُ من الصَّعبِ بالفعل تفعيلُ مسؤوليَّته؛ لأنه لا يملكُ القدرةَ على السَّيطرةِ على الشَّيء. وبالتالي، إذا

(ISSN: 2537- 0758)

كان الهجومُ الحاسوبيُّ الذي تمَّ تنفيذُه على الشَّيءِ المتَّصل لا يمنحُ المتسللَ السَّيطرةَ على سلوكهِ الخارجيّ فحسْب، بل أيضًا السَّيطرة على بنيةِ المنتج، فإن تنفيذَ المسؤوليَّةِ عن الأخيرِ سيكون أكثرَ فعاليَّةً من مسؤوليَّةِ المالك.

ومع ذلك، قد تُواجِهُ المضرورَ عقبةٌ تتمثَّل في التعرُّفِ على المتسلِّل. وهذا الأخيرُ مجهولٌ بشكلٍ عامّ. وفي هذا الشَّأن، يُمكننا النَّظرُ في تنفيذِ مسؤوليَّةِ الشَّركة المصنِّعة كحارسٍ للهيكل. لكن تنفيذَ مسؤوليَّةِ الشَّركة المصنِّعة لن يكون في صالحِ المضرورِ أيضًا بسببِ: "الحقيقة البسيطة المتمثِّلة في أنَّ الشَّركةَ المصنِّعة ضمِنَتْ– أثناءَ تصميمِ المنتجِ وكذلك أثناء التَّحديث– الامتثالَ للالتزاماتِ القانونيَّةِ المتعلِّقةِ بسلامةِ منتجهِ، وهذا سيكون كافيًا منطقيًّا لتبريرِ عدمِ إمكانيَّةِ التَّشكيكِ فيها"[٢٧٥]، وفي حالةِ عدمِ وجودِ تعويضٍ، يُمكن للمضرورِ أن يلجأَ إلى لجنةِ تعويضِ ضحايا الجرائم (CIVI) لكن الشُّروطَ الواجب توافرُها للحصولِ على التَّعويضِ قد لا تكونُ مستوفاة.

وفي الواقع تكمُنُ خصوصياتُ أضرارِ الأشياءِ المُتَّصلة في طبيعتِها الخاصَّة، مع صعوبةِ تحديدِ المسؤولِ عنها، بحيث يبدو من الصَّعبِ تطبيقُ القواعدِ العامَّةِ للمسؤوليَّةِ المدنيَّة وفقًا للنَّهجِ التَّقليديّ بصددها؛ كونه غيرَ مناسبٍ لأضرارِ الأشياءِ المُتَّصلة؛ لذلك يبدو من الضَّروريّ تكييفُ الإطارِ التَّنظيميّ، مع الأخذِ في الاعتبارِ هذه الخصوصيَّة التي يتَّصفُ بها الضَّررُ الذي تتسبَّبُ فيه الأشياءُ المُتَّصلةُ في ظلِّ اتِّصالها المباشرِ بشبكةِ الإنترنت.

ولقد ثبت من خلالِ ما سبق أن المضرورَ لن يستطيعَ الحصولَ على الجبرِ أو التَّعويضِ الفعَّال والكافي لأيّ سببٍ من الأسباب. وفي هذه الحالةِ، يُمكن اللُّجوءُ إلى نظامِ المسؤوليَّةِ الخاصَّةِ بالنِّسبة للمنتجاتِ المَعيبة، فغالبًا ما يتمُّ استبدالُ المسؤوليَّةِ المدنيَّةِ بموجبِ القانون العامِّ لصالحِ المسؤوليَّةِ الخاصَّة أو أنظمة التَّعويض. فلا يُمكن ربطُ معظمِ أنظمةِ المسؤوليَّةِ الخاصَّة بالمسؤوليَّةِ المدنيَّةِ التعاقديَّةِ أو غيرِ التعاقديَّة؛ وبهذا المعنى، فهي تنفصلُ عن المسؤوليَّةِ التعاقديَّةِ والمسؤوليَّةِ خارجَ نطاقِ العقد. وسيتمُّ تخصيصُ هذا الجزءِ لدراسةِ نظامٍ خاصٍّ للمسؤوليَّة: المسؤوليَّة عن المنتجاتِ المَعيبة، وها نحنُ أمامَ نظامِ المسؤوليَّةِ عن المنتجاتِ المعيبة.

(275) Lamy Droit de la responsabilité, n°350-55.

المطلب الثاني
النِّظامُ الخاصُّ للمسؤوليَّةِ عن المُنتجاتِ المَعيبة
Le régime de responsabilité du fait des produits défectueux

تمهيدٌ وتقسيمٌ:

يأتي من توجيهِ المجلسِ EEC/٣٧٤/٨٥ المؤرَّخ ٢٥ يوليو ١٩٨٥ المتعلِّق بتقريبِ الأحكامِ التَّشريعيَّةِ والتنظيميَّةِ والإداريَّةِ للدُّولِ الأعضاءِ فيما يتعلَّقُ بالمسؤوليَّةِ عن المنتجاتِ المعيبةِ، وقد تمَّ أخذُ التَّوجيهِ متأخِّرًا إلى القانونِ الفرنسيِّ، من خلال القانون رقم ٩٨-٣٨٩ المؤرَّخ في ١٩ مايو ١٩٩٨ المتعلِّق بالمسؤوليَّةِ عن المنتجاتِ المَعيبة، والذي أنشأ الموادَّ من ١٣٨٦-١ إلى ١٣٨٦-١٨، والآن من ١٢٤٥ إلى ١٢٤٥-١٧ من القانونِ المدنيِّ الفرنسيِّ[٢٧٦]. ويهدف هذا التَّوجيهُ إلى إرساءِ مبدأ المسؤوليَّةِ الموضوعيَّةِ للمنتج، والتي لا تعتمدُ على الخطأ، بل على الطَّبيعةِ المعيبةِ لمنتجاته. والغرضُ من ذلك هو تطبيقُه تلقائيًّا عندما يتمُّ رفعُ دعوى المسؤوليَّةِ ضدَّ المنتجِ على أساسِ عيبٍ في المنتج[٢٧٧]، ووفقًا للنَّهجِ السَّابق فإنه يمحو أيَّ تمييزٍ يتعلَّقُ بالطَّبيعةِ التعاقديَّةِ أو غير التعاقديَّة. ومن ثم، وفقًا للمادة ١٢٤٥ من القانون المدنيِّ الفرنسيِّ، "يكون المنتجُ مسؤولًا عن الضَّررِ النَّاجمِ عن عيبٍ في منتجه، سواءٌ كان مرتبطًا بعقدٍ مع المضرورِ أم لا". وهو ما يُسمَّى بنظامِ المسؤوليَّةِ المستحقَّة.

وبالتالي، فإن المنتجاتِ المعيبةَ تنطبقُ على كلٍّ من المسائلِ التعاقديَّةِ أو غيرها، بشرطِ وجودِ ضررٍ[٢٧٨]، ومنتجٍ، وعيبٍ في السلامة[٢٧٩]، وطرح المنتجِ للتَّداول

---

(276) (Cass. civ. 1ère, 17 janvier 1995, Bull. civ., I. n°43, p.29; 3 mars 1998, J.C.P., 1998, II, 10049, rapport P. SARGOS– D. aff., 1998, n°113, p.664.

(277) Civ 1ère, 17 mars 2016, n°13-18876; 11 juillet 2018, n°17-20.15.

(٢٧٨) وفقًا للمادة ١٢٤٥-١ من القانونِ المدنيِّ الفرنسيِّ، تنطبق المسؤوليَّةُ عن المنتجاتِ المعيبةِ على التَّعويضِ عن الأضرارِ النَّاجمةِ عن الإصابةِ الشخصيَّة. وينطبقُ أيضًا على التَّعويضِ عن الأضرارِ التي تزيدُ قيمتُها عن ٥٠٠ يورو، الناتجة عن الأضرارِ التي لحقتْ بالممتلكاتِ المستخدمةِ لأغراضٍ مِهنيَّة.

(CJUE 4 juin 2009, moteurs Leroy Somer, aff. C 285/ 08, D. 2009. 1731, et les obs., note J.-S. Borghetti) ou privés autre que le produit défectueux lui-même (Civ. 1ère, 9 juillet 2003, n° 00 21.163 P: RCA 2003, n° 268)

(ISSN: 2537- 0758)

(المواد ١٢٤٥-١، ١٢٤٥-٢، ١٢٤٥-٣ و١٢٤٥-٤ الفقرة ١) من القانونِ المدنيّ الفرنسيّ.

ويكونُ أمامَ الشَّخصِ المسؤولِ وسائلُ دفاعٍ محدودةٌ للدِّفاع عن نفسه، بحيث يُمكنه إما إثباتُ عدمِ استيفاءِ الشُّروطِ الإيجابيَّةِ لتطبيق النِّظامِ أو إثارةُ أسبابٍ قانونيَّةٍ للإعفاء: القوَّة القاهرةُ أو خطأُ المضرورِ الذي يُمثِّل خصائصَ القوَّة القاهرة، وخطر التطوُّرِ حيث تنصُّ المادة ١٢٤٥-١٠ (٤) من القانونِ المدنيّ الفرنسيّ على أنه للمنتجِ الحقُّ في إعفاءِ نفسهِ من مسؤوليَّتهِ إذا كانت حالةُ المعرفةِ العلميَّةِ والتقنيَّة- وقت طرحِ المنتجِ للتَّداول- لا تسمحُ باكتشافِ وجودِ العيب[٢٨٠].

ويعدُّ نظامُ المسؤوليَّةِ عن المنتجاتِ المعيبة، في الوضعِ الحاليّ للقانون، هو الأكثرَ ملاءمةً لإصلاحِ الأضرارِ النَّاجمةِ عن الأشياءِ المُتَّصلةِ، وإن كان يحتاجُ لبعضِ التَّحسين. وجديرٌ بالذِّكر يتماشى قرار الاتِّحادِ الأوروبيّ الصَّادر في ١٦ فبراير ٢٠١٧ مع هذا المنطق، حيث يرى أنَّ المسؤوليَّة عن المنتجاتِ المعيبةِ يُمكن أن تنطبقَ على الأضرارِ التي يسبّبها الروبوت أو AI95. ولذلك سيكونُ من المثيرِ للاهتمامِ عرضُ السِّماتِ المميّزة لهذا النِّظامِ التي تُسهّل تنفيذَه من حيث إصلاحُ الضَّررِ النَّاجمِ عن الأشياءِ المُتَّصلةِ، وهذا ما سيُوضَّح في الفرعِ الأوَّل، غير أنَّ

---

[٢٧٩] وفقًا للمادة ١٢٤٥-٣، يكون المنتجُ معيبًا عندما لا يوفِّر السَّلامةَ التي يُمكن توقُّعُها بشكلٍ مشروعٍ. وعند تقييمِ ذلك، يجبُ أن تؤخذَ جميعُ الظُّروفِ في الاعتبار، ولا سيَّما عرضُ المنتجِ، والاستخدام المتوقَّع منه بشكلٍ معقولٍ ووقت طرحهِ للتَّداول. وفي هذا الصَّدد، من الضَّروريّ التَّمييزُ بين انعدامِ الأمنِ وعدم المطابقةِ والعيوب الخفيَّة. والواقعُ أن عدمَ المطابقةِ يعتمدُ على التَّعريفِ التعاقديّ للشَّيءِ أو استخدامه. في حين أنَّ انعدامَ الأمن هو مفهومٌ موضوعيٌّ. وأما العيبُ الخفيُّ فيقدر بالنِّسبةِ إلى منفعةِ المنتج، ويحلّل بالنِّسبةِ إلى قدرةِ الشَّيءِ على أداءِ غرضه. ومع ذلك، فإن انعدامَ الأمنِ لا يعني حدوثَ تغييرٍ أو نقصٍ ماديٍّ في الشَّيء الذي قد يكونُ في حالةٍ ممتازةٍ. يتعلَّقُ الأمرُ فقط بخرقٍ أمنيٍّ.

Cf. G. Viney, P. Jourdain et S. Carval, Traité de droit civil. Les régimes spéciaux et l'assurance de responsabilité, J. Ghestin (sous la dir.), LGDJ, 4e édition, 2017, p. 35.

[280] Civ 1ère, 20 septembre 2017, n°16 19643.

دعوى المسؤوليَّةِ المرفوعةِ على هذا الأساسِ قد تواجه بعض الصُّعوباتِ، وهو ما سنوضِّحه في الفرعِ الثاني، مع الإشارةِ إلى جانبٍ من الحلولِ لإصلاحِ الأضرارِ النَّاجمةِ عن الذَّكاء الاصطناعيّ.

الفرع الأول: التَّوافقُ بين نظامِ المسؤوليَّةِ عن المنتجاتِ المعيبةِ والتَّعويض عن الضَّررِ النَّاتجِ عن الأشياءِ المُتَّصلة.

الفرع الثاني: الصُّعوباتُ المتعلقةُ بتنفيذِ المسؤوليَّةِ عن المنتجاتِ المعيبةِ فيما يتعلَّق بالأشياءِ المُتَّصلة.

الفرع الثالث: الحلولُ المقدَّمة لإصلاحِ الأضرارِ النَّاجمةِ عن أنظمةِ الذَّكاء الاصطناعيّ.

الفرع الأول
التَّوافقُ بين نظامِ المسؤوليَّةِ عن المنتجاتِ المعيبةِ والتَّعويضِ عن الضَّررِ النَّاتجِ عن الأشياءِ المُتَّصلة

يبرزُ نظامُ المسؤوليَّةِ عن المنتجاتِ المعيبةِ عن الأنظمةِ الأخرى في نقطتين أساسيتين: نطاقُ تطبيقِه، وسهولةُ تحديدِ الشَّخصِ المسؤولِ.

أولًا: نطاقُ التَّطبيقِ:

المسؤوليَّةُ عن عدمِ الخطأِ مفيدةٌ لجميعِ المضرورين، مثل المسؤوليَّةِ عن الأشياءِ، فإن المسؤوليَّةَ عن المنتجاتِ المعيبةِ هي مسؤوليَّةٌ عن عدمِ الخطأ. يجبُ على مقدِّم الطَّلبِ تقديمُ دليلٍ فقط على عيبِ سلامةِ المنتجِ والضَّررِ والعلاقة السببيَّة.

وفيما يتعلَّق بعيبِ السَّلامةِ على وجهِ التَّحديد، فهو موضوعُ تقييمٍ واسع النِّطاقِ من قبلِ القضاة. وهكذا، في المسائلِ الطبيَّة، أدانت محكمةُ النَّقض– في سياقِ قضيَّةٍ تتعلَّق باستخدامِ منتجاتِ منعِ الحملِ عن طريقِ الفم– الشَّركةَ المصنِّعةَ للمنتجِ المذكورِ على أساسِ خطورةِ المخاطرِ المتكبَّدة وتكرار حدوثِها عندما تتجاوزُ هذه المخاطرُ الفوائدَ المتوقَّعةَ من قِبل المستخدم[٢٨١]. ومن ثم يُمكن أخذُ **خطورةِ المخاطرِ المتكبَّدة وتكرار حدوثِها في الاعتبارِ** عند توصيفِ عيبِ المنتجِ إذا تجاوزت الفوائدَ

(281) Décision rendue au sujet des effets nocifs d'un produits contraceptif oral: Civ. 1ère, 26 septembre 2018, n° 17- 21.271 P: D. 2019. 61.

(ISSN: 2537- 0758)

المتوقَّعةَ من قِبل المستخدم. وبالتالي، ونظرًا لخطورةِ بعضِ المخاطرِ النَّاجمةِ عن استخدامِ بعضِ الأشياءِ المُتَّصلة، مثال ذلك: التعرُّض للموجاتِ الكهرومغناطيسيَّة المنبعثةِ من الأجسامِ المُتَّصلةِ يُمكن أن يكونَ مَصدرًا للسَّرطان، يُمكن توسيعُ نطاقِ هذه السَّوابقِ القضائيَّةِ لتشملَ هذا المجال. علاوةً على ذلك، تمكَّنت السَّوابقُ القضائيَّةُ أيضًا من إثباتِ وجودِ خللٍ أمنيٍّ في ظلِّ نقصِ المعلومات.

وبالتَّالي، يُمكن للمضرورين من الشَّيءِ المتَّصلِ الاعتمادُ على هذه السَّوابقِ القضائيَّة، في حالةِ نقصِ المعلوماتِ من الشَّركةِ المصنِّعة، للحصولِ على تعويضٍ عن الأضرار التي لحقتْ بهم. بالإضافةِ إلى ذلك، يُظهر قضاةُ الموضوعِ أحيانًا مرونةً عندما يتعلَّق الأمرُ بتحديدِ العلاقةِ السببيَّة بين عيبِ المنتجِ والضَّرر، طالما كان المدَّعي قادرًا على تقديمِ دليلٍ على العيبِ المتعلِّق بالسَّلامة، ونشيرُ في هذا الصَّددِ إلى قضيَّة TGI Aix-en Provence، حيث تمكَّن قضاةُ الموضوعِ من تحميلِ المنتجِ المسؤوليَّة، على الرَّغم من عدمِ وجودِ علاقةٍ سببيَّةٍ بين عيبِ المنتجِ والضَّرر، حيث تمكَّن المدَّعي من إثباتِ أن المنتجَ لا يوفِّر ضمانًا عاديًّا(٢٨٢).

وبنفسِ المنطقِ، تمكَّنت محكمةُ العدلِ الأوروبيَّة من التحقُّق من المنطقِ الذي يُمكن بموجبهِ للقضاةِ الاعتمادُ على افتراضاتٍ جادَّةٍ ودقيقةٍ ومتَّسقةٍ لتقييمِ وجودِ علاقةٍ سببيَّة، وذلك على الرَّغمِ من أنه منذ هذا الحكمِ الصَّادرِ عن محكمةِ العدل الأوروبيَّة. فإن استخدامَ هذه الافتراضاتِ يُمكن أن يكونَ مفيدًا لحقيقةِ الأشياءِ المُتَّصلة إلى الحدِّ الذي تكونُ فيه السببيَّةُ أيضًا مسألةً حساسةً.

والسُّؤال الذي يطرحُ نفسَه في هذا الشَّأن: هل يُمكن اعتبارُ" إساءة استخدامِ المنتجِ عيبًا في سلامةِ المنتجِ ذاته، بحيث يقعُ على عاتق المصممِ وضع خطأِ المضرورِ في اعتبارِه عند تصميمِ الجهازِ المتَّصل؟

في واقعِ الأمرِ أشارت المادةُ ٣ فقرة ١٣ من لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ إلى الأخذِ بفكرةِ "إساءة الاستخدامِ المتوقَّعة بشكلٍ معقولٍ" فقط، والتي يلتزمُ المصممُ بمراعاتها عند تصميمِ الشَّيءِ المتَّصل، ويقصدُ بها استخدامُ نظامِ الذَّكاءِ الاصطناعيّ بطريقةٍ لا تتَّفق مع الغرضِ المقصودِ منه، ولكنها قد تنتجُ عن

(282) TGI Aix-en Provence, 2 oct. 2001: D. 2001. IR 3092.

سلوكٍ بشريٍّ متوقَّعٍ بشكلٍ معقولٍ أو تفاعلٍ مع أنظمةِ أخرى، بما في ذلك أنظمةُ الذَّكاءِ الاصطناعيّ الأخرى(٢٨٣).

علاوة على ذلك، فإنَّ المسؤوليَّةَ عن المنتجاتِ المعيبةِ أكثر فائدةً للمضرورِ من المسؤوليَّةِ عن الأشياء، بقدرِ ما يُمكن تنفيذُها ضمن إطارٍ تعاقديٍّ. وهذا يُرسي نوعًا من المساواةِ بين المضرورين الذين يحقُّ لهم جميعًا الاتِّصالُ بالمنتجِ مباشرةً للحصولِ على التَّعويض، وهذا الأخيرُ يُمكن التعرُّفُ عليه بسهولةٍ أكبر.

ثانيا: سهولةُ التعرفِ على الشَّخصِ المسؤولِ:

في إطارِ المسؤوليَّةِ عن الأشياء، لا يجوزُ للمضرورِ أن يتَّصلَ مباشرةً بمنتجِ الشَّيءِ الذي كان من شأنِ فعله أن يسبِّب له ضررًا، إلا إذا أثبت وجودَ حراسةٍ للشَّيء. وهذا أمرٌ غير مرغوبٍ، خاصَّةً وأن السَّوابقَ القضائيَّةَ بشأنِ هذا الموضوعِ غير مستقرَّةٍ. ولكنْ مع المسؤوليَّةِ عن المنتجاتِ المعيبة، يصبحُ تحديدُ الشَّخصِ المسؤول أسهل بالنِّسبةِ للمضرور. وتحدِّد المادَّتان ١٢٤٥-٥ و١٢٤٥-٦ من القانون المدنيّ الفرنسيّ بوضوحٍ الأشخاص الذين يجبُ أن يتحمَّلوا المسؤوليَّةَ التي حدَّدتها الهيئةُ التنظيميَّةُ الأوروبيَّةُ، وهم: مصنِّعو المنتجاتِ الصناعيَّة سواءٌ كانت مدمجةً في منتجٍ آخرَ أم لا، والمهنيُّون الذين يستخرجون الموادَّ الخامَّ، والمنظَّمات التي تزيلُ المنتج، والشَّخص الذي يضعُ اسمَه أو علامتَه التجاريَّةَ أو علامةً مميَّزةً أخرى على المنتج، ومستورد المنتجِ إلى الجماعةِ الأوروبيَّةِ بهدفِ توزيعه. ومع ذلك، لا يمكنُ اعتبارُ الأشخاصِ التَّاليين منتجين، ووفقًا للمادَّة ١٢٤٥-٦، في حالةِ عدم تحديدِ هويَّةِ المنتجين، سيتمُّ اعتبارُ أشخاصٍ آخرين، مثل البائعِ أو المؤجِّر، مسؤولين. ومع ذلك، فإنَّ اتِّخاذَ إجراءٍ ضدَّ هذه الأخيرةِ يخضعُ لإشعار مسبقٍ باسم المنتجِ أو المورِّد. وفي حالةِ عدم الردِّ لمدة ٣ أشهرٍ، قد يتحمَّل المضرورُ المسؤوليَّة.

وفي الواقع، يُعطي القانونُ لمفهومِ "المنتج" تعريفًا واسعًا؛ لأنه يُمكن أيضًا أن يكونَ هو صانعَ المنتجِ النهائيّ أو جزءٍ مكوّن منه، أو منتج مادَّة خام، أو الشَّخص

(283) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" Art. (13) " reasonably foreseeable misuse' means the use of an AI system in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behaviour or interaction with other systems, including other AI systems;

(ISSN: 2537- 0758)

الذي يضعُ علامتَه التجاريَّة، وحتى في حالةِ عدم التَّحديدِ يُمكن أن يكونَ "المنتج" البائع أو المورد للمنتجِ المعيب. ويتطلَّب تعويضُ المضرورِ أن يثبتَ الطَّبيعةَ المعيبةَ للمنتج، أي عدم قدرتهِ على توفيرِ السَّلامةِ التي يمكن توقُّعها بشكلٍ مشروعٍ.

وتتضمَّن سلسلةُ قيمة **الذَّكاء الاصطناعي** the AI value chain عديدًا من الأطرافِ التي تتحمَّل مسؤولياتٍ متعدِّدةً على مختلفِ الأصعدة. من **التَّصميمِ** إلى **التَّسويق**، مرورًا بـ **التَّوزيع** و**الاستعمال**، يتحمَّل كلُّ طرفٍ مسؤولياتٍ قانونيَّةً وأخلاقيَّة لضمانِ سلامةِ الأنظمةِ الذكيَّة وحمايتها.

وفي هذا الشَّأن تنصُّ المادة ٢٥ من لائحةِ الاتِّحاد الأوروبيّ على المسؤوليَّاتِ على طولِ سلسلةِ قيمةِ الذَّكاء الاصطناعيّ[٢٨٤]، حيث يعدُّ أيُّ موزِّعٍ أو مستوردٍ أو

(284) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence" article 25, Responsibilities along the AI value chain

1. Any distributor, importer, deployer or other third-party shall be considered to be a provider of a high-risk AI system for the purposes of this Regulation and shall be subject to the obligations of the provider under Article 16, in any of the following circumstances:

(a) they put their name or trademark on a high-risk AI system already placed on the market or put into service, without prejudice to contractual arrangements stipulating that the obligations are otherwise allocated؛

(b) they make a substantial modification to a high-risk AI system that has already been placed on the market or has already been put into service in such a way that it remains a high-risk AI system pursuant to Article 6؛

(c) they modify the intended purpose of an AI system, including a general-purpose AI system, which has not been classified as high-risk and has already been placed on the market or put into service in such a way that the AI system concerned becomes a high-risk AI system in accordance with Article 6.

2. Where the circumstances referred to in paragraph 1 occur, the provider that initially placed the AI system on the market or put it into service shall no longer be considered to be a provider of that specific AI system for the purposes of this Regulation. That initial provider shall closely cooperate with new providers and shall make available the necessary information and provide the reasonably expected technical access and other assistance that are required for the fulfilment of the obligations set out in this Regulation, in particular regarding the compliance with the

ناشرٍ أو طرفٍ ثالثٍ آخر مقدمًا لنظامِ الذَّكاءِ الاصطناعيّ عالي الخطورةِ، ويخضع لالتزاماتِ المزوّد في أيٍّ من الحالات

التَّالية: (أ) وضع اسمهِ أو علامتهِ التجاريَّة على نظامِ ذكاءٍ اصطناعيٍّ عالي المخاطر تمَّ طرحُه بالفعلِ في السُّوق أو تمَّ وضعُه في الخدمة، دون الإخلالِ بالتَّرتيباتِ التعاقديَّة التي تنصُّ على تخصيصِ الالتزاماتِ بطريقةٍ أخرى؛ (ب) إجراء تعديلٍ جوهريٍّ على نظامِ ذكاءٍ اصطناعيٍّ عالي المخاطر تمَّ طرحُه بالفعلِ في السُّوق أو تمَّ وضعُه بالفعلِ في الخدمةِ بطريقةٍ تجعله يظلُّ نظامَ ذكاءٍ اصطناعيٍّ عالي المخاطر. (ج) تعديل الغرضِ المقصودِ من نظام الذَّكاءِ الاصطناعيّ، بما في ذلك نظام الذَّكاءِ الاصطناعيّ للأغراضِ العامَّة، الذي لم يتمَّ تصنيفُه على أنه عالي الخطورة، وتمَّ طرحُه بالفعلِ في السُّوق أو وضعه في الخدمةِ بطريقةٍ تجعل نظامَ الذَّكاءِ الاصطناعيّ المعنيّ نظامَ ذكاءٍ اصطناعيٍّ عالي الخطورة؛ (د) في حالةِ حدوثِ الظُّروف المشارِ إليها بند رقم ١، لن يُعتبرَ المزود الذي طرح نظامَ الذَّكاءِ الاصطناعيّ في السُّوق أو وضعه في الخدمةِ في البدايةِ مزودًا لنظامِ الذَّكاءِ الاصطناعيّ. حيث يجبُ على المزود الأوَّلِ التَّعاونُ بشكلٍ وثيقٍ مع المزوّدين الجُدُد، ويجبُ أن يوفِّر المعلوماتِ اللازمةَ ويوفِّر الوصولَ الفنيَّ المتوقَّع بشكلٍ معقولٍ والمساعدات الأخرى المطلوبة للوفاءِ بالالتزاماتِ المنصوصِ عليها، وخاصَّةً فيما يتعلَّق بالامتثالِ لتقييمِ المطابقةِ لأنظمةِ الذَّكاء الاصطناعيّ عالية الخطورة؛ (هـ) في

---

conformity assessment of high-risk AI systems. This paragraph shall not apply in cases where the initial provider has clearly specified that its AI system is not to be changed into a high-risk AI system and therefore does not fall under the obligation to hand over the documentation.

3. In the case of high-risk AI systems that are safety components of products covered by the Union harmonisation legislation listed in Section A of Annex I, the product manufacturer shall be considered to be the provider of the high-risk AI system, and shall be subject to the obligations under Article 16 under either of the following circumstances:

(a) the high-risk AI system is placed on the market together with the product under the name or trademark of the product manufacturer؛

(b) the high-risk AI system is put into service under the name or trademark of the product manufacturer after the product has been placed on the market.

(ISSN: 2537- 0758)

حالة أنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر التي تعدُّ مكوِّنات أمانٍ للمنتجات، يُعتبرُ مصنعُ المنتجِ هو مقدِّم نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر، ويخضع للمسؤوليَّةِ في أيّ من الظُّروفِ التَّالية: طرح نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر في السُّوق مع المنتجِ تحت اسمٍ أو علامةٍ تجاريَّةٍ لمصنعِ المنتجِ؛ أو وضع نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ في الخدمةِ تحت اسم أو علامة تجاريَّةٍ لمصنعِ المنتجِ بعد طرحِ المنتجِ في السُّوق. (و) يجبُ على مزوِّد نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر والطَّرف الثالث الذي يزوِّد نظامَ الذَّكاءِ الاصطناعيّ أو الأدوات أو الخدمات أو المكوِّنات أو العمليَّات المستخدمة أو المدمجة في نظامِ الذَّكاء الاصطناعيّ عالي المخاطر، بموجب اتفاقيَّةٍ مكتوبةٍ، تحديد المعلوماتِ والقدراتِ والوصول الفني والمساعدة الأخرى اللَّازمة بناءً على أحدثِ التِّقنيَّاتِ المعترفِ بها عمومًا، من أجلِ تمكينِ مزوِّد نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ من الامتثالِ الكامل للالتزاماتِ المنصوصِ عليها في هذه اللَّائحة.

وتعدُّ هذه الأحكامُ المتعلِّقة بتحديدِ المسؤولين ذات أهميَّةٍ فيما يتعلَّقُ بالأشياءِ المُتَّصلة، بقدرِ ما تشملُ هذه الأخيرة عديدًا من المشاركين في سلسلة الإنتاج: المهندس الفني، ومطوِّر البرمجيات، والشَّركة المصنعة، والبائع، وما إلى ذلك. وهكذا، فبدلًا من المطالبةِ بالمسؤوليَّةِ الخاصَّة لحلقة في السِّلسلة، يُمكن للمضرورِ أن يكتفيَ بالرُّجوعِ إلى الشَّخصِ الذي وضع علامتَه التجاريَّةَ أو علامتَه المميّزة على المنتج، أو إلى البائعِ على سبيلِ المثال (في حالةِ عدم قيامِ المنتجِ بذلك). يمكن التعرُّف عليها). وهذا الحلُّ مفيدٌ لأنه يمحو كلَّ الشُّكوكِ الفقهيَّة المتعلِّقة بتعيين حارسِ الهيكلِ من حيث المسؤوليَّة عن الوقائع. كما أنَّه إذا كان الضَّررُ ناجمًا عن نظامِ الذَّكاءِ الاصطناعيّ الذي صنعه مبرمج البرمجيات، فإن الأخيرَ يكونُ مسؤولًا بالتَّضامنِ والتَّكافل مع المنتج.

ووفقًا للمادة ١٢٤٥-٧ من القانونِ المدنيّ الفرنسيّ، والتي تنصُّ على أنه "في حالةِ الضَّررِ النَّاجم عن عيبٍ منتجٍ مدمجٍ في منتجٍ آخر، يكون منتجُ الجزءِ المكون والشَّخص الذي قام بالدَّمجِ مسؤولين بالتَّضامن"[٢٨٥]؛ بحيث يجبُ على المنتجِ النهائيّ أن يطالبَ بالمسؤوليَّةِ على أساسِ هذه المادَّة. وهذا يقودُ Bensamoun

(285) Article 1245-7: «En cas de dommage causé par le défaut d'un produit incorporé dans un autre, le producteur de lapartie composante et celui qui a réalisé l'incorporation sont s olidairement responsables».

وLoiseau إلى القولِ "إن المفهومَ الواسعَ للمنتج– سواءٌ كان صانعَ المنتجِ النهائيّ أو صانعَ الجزءِ المكون– والمسؤوليَّة المشتركة للشَّركةِ المصنعة للجزءِ المكون والشَّخص الذي يقومُ بدمجهِ في المنتجِ يجعلهم يخضعون للمسؤوليَّةِ دون الحاجةِ إلى قواعدَ أخرى"(٢٨٦).

ولكن على الرَّغمِ من هذه المزايا، فإن نظامَ المسؤوليَّةِ عن المنتجاتِ المعيبةِ يحتوي على بعضِ الخصائصِ التي تجعلُ من الصَّعبِ تنفيذه في بعضِ الحالات.

الفرع الثاني
الصُّعوباتُ المتعلقةُ بتنفيذِ المسؤوليَّة
عن المنتجاتِ المعيبةِ فيما يتعلَّقُ بالأشياءِ المُتَّصلة

نظرًا لخصائصَ معيَّنةٍ لنظام المسؤوليَّةِ عن المنتجاتِ المعيبة، فإنَّ تطبيقَه لا يوفِّر دائمًا حماية للمضرورين من الأشياءِ المُتَّصلة، والصُّعوبات التي يُمكن أن تنجمَ عن ذلك.

أولًا: تقديرُ مفهومِ المنتجِ
l'appréciation de la notion de produit

مفهوم المنتجِ المطبَّق على الأشياءِ المُتَّصلةِ بموجبِ التَّوجيهِ الصَّادر في ٢٥ يوليو ١٩٨٥ كما تمَّ أخذُه إلى القانونِ الفرنسيّ، تشكِّل أيُّ ملكيَّةٍ منقولةٍ منتجًا، بما في ذلك منتجاتُ التُّربةِ والماشية والصيد وصيد الأسماك بما في ذلك الكهرباءُ. وفي سياقِ الكائناتِ المُتَّصلةِ المستقلة، يطرحُ السُّؤال (كما هو الحالُ في مسائلِ المسؤوليَّةِ عن الأشياء) حول ما إذا كان من الضَّروريّ مراعاة الدَّعمِ الماديّ أو نظام الذَّكاءِ الاصطناعيّ المدمج في الأشياءِ عند تقييمِ مفهومِ المنتج.

وفيما يتعلَّقُ بالمسؤوليَّةِ عن المنتجاتِ المعيبة، فقد أثيرَ بالفعلِ سؤالٌ حولَ ما إذا كان يُمكن اعتبارُ البرمجياتِ منتجًا. يبدو أنَّ النِّقاشَ حول هذه النُّقطةِ قد تمَّ استبعادُه

(286) «la conception large du producteur– qu'il s'agisse du fabricant du produit fini ou du fabricant d'une partie composante– et la responsabilité solidaire du fabricant de la partie composante et de celui qui en réalise l'intégration dans le produit pourvoient au traitement de la responsabilité sans qu'il soit besoin d'autres règles»
A. Bensamoun et G. Loiseau, «La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité»https://www.slideshare.net/slideshow/responsabilit-civile-du-fait-des-objets-connectes-autonomes/234291821 #47

(ISSN: 2537- 0758)

منذ صدورِ الردِّ الوزاريِّ بعد وقتٍ قصيرٍ من التَّصويتِ على قانونِ تحويلِ التَّوجيهِ إلى القانونِ الفرنسيِّ. اعتبر هذا الرد أن التَّوجيهَ الصَّادر في ٢٥ يوليو ١٩٨٥ "يهدفُ إلى أن يشملَ الفئةَ القانونيَّةَ الكاملة للأثاثِ الإلكترونيِّ الذي تنتمي إليه البرامج"(٢٨٧). وإذا كان لا بدَّ من اعتبارِ حقيقةِ نظامِ الذَّكاءِ الاصطناعيِّ مصدرًا للضَّرر، فقد يكونُ هذا الحلُّ ممكنًا. ولكن، كما هو الحالُ في مسائلِ المسؤوليَّةِ عن القيامِ بالأشياء، يُمكننا التمسُّك بالأشياءِ الماديَّة التي توفِّر الدَّعمَ اللَّازم للذَّكاءِ الاصطناعيِّ أو التي ينشر من خلالها تأثيراته، والتي تشكِّل من حيث المبدأُ منتجاتٍ بالمعنى المقصودِ في المادَّة الجديدةِ ١٢٤٥-٢(٢٨٨). ويثورُ التَّساؤلُ عما إذا كانت الأشياءُ المُتَّصلةُ لا تندرجُ ضِمن فئةِ الخدماتِ أكثر من المنتجات، الأمرُ الذي من شأنه أن يستبعدَ تطبيقَ المسؤوليَّةِ عن المنتجاتِ المعيبة(٢٨٩). فعلى سبيلِ المثال، يُمكننا أن نذكرَ روبوتات المساعدةِ الطبيَّة التي تقدِّم خدماتٍ تتعلَّق بشكلٍ خاصٍّ بمساعدة كبار السنِّ أو الأشخاص ذوي الإعاقة. وفي هذه الحالة، يُمكن استبعادُ المسؤوليَّةِ عن المنتجاتِ المَعيبة؛ لأنها تنطبقُ فقط على المنتجات. وعلى ذلك فإنه في مجالِ الأشياءِ المُتَّصلة، قد يكون تطبيقُ نظامِ المسؤوليَّةِ صعبًا في بعضِ الأحيان. أولًا؛ لأنه من النَّاحيةِ العمليَّة، قد لا تنجمُ الخسارةُ عن الشَّيءِ نفسه كما سلف القول، بل عن الخدمةِ التي يقدِّمها هذا الشَّيء (استخدام نظامِ بياناتٍ غير آمنٍ، على سبيلِ المثال).

بينما يرى البعضُ أن منتجَ الجسمِ يتمُّ شراؤه دائمًا مقابلَ خدمةٍ يقدِّمها. حتى لو لم يتمَّ قبولُ أهليَّةِ المنتج، ويُمكننا دائمًا الرُّجوع إلى المادة L. 421-3 من قانونِ المستهلكِ التي تجعلُ من الممكنِ التَّشكيك في مسؤوليَّةِ المحترفِ عندما لا يتمُّ تقديمُ المنتجاتِ والخدماتِ التي يقترحها(٢٩٠).

(287) Rép. min. à QE N°15677, JOAN Q. 24 août 1998, p. 4728 in Le Lamy Droit de la responsabilité, 350-370

(288) J.-S. Borghetti, «L'accident généré par l'intelligence artificielle autonome», p. 27.

(289) En effet, depuis un arrêt du 12 juillet 2012 la Cour de cassation exclut les services du domaine de la responsabilité du fait des produits défectueux: Civ. 1ère, 12 juillet 2012, n°11-17510. Cf. N. Martial-Braz, «Objets connectés et responsabilité», Dalloz IP/IT 2016 p.399.

(290) Laura Jounda Sonkwa, Responsabilité civile du fait des objets connectés autonomes Master, Droit des assurances Formation en apprentissage RESPONSABILITE CIVILE DU FAIT DES OBJETS CONNECTES

ويُضاف إلى ما سبَقَ مسألةُ تقييمِ الخللِ الأمنيِّ للكائن.

ثانيا: الخللُ الأمني:

Le défaut de sécurité:

قد يكون تقييم الخللِ الأمنيِّ للأشياءِ المُتَّصلةِ أمرًا صعبًا؛ نظرًا لهجماتِ الكمبيوتر التي تتعرَّض لها، وقدرتها على التعلُّم (التعلُّم الآلي). وفي الحالةِ الأولى، السُّؤال الذي يطرحُ نفسَه هو ما إذا كان الشَّيء المتَّصلُ يُمكن أن يكونَ معيبًا لمجرَّد أنه لم يقاوم القرصنة؟. بمعنًى آخر، ما هو الأمانُ الذي يُمكن أن يتوقَّعه أيُّ مستخدمٍ بشكلٍ قانونيٍّ عند استخدامِ شيءٍ متَّصل؟ وإذا كان هذا الأمانُ يتعلَّق بحمايةِ البيانات، فهل يُمكن اعتبارُ عدم الالتزامِ بسياسةِ حمايةِ البياناتِ الشَّخصيَّة النَّاتجة عن اللَّائحةِ العامةِ لحمايةِ البيانات عيبًا أو خللًا أمنيًّا؟ وفي هذه الحالة، يُمكن للمستخدمِ أن ينقلبَ ضدَّ معالجِ البياناتِ أو المقاول من الباطن، الذي سيُصبح بالتَّالي منتجًا بالمعنى المقصودِ في التَّوجيهِ الصَّادر في ٢٥ يوليو ١٩٨٥. وبحسب كريستين جاتو، "تعدُّ معالجةُ البياناتِ الشَّخصيَّة مسؤوليَّةَ مصمِّمي الأشياءِ المُتَّصلةِ وفقًا للمعنى المقصودِ في اللَّائحةِ العامَّة لحمايةِ البيانات"[٢٩١]. وبالتَّالي يُمكن أن يكونَ هناك تعايشٌ بين التَّوجيهِ الصَّادر في ٢٥ يوليو ١٩٨٥ واللَّائحةِ العامَّة لحمايةِ البيانات.

بينما يرى آخرون أنَّه لا يُمكننا أن نستنتجَ أن الشَّيءَ المتَّصلَ معيبٌ؛ لأن طرفًا ثالثًا تمكَّن من التحكُّم فيه، أو اختراق البيانات السِّرية[٢٩٢]. ينبغي أن يتمَّ التَّعايشُ بين اللَّائحةِ العامَّة لحمايةِ البيانات وتوجيهات ٢٥ يوليو ١٩٨٥ من زاويةٍ أخرى: وهي الامتثالُ لقواعدِ حمايةِ البياناتِ بحسب التَّصميم، المنصوص عليها في المادة ٢٥ من اللَّائحةِ العامَّةِ لحمايةِ البياناتِ (الخصوصيَّة بحسب التَّصميم). ولذلك يجبُ على الشَّركةِ المصنِّعة أن تقدِّم دليلًا على أنها قامت– من خلال تصميمِ الجسمِ– بتنفيذِ تدابيرَ لتزويدِه بمستوًى كافٍ من الأمان[٢٩٣]. لكن فيما يتعلَّقُ بهذا الحلِّ

AUTONOMES Mémoire de recherche Par Sous la direction de Monsieur le professeur Louis Perdrix Année: 2018– 2019.

(291) Ch. Gateau, «Objets connectés. Quand la responsabilité du fait des produits défectueux rencontre la protection des données personnelles», Lexisnexis, La semaine juridique, édition générale, n° 12- 19 mars 2018, p. 568.

(292) Lamy Droit de la responsabilité, 350-375.

(293) Lamy Droit de la responsabilité, 350-375.

(ISSN: 2537- 0758)

الفقهيّ، تنشأ مشكلةٌ أخرى: تلك المتأصّلة في القدرةِ التعليميَّةِ للأشياءِ المُتَّصلةِ. وفي الواقع، من المتوقَّع أن يتطوَّر الشَّيءُ المتَّصلُ المجهز بالذَّكاءِ الاصطناعيّ بمرور الوقتِ اعتمادًا على سلوكِ المستخدم. وبالتَّالي، فإنَّ الطَّبيعةَ المعيبةَ للشَّيءِ قد تكونُ ناجمةً عن هذا الأمر.

وبالمثل، فإنَّ الشَّيءَ المتَّصلَ يتطوَّر مع استخدامِ المستخدمِ له: فهو "يتعلَّم". لذلك يُمكننا أن نتخيَّل أن الشَّيءَ المتَّصلَ قد أصبح معيبًا، أو حتى خطيرًا، بسبب سلوكِ مستخدمِهِ. ومع ذلك، بما أن العيبَ في المنتجِ يحدث بعد وقتِ طرحهِ للتَّداول، يتمُّ استبعادُ اللُّجوءِ إلى نظامِ المسؤوليَّةِ عن المنتجاتِ المعيبة. وبالمثل، فإن المادَّة الجديدة ١٢٤٥-١٠ من القانون المدنيّ الفرنسيّ تستبعد المسؤوليَّةَ التلقائيَّة للمنتج، عندما لا تسمحُ حالةُ المعرفةِ العلميَّة والتقنيَّة وقت طرحِ المنتجِ للتَّداولِ باكتشافِ العيبِ في المنتج. ويُمكن لمصنِّعي الأشياءِ المبتكرة الاستفادة بشكلٍ كبيرٍ من هذا الاستبعادِ لمخاطر التَّطوير.

في الختام، إذا كانت آليَّاتُ قانونِ المسؤوليَّةِ الحاليَّة قادرةً بشكلٍ مسبقٍ على الاستجابةِ لقضايا المسؤوليَّةِ في حالةِ فشل الأشياءِ المُتَّصلة،. سيكون من المناسبِ أيضًا بالإضافةِ إلى إنشاءِ نظامٍ محدَّدٍ للمسؤوليَّة، الاستعانة بضماناتٍ تأمينيَّةٍ محدَّد.

الفرع الثالث

الحلولُ المقدَّمة لإصلاحِ الأضرارِ النَّاجمة عن الذَّكاءِ الاصطناعيِّ

يوجدُ حلَّان رئيسان لتسهيلِ إصلاحِ الأضرارِ النَّاجمةِ عن الذَّكاء الاصطناعيّ:

أولًا: تخفيف عبءِ الإثبات عن المضرورين من أنظمة الذَّكاءِ الاصطناعي:

Alléger la charge de la preuve des victimes d'Intelligence Artificielle:

يتمثل التَّدبيرُ الأوَّل من إنشاءِ افتراضٍ قابلٍ للدَّحض لوجودِ علاقةٍ سببيَّةٍ في حالةِ الخطأ، والذي بفضله لن يضطر المضرورُ إلى إثباتِ الخللِ في الذَّكاءِ الاصطناعيّ، وهذا الأمرُ من شأنه افتراضُ السببيَّة، ومن ثم يُعفي المضرورين من الذَّكاءِ الاصطناعيّ من عبءِ الإثباتِ بمجرَّد أن يتمكنوا من إثباتِ أن شخصًا- طبيعيًا أو اعتباريًّا- ارتكب خطأً من خلالِ عدمِ احترامِ التزامٍ ذي صلةٍ بالضَّرر، وأن وجودَ علاقةٍ سببيَّةٍ بين هذا الضَّررِ وأداء الذَّكاءِ الاصطناعيّ أمرٌ محتملٌ بشكلٍ معقول.

وبالتالي، سيتمُّ تقديمُ افتراضِ السببيَّةِ عندما يُمكن اعتبارُ أن الخطأ المعنيَّ قد أثَّر على نتيجةِ نظام الذَّكاءِ الاصطناعيِّ أو عدم قدرتِهِ على إحداثِ نتيجةٍ، حيث تكونَ المحكمةُ قادرةً على افتراضِ أن عدمَ الامتثالِ هذا قد تسبَّب في الضَّرر، وعلى ذلك فإنَّ افتراضَ العلاقةِ السببيَّة هذا يُعفي المضرورَ من الالتزامِ بإثباتِ طبيعةِ الخطأ أو الإغفال الذي تسبَّب في الضَّرر.

ثانيا: تسهيلُ الكشفِ عن الأدلةً.

Faciliter la divulgation d'éléments de preuve

يتمثَّل الإجراءُ الثاني في تبسيطِ الوصولِ إلى الأدلةِ التي يحتفظُ بها الأشخاصُ الذين تؤخَذ في الاعتبارِ مسؤوليَّتهم. وبالتَّالي سيكونُ من الممكنِ للمضرورين أن يَطلبوا من المحكمةِ أن تأمرَ بالكشفِ عن المعلوماتِ المتعلِّقة بأنظمةِ الذَّكاء الاصطناعيِّ التي تعتبر "مخاطرُ يصعبُ العثور عليها «à haut risque»" ويشتبهُ في أنها تسبَّبت في إحداثِ أضرارٍ. ويهدفُ هذا الإجراءُ إلى السَّماحِ للمضرورين من أنظمةِ الذَّكاء الاصطناعيِّ بالتعرُّف بسرعةٍ أكبرَ على الشَّخصِ المسؤولِ عن الضَّرر وسبب المشكلة(٢٩٤).

ومع ذلك، من أجلِ عدمِ الإضرارِ بالمصالحِ المشروعةِ لجميع الأطراف، ولا سيَّما لضمانِ حمايةِ الأسرارِ التِّجاريَّة، فإن هذا الكشفَ سيخضعُ لشروطٍ معيَّنةٍ، ويجب أن يكونَ ضروريًّا ومتناسبًا أيضًا.

وفي الحقيقة لن يفيدَ هذا التَّوجيهُ الجديدُ المضرورين من أنظمةِ الذَّكاء الاصطناعيِّ فحسب، بل سيكون له أيضًا مزايا للشَّركاتِ في هذا القطاع، والتي ستكونُ أكثرَ قدرةً على تقييمِ وتوقُّعِ مخاطرِ مسؤوليَّتها.

(294) Haas Avocats,La création d'un régime spécifique de responsabilité de l'Intelligence Artificielle, https://info.haas-avocats.com/droit-digital/la-creation-dun-regime-specifique-de-responsabilite-de-lintelligence-artificielle.

(ISSN: 2537- 0758)

الخاتمة

بعد دراستِنا لهذا الموضوعِ توصلَّنا إلى النتائجِ والتَّوصياتِ الآتية:

النَّتائج:

- إن الاتِّصالَ بالابتكاراتِ التِّكنولوجيَّةِ لا سيَّما أنظمةُ الذَّكاء الاصطناعيّ يُمثِّل تحدِّيًا للقانون، وبخاصَّةٍ مع انتشارِ إنترنتَ الأشياء، والذي أنتج سيلًا من الأشياءِ المُتَّصلةِ الذكيَّة التي يحتملُ أن تكونَ لا نهائيًّا وغير قابلٍ للحصر.
- إن إنترنتّ الأشياءِ لا يزالُ في مهدِه، وأن ما يجعلُ الشَّيءَ المتَّصل أكثر ثراءً، هو إعطاؤه القدرةَ على مشاركةِ المعلومات، واتِّخاذ القراراتِ، وتنفيذ المهامّ، عن طريقِ الإنترنتّ؛ من أجلِ تحويلِ هذه الأشياءِ من أشياءَ تقليديَّةٍ إلى أشياءَ ذكيَّةٍ مزوَّدةٍ بأنظمةِ الذَّكاء الاصطناعيّ.
- يتطلَّب تشغيل الأشياءِ المُتَّصلة، في أغلبِ الأحيانِ الحصولَ على عديدٍ من المعلوماتِ في مراحلِ تشغيلِه المختلفة، وبخاصَّةٍ الأشياءُ المُتَّصلةُ الذكيَّة والمستقلَّة التي قد تحصلُ بطريقةٍ أو بأخرى على معلوماتٍ وبياناتٍ عن مستخدمها بشكلٍ تلقائيّ كعاداتِه اليوميَّة دون علمه، ولذا يكون من الصَّعب جدًّا العمل على تخصيصِ البياناتِ لا سيَّما في ظلِّ تشابكٍ أكثر من جهازٍ متَّصلٍ مع بعضِهِ في ذات الوقت، والذي قد يختلفُ بطبعِهِ عن الجهازِ الآخر، كما أن تخصيصَ المعالجةِ في نطاقٍ محدَّدٍ قد يحرمُ المستخدمَ من الحصولِ على عديدٍ من مزايا التي يقدِّمها هذا الشَّيء.
- تُثير الأشياءُ المُتَّصلةُ عديدًا من الإشكاليَّاتِ والتَّحدِّيَّات؛ كون أنَّ اتِّخاذ القراراتِ، في إطارِ الأشياءِ المُتَّصلة المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ يتمُّ في أغلبِ الأحيانِ من خلال البرمجيَّاتِ الحاسوبيَّة التي توجدُ بداخلِ هذه الأشياءِ دون تدخُّلٍ بشريّ، كما أنَّ تشغيلَ هذه الأشياءِ يحتاج إلى تزويدِها بالبياناتِ المتعلِّقة بمستخدميها وأحيانًا تكون بياناتٍ ضخمةً.
- لم تقمْ أيُّ دولةٍ حتى الآن بإنشاءِ إطارٍ قانونيّ واضحٍ لتنظيم مسائلِ الأشياءِ المُتَّصلة، ربما حتى لا يؤدِّي إلى تقييدِ الإبداع، وكأنَّه إغفالٌ متعمدٌ لحين إصدارِ الشَّركاتِ المصنعة قائمةً بمسؤوليَّتها.

- لم تحظَ دراسةُ الأشياءِ المُتَّصلة المزودة بأنظمةِ الذَّكاء الاصطناعيّ بالاهتمام الكافي لا سيَّما في ظلِّ غيابِ التَّنظيمِ التَّشريعيّ الخاصّ بهذه الأنظمةِ في مصر، حيث يتمُّ استخدامُها من خلال الشَّركاتِ والعقودِ الخاصَّة بين طالبِ الخدمةِ (الشيء المتَّصل)، والشَّركة المقدمة لها.
- على الرَّغم من أن اللَّائحةَ الأوروبيَّةَ لحمايةِ البيانات (GDPR) قد أسهمت بشكلٍ كبيرٍ في أوروبا في تنظيمِ استخداماتِ البيانات والأشياء المُتَّصلة، إلا أنَّه في ظلِّ تساؤلاتٍ عديدةٍ التي يثيرها إدخالُ الأشياءِ المُتَّصلةِ في الحياةِ اليوميَّة للناس، وعلى جميعِ مستوياتِ المجتمع، لا يزال هناك نقص في تنسيق السياسات العامة من أجل التوصل إلى تطوير إطار قانوني مشترك بين المؤسسات العامة والقانونيَّة والاقتصاديَّة.
- إذا كان المُشرِّع المصري قد سن قوانين تتعلق حماية حقوق الملكيَّة الفكريَّة، وحماية البياناتِ الشَّخصيَّة، لكنَّ التَّطبيقَ الفعليَّ والعمليَّ لاستخدامِ الأشياءِ المُتَّصلة يُشير إلى وجودِ كثيرٍ من الإشكالياتِ لا سيَّما القانونيَّةُ التي تحتاجُ إلى دراسةٍ متخصِّصةٍ وقواعد متعمِّقة؛ كون أن الأضرارَ النَّاجمةَ عن استخدامِ الأشياءِ المُتَّصلة أصبحتْ كثيرةً ومتعدِّدةً.
- يُعدُّ قانونُ تنظيمِ الذَّكاء الاصطناعيّ الأوروبيّ لسنة ٢٠٢٤ خطوةً تاريخيَّةً نحو ضمان الاستخدامِ الآمنِ والمستدام للتِّقنيَّاتِ الحديثة. ومن خلالِ هذا التَّشريع، يسعى الاتِّحادُ الأوروبيُّ إلى تحديدِ إطارٍ شاملٍ للتَّعامل مع الذَّكاءِ الاصطناعيّ مع تحقيقِ التَّوازنِ بين حمايةِ الأفراد وتشجيعِ الابتكارِ في هذا المجالِ المتسارع.
- مبدأ الموافقةِ كحامٍ حقيقيٍّ لخصوصيَّةِ مستخدمي الأشياءِ المُتَّصلة يمرُّ بأزمةٍ قانونيَّةٍ، ولا يزالُ في قلبِ المناقشاتِ حول استخدامِ الأفرادِ وسيطرتهم الحقيقيَّة على بياناتِهم، ناهيكَ عن مبدأ الموافقةِ مقيَّدٌ باستثناءاتٍ عديدةٍ.
- إن علمَ المستخدمِ بتفسيرِ مخرجاتِ النَّظام في الشَّيءِ المتَّصلِ وكيفيَّة استخدامهِ بشكلٍ مناسبٍ، أمرٌ في غايةِ الأهميَّة، حيث إنَّ العلمَ المسبق لدى المستخدمِ بتعليماتِ الجهازِ المتَّصل بصورةٍ صحيحةٍ، وموجزة جعل استخدامَ وتشغيل الشَّيءِ المتَّصلِ واضحًا وشفافًا لدى المستخدمين.

(ISSN: 2537- 0758)

- إذا كان المُشرّعُ المصريُّ في قانونِ رقم ١٥١ لسنة ٢٠٢٠ بشأن حمايةِ البياناتِ الشَّخصيَّةِ قد أشار إلى مسألةِ إخفاء الهوية، وذلك في نصِّ المادة ٤ منه، إلا أنَّه لم يُشرْ إلى آليَّةِ تشفيرِ البيانات، وهو أمرٌ يجعل البياناتِ المجمعة في نطاقِ الأشياءِ المُتَّصلة في خطرٍ دائمٍ.
- إذا كان المُشرّعُ المصريُّ قد ألزم المتحكّم في البياناتِ بضرورةِ القيامِ باتّخاذ جميعِ الإجراءاتِ التقنيَّة والتنظيميَّة وتطبيق المعاييرِ القياسيَّةِ اللَّازمة لحمايةِ البياناتِ الشَّخصيَّة وتأمينها، فضلًا عن حمايةِ وتأمينِ عمليَّةِ المعالجةِ والوسائط والأجهزةِ الإلكترونيَّة المستخدمة في ذلك وما عليها من بياناتٍ شخصيَّة، إلا أنَّ حمايةَ السريَّة تواجهُ إشكاليَّةً لا سيما في ظلِّ الاستخداماتِ المتطوّرة للأشياءِ المُتَّصلةِ فالتحدّي الأكبر الذي يُواجه مبدأ الحفاظِ على سريَّةِ بياناتِ المستخدمِ لخدماتِ الأشياءِ المُتَّصلة يتمثَّل في التَّشخيصِ الآليّ والتلقائيّ الذي تقومُ به هذه الخدمةُ من تلقاءِ نفسِها، باستخدام أجهزةِ الاستشعارِ.
- لم يُشرْ المُشرّع المصريُّ في قانونِ حمايةِ البياناتِ الشَّخصيَّة رقم ١٥١ لسنة ٢٠٢٠ إلى مسألةِ المعالجةِ المؤتمتة، وكيفيَّة حمايةِ البياناتِ الشَّخصيَّة في ظلِّ ظهورِ وتطوُّرِ هذه الآليَّة.
- واجه مركزُ حمايةِ البيانات الشَّخصيَّة المصريّ عدَّة صعوباتٍ في رقابةِ الأشياءِ المُتَّصلة، حيث إنه مع تتعدُّدِ الأجهزةِ والتَّطبيقات المُتَّصلة لا سيَّما المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ، يجعل من الصَّعب تتبع جميعها وفهم خصائص كلِّ جهازٍ، وهذا التنوُّع يعقد عمليَّة وضعِ معاييرَ موحَّدة للحماية، لا سيَّما في ظلِّ قلَّةِ الوعي بأهمية حمايةِ البيانات الشَّخصيَّةِ لدى المُستخدمين والمطورين، حيث يؤدّي ذلك الأمرُ إلى استخدامِ أجهزةٍ غير آمنةٍ أو عدم اتّباع بروتوكولات الأمانِ المناسبةِ.
- إن إدراجَ بندٍ من شأنهِ أن يفرغَ الالتزامَ الأساسيَّ للشَّركةِ المصنعةِ من مضمونهِ وجوهرِه سيكون بمثابةِ خللٍ واضحٍ بحسب نصِّ المادة ١١٧٠ من القانون المدنيّ الفرنسيّ (الجديد) شأنه في ذلك شأن بندِ الإعفاءِ من المسؤوليَّةِ في حالة حدوثِ خرقٍ يتعلَّق بأمنِ البياناتِ(la sécurité des données).

- لا يبدو أنَّ مبدأ التَّناسبِ في معالجةِ البياناتِ الشَّخصيَّة هو الأسهلُ في التَّنفيذِ والتحكُّم.
- يعدُّ مبدآ حمايةِ الخصوصيَّةِ بحسَبِ التَّصميمِ وحماية الخصوصيَّةِ بشكلٍ افتراضيٍ، بمثابة أداتين لإدارةِ مخاطرِ حمايةِ المعلومات المستخدمة لتشغيلِ الأشياءِ المُتَّصلة.
- إن تعدُّد المشاركين في سلسلةِ إنتاجِ الأشياءِ المُتَّصلة المزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ يجعل مهمَّةَ إثباتِ الخطأ صعبةً على المضرورِ. كما أن الضَّررَ الناجمَ عن الأشياءِ المُتَّصلةِ المزودة بأنظمةِ الذَّكاءِ الاصطناعيّ لا يرتبط دائمًا بخطأ، حيث يُمكن أن ينتجَ عن استقلاليَّةِ اتِّخاذ القرارِ التي يتمتَّعُ بها هذا الشَّيء.
- يتحتَّم على المضرورِ تقديم ما يثبتُ انحرافَ الشَّيءِ لإثباتِ وجود علاقةٍ سببيَّة. وهذا هو الحالُ بالتَّحديدِ عندما يكونُ الضَّررُ ناجمًا عن شيءٍ متحركٍ دون أيّ اتِّصالٍ من قبل المضرور، أو عن طريقِ شيءٍ خاملٍ غير متحرِّك، لكن البحثَ على إثباتِ هذه الحالةِ سيكون معقدًا بالنِّسبةِ للمضرور، كون أنَّ الأشياءَ المُتَّصلة تمثِّل نظامًا معقدًا يتطلَّب تدخُّلَ خبيرٍ.
- تكمن خصوصياتُ أضرارِ الأشياءِ المُتَّصلة في طبيعتِها الخاصَّة، مع صعوبةِ تحديدِ المسؤولِ عنها، بحيث يبدو من الصَّعبِ تطبيق القواعدِ العامَّة للمسؤوليَّةِ المدنيَّة وفقًا للنَّهجِ التقليديّ بصددِها، كونها غير مناسبةٍ للحدِّ من أضرارِ الأشياءِ المُتَّصلة.
- يعدُّ نظامُ المسؤوليَّةِ عن المنتجاتِ المعيبة، في الوضعِ الحاليّ للقانون، هو الأكثر ملاءمةً لإصلاح الأضرارِ الناجمةِ عن الأشياءِ المُتَّصلة وإن كان يحتاجُ لبعضِ التَّطوير.
- تتضمَّن سلسلةُ قيمةِ الذَّكاء الاصطناعيّ the AI value chain عديدًا من الأطرافِ التي تتحمَّل مسؤوليَّاتٍ متعدِّدة على مختلفِ الأصعدة. من التَّصميمِ إلى التَّسويقِ، مرورًا بالتَّوزيع والاستعمال، يتحمَّل كلُّ طرفٍ مسؤولياتٍ قانونيَّةً وأخلاقيَّةً لضمانِ سلامةِ الأنظمةِ الذكيَّة وحمايتها.

(ISSN: 2537- 0758)

التَّوصيات:

١- نُوصِي بضرورةِ العملِ على مواجهةِ القضايا التي يُثيرها التطوُّر السَّريعُ للأجهزةِ المُتَّصلة، من خلالِ إنشاءِ برامجَ بحثيَّةٍ في مجالِ اتِّصالاتِ المعلومات في كافَّة التَّخصُّصاتِ للتأكُّد من مراعاةِ الاعتباراتِ الأخلاقيَّةِ والقانونيَّةِ عند تصميم الجهاز، فضلًا عن تقييمِها.

٢- نُوصي بضرورةِ وضعِ إطارٍ قانونيٍّ "عربي مشترك" لتنظيمِ الأشياءِ المُتَّصلة في ظلِّ التطوُّرِ الهائلِ لاستخداماتِ الذَّكاء الاصطناعيّ، من أجل الحدِّ من المخاطرِ المحتملةِ لهذه الأشياء.

٣- نُوصِي المُشرِّعَ المصريَّ بضرورةِ سَنِّ إطارٍ قانونيٍّ يتضمَّن قواعدَ منسجمةً بشأن الأشياءِ المُتَّصلة بشكلٍ عامٍّ والمزوَّدة بأنظمةِ الذَّكاء الاصطناعيّ عالية الخطورةِ على وجهِ الخصوص؛ لتعزيزِ تطوير واستخدامِ واستيعابِ الذَّكاء الاصطناعيّ في السُّوق الداخليّ، بما يلبِّي في الوقتِ نفسه مستوًى عاليًا من حمايةِ المصالحِ العامَّة، مثل الصِّحةِ والسَّلامة وحماية الحقوقِ الأساسيَّة. فضلًا عن حمايةِ مُستخدمي الأشياءِ المُتَّصلة، على أن يراعيَ القواعدَ الآتية:

- ضرورةُ الاعتمادِ على النُّصوصِ الواردةِ في التَّوجيهِ الأوروبيّ، والتَّشريع الفرنسيّ، والقوانين المتعلّقة بأمنِ وحمايةِ البيانات، عند سنِّ قانونٍ خاصٍّ لمواجهةِ التَّحدِّيَّات المعاصرة لاستخداماتِ الأشياءِ المُتَّصلةِ لا سيَّما الأجهزةُ الذكيَّة.
- نقترحُ وضعَ سياساتٍ تنظيميَّةٍ، وذلك فيما يتعلَّق بخدماتِ إنترنتّ الأشياء، بحيث يتحتَّمُ على كلِّ مُزودٍ بخدماتِ إنترنتّ الأشياءِ ضرورة استخدامِ معيارٍ تشفيريٍّ يجعل المستخدمَ هو صاحبَ القرارِ الأساسيّ فيه، وذلك من خلال العملِ على تطويرِ وتحديثِ التِّكنولوجيا المستخدمة في مجالِ التَّشفيرِ واخفاء المعلوماتِ؛ كي تتناسبُ مع تطوُّرِ الأشياءِ المُتَّصلة.
- يلتزم مصمِّمُ الشَّيءِ المتَّصل المزوَّد بأنظمةِ الذَّكاءِ الاصطناعيّ بمراعاةِ إساءةِ الاستخدامِ المتوقَّعة بشكلٍ معقولٍ عند تصميمِ الشَّيء المتَّصل، والتي قد تنتجُ عن سلوكٍ بشريٍّ متوقَّعٍ بشكلٍ معقولٍ.

- يقعُ على عاتقِ الشَّركةِ المصنعة التأكُّدُ من وجودِ "**مكوّن السَّلامة**" باعتبارِه أحدَ مكوّناتِ المنتجِ أو نظام الذَّكاءِ الاصطناعيّ الذي يفي بوظيفةِ السَّلامة، حيث يتحتَّمُ أن يكونَ لأيّ منتجٍ وبخاصَّةٍ المنتجاتُ المُتَّصلةُ إلكترونيًّا مكونٌ يُسمَّى بمكوّن السَّلامة، في حالةِ إذا أدَّى فشلُه أو عُطلُه إلى تعريضِ صحَّةِ وسلامةِ الأشخاصِ أو الممتلكات للخطر.
- ضرورةُ الأخذِ بـ"**نظام مراقبة ما بعد التَّسويق**" جميع الأنشطة التي يقوم بها مزودو أنظمة الذَّكاء الاصطناعي لجمع ومراجعة الخبرة المكتسبة من استخدام أنظمة الذَّكاء الاصطناعي التي يضعونها في السوق أو يضعونها في الخدمة لغرض تحديد أي حاجة لتطبيق أي إجراءات تصحيحية أو وقائية ضرورية على الفور.
- يجبُ تصميمُ الأشياءِ المُتَّصلة وتطوير أنظمةِ الذَّكاءِ الاصطناعيّ وبخاصَّةٍ عاليةُ المخاطرِ بطريقةٍ تضمَن أن يكونَ تشغيلُها شفافًا بدرجةٍ كافيةٍ لتمكينِ المُستخدمين من تفسيرِ مخرجاتِ النِّظام واستخدامه بشكلٍ مناسبٍ، بحيث يجب ضمانُ نوعٍ ودرجةٍ مناسبين من الشَّفافيةِ بهدفِ تحقيقِ الامتثالِ للالتزامات ذات الصِّلة للمزوِّد والمُستخدم. كما يجبُ أن تكونَ الأشياءُ المُتَّصلةُ المدعومة بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطرِ مصحوبةً بتعليماتٍ للاستخدامِ، وذلك بتنسيقٍ رقميٍّ مناسبٍ تتضمَّن معلوماتٍ موجزةً وكاملةً وصحيحةً وواضحةً وذات صلةٍ، ويُمكن الوصولُ إليها وفهمُها من قِبل المُستخدمين.
- يتحتَّم على الجهاتِ الفاعلةِ في معالجةِ البيانات وضعُ تدابيرَ فنيَّةٍ وتنظيميَّة، يتمُّ تحديثُها وتوثيقُها دائمًا، بحيث يجبُ أن تحتويَ تعليمات استخدامِ الشَّيءِ المتَّصلِ على المعلومات التالية:

أ- هويَّة وتفاصيلُ الاتِّصالِ الخاصَّة بالمُستخدم.

ب-خصائصُ وقدراتُ وقيودُ أداءِ نظامِ الذَّكاء الاصطناعيّ عالي المخاطر، بما في ذلك: الغرضُ المقصودُ منه؛ ومستوى الدِّقة، بما في ذلك مقاييسُه وقوَّته وأمنُه السيبرانيُّ، والذي تمَّ اختبارُ نظامِ الذَّكاء الاصطناعيّ عالي المخاطر والتحقُّق من صحَّتهِ على أساسهِ، والذي يُمكن توقُّعه، وأيُّ ظروفٍ معروفةٍ

(ISSN: 2537- 0758)

ومتوقَّعة قد تؤثِّر على هذا المستوى المتوقَّع من الدقَّةِ والمتانةِ والأمن السيبرانيّ؛ فضلًا عن أيّ ظرفٍ معروفٍ أو متوقَّع يتعلَّق باستخدامِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ وفقًا للغرضِ المقصودِ منه أو في ظلِّ ظروفِ إساءةِ الاستخدامِ المتوقَّعة بشكلٍ معقولٍ، والتي قد تؤدِّي إلى مخاطرَ على الصِّحةِ والسَّلامةِ أو الحقوق الأساسيَّة.

- يجبُ على مصمِّم الجهازِ المتَّصلِ إضافةُ معلوماتٍ لتمكينِ المستخدمين من تفسير مخرجاتِ نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ واستخدامها بشكلٍ مناسبٍ؛ فضلًا عن بيانِ التَّغييراتِ التي تطرأ على نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطر وأدائه، والتي تمَّ تحديدُها مسبقًا من قِبل المزوِّد.
- يلتزم مزوِّد الشَّيءِ المتَّصلِ ببيان التدابيرِ الفنيَّةِ الموضوعةِ لتسهيلِ تفسيرِ مخرجاتِ أنظمة الذَّكاءِ الاصطناعيّ عالية المخاطرِ من قبلِ المستخدمين؛ والموارد الحاسوبيَّة والأجهزة اللَّازمة، والعمر المتوقَّع لنظامِ الشَّيءِ المتَّصلِ وأي تدابيرِ صيانةٍ ورعايةٍ ضروريَّة، لضمانِ الأداءِ السَّليم لنظامِ الذَّكاءِ الاصطناعيّ، بما في ذلك تحديثاتُ البرامج.
- يجب على مقدِّمي الخدماتِ ضمان تصميمِ وتطويرِ أنظمة الذَّكاءِ الاصطناعيّ المخصَّصة للتَّفاعلِ المباشرِ مع الأشخاص الطبيعيّين بطريقةٍ تجعل الأشخاصَ الطَّبيعيّين المعنيّين على عِلمٍ بأنهم يتفاعلون مع نظامِ الذَّكاء الاصطناعيّ، ما لم يكن ذلك واضحًا من وجهةِ نظرِ شخصٍ طبيعيّ يتمتَّعُ بقدرٍ معقولٍ من المعرفةِ والملاحظةِ والحذر، مع مراعاةِ الظُّروفِ وسياق الاستخدام.
- يقع على عاتق مقدِّمي الأشياءِ المُتَّصلةِ المزودة بأنظمةِ الذَّكاءِ الاصطناعيّ، بما في ذلك أنظمةُ الذَّكاء الاصطناعيّ للأغراضِ العامَّة، التي تولِّد محتوًى صوتيًّا أو صوريًّا أو فيديو أو نصيًّا اصطناعيًّا، التزامٌ بضمانِ تمييزِ مخرجاتِ نظام الذَّكاءِ الاصطناعيّ بتنسيقٍ قابلٍ للقراءة آليًّا واكتشاف ما إذا تمَّ التَّلاعبُ بها بشكلٍ مصطنعٍ. ويتعيَّن على مقدِّمي خدمات الذَّكاءِ الاصطناعيّ ضمان فعاليةِ حلولِهم التقنيَّةِ وقابليتها للتَّشغيلِ المتبادلِ وقوَّتها وموثوقيتها بقدرِ ما هو ممكنٌ من الناحيةِ التقنيَّة، مع مراعاة خصوصيَّاتِ وقيودِ أنواعٍ مختلفةٍ من المحتوى

وتكاليف التَّنفيذِ والحالة الفنيَّة المعترف بها عمومًا، كما قد تنعكسُ في المعاييرِ التقنيَّةِ ذات الصِّلة.

- يقعُ على عاتقِ الشَّركاتِ احترامُ تقليلِ البياناتِ إلى الحدِّ الأدنى، وذلك تحقيقًا لمبدأ التَّناسبِ من أجلِ تحقيقِ توازُنٍ عادلٍ بين حمايةِ الحياة الخاصَّة وحريَّة الأعمال.
- يجب أن تكونَ الأشياءُ المُتَّصلةُ المدعومة بأنظمةِ الذَّكاءِ الاصطناعيّ مرنةً قدرَ الإمكانِ فيما يتعلَّق بالأخطاءِ أو الأعطالِ أو التَّناقضات التي قد تحدثُ داخلَ النِّظامِ أو البيئة التي يعملُ فيها النِّظام، وخاصَّةً بسببِ تفاعلها مع الأشخاصِ الطَّبيعيّين أو الأنظمة الأخرى. كما يجبُ اتِّخاذ التَّدابيرِ الفنيَّةِ والتنظيميَّة في هذا الصَّدد. ولتحقيقِ قوَّةٍ في أنظمة الذَّكاءِ الاصطناعيّ يمكن الاستفادةُ من خلالِ حلولِ التَّكرارِ الفنيّ، والتي قد تشملُ خطط النَّسخِ الاحتياطيّ أو خطط الأمانِ من الفشل.
- يتحتَّم على المصمِّم تطويرُ الأشياءِ المُتَّصلةِ المدعوَّة بأنظمةِ الذَّكاء الاصطناعيّ التي تستمرُّ في التعلُّمِ بعد طرحِها في السُّوق أو وضعها في الخدمةِ بطريقةٍ تقضي على أو تقلِّل قدرَ الإمكانِ من خطرِ تأثيرِ المخرجاتِ المتحيزةِ المحتملةِ على المدخلاتِ للعمليَّاتِ المستقبليَّة (حلقات التَّغذية الرَّاجعة)؛ وذلك لضمانِ معالجةِ أيّ حلقاتِ تغذيةٍ مرتدة على النَّحو اللائقِ بتدابيرِ التَّخفيفِ المناسبة.
- يقعُ على عاتقِ الشَّركةِ المصطنعة منحُ المستخدمِ المعرفةَ الفنيَّةَ والخبرة والتَّعليم والتَّدريب والافتراضات المختلفة لاستخدام النِّظام.
- يتحتَّم أن تتضمَّنَ أنظمةُ الذَّكاء الاصطناعيّ عند تصميمها لا سيَّما الأجهزةُ عاليةُ المخاطرِ آليَّة لحفظِ السِّجلات تلقائيًّا.
- يجب على مزوِّدي الأشياء المُتَّصلة المرتبطة بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر الاحتفاظ بالسِّجلات والتي يتمُّ إنشاؤها تلقائيًّا بواسطةِ أنظمةِ الذَّكاء الاصطناعيّ، إلى الحدِّ الذي تخضعُ فيه هذه السِّجلات لسيطرتهم لفترةٍ مناسبةٍ للغرض المقصودِ من نظام الذَّكاء الاصطناعيّ عالي المخاطر، لا تقلُّ عن ستةِ أشهر.

(ISSN: 2537- 0758)

- يقع على عاتقِ الشَّركاتِ المسوقة لأيّ تكنولوجيا متَّصلةٍ الالتزامُ بإجراءِ دراسةٍ بشأن تأثيرِ معالجةِ البيانات الشَّخصيَّة على الخصوصيَّة، وذلك تحت مسمَّى "**تقييم تأثير الخصوصيَّة**"؛ قبل طرحِ الشَّيءِ المتَّصلِ في السُّوق.
- يقعُ على عاتقِ المزوِّدين والمصمِّمين وجميع المهنيّين الذين لهم دورٌ في طرحِ الأشياءِ المُتَّصلة (الذكية) فور علمِهم باكتشافِ عيبٍ قد يضرُّ بمستخدمي هذه الأشياء، ضرورة إبلاغ السُّلطاتِ المختصَّة مع العملِ على نشرِ وإعلامِ جميعِ المستخدمين ببيانِ كيفيَّةِ الوقايةِ منها، مع سحبِ هذه الأشياءِ من السُّوق إذا دعت الضَّرورةُ إلى ذلك.

ت–نوصي بضرورةِ سَنّ بعضِ القواعدِ الحاكمة التي تمنعُ استيرادَ أشياءَ متَّصلةٍ وبخاصَّةٍ المزوَّدةُ بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر قبل قيامِ مقدّمي الخدماتِ الموجودين في بلدان أخرى، بموجبِ تفويضٍ مكتوبٍ، بتعيين ممثّلٍ معتمدٍ يقع على عاتقهِ عديدٌ من الالتزاماتِ، والتي من أهمّها: التحقُّق من إعدادِ إعلانِ المطابقة، والوثائق الفنيَّة، فضلًا عن التأكُّد من قيامِ مقدّم الخدمةِ بإجراء تقييمِ شروطِ المطابقةِ المناسب؛ ومدِّ السُّلطةِ المختصَّة، والمقترح أن تكونَ هيئةً مستقلةً تحت مسمَّى "الهيئة العامَّة لرقابةِ تقنيات الأشياءِ المُتَّصلةِ والأمن الرَّقمي"، بناءً على طلبٍ مسبَّبٍ، بجميع المعلوماتِ والوثائق، اللَّازمة لإثبات توافقِ نظامِ الذَّكاء الاصطناعيّ عالي المخاطر مع المتطلَّباتِ المنصوص عليها وفقًا لقوانين الدَّولة، بما في ذلك الوصولُ إلى السِّجلات، وبخاصَّةٍ التي يتمُّ إنشاؤها تلقائيًّا بواسطةِ نظام الذَّكاءِ الاصطناعيّ عالي المخاطر.

ث–نوصي المُشرِّعَ المصريَّ بضرورةِ التَّشديدِ في التزاماتِ المستوردين لأشياءَ متَّصلةٍ مزوَّدة بأنظمةِ ذكاء اصطناعيّ شديدة الخطورة. هديًا بما فعلَهُ الاتِّحادُ الأوروبيُّ في لائحةِ الاتِّحاد الأوروبيّ ١٦٨٩/٢٠٢٤ بشأن التزاماتِ المستوردين:

- يجب على المستوردين قبلَ طرحِ نظامِ الذَّكاء الاصطناعيّ عالي الخطورةِ في السُّوق التأكُّد من أنَّ النِّظامَ متوافقٌ من خلال التحقُّق من أنه تمَّ تنفيذُ إجراءِ تقييمِ

المطابقةِ ذي الصِّلة من قبلِ مزوِّد نظامِ الذَّكاء الاصطناعيّ عالي الخطورة؛ مع التأكُّد من قيام المزوِّد بإعداد الوثائقِ الفنيَّةِ قيامه أيضًا بتعيينِ ممثِّلٍ مفوض.

- يقعُ على عاتقِ المستوردين التأكُّد من مسألةِ التَّخزين أو النقل بشكلٍ صحيحٍ أثناء وجود نظامِ الذَّكاءِ الاصطناعيّ عالي المخاطرِ تحت مسؤوليَّتهم. وتزويد السُّلطاتِ المختصَّة ذات الصِّلة، بناءً على طلبٍ مسببٍ، بجميع المعلوماتِ والوثائقِ اللَّازمة، فضلًا عن التَّعاون مع السُّلطاتِ المختصَّة ذات الصِّلة في أيّ إجراءٍ تتَّخذه تلك السُّلطاتُ فيما يتعلَّق بنظام الذَّكاءِ الاصطناعيّ عالي المخاطر الذي يطرحُه المستوردون في السُّوق، وخاصَّةً للحدِّ من المخاطرِ التي يفرضُها ذلك النِّظامُ والتَّخفيف منها.

ج- نوصي المُشرِّعَ المصريَّ بوضعِ قواعدَ منسجمةٍ بشأن تنظيمِ الأشياءِ المُتَّصلةِ المزودة بأنظمةِ الذَّكاء الاصطناعيّ لا سيما حظرُ بعضِ ممارسات الذَّكاءِ الاصطناعيّ، حيث يتوجَّب على الشَّركاتِ المصنِّعة الالتزامُ بالآتي:

- لا يجوز طرحُ نظامِ ذكاءٍ اصطناعيٍّ في السُّوق أو تشغيله أو استخدامه، طالما يعمل على استخدامِ تقنيَّاتٍ خفيَّةٍ تتجاوز وعيَ الشَّخصِ أو تقنياتٍ تتَّصفُ بالخداعِ المتعمَّد، بهدف تشويهِ سلوكِ شخصٍ أو مجموعةٍ من الأشخاص بشكلٍ ملموسٍ من خلال إضعافِ قدرتِهم على اتِّخاذ قرارٍ مستنير، وبالتالي دفعُهم إلى اتِّخاذ قرارٍ لم يكونوا ليتَّخذوه لولا ذلك بطريقةٍ تسبِّب أو من المحتمل أن تسبِّبَ بشكلٍ معقولٍ ضررًا كبيرًا.
- يحظر على الشَّركاتِ المصنعة استغلال نقاطِ الضَّعفِ لدى شخصٍ طبيعيٍّ أو مجموعة محدَّدة من الأشخاصِ بسببِ سنِّهم أو إعاقتهم أو وضع اجتماعيٍّ أو اقتصاديٍّ محدَّد.
- لا يجوز طرحُ شيءٍ متَّصلٍ ذكيٍّ في السُّوق بغرضِ تقييمِ أو تصنيفِ الأشخاص الطبيعيّين أو مجموعات الأشخاص خلال مدَّةٍ زمنيَّةٍ معيَّنة بناءً على سلوكِهم الاجتماعيّ أو خصائصهم الشَّخصيَّة أو الشَّخصيَّة المعروفة أو المستنتجة أو المتوقَّعة.

(ISSN: 2537- 0758)

- يحظر طرحُ شيءٍ متَّصلٍ في السُّوق، أو تشغيله أو استخدام نظامِ الذَّكاءِ الاصطناعيّ لإجراءِ تقييماتِ مخاطرِ الأشخاصِ الطَّبيعيّين من أجلِ تقييمِ أو التنبؤ بخطرِ ارتكابِ شخصٍ طبيعيٍّ لجريمةٍ جنائيَّة، بناءً على تحديدِ ملفِّ تعريفِ الشَّخص الطبيعيّ أو تقييم سماتٍ شخصيَّتِهِ وخصائصه فقط.
- يحظرُ طرحُ أشياءَ متَّصلةٍ في السُّوق، أو تشغيلها، أو استخدام أنظمةِ الذَّكاء الاصطناعيّ والتي تنشئ أو توسِّع قواعدَ بياناتِ التعرُّف على الوجهِ من خلالِ الكشطِ غير المستهدفِ لصورِ الوجهِ من الإنترنتّ أو لقطات كاميرات المراقبة.
- يحظرُ استخدامُ الأشياءِ المُتَّصلةِ المدعومة بأنظمةِ الذَّكاء الاصطناعيّ لاستنتاجِ مشاعر شخصٍ طبيعيٍّ في مجالاتِ مكانِ العمل والمؤسَّسات التعليميَّة، باستثناءِ الحالاتِ التي يُقصدُ فيها استخدامُ نظامِ الذَّكاءِ الاصطناعيّ لوضعهِ في السُّوق أو طرحه في السُّوقِ لأسبابٍ طبيَّةٍ أو أمنيَّةٍ.
- يحظرُ استخدامُ أنظمةٍ أو أشياءَ متَّصلةٍ تعمل على التَّصنيفِ البيومترية، والتي تصنِّف الأشخاصَ الطبيعيّين بشكلٍ فرديٍّ على أساسِ بياناتهم البيومترية لاستنتاجِ عرقِهم أو آرائِهم السياسيَّةِ أو معتقداتِهم الدينيَّةِ أو الفلسفيَّةِ أو حياتهم الخاصَّة.

ح- نقترحُ إنشاءَ هيئةٍ تكون مسؤولةً عن مراقبةِ تقنيَّاتِ الأشياءِ المُتَّصلة والأمن الرقميّ وذلك تحت مسمَّى "**الهيئة العامة لرقابةِ تقنياتِ الأشياءِ المُتَّصلة والأمن الرقمي**" باعتبارِها هيئةً تكون مسؤولةً عن تنظيمِ ومراقبةِ تكنولوجيا الإنترنت للأشياءِ (IoT) وضمان الأمن الرَّقميّ في البنيةِ التحتيَّةِ الرقميَّة المرتبطة بالأجهزةِ المُتَّصلة، حيث إن تأسيسَ مثل هذه الهيئةِ يعكسُ اهتمامَ الدَّولةِ بتطويرِ تقنياتٍ ذكيَّةٍ وآمنةٍ من أجلِ حمايةِ البياناتِ الشَّخصيَّةِ والأمنِ السيبرانيّ في عالمٍ مليءٍ بالأجهزةِ المُتَّصلةِ والشَّبكات الذكيَّة.

خ- نوصي المُشرِّعَ المصريَّ **بإنشاء نظامٍ لإدارةِ المخاطرِ** فيما يتعلَّق بالأشياءِ المُتَّصلةِ المزودة بأنظمةِ الذَّكاء الاصطناعيّ عالية المخاطر، حيث يقصدُ بنظامِ إدارةِ المخاطرِ على أنه عمليَّةٌ تكراريَّةٌ مستمرَّة يتمُّ التَّخطيطُ لها وتنفيذُها طوالَ

دورةِ حياةِ نظام الذَّكاءِ الاصطناعيّ عالية المخاطر بالكامل، وتتطلَّب مراجعةً وتحديثًا منتظمين ومنهجيَّين.

د- الأخذ بفكرةِ "**إساءة الاستخدامِ المتوقَّعة بشكلٍ معقولٍ**" فقط، والتي يلتزمُ المصمِّم بمراعاتها عند تصميمِ الشَّيءِ المتَّصل.

ذ- الأخذ بفكرةِ المسؤوليَّاتِ على طول سلسلةِ قيمةِ الذَّكاء الاصطناعيّ، حيث يعتبر أيُّ موزِّعٍ أو مستوردٍ أو ناشرٍ أو طرفٍ ثالثٍ آخر مقدمًا لنظامِ الذَّكاءِ الاصطناعيّ عالي الخطورةِ ويخضع لالتزاماتِ المزود في أيٍّ من الحالاتِ التالية:-

- وضعُ اسمهِ أو علامتهِ التجاريَّة على شيءٍ متَّصلٍ مزودٍ بنظام ذكاءٍ اصطناعيٍّ عالي المخاطر تمَّ طرحُه بالفعلِ في السُّوق أو تمَّ وضعُه في الخدمة.
- إجراء تعديلٍ جوهريٍّ على نظامِ ذكاءٍ اصطناعيٍّ عالي المخاطر تمَّ طرحُه بالفعل في السُّوق أو تمَّ وضعُه بالفعلِ في الخدمةِ بطريقةٍ تجعله يظلُّ نظامَ ذكاءٍ اصطناعيٍّ عالي المخاطر.
- تعديل الغرضِ المقصود من نظامِ الذَّكاءِ الاصطناعيّ، بما في ذلك نظامُ الذَّكاءِ الاصطناعيّ للأغراض العامَّة، الذي لم يتمَّ تصنيفُه على أنه عالي الخطورةِ وتمَّ طرحُه بالفعلِ في السُّوقِ أو وضعه في الخدمةِ بطريقةٍ تجعل نظامَ الذَّكاءِ الاصطناعيّ المعنيَّ نظامَ ذكاءٍ اصطناعيٍّ عالي الخطورة.

ر- يجب الاعتمادُ على نظامِ المسؤوليَّةِ عن المنتجاتِ المعيبةِ في سياقِ الأشياءِ المُتَّصلةِ المزودة بأنظمةِ الذَّكاءِ الاصطناعيّ؛ كونها أكثر فائدةً للمضرورِ من المسؤوليَّةِ عن الأشياء.

(ISSN: 2537- 0758)

قائمة المراجع

المراجعُ باللُّغة العربيَّة:

المراجع العامة:

- **د. أحمد شرف الدِّين:**

– نظريَّة الالتزام، الجزء الأول، مصادرُ الالتزام، الكتاب الأول: المصادر الإراديَّة (العقد– والإرادة المنفردة) بدون ناشر، سنة ٢٠٠٣.

- **د. أنور سلطان:**

– الموجز في النظريَّة العامَّة للالتزام، مصادر الالتزام، دار المطبوعات الجامعيَّة، سنة ١٩٩٨.

- **د. أيمن سعد سليم:**

– مصادر الالتزام، دراسةٌ مقارنةٌ بين القانونِ المدنيّ المصريّ ومشروع مقترح للقانون المدنيّ المصريّ طبقًا لأحكامِ الشَّريعةِ الإسلاميَّة، الطَّبعة الثانية، دار النَّهضة العربيَّة، القاهرة، سنة ٢٠١٧.

- **د. إسماعيل غانم:**

– النظريَّةُ العامَّةُ للالتزام، مصادرُ الالتزام، مكتبة عبد الله وهبة، بدون سنة نشر.

- **د. حسام الدِّين كامل الأهواني:**

– الجزء الأول، مصادرُ الالتزام، الطبعة الثانية، بدون ناشر، سنة ١٩٩٥.

- **د. حمدي عبد الرحمن:**

– الوسيط في النظريَّة العامةِ للالتزامات، الكتاب الأول، المصادر الإراديَّةُ للالتزام، العقد والإرادة المنفردة، الطَّبعة الأولى، دار النَّهضة العربيَّة، القاهرة، سنة ١٩٩٩.

- **د. رمضان أبو السعود:**

– مصادرُ الالتزام، دار الجامعةِ الجديدة، الإسكندريَّة، سنة ٢٠١٨.

- **د. رضا عبد الحليم عبد المجيد عبد الباري:**

– مصادرُ الالتزام، الكتاب الأول، المصادرُ الإراديَّةُ للالتزام (العقد– الإرادة المنفردة)، الطَّبعة الأولى، دار النَّهضة العربيَّة، القاهرة، سنة ٢٠١٢.

- **د. سعيد سعد عبدالسلام:**

– مصادر الالتزامِ المدنيّ، الطَّبعة الأولى، دار النَّهضة العربيَّة، القاهرة، سنة ٢٠٠٣.

- **د. سليمان مرقص:**

– النظريَّة العامَّة للالتزام، ديوان المطبوعات الجامعيَّة، ج١، ط ٥، سنة ١٩٩٢.

- **د. سمير عبد السيد تناغو:**

– مصادر الالتزام (العقد– الإرادة المنفردة– العمل غير المشروع– الإثراءُ بلا سببٍ– القانون)، مصدران جديدان (الحكم– القرارُ الإداريُّ)، الطَّبعة الأولى، مكتبة الوفاء القانونيَّة، الإسكندريَّة، سنة ٢٠٠٩.

- **د. عبد الحي حجازي:**

– النظريَّة العامَّة للالتزام، الجزء الثاني، مصادر الالتزام، مكتبة عبد الله وهبة، بدون سنة نشر.

- **د. عبد الرزاق أحمد السنهوري:**

– الوسيط في شرحِ القانونِ المدنيّ، الجزء الأول: نظريَّة الالتزامِ بوجهٍ عامٍّ، مصادر الالتزام، منشأة المعارف، الإسكندريَّة، سنة ٢٠٠٤.

- **د. عبد العزيز المرسي، د. محمد محمد أبو زيد:**

– مصادر الالتزام، العقدُ والإرادةُ المنفردة، كليَّة الحقوق، جامعة المنوفيَّة، (بدون تاريخ نشر).

- **د. عبد المنعم فرج الصدة:**

– مصادرُ الالتزام، دار النَّهضة العربيَّة، القاهرة، سنة ١٩٩٢.

- **د. علي نجيدة:**

– النظريَّةُ العامَّة للالتزام، الكتابُ الأول، مصادرُ الالتزام، دار النَّهضة العربيَّة، سنة ٢٠٠٤–٢٠٠٥.

- **د. محمد حسام لطفي:**

– النظريَّة العامَّة للالتزام، مصادرُ الالتزام، دار النَّهضة العربيَّة، القاهرة، سنة ٢٠١٧–٢٠١٨.

- **د. محمد حسن عبد الرحمن:**

– مصادرُ الالتزام، دراسةٌ مقارنةٌ، الطَّبعة الثانية، دار النَّهضة العربيَّة– القاهرة، سنة ٢٠١٠.

- **د. محمد حسن قاسم:**

– الوجيزُ في نظريَّةِ الالتزام، المصادر– الأحكام، دار الجامعة الجديدة، سنة ١٩٩٤.

– القانون المدني، الالتزاماتُ، المصادرُ، العقد، تعريف العقدِ وتقسيماته– تكوين العقد، دراسة فقهيَّة قضائيَّة مقارنة في ضوءِ التوجيهاتِ التَّشريعية والقضائية الحديثة وقانون العقود الفرنسي الجديد (٢٠١٦)، المجلد الأول، دار الجامعة الجديدة، سنة ٢٠١٧.

(ISSN: 2537- 0758)

- القانون المدنيُّ، المصادر، العقد (آثار العقد– جزاء الإخلال بالعقد)، دراسةٌ فقهيَّةٌ قضائيَّةٌ مقارنةٌ في ضوء التَّوجيهاتِ التَّشريعيَّةِ والقضائيَّة الحديثة وقانون العقودِ الفرنسي الجديد (٢٠١٦)، المجلد الثاني، الطَّبعة الأولى، منشورات الحلبي الحقوقيَّة– لبنان، سنة ٢٠١٨.

المراجع المتخصصة:

١. أحمد علي حسن عثمان، انعكاساتُ الذَّكاء الاصطناعيّ على القانون المدنيّ: دراسة مقارنة، مجلة البحوث القانونيَّة والاقتصاديَّة، ع٧٦، جامعة المنصورة– كليَّة الحقوق سنة ٢٠٢١.
٢. أيمن إبراهيم العشماوي، تفويت الفرصة، دراسة مقارنة، دار النَّهضة العربيَّة، سنة ٢٠٠٤.
٣. أيمن مصطفى أحمد البقلي، التَّعويض عن فواتِ الفرصةِ في إطار المسؤوليَّة المدنيَّةِ للأطباء، مجلة الدِّراسات القانونيَّة، كليَّة الحقوق– جامعة أسيوط، ٢٠١٣.
٤. إيهاب خليفة، "إنترنت الأشياء": تهديداتٌ أمنيةٌ متزايدةٌ للأجهزة المُتَّصلة بالإنترنت، مجلة اتِّجاهات الأحداث، ع١٩، مركز المستقبل للأبحاث والدِّراسات المتقدِّمة، سنة ٢٠١٦.
٥. بشار طلال أحمد المومني، التَّحدِّيَّاتُ القانونيَّةُ المعاصرة لاستخداماتِ "إنترنت الأشياء": دراسةٌ في النِّظام القانونيّ الإماراتيّ، مجلة كليَّة القانون الكويتيَّة العالميَّة، مج١٠، ع٤٠، كليَّة القانون الكويتيَّة العالميَّة، ٢٠٢٢.
٦. د.مصطفى بن أمينة، الذَّكاء الاصطناعيُّ التوليديُّ: أزمةٌ جديدةٌ في حقوقِ الملكيَّةِ الفكريَّة، المجلة الأكاديميَّة للبحوثِ القانونيَّةِ والسياسيَّة، مج٧،ع٢، جامعة عمار ثليجي الأغواط– كليَّة الحقوق والعلوم السياسية، ٢٠٢٣.
٧. رضا إبراهيم عبد الله البيومي، الحمايةُ القانونيَّةُ من مخاطر الذَّكاء الاصطناعيّ: دراسة تحليليَّة مقارنة، المجلة القانونيَّة، مج١٨،ع٣، جامعة القاهرة– كليَّة الحقوق– فرع الخرطوم، سنة ٢٠٢٣.
٨. سمية محمد سعيد محمود، التَّحدِّيَّاتُ القانونيَّةُ للذَّكاء الاصطناعيّ: الروبوت نموذجًا، مجلة العلوم القانونيَّة والاقتصاديَّة، مج٦٦،،ع١، جامعة عين شمس– كليَّة الحقوق٢٠٢٤.
٩. علي بن ذيب الأكلبي، تطبيقاتُ إنترنتّ الأشياء في مؤسَّسات المعلومات، ع١٩، الناشر: الاتِّحاد العربي للمكتباتِ والمعلومات، ٢٠١٧.

١٠. عماد عبد الرحيم الدحيات، نحوَ تنظيمِ قانون للذَّكاءِ الاصطناعيّ في حياتنا: إشكاليَّةُ العلاقة بين البشرِ والآلة، مجلة الاجتهادِ للدِّراسات القانونيَّة والاقتصاديَّة، مج٨، ع٥ ٢٠١٩
١١. فتيحة قندوز، الجوانبُ القانونيَّةُ لاستخدام الذَّكاء الاصطناعيّ، المجلة الجزائريَّة للحقوق والعلوم السياسيَّة، مج٩، ع١، المركز الجامعيُّ أحمد بن يحيى الونشريسي تيسمسيلت– معهد العلوم القانونيَّة والإداريَّة، ٢٠٢٤.
١٢. كريم علي سالم، الجوانبُ القانونيَّةُ للذَّكاء الاصطناعيّ، مجلة جيل الأبحاثِ القانونيَّةِ المعمقة، ع٥، مركز جيل البحث العلميّ، ٢٠٢٢.
١٣. محمد إبراهيم حسانين، الذَّكاء الاصطناعيُّ والمسؤوليَّةُ المدنيَّةُ عن أضرارِ تطبيقه، دراسةٌ تحليليَّةٌ تأصيليَّةٌ، المجلة القانونيَّة، مج١٥، ع١، جامعة القاهرة– كليَّة الحقوق– فرع الخرطوم، سنة ٢٠٢٣.
١٤. محمد أحمد الشرايري، المسؤوليَّةُ المدنيَّةُ الذكيةُ عن أضرارِ الذَّكاء الاصطناعيّ: دراسةٌ مسحيةٌ مقارنةٌ، مجلة كليَّة القانون الكويتيَّة العالميَّة، مج١٠، ع٣٨، كليَّة القانون الكويتية العالميَّة، سنة ٢٠٢٢.
١٥. محمد أحمد المعداوي عبد ربه مجاهد، المسؤوليَّةُ المدنيَّةُ عن الروبوتاتِ ذاتِ الذَّكاءِ الاصطناعيّ: دراسةٌ مقارنةٌ، المجلة القانونيَّة، مج٩، ع٢، جامعة القاهرة– كليَّة الحقوق– فرع الخرطوم، سنة ٢٠٢١.
١٦. محمد المبطول، المسؤوليَّةُ المدنيَّةُ عن الذَّكاءِ الاصطناعيّ، مجلَّة عدالة للدِّراساتِ القانونيَّةِ والقضائيَّة، ع٣٤، ٢٠٢٣.
١٧. محمد بومديان، الذَّكاءُ الاصطناعيُّ تحدٍّ جديدٌ للقانون، مساراتٌ في الأبحاثِ والدِّراسات القانونيَّة، ع٩,١٠، تاريخ: ٢٠١٩.
١٨. محمد حسن عبد الرحيم حمزة، الاعترافُ بالشَّخصيَّةِ القانونيَّةِ لأنظمةِ الذَّكاءِ الاصطناعي، مجلة القانون والتِّكنولوجيا، مج٣، ع٢، الجامعة البريطانيَّة– كليَّة القانون، سنة ٢٠٢٣.
١٩. محمد حماد مرهج الهيتي، مركباتُ الذَّكاءِ الاصطناعيّ: المنافع والمخاطر وتحدياتُ المسؤوليَّةِ الجنائيَّة عمَّا تتسبَّب به من حوادثَ: نظرة...، ع١٣، هيئة التَّشريع والإفتاء القانوني٢٠٢٣.
٢٠. محمد شاكر محمود محمد، دور الذَّكاءِ الاصطناعيّ في تطويرِ قواعدِ المسؤوليَّةِ المدنيَّة: دراسةٌ تحليليَّةٌ، مجلة كليَّة القانون للعلوم القانونيَّةِ والسياسيَّة، مج١١، ع٤٢ جامعة كركوك– كليَّة القانون والعلوم السياسيَّة، سنة ٢٠٢٢.

(ISSN: 2537- 0758)

٢١. محمد عرفان الخطيب، المسؤوليَّةُ المدنيَّة والذَّكاء الاصطناعيُّ، إمكانيَّة المُساءلة: دراسة تحليليَّةٌ معمقةٌ لقواعدِ المسؤوليَّةِ المدنيَّة، مجلة كليَّة القانون الكويتيَّة العالميَّة، مج٨، ع٢٩، كليَّة القانون الكويتيَّة العالميَّة، سنة ٢٠٢٠.
٢٢. محمد عماد فلاح العتوم، المسؤوليَّةُ المدنيَّةُ لتطبيقاتِ الذَّكاء الاصطناعيّ بين الواقع والحاجةِ للتَّجديد: دراسةٌ تحليليَّةٌ في القانون، رسالة ماجستير، جامعة اليرموك، ٢٠٢٢.
٢٣. محمد فتحي محمد إبراهيم، التَّنظيم التَّشريعيُّ لتطبيقاتِ الذَّكاء الاصطناعيّ، مجلة البحوث القانونيَّة والاقتصاديَّة، ع ٨١، جامعة المنصورة- كليَّة الحقوق، سنة ٢٠٢٢.
٢٤. محمد محمد عبد اللطيف، المسؤوليَّةُ عن الذَّكاءِ الاصطناعيّ بين القانونِ الخاصّ والقانون العامّ، مجلة البحوثِ القانونيَّةِ والاقتصاديَّة، عددٌ خاصٌّ، جامعة المنصورة- كليَّة الحقوق ٢٠٢١.
٢٥. محمد منصور خليل خزيمية، المسؤوليَّةُ المدنيَّةُ عن أضرارِ الذَّكاء الاصطناعيّ: دراسة مقارنةٌ، رسالة ماجستير، الجامعة العربيَّة الأمريكيَّة- جنين، ٢٠٢٣.
٢٦. محمود محمد علي محمد، مدى استيعابِ نصوصِ القانون المدنيّ لوقائعِ الذَّكاء الاصطناعيّ، دراسةٌ فقهيَّةٌ مقارنةٌ، مجلة الشَّريعةِ والقانون، ع٤٢، جامعة الأزهر- كليَّة الشَّريعة والقانون بالقاهرة، ٢٠٢٣.
٢٧. مصعب ثائر عبد الستار، المسؤوليَّة التقصيريَّة المتعلِّقة بالذَّكاءِ الاصطناعيّ، مجلة العلوم القانونيَّة والسياسيَّة، مج١٠، ع٢، جامعة ديالى- كليَّة القانون والعلوم السياسيَّة، سنة ٢٠٢١.
٢٨. منية نشناش، متعاقدُ الذَّكاءِ الاصطناعيّ: شخصٌ قانونيٌّ جديدٌ؟، مجلَّة أبحاثٍ قانونيَّةٍ وسياسيَّة، مج٧، ع١ جامعة محمد الصِّديق بن يحيى جيجل- كليَّة الحقوق والعلوم، السياسية، ٢٠٢٢.
٢٩. مها رمضان محمد بطيخ، المسؤوليَّةُ المدنيَّةُ عن أضرارِ أنظمةِ الذَّكاء الاصطناعيّ: دراسةٌ تحليليَّةٌ مقارنة، المجلة القانونيَّة، مج٩، ع٥، جامعة القاهرة- كليَّة الحقوق- فرع الخرطوم، ٢٠٢١.
٣٠. مها يسري عبد اللطيف عبد اللطيف نصار، الوضعُ الذاتيُّ للذَّكاء الاصطناعيّ في القانون المدنيّ، المجلة القانونيَّة، مج٢٠، ع٢، جامعة القاهرة- كليَّة الحقوق- فرع الخرطوم ٢٠٢٤.
٣١. نور خالد العبد الرزاق، المسؤوليَّةُ المدنيَّةُ الناشئةُ عن استخدام الذَّكاء الاصطناعيّ، أعمال مؤتمر التَّحدِّيَّات والآفاق القانونيَّة والاقتصاديَّة للذَّكاء الإصطناعيّ، جامعة عين شمس- كليَّة الحقوق، ٢٠٢٤.

المراجع باللغة الأجنبية:

1- A. Bensamoun et G. Loiseau, «La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité»https://www.slideshare.net/slideshow/responsabilit-civile-du-fait-des-objets-connectes-autonomes/234291821 #47- Rép. min. à QE N°15677, JOAN Q. 24 août 1998, p. 4728 in Le Lamy Droit de la responsabilité.
2- A. Bensamoun et G. Loiseau, «La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité», JCP G 2017, I, n° 1204.
3- Arruabarrena, B.. *Le Soi augmenté: les pratiques numériques de quantification de soi comme dispositif de médiation pour l'action* (Thèse de doctorat). CNAM, Paris. (2016).
4- Arnaud de Baynast, Jacque Lendrevie, et Julien Lévy, Mercator, Malakoff, Dunod, 12e éd., 2017.
5- Arruabarrena, B. (2022). Technologie numérique de quantification des corps à l'épreuve du comportementalisme: vers un design de la médiation homme-données. Dans A. Khatchatourov, O. Avenati, P. A. Chardel, I. Quéval (dir.), *Corps connectés, figures, fragments, discours* (p.118-135). Paris, France: Presse des mines.
6- Alain Bensoussan et Frédéric Forster, Droit des objets connectés et télécoms, Edition Bruylant, 2017.
7- Arnaud de Baynast, Jacque Lendrevie, et Julien Lévy, Mercator, Malakoff, Dunod, 12e éd., 2017.
8- Alexandra Bensamoun et Grégoire Loiseau, «L'IA à la mode éthique», D.2017.
9- Andrieu, B. Les avatars du corps. Une hybridation somatechnique. Montréal, Canada: Editions Liber Canada. (2011).
10- Alexandre Plourde, «Retour vers le futur: l'Internet des objets et la protection de la vie privée», Volume 465- Développements récents en droit à la vie privée, JuriBistro eDoctrine, 2019, en ligne: < https://edoctrine.caij.qc.ca/developpements-recents/465/369051330/> (consulté le 12/05/2020).

(ISSN: 2537- 0758)

11- Banque des territoires. Caisse des dépôts (2020). Rapport État des lieux du marché de l'IOT en France avec un focus sur les zones peu denses. (2020). Repéré à https://www.banquedesterritoires.fr/sites/default/files/2021-01/20201109_LesReseauxIOTenZonePeuDense_Vdef_comm.pdf
12- Béa ARRUABARRENA, Objets connectés: penser les enjeux des technologies connectées sous l'angle de la médiation infocommunicationnelle, Vol. 15, N° 2-3 | 2ème semestre 2021- 1er semestre 2022 Objets connectés: enjeux technologiques, enjeux
13- Benghozi, P. J., Bureau, S. et Massit-Folea, F. (2008). L'Internet des objets. Quels enjeux pour les Européens? Paris, France: Éditions de la Maison des sciences de l'homme. Repéré à https://hal.archives-ouvertes.fr/hal-00405070/document
14- Bhöme, R. et Köpsell, S. (2010). Trained to accept? A field experiment on consent dialogs. Proceedings of the SIGCHI Congerence on human factors in computing systems (p. 2403-2406). Association for Computing Machinery. Repéré à https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.182.8938&rep=rep1&type=pdf.
15- Bradley, J., Barbier, J. et Handler, D. (2013). White Paper: Embracing the Internet of everything to capture your share of $14.4 trillion. Cisco, 318.
16- Briard, A. et Faure, M. Ce que l'économie comportementale peut apporter aux juristes: illustrations européennes. Revue Trimestrielle de Droit Européen, 4, (2015).
17- Cambon, L. (2016). Le nudge en prévention… troisième voie ou sortie de route? Santé Publique, 28, (2019).
18- Castets-Renard, C. (2016). Brève analyse du règlement général de la protection des données. Dalloz IP/IT, 7-8, 331-334.
19- Centre de recherche critique sur le droit (CERCRID), Le droit au contact de l'innovation technologique, SaintEtienne, Université Jean Monnet, 1989.

20- Cédric= Renaud Claude Bernard, Nicolas Burger, La synchronisation du droit et de l'innovation. Regard sur les objets connectés, Ecole doctorale de droit de l'Université de Lyon 3; Institut universitaire de France; Institut sur les systèmes complexes, Feb 2017.
21- Cédric Villani, Donner du sens à l'intelligence artificielle: pour une stratégie nationale et européenne, Paris, 28 mars 2018.
22- Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01, 18 décembre 2000.
23- Ch. Gateau, «Objets connectés. Quand la responsabilité du fait des produits défectueux rencontre la protection des données personnelles», Lexisnexis, La semaine juridique, édition générale, n° 12- 19 mars 2018.
24- Cf. G. Viney, P. Jourdain et S. Carval, Traité de droit civil. Les régimes spéciaux et l'assurance de responsabilité, J. Ghestin (sous la dir.), LGDJ, 4e édition, 2017.
25- CJUE, 21 juin 2017, semaine juridique, Ed. gén., 2017, note 908.
26- (CJUE 4 juin 2009, moteurs Leroy Somer, aff. C 285/ 08, D. 2009. 1731, et les obs., note J.-S. Borghetti) ou privés autre que le produit défectueux lui-même (Civ. 1ère, 9 juillet 2003, n° 00 21.163 P: RCA 2003, n° 268)
27- Commissariat à la protection de la vie privée du Canada, «Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'IA», 13 mars, 2020, en ligne: < https://priv.gc.ca/fr/a-propos-ducommissariat/ce-que-nous-faisons/consultations/consultation-ai/pos_ai_202001/> (consulté le 13/07/2020).
28- Conseil d'État, Les rapports du Conseil d'État– Le numérique et les droits fondamentaux, La documentation française, 9 septembre 2014.
29- Cour constitutionnelle fédérale Allemande, 16 février 1983, «BVerfGE»
30- Dagiral, E. Extension chiffrée du domaine de perfectionnement? La place des technologies de quantification

(ISSN: 2537- 0758)

du soi dans les projets d'auto-optimisation des individus. Ethnologie française, 176, (2019)
31- Daniel Le Metayer, Christophe Lazaro, «Le consentement au traitement des données personnelles: une perspective comparative sur l'autonomie du sujet», Revue juridique Themis, 43(3), 768-815, 2015.
32- DEVEZEAUD C., «Objets connectés & Protection des données à caractère personnel: un mariage nécessaire pour la confiance des utilisateurs», dpo-consulting.fr, mis en ligne le 27 mars 2017.
33- Décision rendue au sujet des effets nocifs d'un produits contraceptif oral: Civ. 1ère, 26 septembre 2018, n° 17- 21.271 P: D. 2019.
34- del Río Carral, M., Schweizer, A., Papon, A. et Santiago Delefosse, M. Les objets connectés et applications de santé: étude exploratoire des perceptions, usages (ou non) et contextes d'usage. Pratiques psychologiques.
35- Décret n° 2018-211 du 28 mars 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques; Arrêté du 17 avril 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques
36- Depincé, M. Du consommateur fidèle au consommateur captif: Analyse de droit du marché. Revue Lamy Droit des affaires, 150, (2019). 341-365.
37- DEVEZEAUD C., «Objets connectés & Protection des données à caractère personnel: un mariage nécessaire pour la confiance des utilisateurs», dpo-consulting.fr, mis en ligne le 27 mars 2017< http://www.dpo-consulting.fr/single-post/2017/03/27/Objets-connect%25C3%25A9s-Protection-des-donn%25C3%25A9es-%25C3%25A0-caract%25C3%25A8re-personnel-un-mariage-n%25C3%25A9cessaire-pour-la-confiance-des-utilisateurs>
38- DIANE MULLENEX, Les objets connectés: une législation déconnectée de l'avenir industriel?, 29 AVRIL 2014, https://www-lemondedudroit-fr.translate.goog/decryptages/8744-les-objets-connectes-une-

legislation-deconnectee-de-lavenir-industriel.html?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc

39- Document de la CNIL consultable sur le lien suivant: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf

40- Fabre-Magnan, M. De l'obligation d'information dans les contrats: essai d'une théorie. Paris, France, Librairie générale de droit et de jurisprudence. (1992).

41- Gérard Haas, Amanda Dubarry, Marie D'Auvergne, Rachel Ruimy, «Enjeux et réalités juridiques des Objets Connectés», Dalloz IP/IT 2016, p.394.

42- GALICHET C., «Les grands principes du Règlement européen sur la protection des données personnelles.», village-justice.com, mis en ligne le 23 août 2017, consulté le 9 décembre 2017. https://www.village-justice.com/articles/les-grands-principes-reglement-europeen-sur-protection-des-donnees-personnelles,25684.html

43- Gwenaëlle DONADIEU, Le RGPD et la protection de la vie privée face à l'essor des objets connectés, Vol. 15, N° 2-3 | 2021- 2022.

44- J.-S. Borghetti, «L'accident généré par l'intelligence artificielle autonome», in Le droit civil à l'ère du numérique. Acte du colloque du Master 2 droit privé général et du Laboratoire de droit civil, 21 avril 2017, JCP G 2017, numéro spécial, décembre 2017.

45- Laura Jounda Sonkwa, Responsabilité civile du fait des objets connectés autonomes Master, Droit des assurances Formation en apprentissage RESPONSABILITE CIVILE DU FAIT DES OBJETS CONNECTES AUTONOMES Mémoire de recherche Par Sous la direction de Monsieur le professeur Louis Perdrix Année: 2018– 2019.

46- Laure Marino, «To be or not to be connected: ces objets connectés qui nous espionnent. A propos des téléviseurs LG» Recueil Dalloz Sirey, 09/01/2014.

(ISSN: 2537- 0758)

47- Licoppe, C. Formes de la présence et circulations de l'expérience. Réseaux, 6, 2014).
48- Loi sur la protection des renseignements personnels et les documents électroniques, LPRPDE, LC 2000
49- Luc Bégin, «Légiférer en matière d'éthique: le difficile équilibre entre éthique et déontologie», Éthique publique, Revue internationale d'éthique sociétale et gouvernementale, printemps 2011, vol.13, #1, p. 39-61, en ligne: https://journals.openedition.org/ethiquepublique/361
50- Mady Delvaux, auteure du rapport Delvaux concernant les règles de droit civil sur la robotique.
51- Mac Donald, A. et Cranor, L. (2008). The cost of reading privacy policies. Journal of law and policy for the information society, 4(3), 331-354.
52- Marchand, G. et Dufour, S. (2020). L'influence réciproque de la maison intelligente sur les styles de vie et ses implications sur la fonction d'architecte. *Communication & management*
53- Manon Delaby, L'ENCADREMENT JURIDIQUE DES OBJETS CONNECTÉS: VERS LA POSSIBILITÉ D'UN ENCADREMENT SPÉCIFIQUE, Publié le 26 décembre 2017
54- Mathilde Bondu, Ethique et objets connectés, Maîtrise en droit, Université Laval, Québec, Canada et Université Paris-Saclay Cachan, France Mathilde Bondu, 2020.
55- Mathieu-Fritz, A. et Gaglio, G. (2018). À la recherche des configurations sociotechniques de la télémédecine. *Réseaux*.
56- Mathilde Bondu, Ethique et objets connectés, Maîtrise en droit, Université Laval, Québec, Canada et Université Paris-Saclay Cachan, France Mathilde Bondu, 2020
57- Mekki (M.), Darrois (J.-M.), Gauvain (J.-M.), Se conformer au nouveau droit des contrats: Regards croisés sur les clauses potentiellement excessives, J.C.P. E, No 25, 23 Juin 2016.
58- Metallinos, N. «Unique dans la foule»: l'impossible anonymisation de l'analyse des flux piétons. Communication Commerce électronique, 6, (2016).

59- Ministère des Communications et ministère de la Justice, L'ordinateur et la vie privée: rapport du Groupe d'étude, Information Canada, Ottawa, 1972.
60- Ministère de l'économie et des finances, Marché des objets connectés à destination du grand public, 2018.
61- Myriam, Quéméner Internet, des objets et cybercriminalité et cybersécurité Revue Banque, revue. banque- (19.04.2022.
62- N. Nevejans, Traité de droit de la robotique civile, LEH Edition, Bordeaux 2017, n°135
63- Offre aux utilisateurs finaux et aux applications une architecture de stockage virtuel évolutive en fonction des besoins des applications», https://www.techopedia.com/definition/26535/cloud-storage
64- Pastor, P.-M. L'anonymisation d'une donnée doit rendre l'identification impossible: Conseil d'État 8 février 2017, Actualité Juridique Droit Administratif, (2017).
65- Perray, R. et Uzan-Naulin, J. Existe-t-il encore des données non personnelles? Dalloz IP/IT, 5, (2017), 286-289.Pour quelques illustrations: https://www.francesoir.fr/politique-societe
66- Ph. Brun, Responsabilité civile extracontractuelle, 4ème Edition, LexisNexis, 2016, Paris.
67- Pierre-Jean Benghozi, Sylvain Bureau et Françoise Massit-Folléa, L'internet des objets– Quels enjeux pour l'Europe, Paris, Éditions de la Maison des sciences de l'homme, 2019.
68- Peyroux, E. et Ninot, O. De la «smart city» au numérique généralisé: la géographie urbaine au défi du tournant numérique. L'information géographique, 83(2),. (2019).
69- Simon, PLes leçons apprises des principales études sur les objets connectés en télémédecine. European Research in Telemedicine/La Recherche européenne en télémédecine, 6(2),. (2017).
70- Règlement (UE) n° 2016/679, 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOUE 4 mai, n° L 119, transposé en droit français par

(ISSN: 2537- 0758)

la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.
71- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence"
72- Rogue, F. Capacité et consentement au traitement de données à caractère personnel et au contrat. AJ Contrats, (2019).
73- Roxin, I. et Bouchereau, A., Écosystème de l'Internet des Objets. Dans N. Bouhaï et I. Saleh (dir.), Internet des objets: Évolutions et Innovations. Londres, Royaume-Uni: ISTE Éditions Londres.
74- Radio Canada, "Le Vatican lance un chapelet intelligent pour encourager les jeunes à prier", Radio canada, 18 octobre 2019, en ligne: (consulté le 13/08/2020).
75- Rosenberger, M. E., Buman, M. P., Haskell, W. L., McConnell, M. V. et Carstensen, L. L. (2016). 24 hours of sleep, sedentary behavior, and physical activity with nine wearable. *Medicine and science in sports and exercise*, 48(3).
76- S. BERNHEIM-DESVAUX, «Objets connectés- L'objet connecté sous l'angle du droit des contrats et de la consommation», Contrats Concurrence Consommation n° 1, Janvier 2017.
77- Saleh, I. Les enjeux et les défis de l'Internet des Objets (IdO). Internet des objets, 1(1) (2017).
78- Sadin, E.. *L'humanité augmentée. L'administration numérique du monde*. Montreuil, France: L'Échappée. (2013)
79- Sénat, Résolution européenne sur la régulation des objets connectés et le développement de l'internet des objets en Europe, Session ordinaire-n°106, 22 mai 2018.
80- Stockage et l'accès aux données par l'intermédiaire d'internet plutôt que via le disque dur d'un ordinateur», in Cloud Computing: Définition, avantages et exemples d'utilisation, https://www.lebigdata.fr/definition-cloud-computing
81- Stéphane Grumbach et Stéphane Frénot, «Tribune- Vers un principe de précaution numérique?», Le Monde, 15 avril 2013, en ligne: (consulté le 13/07/2020).

82- Soriano, Préface du livre de F. Forster et A. Bensoussan, Droit des objets connectés et télécom, Bruxelles, Editions Bruylant, 2017.
83- Thebault, P.. La conception à l'ère de l'Internet des Objets: modèles et principes pour le design de produits aux fonctions augmentées par des applications (Thèse de doctorat). Paris, ParisTech. (2013).
84- Thierry Piette-coudol, Les objets connectés: Sécurité juridique et technique dans l'Internet des objets (2e édition), Lexisnexis Actualite 15 Novembre 2023.
85- Xavier Guérin, «Comment La 5G Va Affecter La Gestion Des Données», Forbes, 28 juin 2019, en ligne: < https://www.forbes.fr/technologie/comment-la-5g-va-affecter-votre-strategie-de-gestion-des-donnees/
86- Zhang, Y. L'hégémonie du QR code en Chine. Communication présentée au Congrès de la SFSIC 2020. Repéré à https://sfsic2020.sciencesconf.org/325620/document

المواقع الالكترونية:

- https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431
- http://www.autoguide.com/auto-news/2015/10/volvo-google-and-mercedes-to-accept-responsibility-in-self-driving-car-collisions.html
- Quel cadre pour la responsabilité du fait des objets connectés?, 11 juin 2020, https://www-cabinetderoulez-com.translate.goog/fr/blog/2020/6/10/responsabilite-objets-connectes?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
- Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsable
- Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-

(ISSN: 2537- 0758)

partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsablee

- https://www.lebigdata.fr/google-donnees-geolocalisation-confinement
- Félix GAFFIOT, Dictionnaire latin-français, Paris, Hachette, 1934.
- Voir OCDE, Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data, OCDE et Eurostat, 3e édition, 2005. disponible sur http://www.oecdilibrary.org/science-and-technology/oslo-manual_9789264013100-en
- http://www.autoguide.com/auto-news/2015/10/volvo-google-and-mercedes-to-accept-responsibility-in-self-driving-car-collisions.html
- https://www.pwc.co.uk/issues/megatrends/technological-breakthroughs.html#4
- à https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy.pdf
- http://www.village-justice.com/articles/Objets-connectes-challenge-des,17 html–
- http://www.lesnumeriques.com/objets-connectes-securite-donnees-a1790.html-
- https://www-murielle--cahen-fr.translate.goog/objets-connectes-et-donnees-personnelles/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
- https://www-murielle--cahen-fr.translate.goog/objets-connectes-et-donneespersonnelles/?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc- https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431
- https://www.slideshare.net/slideshow/responsabilit-civile-du-fait-des-objets-connectes-autonomes/234291821

- https://www.maxicours.com/se/cours/les-objets-connectes/.
- Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence Article 53, Obligations for providers of general-purpose AI models.
- https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431
- https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431
- Objets connectés: Définition, bénéfices et astuces pour optimiser leur usage, 1 mai 2023, https://maisonetfinance.fr/smart-home/objets-connectes-definition-avantages-conseils-utiliser/
- Les objets connectés: risques généraux et risques particuliers, https://www.apssis.com/tribune-ssi/88/les-objets-connectes-risques-generaux-et-risques-particuliers.htm
- Les objets connectés d'aujourd'hui: Nouveaux défis de demain, https://www.entreprisesmagazine.com/fr/articles/les-objets-connectes-d-aujourd-hui-nouveaux-defis-de-demain
- https://www.pwc.co.uk/issues/megatrends/technological-breakthroughs.html#4
- https://www.cairn.info/revue-communication-et-management-2020-1-page-53.htm
- CNIL, «Objets connectés: n'oubliez pas de les sécuriser!» (04 décembre 2017), en ligne: < https://www.cnil.fr/fr/objets-connectes-noubliez-pas-de-les-securiser. (consulté 12/05/2020)
- https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i43 62.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_152431
- http://www.village-justice.com/articles/Objets-connectes-challenge-des,17 html

(ISSN: 2537- 0758)

- https://www-assemblee--nationale-fr.translate.goog/14/rap-info/i4362.asp?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc#P586_1524
- https://www.librairiedalloz.fr/livre/9782711039371-les-objets-connectes-securite-juridique-et-technique-dans-l-internet-des-objets-2e-edition-thierry-piette-coudol/
- Objets connectés et consentement de l'utilisateurCycle de Conférences du Club des Partenaires de la Faculté DEG, https://centrejeanbodin-univ--angers-fr.translate.goog/fr/activites/manifestations/manifestations-2019/oc--consentement.html?_x_tr_sl=fr&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc
- Un objet connecté peut-il être responsable? La technologie est faillible,23 juin 2020, https://www.sia-partners.com/fr/publications/publications-de-nos-experts/un-objet-connecte-peut-il-etre-responsable
- https://www.cnil.fr/fr/assistants-vocaux-les-bons-reflexes-pour-les-professionnels