التحديات القانونية المعاصرة لاستخدامات «إنترنت الأشياء»: دراسة في النظام القانوني الإماراتي والمقارن(*)

د. بشار طلال المومني
أستاذ القانون المدني المشارك
قسم القانون الخاص
كلية الشريعة والقانون
جامعة خور فكان، الشارقة، الإمارات

د. معمر بن طرية
أستاذ القانون المدني المساعد
قسم القانون الخاص
كلية القانون
جامعة الشارقة، الإمارات

الملخص

يتناول هذا البحث – بالدراسة – موضوع إنترنت الأشياء من جانب قانوني، باعتباره من موضوعات الساعة؛ في ظل التطور المتسارع لتكنولوجيات الرقمنة، وما رافقه من تغيير في نمط العيش والعمل، والذي أدى – من دون شك – إلى تعاظم المخاطر الناشئة عن استخدام هذه التكنولوجيا، وما يشكّله من مساسٍ بالبيانات الشخصية للأفراد، وبالحق في الخصوصية. وهذه المبررات قد تحول دونَ كسب ثقة المُسْتَخْدِم بخدمات «إنترنت الأشياء» في قادم السنوات.

وتبحث هذه الدراسة في إشكالٍ جوهري قلت – إلى حد الساعة – محاولات الفقه العربي في الإحاطة به، وهو مدى كفاية القواعد المدنية المقرَّرة في مجال حماية البيانات الشخصية والخصوصية، أو حماية مصالح المستهلكين بوجه عام، لإقرار الحماية الكافية من مخاطر استخدامات «إنترنت الأشياء»، في ظل الفكر الجديد الذي جاءت به؛ لتكون هذه الدراسة نواةً أولى تحتاج إلى إضافات وتعقيبات أخرى مستقبلاً.

وتأتي أهمية البحث – في هذا الموضوع – في ظل الاستجابات التي أبانت عنها بعض التشريعات المقارنة لعدم كفاية التشريعات والإطار القانوني الحالي لتحقيق الحماية القانونية المنشودة من مخاطر استخدامات «إنترنت الأشياء»، في ظل التطور التكنولوجي، الأمر الذي دفع السلطات العامة في بعض الدول إلى سن قوانين خاصة لضمان أمن هذه التكنولوجيا، وأهمها النظام الأمريكي والتشريع الأوروبي، والتصرف بعقلانية، وعدم إطلاق العنان للشركات المصنِّعة لهذه التكنولوجيا من دون رقابة كافية، من خلال وضع خطة متوازنة لإيجاد سبل تأطير استخدامات هذه التكنولوجيا المعلوماتية الحديثة. وقد

(*) تم تقديمه للنشر في: 14 مارس 2022 تم قبوله للنشر في: 27 أبريل 2022

عمل المُشَرِّع الإماراتي على الاستفادة من هذه الخطوات، بسن أول سياسة تنظيمية لخدمات «إنترنت الأشياء» في دولة عربية، وذلك في سنة 2018، كما أقرَّ قانونًا خاصًا بحماية البيانات الشخصية للأفراد سنة 2021.

وقد خَلُصَ البحث إلى جملة من النتائج والتوصيات أوصى بها الباحثان، لعلها تفيد منظومتنا القانونية العربية في ضرورة العمل على عقد اتفاقيات عربية تنظم استخدامات «إنترنت الأشياء»، في ظل الذكاء الاصطناعي، والحرص على تشديد التزامات الشركات المُصنِّعة والمصمِّمة لها، للحد من حجم التهديدات التي تحملها هذه الأجهزة المتصلة بالإنترنت، مثل قرصنة بياناتهم الشخصية بصفة سرية، أو تسويقها من دون علمهم الكافي، أو من دون دراية بما سيؤول إليه تداولها مستقبلًا.

كلمات دالة: الذكاء الاصطناعي، والأجهزة المُتصلِة، والحق في الخصوصية، والبيانات الشخصية، وتوقعات المستهلكين.

المقدمة

أولًا: موضوع الدراسة

الثورة التكنولوجية الجديدة لـ «إنترنت الأشياء» Internet of Things، أو كما يحلو للبعض تسميتها «الأشياء المُتصلة» Connected Things تارة، أو «الأجهزة المُتصلة» Connected Devices تارة أخرى، هي تعابير جرى استخدامها اليوم في قاموسنا الفني، أو حتى القانوني؛ للتدليل على ظاهرة تجهيز بعض الأشياء واسعة الاستخدام في مجتمعاتنا، بأنظمة استشعار، مثل: المركبات، والساعات، والنظارات... وغيرها؛ مما يتيح لها إمكان جمع البيانات المتعلقة بسلوك مُسْتَخْدِميها، أو بيئتهم (على سبيل المثال: درجة الحرارة، ومستوى الصوت، وظروف حركة المرور... إلخ)، ثم إرسالها إلى المُشغِّل؛ متمثلة إما في الشركة المُصنِّعة للشيء، أو مُشغِّل الشبكة التي تتصل بها هذه الكيانات، ليصبحَ في إمكانها التفاعل – بصفة ذكية وتلقائية – مع محيطها الخارجي[1].

لقد جرى استخدام تعابير، في قاموسنا الفني والقانوني، تتعلق بالثورة التكنولوجية الجديدة؛ حيث زاد الاهتمام القانوني بموضوع الذكاء الاصطناعي، وتطبيقاته المختلفة، مثل: الطائرات، والسيارات ذاتية القيادة، والروبوت الآلي، خاصة في ظل جائحة كورونا، والأعمال من بعد، والتسارع الهائل في التكنولوجيا. ورافق ذلك كثير من الاستخدامات والمخاطر الناتجة عن إنترنت الأشياء التي تمس الحياة الخاصة، أو الحق في الخصوصية، والمسؤولية القانونية، وآليات التعويض، والتنظيم القانوني المأمول لهذه التقنية الجديدة، وهو ما شكَّل تحديًّا واضحًا للمنظومة القانونية. وارتبط موضوع إنترنت الأشياء بضرورة احترام حقوق الإنسان، والسعي لتحقيق الحماية التقنية والقانونية المنشودة؛ في ظل الاعتداءات المتكررة على خصوصية الأشخاص، من خلال اختراق بياناتهم الشخصية، وإمكان استخدامها وتداولها، والرقابة والتجسس على الشبكة العالمية.

ثانيًا: أهمية الدراسة

لم يحظ موضوع إنترنت الأشياء بالعناية الكافية والمنشودة في ظل غياب التنظيم التشريعي لهذه التقنية في الدول العربية، والبدء في استخدامها من خلال الشركات والعقود الخاصة بين طالب الخدمة، والشركة المقدمة لها؛ الأمر الذي يبرز الحاجة الماسة إلى هذه الدراسة وغيرها؛ لمناقشة الموضوع بكل جوانبه المتعددة.

(1) Matthieu Bourgeois et Marion Moine, Internet des objets (IOT): Quand l'inerte s'anime, Revue pratique de la prospective et de l'innovation, Commission Prospective du Conseil national des barreaux and LexisNexis, Paris, N°2, oct. 2019, p.34.

وفي الواقع فإن ما أثار فضولنا، لدراسة هذا الموضوع، هو الاهتمام اللافت لدولة الإمارات العربية المتحدة بتطوير خدمات الذكاء الاصطناعي وإنترنت الأشياء، ومثل هذا الاهتمام تجسَّد في الواقع التشريعي بصدور أول تنظيم لخدمات إنترنت الأشياء في دولةٍ عربية سنة 2018، متمثلة في السياسة التنظيمية لخدمات إنترنت الأشياء التي سنتها هيئة تنظيم الاتصالات في دولة الإمارات العربية المتحدة سنة 2018م، كما تُوِّج هذا الاهتمام بتعديل وتحديث قانون حماية المستهلك الإماراتي الاتحادي رقم 15 لسنة 2020م، ثم بصدور القانون الاتحادي الإماراتي رقم 45 لسنة 2021م، بشأن حماية البيانات الشخصية.

كما استلهمنا – في هذه الدراسة – الحلول التي توصلت إليها تشريعات رائدة في هذا المجال، على رأسها التشريعات الأمريكية التي شهدت، منذ عامين، دخول أول قانون منظِّم للأمن السيبراني لخدمات إنترنت الأشياء (الذي يحمل رقم SB–327، والصادر في أغسطس 2018) حيز النفاذ، وذلك في يناير 2020[2]، بالإضافة إلى القانون الأمريكي لولاية إيلينوي الأمريكية لسنة 2015، باعتباره أحد أهم التشريعات، والذي أولى عناية خاصة بحماية البيانات البيوميترية للمُسْتَخْدِم، في إطار إنترنت الأشياء، وعُرِف بقانون BIPA[3].

كما حللنا – كذلك – الأحكام المقرَّرة في التوجيه الصادر عن الاتحاد الأوروبي رقم 2016–679، والمؤرخ في 27 أبريل 2016، بشأن حماية البيانات الشخصية[4]. وكذا المبادئ العامة التي أسس عليها التشريع الأسترالي الحق في الخصوصية، بموجب قانون حماية الخصوصية Australian Privacy Act لسنة 1988 المُعدَّل والمُتمِّم[5].

ثالثًا: أهداف الدراسة

تهدف دراسة هذا الموضوع إلى وضع نواة أولية لأبحاث مستقبلية؛ تقدّم تصورًا واضحًا لخصوصية استخدامات إنترنت الأشياء، والمخاطر الحالية والمستقبلية تقنيًا وقانونيًا، والتنظيم القانوني المأمول لها، سعيًا إلى مواجهة تحدٍّ جديد لمنظومتنا القانونية، والمساهمة في تحقيق حماية قانونية من أضرارها قبل حدوثها لمُسْتَخْدِمي

(2) Senate Bill No. 327, Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018. https://leginfo.legislature.ca.gov/faces/billPdf.xhtml?bill_id=201720180SB327&version=20170SB32791CHP, Last Accessed on: 05.02.2022.

(3) 740 ILCS 14/ Biometric Information Privacy Act. (ilga.gov)

(4) Règlement de UE n°2016-679 du 27 avril 2016 art. 25.

(5) Australian Privacy Act no 119 of 1988, 14 Dec. 1988. Privacy Act 1988 (legislation.gov.au), Last Accessed on: 05.02.2022.

هذه التقنية المتقدمة، ومشكلاتها الفعلية، مع الاستفادة من التجارب الغربية بهذا الشأن، الأوروبية منها والأمريكية.

رابعًا: إشكالية الدراسة

في ضوء ما سبق يجدر بنا التساؤل عن المخاطر والتحديات الناتجة عن استخدام إنترنت الأشياء، من خلال الإجابة عن إشكالية جوهرية ذات شقين: ما السبل القانونية التي لا بد من تجهيزها لتأطير محاذير استخدام هذه التكنولوجيا والحد منها؟ وإلى أي مدى باتت القواعد المقررة في التشريعات المدنية الخاصة تكفي لحماية البيانات الشخصية، وإقرار حق الفرد في الحماية من مخاطر خدمات إنترنت الأشياء؟

ويتفرع عن الإشكالية السابقة تساؤلات فرعية، يجدر الوقوف عندها، وتتمثل في التالي:

1- ما الجديد الذي أتت به تكنولوجيا إنترنت الأشياء على الصعيد الفني والقانوني مقارنة ببقية التكنولوجيات المعلوماتية؟

2- ما أشكال الانتهاكات التي تتسبب فيها الأشياء المتصلة بحقوق مُسْتَخْدِميها؟

3- هل ثمة إجابات شافية وكافية في منظومتنا القانونية العربية حاليًا، للحد من مآرب ومخاطر استخدام إنترنت الأشياء؟

4- هل يكفي حاليًا التعويل على ما ورد من حماية في القواعد العامة، دستوريًا ومدنيًا، لتوفير الحماية الكافية من جراء الانتهاكات التي تسببها إنترنت الأشياء بحق الخصوصية وحرمة الحياة الخاصة؟

5- ما الحلول التي توفرها القوانين الرائدة في هذا المجال اليوم، من أطر نظرية وتدابير عملية، للتحكم في مخاطر استخدام الأشياء المتصلة، خاصة في مجال حماية الخصوصية، والتعويض عن أضرار الأشياء المتصلة، في حال عدم استجابتها للرغبات المشروعة للمستهلك؟

خامسًا: منهجية الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي والمقارن، والاستقرائي، من خلال إعطاء رؤية وتصور واضحين عن موضوع إنترنت الأشياء: مفهومه وتطوره، وتمييزه عن غيره، وأبعاده وتحدياته، استنادًا إلى المعلومات والحقائق التي تمّ الرجوع إليها، وواقع هذا الموضوع، وصولًا إلى حقيقة معيَّنة، بالتركيز على القانون الإماراتي، مقارنة

بالتشريعات الغربية، بما يخدم الموضوع، والانتقال من الجزء إلى الكل بالرجوع إلى النصوص القانونية، والأحكام القضائية، والأبحاث والآراء الفقهية المختلفة، لوضع تصور عام للموضوع مع إعطاء الرأي الشخصي في موضعه المناسب.

سادسًا: خطة الدراسة

وقد عملنا على تقسيم خطة الدراسة إلى مبحثين: تناولنا في المبحث الأول الرهانات القانونية لاستخدامات إنترنت الأشياء في ظل الذكاء الاصطناعي، وتناولنا في المبحث الثاني التنظيم القانوني المأمول لاستخدامات إنترنت الأشياء، وذلك على النحو الآتي:

المبحث الأول

الرهانات القانونية لخدمات «إنترنت الأشياء»

في ظل الذكاء الاصطناعي

تعد الإنترنت وسيلة إلكترونية لها مزايا عديدة، مثل اختصار الوقت، والكلفة الزهيدة، والسرعة في إبرام المعاملات المدنية والتجارية، كما أنها تعد وسيلة أساسية يعتمد عليها المستهلك في الوصول إلى السلعة أو الخدمة التي يسعى إلى الحصول عليها، إضافة إلى سهولة البحث والاختيار للسلعة أو الخدمة المطلوبة.

لكن في المقابل فإن لها سلبيات لا أحد يستطيع إنكارها، تتمثل في الاعتداء غير المشروع على معاملاتنا المدنية والتجارية، وفي اختراق خصوصية الأشخاص وبياناتهم الخاصة، إضافة إلى تعقب المواقع عند استخدام الشبكة العالمية.

ولعرض الرهانات التي يثيرها استخدام هذه التكنولوجيا الحديثة والمُغيِّرة لواقعنا الحالي، تستدعي الدراسة الوقوف عند المفهوم الاصطلاحي والفني الدقيق لإنترنت الأشياء، والتدقيق في ارتباطاتها مع مفهوم الذكاء الاصطناعي (المطلب الأول)، ثم طرح خصوصية استخدامات إنترنت الأشياء من خلال البحث في تطور السلوك البشري من رقابة الشخص العادي إلى ذاتية الشيء في السلوك الآلي، والتَّعلُّم الآلي واتخاذ القرار من الآلة بشكل ذاتي (المطلب الثاني)، وما يرافق ذلك من مخاطر تمس الخصوصية التي يحتاج إليها الإنسان، ويسعى إلى المحافظة عليها، من دون اعتداء على بياناته الخاصة (المطلب الثالث).

المطلب الأول

الإطار المفاهيمي لـ «إنترنت الأشياء»

وعلاقته بالذكاء الاصطناعي

ثمة أخطاء شائعة عديدة يتم تداولها من قبل العامة بشأن مفهوم «إنترنت الأشياء»، فهناك من يعتقد أن هذه التكنولوجيا المعلوماتية تعمد فقط إلى توصيل الأشياء بأجهزة الاستشعار لجمع المعلومات وتخزينها، بينما يقع البعض في خلط بين الحدود التي تفصل بين خدمات إنترنت الأشياء، والحلول التي توفرها نظم الذكاء الاصطناعي.

من هذا المنطلق، سنتتبع مسار تطور ملامح مفهوم «إنترنت الأشياء»، ودراسة تركيبتها وأنواعها (الفرع الأول)، وثم نبحث في الارتباطات التي يشهدها إنترنت الأشياء مع نظم الذكاء الاصطناعي (الفرع الثاني).

الفرع الأول

مسار تطور مفهوم «إنترنت الأشياء»

وتركيبتها وأنواعها

بدأ مصطلح «إنترنت الأشياء» يرتسم ويشيع تداوله على لسان عوام الناس – على نحو واسع وكبير – خلال السنوات الماضية، وذلك في ظل الاهتمام المتنامي من المختصين في هذا المجال، والترقبات والإحصائيات المذهلة في المجال نفسه؛ فثمة أرقام تفيد بأنه في عام 2021 تم توصيل 50 مليار كائن أو شيء بشبكة الإنترنت، بقيمة سوقية تبلغ 19 ألف مليار دولار. ومن جانبه أقرَّ شاك روبينس Chuck Robbins المدير العام لشركة سيسكو Cisco[6]، المتخصصة في تسويق خدمات «إنترنت الأشياء»، بأن التحول الثوري الذي تعيشه مجتمعاتنا حاليًا، وحمى انتشار خدمات «إنترنت الأشياء»، سيكون تأثيرهما أكثر حدّةً وخطورة من تلكما اللتين شهدتهما مجتمعاتنا عند ظهور أول موجة من الإنترنت[7].

وفي العام 2019 رفعت دولة الإمارات العربية المتحدة ميزانية إنفاقها على تقنيات وحلول إنترنت الأشياء إلى نحو 38,2 مليار درهم، ومن المتوقع أن تبلغ هذه الميزانية في هذا العام (2023) نحو 14,5 مليار درهم، وفق دراسة لمؤسسة الأبحاث والاستشارات التكنولوجية العالمية (IDC)؛ والتي أشارت أيضًا أن الإمارات والمملكة العربية السعودية تتصدران عربيًا حجم الإنفاق على صناعة إنترنت الأشياء[8].

---

(6) سيسكو هي الشركة العالمية الأولى في تقديم خدمات «إنترنت الأشياء»، واشتهرت بشعار ربط كل شيء بشبكة الإنترنت؛ لتقديم حلول لقطاع الأعمال في مجال خدمات البث التلفزيوني، والنقل بربطها بإنترنت الأشياء؛ للمزيد راجع المقال التالي: بتول عتوم، من سيتحكم في إنترنت الأشياء، 24 يونيو 2020: من سيتحكم في إنترنت الأشياء؟، منشور على موقع إي عربي– e3arabi على الرابط التالي: https://e3arabi.com/technology/، تاريخ الزيارة: 20/2/2022.

(7) Jean- Paul Crenn, Les objets connectés décryptée pour les juristes, Revue Dalloz IP/IT, Paris, Sept. 2018, p.389.

(8) يوسف العربي، 2.4 مليار درهم الإنفاق على إنترنت الأشياء في الإمارات العربية المتحدة خلال 2019، جريدة الاتحاد، 17 أغسطس 2019، متاح على الموقع التالي: alittihad.ae، تاريخ الزيارة: 18/2/2022.

ومع ذلك فإن هناك كثيرًا من عوام الناس لهم تصور يُجانب حقيقة تكنولوجيا إنترنت الأشياء، ويُسيئون فهم هذا المصطلح بمعناه الفني الدقيق. وإذا كانت تكنولوجيا إنترنت الأشياء تقوم على أساس ربط، أو توصيل، أشياء وكائنات بشبكة الإنترنت؛ للتحكم فيها والسيطرة عليها، فإن حقيقية التحديات الفنية والاقتصادية والقانونية التي تثيرها هذه التكنولوجيا لا تتمثل في الكائنات، أو الأشياء المُتصلة بشبكة الإنترنت، بقدر ما هي مرتبطة بالبيانات والمعطيات المُسْتَخْدَمة من طرف هذه الكيانات، فهذه الأخيرة هي «الأشجار التي تخفي الغابة وراءها»[9].

وقد كان للعالم البريطاني أشتون كيفين Ashton Kevin، مؤسس مركز أوتو آيدي التابع لمعهد ماساتشوستس للتكنولوجيا، السبق في استخدام مصطلح «إنترنت الأشياء»، وذلك في عام 1999، في إطار تقديمه هذه التكنولوجيا لشركة بروكتر آند جامبل Procter and Gamble Co.[10].

وقد قدَّم هذا العالم إنترنت الأشياء على أنها بمنزلة شبكة من «العينين والأذنين» يجري توصيلها بأجهزة الكمبيوتر[11]، ولكن هذا التشبيه لا يعني البتة أنها تقتصر على توصيل الأشياء بأجهزة استشعار ترسل المعلومات وتستقبلها عبر الإنترنت؛ فحقيقة الأمر تبدو أكثر تعقيدًا بسبب اتصالها بشبكة الإنترنت[12]؛ فالغاية من توصيل الأشياء بشبكة الإنترنت هي تزويدها بالقدرة على تجميع المعلومات المُنبعثة من الشبكة؛ لجعلها أكثر ثراءً، وإعطائها القدرة على مشاركة المعلومات، واتخاذ القرارات، وتنفيذ المهام، عن طريق الإنترنت؛ من أجل تحويل هذه الأشياء من أشياء تقليدية إلى أشياء ذكية، تحاكي التصرفات والذكاء الإنساني[13].

وتجدر الإشارة إلى أن اتخاذ القرارات، في إطار الأشياء المتصلة، يتم عن طريق التدخل البشري، أو عن طريق البرمجيات الحاسوبية التي تُوجَد بداخل هذه الأشياء التي شاركت المعلومات، إما بواسطة أشياء أخرى، وإما بواسطة برمجيات تُوجَد داخل سحابة الحوسبة السحابية المخصصة لإنترنت الأشياء Cloud of IoT[14].

(9) John Fruehe, The Internet of things is about Data, not Things, Fobes, 30 June 2018, Last Accessed on: 20.02.2022.

(10) Imad Saleh, Internet des Objets (IdO): Concepts, Enjeux, Défis et Perspectives, Revue Internet des objets, ISTE Open Science, London, UK, 2017, 1, p.3.

(11) مارية الحصين، نظام تشريعي مقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية: دراسة استشرافية، مجلة الدولية للمعلوماتية والإعلام وتكنولوجيا الاتصال، جامعة بني سويف، مصر، مج3، ع2، السنة2021، ص30 و31.

(12) Jean- Paul Crenn, op. cit., p.389.

(13) مارية الحصين، مرجع سابق، ص31.

(14) Jean- Paul Crenn, op. cit., p.389.

أولًا: التركيبة الهرمية لـ «إنترنت الأشياء»

يمكن وصف مكونات «إنترنت الأشياء» بأنها على شكل هرمين تتدرج من خلالهما قدرات إنترنت الأشياء، بالنظر إلى الخاصيات التي يتم تزويدها بها، وتنقسم هذه المكونات إلى أربعة أنواع، هي كالآتي[15]:

أ- أجهزة الاستشعار:

هي المُكوّن الأول لإنترنت الأشياء، ويُمكنها التقاط معلومات من العالم الخارجي، مثل: درجة الحرارة، أو الضغط، أو السرعة، والاتجاه... وما إلى ذلك، وقد يتم ذلك من خلال التحاور عبر سحابة الأشياء. ويتم تزويد الأشياء بهذه الأجهزة بالعمل المشترك بين الشركات المُصنِّعة لأجهزة الاستشعار، والشركات المُصنِّعة لإنترنت الأشياء[16].

ب- إدماج البيانات:

وتأتي هذه المرحلة بمجرد التقاط البيانات الدقيقة والموثوقة بواسطة أجهزة الاستشعار؛ فالأمر يتعلق بتجميع البيانات المُلْتَقطَة، سواء بداخل الشيء ذاته، أو في موْضّع آخر، كما في السحابة المخصَّصة لذلك، لدمجها وتجميعها؛ وفي هذه المرحلة يكون في مقدور الأشياء المتصلة دمج البيانات المُخَزَّنَة بها مع بيانات أخرى، علمًا بأن ذكاء إنترنت الأشياء، على النحو سالف الذكر، مرهون بتعايشها وتفاعلها مع أشياء أخرى متصلة في إطار بيئة متكاملة، تُقارَن فيها بيانات كل الأشياء فيما بينها؛ لمدِّها بذكاء أكثر، ومحاكاة العالم الخارجي، وتوفير مستويات من التطور ترقى لتوقعات مُسْتَخْدِميها[17].

ج- تحليل الأشياء:

أو ما يدعى أيضًا «تحليلات الأشياء» Analytics of Things؛ ففي هذه المرحلة يجري تحويل، وإعادة تحوير المعلومات الأولية المُلْتَقطَة إلى معلومات مطورة؛ للسماح لاحقًا باتخاذ القرار والعمل؛ فالتحدي الذي تواجهه الأشياء – في إطار هذه العملية – هو تحدي التعامل مع البيانات الضخمة وفق نهجٍ جديد لمُعَالَجتها واستغلالها بشكل سليم[18].

(15) Ibid.

(16) Terrell MC Sweeny, Consumer Protection in the Age of Connected Everything, Exploring the Things in the Internet of Things: Implications For Business, Consumers, and the Law, Volume 62, Issue 2, Jan. 2018, p.212.

(17) Terrell MC Sweeny, op. cit., p.233.

(18) Jean- Paul Crenn, op. cit., p.392.

د- السلوك الإدراكي:

وهو المستوى الأخير من الهرم؛ ويعتبر بمنزلة ردة الفعل الانعكاسية للشيء؛ فالمطلوب من الأشياء المتصلة هنا أن تحاكي ما يتولاه البشر أو الآلات من تغيير سلوكياتهم استجابةً للبيانات المتحصل عليها، وتحليلات موثوقة. وتعتبر هذه الخطوة التحدي الأصعب، فهو تتطلب الدقة في اتخاذ القرارات، وتتطلب هذه المرحلة – في أغلب الأحيان – تدخل الذكاء الاصطناعي؛ لذلك فإن الإدراكية لإنترنت الأشياء تتفاوت تفاوتًا ملموسًا بالنظر إلى مستويات التقدُّم المُزَوَّدة بها هذه الأشياء، فليست كل الأشياء المتصلة بالإنترنت على درجة واحدة من التطور والتفاعل مع العالم الخارجي؛ فهذا مرهون بمدى استقلاليتها وذكائها في اتخاذ القرارات.

ثانيًا: مستويات تطور «إنترنت الأشياء»

وفقًا للتركيبة الهرمية لإنترنت الأشياء المشار إليها آنفًا، تتدرج مستويات الأشياء إلى أربعة مستويات تكاملية؛ أعلاها مستوى «الاستقلالية» أو الذاتية، يليها مستوى «تحسين القدرات»، وكلاهما مرتبطان بمرحلتي «التحكم»، و«رصد البيانات».

أ- مستوى رصد البيانات (Monitoring):

خلال هذه المرحلة تسهر أجهزة الاستشعار المُزَوَّد بها الشيء المتصل لالتقاط بيانات من العالم الخارجي المحيط بالشيء، ويستجيب بناءً عليها لمراقبة سلوكات الإنسان، ويمكن أن نضرب مثالًا على هذا النوع من إنترنت الأشياء بمضرب التنس بابولا Babolat tennis racket، الذي يقيس سرعة تأثير الكرة على مضرب التنس، مباشرة على السوار الذي يرتديه الرياضي على معصمه، فيقوم هذا السوار بتقييم الضربات، ويسجل مدة وعدد التبادلات بين المتنافسين، ثم تصبح جميع هذه البيانات متاحة على الهاتف الذكي، وما يميز هذه التكنولوجيا أنها لا تتمتع بذكاء كبير، بل إن دورها ينحصر في وظيفة المراقبة، وذلك بالنظر إلى اتصالها النسبي مع الإنترنت[19].

ب- مستوى التحكُّم (Control):

وفي هذا المستوى ترتفع قدرات الشيء المُتصّل؛ بحيث يكون في استطاعته الاستجابة والتحكّم في التجربة الشخصية للمستهلك، والتفاعل بطريقة أذكى من سابقتها، وهذه التجربة يمكن اكتشافها من خلال الجهاز الذكي المخصَّص للتحكم في النباتات المعروفة بـ«الباروت فلاور باور» Parrot flower power، وهو جهاز يقوم بتخزين كمية من المياه

(19) Jean- Paul Crenn, op. Cit., p.392.

قد تصل إلى 2.2 لتر، فيتيح للمُسْتَخْدِم مراقبة حاجيات النبتة بفضل أجهزة الاستشعار التي تتلمس معدلات رطوبة الأرض والأسمدة ودرجة حرارة الهواء، ويسهر على تقطير وسقي الماء وفقًا للاحتياجات الخاصة بالنبتة. ويُمكِّن المُسْتَخْدِم من استشعار جميع البيانات المُلْتَقطَة، وتوجيه نصائح للاعتناء بحياة النبتة عبر تطبيق متوفر على الهواتف النقالة[20].

ج- مستوى تحسين القدرات (Optimization):

وتشهد قدرات الشيء، خلال هذه المرحلة، تحسينات معتبرة، مقارنة بالمرحلتين السابقتين، فتتيح الخوارزميات تحسين استخدامات المُنْتَج بالاستعانة بخاصية الصيانة التنبؤية، والتحكم والإصلاح من بعد. وتعتبر السيارات ذات المحركات الكهربائية للشركة الأمريكية TESLA، مثالًا على الأشياء المتصلة التي تسمح بتحسين استخدام وصيانة السيارة[21].

د- مستوى الاستقلالية (الذاتية) Autonomy:

وخلال هذه المرحلة يتمتع الشيء بالاستقلالية وذاتية التصرف؛ فيستجيب ويأخذ بيئته في الاعتبار، ويتفاعل مع الأشياء الأخرى المتصلة، ويُزوَّد بخاصية التَّعلُّم والتحسن الذاتي، وقد يصل إلى مستوى الصيانة والإصلاح الذاتي. وتعتبر المركبة ذاتية القيادة لشركة جوجل Google Car مثالًا لإنترنت الأشياء التي ترقى إلى هذا المستوى من الذكاء والاستقلالية[22].

الفرع الثاني

علاقة «إنترنت الأشياء» بالذكاء الاصطناعي

كما سبقت الإشارة، فإن مستويات إنترنت الأشياء، بمفهومها الواسع، تتفاوت باختلاف القدرات التي تزود بها هذه الأشياء؛ من أجهزة الاستشعار، والمُشَغِّلات، وأدوات تخزين البيانات، وقدرات مُعَالَجَة البيانات المترابطة عبر الإنترنت؛ لذلك ففي مرحلتي رصد البيانات، وتحليلها ومُعَالَجَتها، وهما المستويان الأول والثاني لإنترنت

(20) The Parrot Flower Power user guide, Parrot S.A, flower-power_user-guide_uk.pdf (pa - rot.com) (19.02.2022).

(21) Yaël Cohen-Hadria, Le véhicule connecté: Un objet connecté comme les autres? Revue Dalloz IP/IT, Paris, Mars 2018, p.179.

(22) Ibid. p.393.

الأشياء، يمكن لأي جهاز مُزَوَّد بإنترنت الأشياء أن يشعر بمحيطه، ويرصد وينقل ويُخزن البيانات المُلْتَقطَة ويشتغل وفقًا لها؛ لكن المستويين اللذين يتطلبان قدرات أعلى هما تحليل الأشياء Analytics of things، واتخاذ السلوك الإدراكي Cognitive action الموائم، ويتم تحديد مدى الذكاء الحقيقي لخدمة إنترنت الأشياء من خلال هاتين الخاصيتين.

ويتأتى من ذلك أن نظام إنترنت الأشياء غير الذكي ستكون له قدرات محدودة؛ لذلك فإن توطيد قدرات نظام إنترنت الأشياء، باستخدام الذكاء الاصطناعي، سيخدم الهدف الرئيسي لهذا النظام، وهو تحقيق مستوى الأتمتة والتكيُّف مع المحيط الخارجي.

وتشهد السوق العالمية حاليًا طرح بعض المنتجات المُزَوَّدة بخدمات إنترنت الأشياء، والتي تشتغل بوظائف الذكاء الاصطناعي، ويمكن إعطاء بعض الأمثلة عن هذه الخدمات التي توفرها شركات عالمية متخصصة، كالتالي[23]:

1- أجهزة الاستشعار الصوتي Voice Assistants:

هناك بعض البرمجيات الصوتية التي تشتغل باستخدام سحابة الحوسبة السحابية Cloud، لتأدية مهام المساعدات الذكية للإجابة عن استفسارات المُسْتَخْدِمين، أو إجراء بعض الخدمات المتخصصة، مثل: الحجز في الفنادق والمطاعم، وتشغيل الموسيقى، والتحكم في بعض الخدمات بناءً على أوامر صوتية، ومن أبرزها: تطبيق أليكسا Alexa الذي تم تسويقه من شركة أمازون لتحسين خدمات البيع الإلكتروني وتشخيص رغبات المُسْتَخْدِمين. وهناك أيضا تطبيق سيري لشركة أبل Siri وكذلك التطبيق الصوتي المساعد لشركة جوجل Google assistant.

ب - الروبوتات Robots:

ظهرت في الآونة الأخيرة بعض الأجهزة الذكية التي تحاكي بعض قدرات البشر، في الفهم والاستيعاب وتقليد الأحاسيس، وهذه الروبوتات هي عبارة عن إنترنت للأشياء في ذاتها، لأنها تحتوي على أجهزة ومُشَغِّلات للاستشعار، تشتغل مع الذكاء الاصطناعي؛ لتطوير قدراتها في التَّعلُّم والتكيُّف مع البيئة الخارجية، ويمكن إعطاء بعض المنتجات المشابهة لهذه الأشياء والروبوتات الذكية، مثل: الروبوت بيبر لشركة سوفت بنك روبوتيكس Pepper [24]، وهو روبوت مصمم على شكل إنسان، ويوصف

(23) Ashish Ghosh and Debasrita Chakraborty and Anwesha Law, Artificial Intelligence in Internet of Things, IET Research Journals, The Institution of Engineering and Technology 2015, pp. 4-5.

(24) Ashish Ghosh and Debasrita Chakraborty and Anwesha Law, op. cit., p.7.

بأنه رفيق بشري يمكنه التفاعل مع البشر، وفي إمكانه استيعاب وفهم مشاعر الإنسان، من خلال تعبيرات الوجه، وحركة الجسم، ونبرة الصوت، وتبادل الكلام معه.

جـ- الأجهزة الذكية Smart Devices:

وهي عبارة عن أشياء وأجهزة ذكية مُزَوَّدَة بخاصيات الذكاء الاصطناعي المساعدة للبشر في أداء بعض المهام، وتشتغل عن طريق أدوات التعرف على بصمات الوجه، أو نبرة الصوت، أو بصمة العينين؛ لتشخيص الرغبات الشخصية للمُسْتَخْدِم، ومن أبرز هذه الأجهزة الذكية الفرن الذكي المُسوَّق من شركة جون[25] Smart oven by June، وهو عبارة عن جهاز يسهر على الطهي الذاتي للطعام، باستخدام كاميرات عالية الدقة، ومقياس للحرارة؛ مما يساعده على مراقبة الطعام الذي يتم طهيه بشكل ذاتي من طرف الفرن، كما يتم تشغيل هذا الفرن باستخدام تطبيق أليكسا الصوتي، لتشخيص الخدمة وتحديد الرغبات الشخصية للمُسْتَخْدِم في تقديم خدمة الطهي[26].

وحسنًا فعل المُشَرِّع الإماراتي، من خلال وقوفه عند المفهوم الدقيق والسليم لإنترنت الأشياء، عند سن سياسته التنظيمية لخدمات إنترنت الأشياء[27]، بحيث أقر، في البند 9,1 من هذه السياسة، بأن المقصود من إنترنت الأشياء «هو أي بنية تحتية عالمية لمجتمع المعلومات تُمكِّن الخدمات المتقدمة، من خلال ربط الأشياء (ماديًّا أو افتراضيًّا) المرتكزة على تقنيات المعلومات والاتصال الحالية والمتطورة»[28].

(25) June Smart Oven Reviews | June Oven (20.02.2022).

(26) Ashish Ghosh and Debasrita Chakraborty and Anwesha Law, p.6.

(27) السياسة التنظيمية لخدمات إنترنت الأشياء، الإصدار 1، الهيئة العامة لتنظيم قطاع الاتصالات، الإمارات، 22 مارس 2018.

(28) وهو التعريف نفسه الذي أعطاه الاتحاد الدولي للاتصالات (ITU) سنة 2012، في البند 3.2.2 من توصيتها رقم Y 2060 حول رؤيتها العامة عن إنترنت الأشياء فعرَّفتها بأنها:

«A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies». Overview of the Internet of things, Recommendation ITU-T Y.2060, 2012. https://academy.itu.int/sites/default/files/media/file/IoT%20TP%20Report.pdf#:~:text=In%202012%20the%20ITU%20defined%20IoT%20in%20Recommendation,existing%20and%20evolving%20interoperable%20information%20and%20communication%20technologies. (20.02.2022).

'Union Internationale des Télécommunications (UIT) définit ainsi en 2012 l'internet des objets comme une « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

كما وقف في البند 27,1 على الفرق بين الأشياء المادية أو الافتراضية في العالم السيبراني بقوله: «يعني مفهوم الأشياء، في هذا التنظيم، مواد العالم الحقيقي (الأشياء المادية)، أو العالم المعلوماتي (الأشياء الافتراضية) التي يمكن تعريفها ودمجها في شبكات الاتصالات. يكون للأشياء معلومات مرتبطة بها، ويمكن أن تكون ثابتة، وكذلك متغيرة. تشير الأشياء المادية إلى أي شيء موجود في العالم الحقيقي يمكن استشعاره وتوجيهه وتوصليه، في حين تشير الأشياء الافتراضية إلى شيء موجود في العالم المعلوماتي يمكن تخزينه ومُعَالَجَته والوصول إليه».

المطلب الثاني

استخدامات «إنترنت الأشياء»

تتعدد استخدامات إنترنت الأشياء في حياتنا المعاصرة، وفي جوانب مختلفة منها، مثل استخدامها في المساعدة على الاصطفاف الذكي، ومساعدة السائقين في إيجاد أماكن الاصطفاف، واستخدام تقنية المراقبة عبر الفيديو، ومساعدة رجال الشرطة وإرسالهم إلى المواقع المطلوبة بشكل أوتوماتيكي، ومراقبة استهلاك الماء وتسربه، والكهرباء والغاز، وتزويد حاويات النفايات بأجهزة استشعار من بعد؛ لإشعار العاملين عليها بامتلائها، من غير تفتيش يدوي مرهق، وكذلك أجهزة الاستشعار عن حالة الطقس وتنبيه السائقين، وإنشاء أنظمة المشورة الصحية من بعد... وغير ذلك من الاستخدامات التي لا يمكن حصرها[29].

لذا سيتم تناول هذه الجزئية بالتركيز على خصوصية استخدامات إنترنت الأشياء، من خلال رقابة البشر وذاتية الشيء في السلوك الآلي (الفرع الأول)، بالإضافة إلى التَّعلُّم الذاتي من الآلة واتخاذ القرار (الفرع الثاني).

(29) للمزيد من التفاصيل حول استخدامات إنترنت الأشياء، انظر: «إنترنت الأشياء لخدمات حكومية أفضل»، مركز محمد بن راشد للابتكار الحكومي، ابتكر، دبي، بتاريخ 30 سبتمبر 2020، وكذلك انظر: علي بن ذيب الأكلبي، العائد من تطبيقات إنترنت الأشياء على العملية التعليمية، المجلة الدولية للبحوث في العلوم التربوية، المؤسسة الدولية لآفاق المستقبل، تالين–أستونيا، مج2، ع3، س2019، ص103. منشور عبر موقع دار المنظومة (Search.Manthumah.com.Record/949101)، تاريخ آخر زيارة 17 فبراير 2022. وأيضا: أكمى تكيوكا تشاتفيلد، إطار عمل للحكومة الذكية الممكنة بإنترنت الأشياء: دراسة حالة لسياسات الأمن السيبراني لإنترنت الأشياء وحالات الاستخدام في الحكومة الفيدرالية الأمريكية، معهد الإدارة العامة، الرياض، س60، ع3، مارس 2020م، ص549. منشور عبر موقع دار المنظومة، آخر زيارة 17 فبراير 2022.

الفرع الأول

رقابة البشر وذاتية الشيء في السلوك الآلي

في ظل التطور المعاصر والتكنولوجيا المتقدمة، لم تعد الكيانات الأكثر شيوعًا تقتصر على وظيفتها التقليدية أو البدائية التي أُسندت إليها من البشر يوم صنعها، بل أصبحت هذه الكيانات المتصلة (إنترنت الأشياء–IOT)، تُستَخدَم بشكل إيجابي في جمع واستقاء المعلومات التي تسمح لها أحيانًا، وفي حالات محددة، بأن تعمل بذاتها انطلاقًا من هذه البيانات، مثل: الأجهزة المنزلية، والمكنسة الكهربائية «المستقلة» التي يمكن أن تتحرك ذاتيًا.

وقد تبادر هذه الأشياء المتصلة، في العديد من الأحيان، إلى تقديم، أو عرض، خدمة جديدة، مثل الساعة المتصلة التي تعطي إضافة إلى خدمة تحديد الوقت، وإمكان قياس النشاط البدني، و/ أو الفسيولوجي، لتقديم دورات اللياقة أو التدريب الرياضي، الأمر الذي يشكل تعدُّدًا واضحًا وملموسًا لاستخدامات إنترنت الأشياء بالنظر إلى طابعها الثنائي في الاستخدام، وتمثل مصدرًا للقوة، أو الابتكار والفعالية[30]. وكذلك تمّ استخدام ساعة متصلة لشركة أمريكية تدعى: Fit Bit، تُمكّن من حسم نتائج التحقيق في جريمة قتل بين الزوجين[31].

وفي المقابل هناك استخدامات سلبية، كأن تستخدم الشركة الخاصة بتقديم خدمة إنترنت الأشياء لشخص ما، وتقوم بإعطاء بياناته للغير؛ مما قد يؤدي إلى اختراق تلك البيانات، والاعتداء على الخصوصية[32]، الأمر الذي يحتاج إلى تدخل تشريعي، بإصدار قوانين تشجع على الاستخدامات الإيجابية، وتسعى إلى تحقيق الحماية من الأضرار، خاصة متى علمنا أن إنترنت الأشياء تشكل تحديات جديدة تتجاوز الأرقام.

وهذا البعد الجديد الذي أفرزته التكنولوجيا، وتطبيقات الذكاء الاصطناعي، سيعدّل علاقتنا كبشر بها، ويتحول اهتمام الإنسان، أو المجتمع، بهذه التقنية التي تشكل تواصلًا لحركة الربط الشبكي في العالم من جهة أولى، ومن جهة أخرى فإن قدرتها على جمع

(30) Matthieu Bourgeois et Marion Moine, Internet des objets (IOT): Quand l'inerte s'anime, Revue pratique de la prospective et de l'innovation, LexisNexis n°2, oct. 2019, pp.36.

(31) Anaëlle Grondin, Quand les objets connectés aident la police à résoudre des affaires cr - minelles, Journal les Echos, Paris, 26 avr. 2017.

(32) Matthieu Bourgeois et Marion Moine, Internet des objets (IOT), op. cit., p. 34.
وللمزيد من التفاصيل انظر: مالك محمد، المعلومات والأمن – رهان استراتيجي وأدوات جديدة للصراع، مجلة الحكمة، مركز الحكمة للبحوث والدراسات، الجزائر، ع27، لسنة 2013م، ص308. منشور عبر موقع دار المنظومة، تاريخ آخر زيارة: 17 فبراير 2022.

المعلومات، وإعادة استخدامها تلبية لحاجة مسجلة فيهما نوع من شبه المخاطر المُحْتَمَلة في المستقبل؛ بما يشكّل مساسًا بالمعلومات ذاتها، من إساءة استخدامها، وبمراقبتها، أو إفشائها للغير، من دون المحافظة على سريتها؛ ولذلك فإن إنترنت الأشياء لا تعدّل وظيفة المنفعة الأساسية للأشياء؛ فمثلا سيكون لزوج من النظارات دائما الوظيفة نفسها لتحسين البصر، و«ستحتفظ» الثلاجة بوظيفتها الأساسية المتمثلة في حفظ الطعام؛ فالأشياء المتصلة ستحقق منافع للبشرية بالتقاط معلومات لإعادة توزيعها في شكل خدمات[33].

نتيجة لذلك تُعطى الكائنات المتصلة وظائف جديدة تعدل استخدامها، ولكن بشكل أكثر دقة من حيث الوجهة والقيمة. وعصر الأشياء المتصلة، يطرح تساؤلات عن المفاهيم الاقتصادية والقانونية، وبشكل أعم سيادة القانون، إلا أنه لا يدعو إلى تشريع متسرع في محاولة للرد على عدم وجود قيود صارمة في الموقف، ولكن من أجل تفكير أعمق في هذه العلاقة الجديدة مع الأشياء، والتي يجب أن يفهمها قانون التنظيم والحماية[34].

ويُلاحَظ أن المُشَرِّع الإماراتي لم يقف مكتوف الأيدي في مواجهة هذا التطور، وسندنا في ذلك السياسة التنظيمية لخدمات إنترنت الأشياء، الصادرة عن هيئة تنظيم الاتصالات في الدولة، حيث بيّنت – ضمن نطاق العمل – أنه «بإصدار هذه السياسة، تعتزم الهيئة تنظيم خدمات إنترنت الأشياء داخل دولة الإمارات العربية المتحدة؛ من أجل تطوير النظام البيئي لخدمات إنترنت الأشياء؛ بطريقة منسقة ومتماسكة وآمنة ومضمونة»[35].

والمقصود بهذه الخدمات أنها «تعني مجموعة من الوظائف والتسهيلات يتم عرضها لأي مُسْتَخْدِم من قبل أي مُزَوِّد لخدمات إنترنت الأشياء، ولا يشمل ذلك الاتصال الخاص بخدمات إنترنت الأشياء»[36] الذي يكون من خلال مُشَغِّل مُرخَّص له، استنادًا إلى ما هو محدَّد في قانون الاتصالات الإماراتي[37]؛ إذ يقوم المُزَوِّد بتوفير الخدمة للمُسْتَخْدِمين من الأشخاص والشركات والحكومة[38].

(33) Stéphane Larrière, Internet des objets, le droit à l'envers du décor?, 27 Juin 2016, p.4. https://laloidesparties.fr/internet-des-objets-droit.

وانظر أيضًا: مالك محمد، المعلومات والأمن ... ، مرجع سابق، ص326.

(34) Ibid.

(35) انظر البند الثالث، 3/ ف1 (نطاق العمل) من السياسة التنظيمية لخدمات إنترنت الأشياء (IOT)، الهيئة العامة لتنظيم قطاع الاتصالات، أبوظبي، دولة الإمارات العربية المتحدة، 22 مارس2018 م، ص7، منشور عبر الموقع التالي: www.tra.gov.ae.

(36) بند 1/ ف11 من السياسة التنظيمية لخدمات إنترنت الأشياء، المرجع السابق، ص4.

(37) انظر: المرسوم بقانون اتحادي رقم 3 لسنة 2003م وتعديلاته المتعلق بقطاع تنظيم الاتصالات.

(38) بند 1/ ف12 من السياسة التنظيمية، مرجع سابق، ص5.

ويتضح من ذلك أن المُشَرِّع الإماراتي كان دقيقًا حين فرَّق بين خدمات الإنترنت، كمعنى، بتحديد المقصود منها، وبين الاتصال الخاص بهذه الخدمات، والشخص المُرخَّص له بتوفيرها للأشخاص، والشركات والحكومة. ثم جاء وبيَّن نطاق تطبيق هذه التقنية باقتصارها على من هم داخل الدولة، سواء كان المُرخَّص لهم، أو مُزَوِّدي الخدمة، أو المُسْتَخْدِمين[39].

إلا أن السؤال الذي يتبادر إلى الذهن، هو: ما الموقف من تَعطُّل خدمات إنترنت الأشياء، وما الآثار الضارة التي قد تحدث من جرَّاء ذلك؟ أجابت السياسة التنظيمية عن ذلك، بأن هيئة قطاع الاتصالات وضعت متطلبات محددة للخدمات الحرجة التي تحتاج إلى مستوى مُتقدِّم من السلامة والأمن؛ لإمكان تسببها في آثار سلبية كبيرة على المُسْتَخْدِمين في الدولة في حال تعطلها؛ ومن هذه المتطلبات ما يتعلق بالترخيص والموافقة من الهيئة، ثم تقييم هيئة تنظيم قطاع الاتصالات كل حالة على حدة؛ لتوفير السلامة والأمن، وتجنب الآثار السلبية المُحْتَمَلة[40].

ويرى الباحثان أن مثل هذه الخطوة، من المُشَرِّع الإماراتي، هي النواة الأولى نحو التنظيم، والسعي إلى تطوير المنظومة القانونية، وتحقيق الحماية والأمان والضمانات المنشودة؛ لتفعيل مثل هذه السياسات النظرية... ويبقى التنفيذ والتطبيق العملي هما الرهان الحقيقي نحو التطوير، بما يخدم الاستفادة من خدمات إنترنت الأشياء، بإيجابياتها في العمل والترفيه والتفاعل من جهة الأشخاص فيما بينهم، وبين الأشياء، وتقديم خدمات حكومية فعّالة؛ خاصة متى علمنا أن إنترنت الأشياء – كتقنية – ترتكز على جعل كل ما يحيط بالأشخاص متصلًا بالإنترنت، وبالأشياء بينها وبين بعضها، وبين الإنسان والآلة، بما يخدم الأول، ويستفيد من إيجابيات هذه التقنية في كل نواحي الحياة؛ بينما يظهر التساؤل هنا: ما مدى إمكان الاستغناء عن البشر، واتخاذ قرار آلي بمعزل عن الأشخاص؟ وهو ما نعالجه تاليًا:

الفرع الثاني

التَّعلُّم الذاتي من الآلة واتخاذ القرار من غير تدخل بشري

الأصل التقليدي المتعارف عليه أن يتم اتخاذ القرار – بشكل مباشر – من الشخص البشري، ورقابته الفعلية في كثير من استخدامات الأشياء، لكن استثناءً من هذا الأصل، وفي ظل الذكاء الاصطناعي وتطبيقاته المختلفة، نذكر مثلًا السيارات ذاتية القيادة التي

(39) بند 3/ ف3 من السياسة التنظيمية، مرجع سابق، ص7 و8.

(40) بند 5/ ف3. وبند 6/ ف5 من السياسة التنظيمية، مرجع سابق، ص9.

أصبحت تعمل بموجب نظام المحاكاة للسيارة على الطريق بمواصفات تعتمدها هيئة الطرق والمواصلات في دبي، ويقصد بنظام المحاكاة هو نظام إلكتروني ذكي مصمَّم من الشركة المُصنِّعة للمركبة ذاتية القيادة، كوسيلة للتواصل بين المركبة وعناصر الطريق، يحقق مستويات مختلفة من التحكم في المركبة، قد تصل إلى قيادتها من دون تدخل بشري[41].

غير أن الاستخدام الخطأ للنظام الإلكتروني قد يسبّب مخاطر للشخص ذاته، ولغيره من الأشخاص. ونعرض – تطبيقًا لذلك – قضية تتلخص وقائعها في أنه «في تاريخ 27 مايو 2021 أخطأت السائقة ما أدى إلى وفاة شخص نتيجة الإهمال والرعونة، وعدم الاحتراز، والانشغال عن الطريق، وانحرافها عن الطريق، وعدم اتباع قانون السير في أثناء قيادة المركبة على شارع مليحة/ إمارة الشارقة؛ ففي أثناء السير اختارت القيادة الذاتية، وخلال الكتابة؛ لتحديد الوجهة على اللوحة الإلكترونية، شعرت باصطدام قوي من مركبتها في جسم ثابت، وشاهدت الغبار، وأصوات انفجار، وتوقف المركبة، ولعدم قدرة السائقة على الوقوف والجلوس، بدأت تلوّح للسيارات بيديها، واعترفت بأنها لم تتوقع وقوع الحادث المروري؛ حيث نتج عن الحادث وفاة سائق دورية الشرطة، وأضرار جسيمة بمركبتين على الطريق».

صدر حكم قضائي بإلزام السائقة بسداد دية بمبلغ مائتي ألف درهم إماراتي، لورثة المتوفى، ومنعها من استعمال رخصة قيادة لمدة سنة من تاريخ تنفيذ الحكم، مع حفظ الحق المدني للمتضررين من حادث السير[42].

ويتفق الباحثان مع الحكم القضائي، كونه عكس التطبيق السليم لنصوص القانون، وجاء مسبَّبًا بشكل واضح بارتكابها المخالفة؛ إذ كان يجب عليها الوقوف في منطقة آمنة على جانب الطريق، ثم الكتابة وتحديد الوجهة على اللوحة الإلكترونية، بتحويل السياقة إلى القيادة الذاتية، لا أن تكتب وهي تقود السيارة.

وفي القطاع المالي أصبحت الأسواق المالية الكبرى تستخدم برامج ذكية لتحليل البيانات، وتوقُّع تقلبات أسعار الأسهم والسندات، حتى وصل الأمر بهذه البرامج إلى

(41) انظر: م1 من قرار المجلس التنفيذي رقم 3 لسنة 2019م، حكومة دبي، بشأن تنظيم التجربة التشغيلية للمركبة ذاتية القيادة في إمارة دبي. وللمزيد من التفاصيل راجع: جعفر حافظ، المركبات ذاتية القيادة: قضايا التنظيم والمسؤولية المدنية بالتركيز على بعض القوانين الرائدة، مجلة كلية القانون الكويتية العالمية، السنة الثامنة، ع3، العدد التسلسلي 31، سبتمبر 2020، ص511.

(42) القضية رقم 373/3021 جزاء مرور الشارقة، محكمة الشارقة الاتحادية الابتدائية، دائرة الجنح الثانية عشرة (جنح ومخالفات المرور)، بتاريخ 21 يونيو 2021 (حكم قضائي غير منشور).

حد التفاوض بشأن الصفقات وإبرامها؛ بمعزل عن أي تدخل بشري[43].

وفي الوقت الحاضر أصبح التَّعلُّم الآلي[44] هو النهج السائد في الذكاء الاصطناعي. وليس المقصود بالتَّعلُّم الآلي أن الآلة تتعلم كما يتعلم البشر، بل يعتمد التَّعلُّم الآلي على البيانات الهائلة؛ حيث تستخدم أنظمة التَّعلُّم الآلي أنماطا في البيانات حتى تحقق نتائج ذكية، ومثالُ ذلك مرشح رسائل البريد الإلكتروني النمطي للرسائل المزعجة؛ إذ إن أغلب برامج البريد الإلكتروني تستخدم التَّعلُّم الآلي حتى تكتشف الرسائل المزعجة تلقائيًّا (أوتوماتيكيًّا)، وتحولها إلى مجلد منفصل مستقل بالرسائل المزعجة[45].

وعلى الرغم من الفوائد التي تنتج عن تكنولوجيا الذكاء الاصطناعي وتطبيقاته المختلفة، فإننا نتفق مع من يرى أنها تثير العديد من التحديات؛ خاصة ما يتعلق بمدى ملاءمة التشريعات الحالية لمواجهتها، ومقدرتها على استيعاب الخصائص الفريدة، إضافة إلى أن مثل هذه التكنولوجيا لم تصل إلى درجة الكمال؛ لكونها عرضة للإصابة بالفيروسات والأعطال الفنية من جهة تقنية، وما قد ينتج عنها من أضرار غير متوقعة[46]، وإمكان اختراق البيانات في إنترنت الأشياء من الغير، وسعي الشركات إلى وضع شروط تعاقدية تعفي نفسها – بموجبها – من المسؤولية القانونية تجاه المستهلك أو طالب الخدمة، مما يشكِّل – في رأي الباحثين – قصورًا تشريعيًّا يحتاج إلى وقاية فعلية في التشريعات المرتقب صدورها في المستقبل.

(43) عماد عبدالرحيم دحيات، إشكالية العلاقة بين البشر والآلة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تامنراست، الجزائر، مج8، ع5، لسنة 2019، ص16.

(44) تشمل تقنيات التعلم الآلي (الشبكات العصبية – التعلم العميق، وخوارزمية الغابات العشوائية، والانحدار اللوجستي... وغيرها). انظر: حول هذه التقنيات: براند مار، أهم عشر حالات استخدام في الذكاء الاصطناعي والتعلم الآلي التي يجب على الجميع التعرف عليها، 30 سبتمبر 2016.What are the top 10 use cases for انظر: الموقع التالي: www.forbes.com/sites/bernardmarr/2016، تاريخ الزيارة 17 مارس 2021.
وانظر كذلك: ماندیب سیدانا، أنواع خوارزميات التصنيف في التعلم الآلي، 28 فبراير 2017، منشور على الموقع التالي: Mandysidana/Machine-learning-types-of-classification

(45) سوردين هاري، الذكاء الاصطناعي والقانون .. لمحة عامة، مجلة معهد دبي القضائي، ع11، السنة الثامنة، أبريل لسنة 2020، ص186 و187.

(46) Emad Dahiyat, Intelligent agents and liability: is it a doctrinal problem or merely a pr - blem of explanation? Artificial Intelligence and Law, Springer Nature, Volume 18, Issue 1, (2010), p.113.

المطلب الثالث

مخاطر «إنترنت الأشياء»

ترتكز تقنية إنترنت الأشياء – بشكل كبير – على البيانات؛ لذا فإنها تحتاج إلى شبكة وبنية تحتية مخصَّصَة لها قادرة على تحمل عدد كبير من التعاملات في وقت واحد، وبشكل مستمر ومتكرر، الأمر الذي يوجب على الجهات الحكومية تَملُّك شبكة قوية بما فيه الكفاية؛ لدعم البنية التحتية المُصمَّمة لتشغيل تقنية إنترنت الأشياء، وتؤدي بالنتيجة إلى تقديم الخدمات الحكومية الأمثل والأفضل[47].

إن الحجم الضخم من المعلومات السرية، والشخصية والعادية، عبر الإنترنت يبرز مشكلة الحماية الفنية للمعلومات، والمتمثلة في عدم قدرة برامج التأمين على تحقيق الحماية، والتأمين الكافي للحفاظ على المعلومات والأسرار؛ الأمر الذي يهدد أصحابها بإفشائها والإفصاح عنها، واستخدامها بشكل غير مشروع، فيلحق الأضرار بالأشخاص الطبيعية في الحفاظ على خصوصيتهم وأسرارهم وبياناتهم الشخصية[48].

وهذا يتطلب منا مُعَالَجَة المراقبة السرية لبيانات الأشخاص (الفرع الأول)، ثم الاعتداء على البيانات (الفرع الثاني) وفق التالي:

الفرع الأول

مُعَالَجَة المراقبة السرية لبيانات الأشخاص

جاء في السياسة التنظيمية لخدمات إنترنت الأشياء، في الإمارات، أن على مُزَوِّدي هذه الخدمة التَّقيُّد بأحكام معيَّنة لتخزين البيانات، تتمثل في وجوب تخزين البيانات الحساسة والسرية للغاية، للأشخاص والشركات، بشكل أساسي في الدولة. ولا يجوز تخزينها خارج الدولة إلا بعد إثبات استيفاء بلد التخزين متطلبات/ سياسات/ تنظيمات أمن البيانات الشخصية، وحماية المُسْتَخْدِمين المتبعة داخل الدولة أو يتجاوزها، وتنطبق هذه الاشتراطات على البيانات الشخصية؛ كون هيئة تنظيم قطاع الاتصالات الإماراتية تعتبر البيانات الشخصية سرية للأشخاص. ويجب أن تبقى البيانات السرية والحساسة

(47) مركز محمد بن راشد للابتكار الحكومي، إنترنت الأشياء لخدمات حكومية أفضل، تمّ نشره بتاريخ 30 سبتمبر 2020.

(48) سعيد عبداللطيف إسماعيل، رؤية وتحليل للتحديات المستجدة للحق في الخصوصية الناتجة عن الثورة الرقمية وتطور الاتصالات والإنترنت، مجلة كلية القانون الكويتية العالمية، السنة الثالثة، ع12، ديسمبر 2015، ص92 – 90.

والسرية للغاية، الخاصة بالحكومة، داخل الدولة في كل الأحوال. ويجوز تخزين البيانات المفتوحة للأشخاص والشركات والحكومة داخل الدولة، و/ أو خارجها[49].

وعلى الرغم من وجود مثل هذه الاشتراطات، على مُزَوِّدي الخدمة، التي فرّقت بين البيانات المذكورة أعلاه بالنسبة إلى الأشخاص والشركات من جهة، والبيانات الخاصة بالحكومة من جهة أخرى، والتي لا يجوز بالنسبة للأخيرة تخزينها إلا داخل الدولة، فإنه يحتمل – بعد حيازتها – إفشاؤها للغير بقصد الإضرار غير المشروع بصاحب هذه البيانات، وهو ما يتطلب حماية خاصة لأصحابها؛ لمنع مثل هذه الاعتداءات، وآثارها السلبية، وتشديد الرقابة على مُزَوِّدي الخدمة؛ بتطبيق قانون الاتصالات، والسياسة التنظيمية، واللوائح ذات العلاقة.

ويرى الباحثان أن تعليق الخدمة المؤقت، أو الدائم، لخدمات المُزَوِّدين المخالفين للأحكام والشروط المنصوص عليها، لا يشكّل إنصافًا للمُسْتَخْدِمين، ولا يزيل الضرر عنهم بعد حدوثه. ونقترح هنا متى ثبتت المخالفة تعويض المتضرر صاحب البيانات، بعد طلبه التعويض العادل الذي يقدره أهل الخبرة.

وحسنًا فعل المُشَرِّع الإماراتي في قانون حماية البيانات الشخصية الاتحادي؛ حين عرَّف البيانات بشكل عام بأنها «مجموعة منظمة، أو غير منظمة، من المعطيات، أو الوقائع، أو المفاهيم، أو التعليمات، أو المشاهدات، أو القياسات، تكون على شكل أرقام، أو حروف، أو كلمات، أو رموز، أو صور، أو فيديوهات، أو إشارات، أو أصوات، أو خرائط، أو أي شكل آخر، يتم تفسيرها، أو تبادلها، أو مُعَالَجَتها، عن طريق الأفراد، أو الحواسيب، وتشمل المعلومات أينما وردت في هذا المرسوم»[50].

غير أن المُشَرِّع الإماراتي لم يفرّق بين البيانات والمعلومات في المعنى الذي ذكره، كون البيان حقيقة لم تتم مُعَالَجَتها، مثل: اسم الشخص، أو رقم هاتفه، أو عنوانه. في حين أن المعلومات هي بيانات عُولِجت لاستخدامها في غاية محددة[51]، ثم جاء (المُشَرِّع

(49) بند 7.8.2/ ف 3،2،1 من السياسة التنظيمية لخدمات إنترنت الأشياء، مرجع سابق، ص12.

(50) م1 من مرسوم بقانون اتحادي إماراتي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية.

(51) للمزيد من التفاصيل حول التفرقة بين البيانات والمعلومات في التشريعات المقارنة، انظر: محمد حسن علي، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونيًا: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة، مجلة العلوم القانونية، كلية القانون، جامعة عجمان، الإمارات، مج7، ع14، يوليو 2021، ص83. وكذلك أيضا: راجع: نهى بنت عوض الدارودي، كيف تحدد البيانات الضخمة مستقبلنا، أوراق عمل المؤتمر السنوي الخامس والعشرين لجمعية المكتبات المتخصصة، فرع الخليج العربي، إنترنت الأشياء: مستقبل الأشياء المتصلة، أبوظبي، لسنة 2009م، ص650، منشور عبر موقع دار المنظومة (search.manthumah.com/Record/946964)، آخر زيارة 17 فبراير 2022.

الإماراتي) وصنّف البيانات إلى أنواع، منها ما هي بيانات شخصية، ومنها بيانات شخصية حسّاسة، ومنها بيانات حيوية[52]، بينما جاءت السياسة التنظيمية لخدمات إنترنت الأشياء أكثر تفصيلًا، بإضافة البيانات المفتوحة، والسرية، والسرية للغاية إلى التصنيفات المذكورة في قانون حماية البيانات الشخصية؛ مستندة في هذا التصنيف على أساس التأثير السلبي المُحْتَمَل عند الاعتداء على السرية، أو الإفصاح المطلق عن المعلومات من دون خضوعه للرقابة[53].

وحدد القانون، السابق ذكره، المقصود بصاحب البيانات بأنه «الشخص الطبيعي»[54]، كما حدد الشخص المسؤول عن حماية البيانات، بأنه «أي شخص طبيعي أو اعتباري يتم تعيينه من قبل المُتَحَكْم أو المُعالِج، يتولى مهام التأكد من مدى امتثال الجهة التي يتبعها لضوابط واشتراطات وإجراءات وقواعد مُعَالَجَة حماية البيانات الشخصية المنصوص عليها في هذا المرسوم بقانون، والتأكد من سلامة أنظمتها وإجراءاتها من أجل تحقيق الالتزام بأحكامه»[55].

ويُلاحَظ أن المُشَرِّع الإماراتي، بعد أن عرَّف أمن البيانات الشخصية بأنها «مجموعة من التدابير والإجراءات والعمليات التقنية والتنظيمية المحدَّدَة وفقًا لأحكام هذا المرسوم بقانون، والتي من شأنها الحفاظ على حماية خصوصية، وسرية، وسلامة، ووحدة البيانات الشخصية، وتكاملها وتوافرها»[56]، بيَّن أنه يشمل ما يلي[57]:

1- تشفير البيانات الشخصية وتطبيق آلية إخفاء البيانات.

2- تطبيق إجراءات وتدابير استمرار سرية أنظمة وخدمات المُعَالَجَة، وسلامتها وصحتها ومرونتها.

3- تطبيق إجراءات وتدابير تضمن استرجاع البيانات الشخصية والوصول إليها في الوقت المحدد، في حال حدوث أي عطل فعلي أو فني.

4- تطبيق إجراءات تضمن سلامة عملية اختيار وتقييم وتثمين فاعلية التدابير التقنية والتنظيمية بما يضمن أمن المُعَالَجَة.

(52) المادة (1) من المرسوم الاتحادي الإماراتي رقم 45، لسنة 2021، المتعلق بحماية البيانات الشخصية.
(53) انظر: بند 1.3 من السياسة التنظيمية لخدمات إنترنت الأشياء، مرجع سابق، ص3.
(54) المادة (1) المرسوم الاتحادي الإماراتي رقم 45، لسنة 2021، بشأن حماية البيانات الشخصية.
(55) المرجع السابق.
(56) المرجع السابق.
(57) المرجع السابق.

ويُلاحَظ أن المُشَرِّع الإماراتي لم يحدد طبيعة الإجراءات المراد تطبيقها لتحقيق الحماية الفعلية الآمنة لسرية البيانات الشخصية، وهو ما نقترحه بتوضيح طبيعة هذه الإجراءات الاستباقية؛ تجنّبًا لأي قصور تشريعي، وسعيًا إلى تحقيق الحماية الوقائية، لا العلاجية، من الاعتداء على سرية البيانات للأشخاص الطبيعيين، في ظل التطور التكنولوجي المتسارع.

وتطبيقًا لذلك يمكن الإشارة إلى قضية في الولايات المتحدة الأمريكية بشأن أجهزة القياسات الحيوية في حالات انتهاك الخصوصية، تتمثل وقائعها في ادّعاء المستهلكين أن شركات التكنولوجيا قد حصلت – بشكل غير قانوني – على «معرفات بيومترية» شخصية، أو استخدمتها، أو تشاركتها – بشكل عام – بصمات الأصابع، وبصمات الصوت، ومسح الشبكية، والوجه من دون موافقة، بما ينتهك قوانين الخصوصية، فأيّدت محاكم ولاية إلينوي، والمحاكم الفيدرالية بعض هذه المطالبات، ووافقت على التسويات[58]. وهذا يشكّل – في رأينا – حماية قضائية لخصوصية الأشخاص، وسرية بياناتهم الشخصية.

كما يتحقق المساس بالحياة الخاصة في جوانب متعددة، مثل: التجسس على الحياة الخاصة (من خلال الدخول إلى منزل الشخص والتنصت عليه، أو اختلاس النظر، والتصوير، والتسمع عن طريق الأجهزة)[59]، أو نشر وقائع تتعلق بخصوصية الشخص بأي وسيلة كانت، والإساءة إلى سمعته (بالتشهير، بهدف الحصول على ربح مادي)، وإفشاء سرية المحادثات (بالتنصت عليها، أو تسجيلها، وحفظها، واستعمالها) وهي كلها تعد اعتداءً وانتهاكًا غير مشروعين، يمسان بكرامة الإنسان، وآدميته، باعتبارها حقًّا دستوريًّا ملازمًا لشخص الإنسان وحرياته[60].

(58) راجع: ريفيرا ضد جوجل
Google Inc, No 16 -C-02714 ، 2017 U.S. Dist. LEXIS 27276 (ND Ill. 27.2.2017 Sekura v. L.A. Tan Enterprises، No. 2015-CH-16694 (Cir. Ct. Cook. County Illinois); http://www.chicagotribune.com/bluesky/originals/ct-biometric-illinois-privacy-whats-next-bsi-20170113-story.html. (Last-visited: 18-03-2021).

حالات جهاز إنترنت الأشياء هذه، سواء في القضايا المدنية أو الجنائية، مشار إليها على الموقع التالي:
(Last-visited: 18-03-2021) https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/

(59) حسام الدين الأهواني، حماية الحق في الخصوصية في ظل قانون دولة الإمارات العربية المتحدة، مجلة الأمن والقانون، أكاديمية شرطة دبي، مج16، ع2، لسنة 2008، منشور على موقع دار المنظومة search.manthumah.com/Record/369259، تاريخ آخر زيارة 15 فبراير 2022، ص10، وص11. انظر كذلك: حسام الدين الأهواني، الحق في احترام الحياة الخاصة (الحق في الخصوصية): دراسة مقارنة، دار النهضة العربية، القاهرة، 1978، ص24، فقرة 16.

(60) فيصل عقلة خطار وآخرون، الحماية الدستورية والقانونية للحق في الحياة الخاصة، مجلة دراسات، علوم الشريعة والقانون، الجامعة الأردنية، مج4، ع1، لسنة 2020، منشور على موقع دار المنظومة، ص1–6.

الفرع الثاني

الاعتداء على بيانات الأشخاص

أخذ موضوع حرمة الحياة الخاصة اهتمامًا تشريعيًّا وفقهيًّا واضحًا، لارتباطه بحريات الأشخاص، باعتبارها من أهم حقوق الإنسان، وكفالة الدساتير[61] لمنع الاعتداء عليها، وصونها وحمايتها، خاصة في ظل التطور التكنولوجي الهائل والمتسارع، وما رافقه من خروق من قبل الغير[62].

ويُلاحَظ أن المُشَرِّع الإماراتي، في السياسة التنظيمية لخدمات إنترنت الأشياء، استند في تصنيفه البيانات الشخصية – كما بيّنا سابقًا – على أساس التأثير السلبي المُحْتَمَل من انتهاك السرية، والإفصاح عن البيانات، بما يحققه من أضرار؛ منها ما يؤدي إلى أضرار محدودة للأشخاص، أو الشركات، أو الحكومة (البيانات السرية)، ومنها ما يؤدي إلى وقوع أضرار جسيمة (البيانات الحساسة)، أو أضرار فادحة تمس بالمصالح العليا، وأضرار جسيمة وفادحة معا (البيانات السرية للغاية)[63].

وأكّد قانون حماية البيانات الشخصية الإماراتي أن خرق أو انتهاك البيانات الشخصية قد يتم بوسائل مختلفة، مثل: الدخول غير المشروع، أو غير المُصرَّح به، أو نسخ البيانات، أو تبادلها، أو توزيعها، أو مُعَالَجَتها بصورة تؤدي إلى الإفصاح للغير عن هذه البيانات، أو إتلافها أو تعديلها[64]. وأعطى الحق للمتضرر (صاحب البيانات) في تقديم شكوى إلى مكتب الإمارات للبيانات (المنشأ بموجب المرسوم بقانون اتحادي رقم 44 لسنة 2021م) عند وقوع أي مخالفة تتعلق ببياناته، غير أن الجزاءات التي يصدرها المكتب هي إدارية[65]. وفي رأي الباحثَين أن الجزاء الإداري لا يحقق إنصافًا للمتضرر،

(61) المواد (26)، و(31)، و(36) من الدستور الإماراتي لسنة 1971م وتعديلاته حتى سنة 2009 التي بيَّنت أن الحرية الشخصية مكفولة لجميع المواطنين، وأنه لا يجوز تفتيشه إلا وفقًا لأحكام القانون، ونصت على كفالة حرية المراسلات البريدية والبرقية وغيرها من وسائل الاتصال، وسريتها، وحرمة المساكن وعدم دخولها إلا بإذن صاحبها، وفق القانون والأحوال المحدَّدة. وقد ورد المعنى نفسه في المواد (30)، و(31)، و(38)، و(39) من الدستور الكويتي لسنة 1962، كما جاء في المواد (26)، و(37)، و(40) من النظام الأساسي للحكم في المملكة العربية السعودية لسنة 1992.

(62) عبدالرحمن الدراجي خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري: دراسة تحليلية مقارنة، مجلة جامعة الملك سعود – الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الملك سعود، الرياض، مج24، ع2، يوليو 2012م/ 1433هـ، 237.

(63) بند 1.3 من السياسة التنظيمية لخدمات إنترنت الأشياء، مرجع سابق، ص3.

(64) المادة (1) من المرسوم بقانون اتحادي رقم 45، لسنة 2021.

(65) المادة (26) من المرسوم بقانون اتحادي رقم 45، لسنة 2021.

وليس هناك ما يمنع من لجوئه إلى القضاء للمطالبة بالتعويض العادل، وفقًا لجسامة الضرر، وما يقدره أهل الخبرة.

ويتضّح من ذلك مدى خطورة كل نوع من البيانات على الأشخاص والشركات والحكومة؛ متى تمّ الإفصاح عنه، أو تبادله من دون موافقة صاحبه، أو من دون تصريح؛ الأمر الذي يحتاج إلى رقابة مشدّدة حفاظًا على خصوصية البيانات، ومنعًا للاعتداء غير المشروع، وتجنبًا للأضرار المستقبلية الناتجة عن ذلك.

وعلى الرغم من غياب قانون خاص بإنترنت الأشياء حتى الآن في الدول العربية، فإن عددًا منها وضع بعض الحلول الأولية في قوانين الملكية الفكرية، لحماية المعلومات، وبرامج الحاسب الآلي، وقواعد البيانات، وحماية الحريات الشخصية وحرمتها[66]، ونصوصًا دستورية عامة، حيث نص الدستور الإماراتي على أن من الدعامات الأساسية، اجتماعيًا واقتصاديًا في الدولة، هي توفير الأمن والطمأنينة للجميع، وبيَّن أن حرية المراسلات البريدية والبرقية، وغيرها من وسائل الاتصال، مصونة ومكفولة بموجب القانون[67]، وبذلك يكون الدستور هو أصل الحماية القانونية والنظامية للمعلومات، خاصة وسائل الاتصال الحديثة، بوصفها وسائل تقنية متقدمة[68].

لكن هناك من يرى أن هذا الأصل يحتاج إلى التطبيق الفعلي، والحماية العملية، بتفعيلها على أرض الواقع؛ إذ إن كثيرًا من الدول تضع النصوص القانونية، وتبقى الإشكالية في مدى تفعيل هذه النصوص، وتحقيق الحماية الفعلية من مخاطر التطور التكنولوجي الهائل، الأمر الذي يحتاج إلى الرقابة على تطبيق النصوص النظرية وتنفيذها[69].

وتبقى الحاجة ماسة إلى الحماية الوقائية (التقنية والقانونية) من مخاطر وسلبيات استخدام إنترنت الأشياء، قبل وقوع الضرر على الأشخاص والاعتداء على بياناتهم الخاصة.

---

(66) القانون الخاص الإماراتي الاتحادي، رقم 40 لسنة 1992، بشأن حقوق المؤلف والمصنفات الفكرية. وكذلك المادة (2) من المرسوم بقانون لحقوق المؤلف البحريني رقم 10 لسنة 1993، والذي نص على حماية برامج الحاسب الآلي. وكذلك المادة (1) من القانون بمرسوم رقم 5 لسنة 1995 الكويتي لحماية المصنفات والحاسب الآلي من البرامج وقواعد البيانات. والمادة (30) من القانون العماني رقم 37 لسنة 2000، لحماية الحريات الشخصية وحرمتها.

(67) المادة (14)، والمادة (31) من الدستور الإماراتي لسنة 1971 وتعديلاته لغاية 2009.

(68) إبراهيم حسن الملا، الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون، أكاديمية شرطة دبي، س26، ع19، يناير 2018، ص155.

(69) بشار طلال المومني ومنذر طلال المومني، الحماية المدنية من مخاطر الذكاء الاصطناعي في التشريع الإماراتي، مجلة الحقوق، كلية الحقوق، جامعة البحرين، مج17، ع2، لسنة 2021م، ص292.

ويرى الباحثان أنه ينبغي أن يبقى العنصر البشري هو المحرك الفعلي لإنترنت الأشياء، لا أن تكون الأشياء المتصلة هي صاحبة القرار بمعزل عن البشر، في آلية التفاعل والتواصل واتخاذ القرارات، وأنه يتوجب العمل على إصدار تشريعات متقدّمة تحمي المُسْتَخْدِمين لخدمات إنترنت الأشياء وتقيهم الأضرار المستقبلية قبل وقوعها.

المبحث الثاني

التنظيم القانوني المأمول لاستخدامات «إنترنت الأشياء»

أصدرت المفوضية الأوروبية في يونيو 2009 تقريرًا بعنوان «إنترنت الأشياء ... خطة عمل لأوروبا؛ بغية تأكيد الدور الاستراتيجي المتوقع من السلطات العامة؛ في سبيل إنشاء بيئة موائمة لتطوير إنترنت الأشياء»[70]، وذلك بالنظر إلى التحولات الثورية التي سيجلبها الجيل الجديد من تكنولوجيا المعلومات إلى المجتمعات الأوروبية؛ مؤكدة على أنه «لذلك ليس من الحكمة والحيطة بتاتًا أن تُترك إنترنت الأشياء في يد القطاع الخاص أو دول أخرى، لتطويرها من دون رقيب ولا حسيب».

ودعت المفوضية إلى التعقل والتبصر في وضع خطة ممنهجة لرسم مسار العمل على المستوى الأوروبي، بطرح أربعة عشر مقترحًا للسير على هداها؛ ثلاثة منها استوقفتنا في دراستنا، هي: الخصوصية، وحماية البيانات الشخصية للأفراد، وضمان كسب ثقة المستهلك بالاستخدام الآمن لهذه التكنولوجيا، بتقرير جملة من التدابير التشريعية.

وسيُخصَّص هذا المبحث لبيان الإجراءات الوقائية التي تم إقرارها لضمان الاستخدام الآمن والمعقول لخدمات إنترنت الأشياء، بشكل يحفظ له أمن بياناته الشخصية وخصوصيته من أي انتهاك (المطلب الأول)، وإذا اقتضى الأمر ضمان تعويضه عن الأضرار التي تقع بفعل هذه الخدمات، في حال وقع الانتهاك (المطلب الثاني).

المطلب الأول

حق المستهلك في الاستخدام الآمن لإنترنت الأشياء وجَلب ثِقته بها

لعل من أبرز التحديات التي تواجه السلطات العامة، في مجال استخدام تكنولوجيا إنترنت الأشياء، هي وضع إطار نظامي يوفر لمُسْتَخْدِمي هذه التكنولوجيا الثقة والموثوقية في النظام المُسخَّر لضمان سلامة البيانات الشخصية وحمايتها من كل أشكال الانتهاك (الفرع الأول)، وكذا ضمان صون حرمتهم وخصوصية حياتهم الخاصة (الفرع الثاني).

(70) Doc.COM(2009) 278final, 18 juin 2009.

الفرع الأول

حماية البيانات الشخصية من جميع أشكال الانتهاك

بالنظر إلى أن تكنولوجيا إنترنت الأشياء تعتمد على جلب أكبر قدر من البيانات التي تخص الأفراد المُسْتَخْدِمين لها، فإن اتصالها بالشبكة العنكبوتية يُعرضها – بشكل مستمر – لأخطار اختراق الكيانات المُتصلة بها، وتجعلها عرضة للسرقة، أو الضياع، أو الاختلاس في أي وقت، وهذا ما أظهرته الدراسات بأن 80% من الأشياء المتصلة Objets connectés تتخللها ثغرات في نظام تأمينها؛ إما بسبب عدم كفاية سياسة كلمة المرور، وإما لعدم تشفير البيانات المُتدَاوَلَة فيها[71].

من المُحْتَمَل جدًا، في ظل المركبات الذكية المتصلة بالشبكة العنكبوتية، وأشياء متصلة بالمحيط الخارجي، أن تخضع للقرصنة أو الاختراق، وتعطيل نظام الكبح مثلًا، بسبب عدم كفاية نظام حماية البيانات الشخصية للتحكم في المركبة، وحينئذ سيفضي هذا المساس بالبيانات الشخصية إلى تهديد السلامة الجسدية للمُسْتَخْدِمين لعدم أمان نظام الحماية.

وتجدر الإشارة إلى أن ما يثير مخاوف أهل التخصص، هنا، هو أن أمن هذه الأشياء المتصلة قد لا يتناسب – بالضرورة – مع النهج الكلاسيكي لأمن الأنظمة المعلوماتية المعمول بها في السنوات الماضية؛ لذلك لا بد – من وجهة نظر قانونية – من مواءمة النصوص العامة التي تهدف إلى حماية البيانات الخاصة للأفراد عبر شبكة الإنترنت، سواء في قانون العقوبات، أو القوانين الخاصة بالتكنولوجيا المعلوماتية، أو حتى التشريعات المدنية، بإقرار نصوص قانونية تختص بحماية مُسْتَخْدمي إنترنت الأشياء، من جميع صور الانتهاكات الماسة بحقوقه الشخصية؛ ذلك أن المَخاوف الناجمة عن استخدامات تقنية إنترنت الأشياء، لا تنحصر فقط في مسألة تجميع البيانات الشخصية وتخزينها بطريقة آمنة، بل تتعداها لتشمل إشكالات أكثر تعقيدًا، تتمثل أساسًا في نقل هذه البيانات والإفصاح عنها إلى الغير، أو مدى جواز تمريرها لاستغلال خدمات أخرى.

لذلك، فإن عملية نشر هذه البيانات المُجَمَّعة والمُخَزَّنَة، بشكل سليم، تحتاج إلى عناية أكبر، باعتبار أن تقنية إنترنت الأشياء، خلافًا للنظم المعلوماتية التقليدية، تعتمد على دمج البيانات التي تم تجميعها؛ لاستغلال خدمات أخرى مجاورة، غير الخدمة التي تم

(71) Myriam Quéméner, Internet des objets et cybercriminalité et cybersécurité, Revue Ba - que, (16.09.2019). Internet des objets, cybercriminalité et cybersécurité, Revue Banque (revue-banque.fr) (19.04.2022).

التجميع تلبية لها في الأصل، وهذا ما يفضي – في أغلب الأحيان – إلى صعوبة التحكم في هذه العمليات، بل قد يكون شبه مستحيل[72].

ومن هذا المُنطَلق يبدو للباحثَين، أن بعض المبادئ التي جاء بها قانون حماية البيانات الشخصية الإماراتي، في الآونة الأخيرة، قد يصعب إنفاذها في العديد من الجوانب القانونية والفنية، لتعارضه مع الفلسفة التي تشتغل وفقها خدمات إنترنت الأشياء، للاعتبارات التالية:

أ- فيما يتعلق بإعمال مبدأ تخصيص استغلال البيانات:

نص المُشَرِّع الإماراتي، في قانون حماية البيانات الشخصية لسنة 2021، على هذا المبدأ، في المادة (5)، بالقول: «تكون البيانات قد جُمعت لغرض واضح ومُحدَّد، وألَّا تتم مُعَالَجَتها، في أي وقت لاحق، على نحو يتنافى مع ذلك الغرض». كما أكد في الفقرة الثانية من المادة نفسها على «عدم جواز الاحتفاظ بالبيانات الشخصية بعد استنفاد الغرض من مُعَالَجَتها».

ومع ذلك أجاز هذا القانون، في المادة ذاتها، إمكان استخدام البيانات المُجَمَّعَة لغير الغرض الذي جُمعت من أجله، متى كان الغرض منها مشابهًا، أو متقاربًا، مع الغرض الأصلي الذي تم التجميع بناء عليه. ويرى الباحثان أنه يبقى من الصعب على القاضي، هنا، تقدير مدى هذا التقارب من الناحية العلمية.

كما قضت بهذا المبدأ، أيضًا، السياسة التنظيمية لخدمات إنترنت الأشياء في دولة الإمارات، في البند 8,7، والذي أوجب على مُزَوِّد خدمات إنترنت الأشياء اتباع مبادئ ومشارطات أساسية أقرها هذا القانون، ومن بينها أن يقف عند «حدود الغرض الذي تم تحصيل البيانات تحقيقًا له».

ب- فيما يتعلق بإعمال مبدأ تقليل البيانات المُسْتَخْدَمَة:

نص على ذلك قانون حماية البيانات الخاصة في مادته الخامسة، بقوله «أن تكون البيانات الشخصية كافية ومقتصرة على ما هو ضروري، وفقًا للغرض الذي تمت المُعَالَجَة من أجله»، والأمر نفسه أقرت به السياسية التنظيمية لخدمات إنترنت الأشياء؛ بالتزام المُزَوِّد بالتقليل من البيانات، وبأن تقتصر على مجرد البيانات الكافية، وذات الصلة بالأغراض التي تتم مُعَالَجَتها لأجلها.

(72) Xavier Caron, Rachelle Bosua, Sean B. Maynard, Atif Ahmad, The Internet of Things (IoT) and its Impact on Individual Privacy: An Australian Perspective, Computer Law & Security Review 32, (2016), p.9.

ج- فيما يتعلق باستخدام آلية التشفير وضمان خاصية إغفال هوية المُسْتَخْدِم:

لقد عَرّفَ التشريع الإماراتي آلية التشفير بغرض إخفاء البيانات، بأنها: التقنية التي تتم من خلالها مُعَالَجَة البيانات الشخصية للمُسْتَهلِك، على نحو لا يتيح فرصة التتبُع والربط، وتنسيب هذه البيانات بصاحبها، من دون استخدام معلومات إضافية[73]. كما أوجب على كل مُزَوِّد – في السياق ذاته؛ توطيدًا لمبدأ تخصيص استخدام البيانات الشخصية – عدم الاحتفاظ بهذه البيانات، بعد استنفاد الغرض من مُعَالَجَتها. واستثناءً أجاز الإبقاء عليها؛ لكن بشرط تشغيل آلية إخفاء هوية صاحب البيانات[74].

هذا ويرى الباحثان أن مبدأ سرية المعلومات ومجهولية الهوية من المُسَلَّمَات التي أقرت بها جُلُّ التشريعات الوطنية[75]، والتنظيمات الإقليمية[76]، لأغراض الحفاظ على البيانات الشخصية للأفراد، وعدم كشفها للعوام، وهذا الذي سارت عليه إمارة دبي في سياستها التنظيمية لخدمات إنترنت الأشياء، حين ألزمت كلَّ مُزوّد بخدمات إنترنت الأشياء باستخدام معيار تشفيري بمتطلبات الجهات المعتمدة داخل الدولة. وعليه أن يلتزم أيضًا بتوجيهات السلطات المختصة، خاصة في شأن متطلبات المصلحة العامة، والسلامة، والأمن الوطني[77].

---

(73) المادة (1) من المرسوم بقانون اتحادي رقم 45 لسنة 2021م، بشأن حماية البيانات الشخصية.

(74) المادة (5) من قانون حماية البيانات الشخصية لسنة 2021، «عدم الاحتفاظ بالبيانات الشخصية بعد استنفاد الغرض من معالجتها، ويجوز الإبقاء عليها في حال تم إخفاء هوية صاحب البيانات باستخدام آلية إخفاء الهوية».

(75) وهو من بين المسوِّغات التي قعَّد عليها المشرع الأسترالي سياسته الخاصة بحماية الخصوصية Australian Privacy Protection (APP)، كمبدأ ثانٍ تحت مسمى «مبدأ السرية وإغفال الهوية» and Pseudonymity Anonymity، بقوله: «يجب أن يُمنح للأفراد خيار عدم الإفصاح عن هويتهم، أو استخدام اسم مُسْتَعَارَ، عند التعامل مع الهيئة الأسترالية العامة، أو هيئات خاصة، في شأن مسألة معينة».
Australian Privacy Act No.119 of 1988, 14 Dec.1988. Privacy Act 1988

(76) وهذا ما أقره النظام الأوروبي العام لحماية البيانات (GDPR) في المادة (26) بخصوص مبدأ سرية المعلومات:
Art.26 GDPR: "The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.", on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing, Directive 95/46/EC (General Data Protection Regulation).Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(77) البند 7.11 من السياسة التنظيمية لخدمات إنترنت الأشياء.

كما ألزم – من جهته – قانون حماية البيانات الشخصية الجديد، حفاظًا على أمان استخدام البيانات الشخصية، كلًا من المُتَحَكِّم والمُعَالِج بوضع إجراءات خاصة للتشفير، وتطبيق آلية إخفاء البيانات، وإعمال كل الإجراءات التي تضمن استمرارية سرية أنظمة وخدمات المُعَالَجَة، وسلامتها وصحتها ومرونتها[78].

غير أن الإشْكَال الذي يُطْرَح، هنا، هو صعوبة تطبيق آلية التشفير بصدد استخدامات إنترنت الأشياء؛ فالتحدي الأكبر الذي يواجهه مبدأ الحفاظ على سرية ومجهولية المُسْتَخْدِم لخدمات إنترنت الأشياء هو التشخيص التلقائي الذي تقوم به هذه الخدمة، بالاستخدام البَيْني بين أجهزة الاستشعار، أو بين الخدمة وخدمة أخرى[79].

وبهذا النمط المُعْتَمَد، في إطار تقنية إنترنت الأشياء، سيَصْعُب استخدام خاصية الأسماء المُسْتَعَارة لإغفال هوية المُسْتَخْدِمين، بما أنه في مرحلة عملية جمع المعلومات الخاصة بهؤلاء المُسْتَخْدِمين يتم تجاهل هذه الخاصية، وهذا يؤدي إلى مخاطر جديدة تقتضي تطوير وتحديث التكنولوجيا المُسْتَخْدَمة في مجال التشفير، وإخفاء المعلومات، تتناسب مع مستويات تطور إنترنت الأشياء، ومع حجم التهديدات التي تمثلها[80].

ويؤكد الباحثان ضرورة استحداث أدوات قانونية خاصة، تسعى إلى حماية البيانات الشخصية للمُسْتَخْدِم، وإعلامه بمحاذير خدمات إنترنت الأشياء، من خلال التغليظ من التزامات المهنيين المُكلَّفين برقابة هذه البيانات، مثل: الالتزام بالإعلام والتبصير، والالتزام بأمان استخدام إنترنت الأشياء، وكسب ثقة المُسْتَخْدِم بهذه الخدمات؛ بإقرار حق المُسْتَخْدِم في الرضا المُستنير، وهذا ما أقرته المادة (13) من القانون الإماراتي الخاص بحماية البيانات الشخصية، بحق المُسْتَخْدِم صاحب البيانات في الحصول على المعلومة متى طلبها من المُتَحَكِّم، من دون دفع أيّ مقابل، حول نوع البيانات الشخصية المراد مُعَالَجتها، وأغراضها، وضوابط ومعايير ومدد تخزينها، وكذا إجراءات تصحيح هذه البيانات، أو محوها، أو تقييد مُعَالَجتها، أو الاعتراض عليها، والتدابير المتوقع اتخاذها في حال اختراق، أو انتهاك، هذه البيانات الشخصية[81].

(78) المادة (1) من المرسوم بقانون اتحادي رقم 45 لسنة 2021، بشأن حماية البيانات الشخصية.

(79) Xavier Caron and Rachelle Bosua and Sean B. Maynard and Atif Ahmad, The Internet of Things (IoT) and its Impact on Individual Privacy: An Australian Perspective, Computer Law & Security Review 32, (2016), p.9.

(80) Luigi Atzori and Antonio Iera and Giacomo Morabito, The Internet of Things: A Survey, Computing Networks, 54, (2010), p.2291.

(81) تنص المادة (13) من قانون حماية البيانات الشخصية على أنه: «يحق لصاحب البيانات، وبناءً على طلب يقدمه إلى المُتَحَكِّم، ومن دون أي مقابل، الحصول على المعلومات التالية:
هـ – ضوابط ومعايير مدد تخزين وحفظ بياناته الشخصية.

ويرى الباحثان أن هذه الأحكام ليست كافية لإعلام المُسْتَخْدِم بمخاطر خدمة إنترنت الأشياء؛ إذْ لا بد – من وجهة نظرهما – من الإقرار بالتزام عام بالإعلام المتبصر لصاحب البيانات بمخاطر الاستخدام، من غير الحاجة إلى طلبها من هذا الأخير، وهذا ما أقرَّ به – مثلًا – التنظيم الأوروبي العام بشأن حماية البيانات، في المادة (25)، والتي استحدثت التزامًا عامًا على عاتق المُتَحَكِّم في البيانات، بالسهر على ضمان خصوصية البيانات، خلال مرحلة تصميم الخدمة Privacy by Design، وحتى مرحلة الاستخدام؛ بحيث يكون المُسْتَخْدِم مطمئنًا إلى أن هذه الخصوصية لن تُنْتَهك افتراضيًا، وهذا سيسمح له بقياس حجم المَخاطر المُهدِّدَة المُتَوقَعَة لحقه في الخصوصية، واتخاذ قرار مستنير وواضح[82].

بالإضافة إلى ذلك، ألزم التنظيم الأوروبي المهني المُتَحَكِّم في البيانات «بضرورة إعلام المُسْتَخْدِم عن المخاطر المُحْتَمَلَة من مُعَالَجَة بياناته الشخصية في شكل واضح وسليم، باستخدام لغة واضحة ومقروءة»[83]، وحمايةً له كذلك من الاستخدام المفرط لبياناته الشخصية. كما بيَّن التنظيم أن تقدير مدى حرية وسلامة رضا المُسْتَخْدِم بالمعلومات الممنوحة له تقاس بمدى اعتبار «البيانات الشخصية غير الضرورية لتنفيذ العقد» جزءًا من الموافقة الحرة التي أبداها المُسْتَخْدِم يوم التعاقد[84].

الفرع الثاني

حماية الخصوصية والرغبات المشروعة لمُسْتَخْدِم إنترنت الأشياء

لعل من الملاحظ، هنا، عدم كفاية النصوص العامة لحماية الخصوصية؛ لتطبيقها بشكل سليم بصدد إنترنت الأشياء، وذلك في ظل غياب تشريع اتحادي واضح المعالم،

و– إجراءات تصحيح أو محو أو تقييد المعالجة، والاعتراض على بياناته الشخصية.

ز– الإجراءات التي ستتخذ في حال اختراق أو انتهاك بياناته الشخصية، خاصة إن كان الاختراق أو الانتهاك لخطر مباشر وجسيم على خصوصية وسرية بياناته الشخصية».

(82) Sandra Wachter, Normative challenges of identification on the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, 34, (2018), p.445.

(83) Art. 7.2 GDPR: "If the data subject's consent is given in the context of a written decl - ration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language".

(84) Art. 7.4 "When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract…, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract".

في دولة الإمارات العربية المتحدة، بخصوص استخدام إنترنت الأشياء والتشريعات العربية عمومًا، مع التأكيد أن الحماية المكفولة، دستوريًا، لحق الفرد في الخصوصية[85]، أو تلك التي أقرها التشريع الخاص بحماية البيانات الشخصية[86]، وكذلك الحماية المُقرَّرَة في النصوص العقابية الخاصة[87]، وبقية القوانين الناظمة للأنشطة على شبكة الإنترنت ومواقع التواصل[88]، هذه الحماية لم تعد كافية لاستيعاب مخاطر إنترنت الأشياء، بالنظر إلى المستويات العالية من التقانة والتعقيد التي وصلت إليها هذه التكنولوجيا، والتي تشكك في مدى إعمال النظرة الكلاسيكية لحماية البيانات والخصوصية بوجه عام، الواردة في القواعد العامة المدنية منها، أو الجزائية.

ولعل هذا ما أبانت عنه الرؤية المُسطَّرة في السياسة التنظيمية لإمارة دبي؛ بشأن توفير بيئة آمنة لخدمات إنترنت الأشياء، يكمن في تحجيم التجاذب الموجود بين تحقيق حماية حقوق ومصالح المُسْتَخْدِمين في خصوصيتهم من جهة، وضمان تطوير خدمات إنترنت الأشياء، والتي ترتكز – في الأساس – على مدى الاستغلال الواضح والشفاف للبيانات الضخمة[89].

ويُثمِّن الباحثان التحديث الذي جاء به القانون الإماراتي الاتحادي رقم 15، المُؤرَّخ في نوفمبر 2020، والخاص بحماية المستهلك، بحيث جعل حق حماية خصوصيته، وأمن بياناته، وعدم استخدامها في أغراض الترويج والتسويق (المادة 4) من الحقوق الأساسية[90]. وهذه الأحكام ستوفر – من دون شك – حماية لمُسْتَخْدِمي الأشياء الذكية والمتصلة، والتي تعتمد في الأساس على استغلال بياناته الشخصية لأغراض تجارية بحتة.

ويرى الباحثان أن السياسة التشريعية الأوروبية، في مجال حماية الخصوصية في إنترنت الأشياء، تعتبر نموذجًا يمكن الاهتداء به للحد من الخروقات التي تشكلها

(85) بيّنت المواد (26)، و(31)، و(36) من الدستور الإماراتي لسنة 1971م وتعديلاته لغاية سنة 2009م أن الحرية الشخصية مكفولة لجميع المواطنين، وأنه لا يتم تفتيشهم إلا وفقًا لأحكام القانون.

(86) المرسوم بالقانون الاتحادي الإماراتي رقم 45 لسنة 2021م، بشأن حماية البيانات الشخصية.

(87) منها المادة (378) من قانون العقوبات الاتحادي، والتي عاقبت كل من اعتدى على حرمة الحياة الخاصة أو العائلية للفرد.

(88) كالمادة (21) من القانون الاتحادي رقم 12 لسنة 2016، في شأن مكافحة جرائم تقنية المعلومات، والتي منعت كل استخدام للشبكة المعلوماتية أو نظام معلوماتي فيه مساس واعتداء على خصوصية الأفراد.

(89) البند (4) من السياسة التنظيمية لخدمات إنترنت الأشياء بإمارة دبي.

(90) المادة (4) من القانون الاتحادي رقم 15 بشأن حماية المستهلك، المؤرخ في 15 نوفمبر 2020، العدد 690، السنة 50، ص37: «تعتبر كل الالتزامات المقررة بموجب هذا القانون حقوقًا للمستهلك، وبما يشمل: (....) حماية خصوصية وأمن بياناته، وعدم استخدامها في أغراض الترويج والتسويق».

إنترنت الأشياء بحق الخصوصية، وحرمة الحياة الخاصة، فنجد أنها قطعت أشواطًا بعيدة لتطوير مظلة الحماية طوال مرحلة استخدام هذه التكنولوجيا؛ انطلاقًا من الصنع والتصميم، بموجب توجيه الاتحاد الأوروبي رقم 679–2016 المؤرخ في 27 أبريل 2016، بشأن حماية البيانات الشخصية[91].

ويختص هذا التوجيه – بشكل مباشر – بحماية الخصوصية، في إطار استخدام الأشياء المتصلة، من خلال تكريس نهجين لحمايتها بقواعد أمنية خاصة؛ الأولى هي: استراتيجية «حماية الخصوصية بحسب التصميم»[92]، والثانية هي: «حماية الخصوصية بشكل افتراضي».

ويمكن اعتبار هاتين الاستراتيجيتين بمنزلة السياسية المعتمدة على المستوى الأوروبي، لإدارة مخاطر حماية المعلومات المُسْتَخْدَمة لتشغيل الأشياء المتصلة، والتي جعلت حجَرَ زاويتِها هو مبدأ الحظر من المساس بخصوصية العملاء ومُسْتَخْدِمي هذه التكنولوجيا، وذلك بتسليط الرقابة على المُكلَّف بصَوْنِ هذه البيانات، والتأكد من مدى امتثاله لهذا الالتزام، بدءًا من مرحلة تصميم النظام، مرورًا بمراحل تطوير المُنتج أو الخدمة[93].

كما ذهب التنظيم الأوروبي إلى أبعد من ذلك، عندما أقرَّ بضرورة التزام الشركات المُسوِّقة لهذه التكنولوجيا بإجراء دراسة بشأن تأثير مُعَالَجَة البيانات الشخصية على الخصوصية، والمعروف أيضًا باسم تقييم تأثير الخصوصية؛ قبل طرح الشيء المتصل للتداول في السوق، على أن تنصب هذه الدراسة على تحليل التفاعلات الجارية بين هذه الكيانات والعملاء، وذلك للتأكد من كسب ثقة المستهلكين بخدماتهم، وتحسين صورة وسمعة الشركات ومنتجاتها، من خلال طمأنة زبائنها؛ بوضع حقهم في حماية الخصوصية في صميم اهتماماتها[94]، مع وضع عقوبات شديدة في حال الإخلال بهذه الالتزامات الجديدة؛ بغية تشجيع الشركات على الامتثال؛ إذ قضى التنظيم الأوروبي

(91) Règlement de UE n°2016-679 du 27 avril 2016 art. 25.

(92) منى الأشقر جبور ومحمد جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، ط1، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، 2018، ص143.

(93) Caroline Laverdet, Les Enjeux Juridiques de L'Internet des Objets, La Semaine Juridique, édition générale, n° 23, 9 juin 2014, Dalloz, Paris, pp.1154-1155.

(94) Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.

بتغريم الشركات المخالفة بغرامات قد تصل إلى 10 ملايين يورو، أو ما يصل إلى 2% من الإيرادات السنوية في جميع أنحاء العالم، في حال عدم امتثال الشركة للالتزامات المحدد[95].

كما أدرك التنظيم الأوروبي، أيضًا، أن البيانات أصبحت اليوم هي شريان القطاع الاقتصادي والمادة الخام، وأن تحليل البيانات الضخمة للمستهلكين، بشكل غير متزن، سيفضي غدًا إلى تعاظم مخاطر تنميط المستهلك، وقولبة الخدمات والحاجيات الشخصية للأفراد؛ فسعى إلى حماية المُسْتَخْدِم من أخطار التنميط، واستقراء ميولات، وتطلعات الأفراد من الخدمات المنتَظَرة منهم، باستخدام تقنيات الربط والدمج بين أجهزة الاستشعار التي تزود بها خدمات إنترنت الأشياء، وإشراك جهات خارجية في هذه البيانات، مثل شركات التأمين، والمؤسسات الكبرى، لاستغلالها بشكل غير ملائم.

كما أبدى المُشَرِّعون الأوروبيون مخاوفهم من الاستخدام غير المضبوط لإنترنت الأشياء، معترفين بأن هذا التنميط العام للخدمات سيفتح المجال أمام التمييز غير المشروع الذي قد تفضي إليه خدمات إنترنت الأشياء، لاسيما عند اتساع نطاق مشاركة البيانات الشخصية للأفراد، ودمجها في القطاع الخدماتي من غير حدود؛ فدعت المفوضية الأوروبية إلى وضع مجموعة من المبادئ التوجيهية للتحكم في تنظيم إنترنت الأشياء، وحثت على أن «ارتباط الأفراد بخدمات إنترنت الأشياء، من شأنه تسليط مزيد من التصنت والترصد والرقابة على الأفراد، من خلال تنميط وقولبة الخدمات التي تقوم بها السلطة العامة والهيئات الخاصة، على حد سواء»[96].

وللتصدي للتحديات سالفة الذكر، أقرَّ التنظيم الأوروبي العام لحماية البيانات مجموعة من الأدوات، تم تزويد المُسْتَخْدِمين أصحاب البيانات بها، لضمان التحكم في الاستخدام الآمن لبياناتهم، وتقرير مآل هذه البيانات، من خلال الإقرار بالآليات التالية:

أ- **الإقرار بحق مُسْتَخْدِم إنترنت الأشياء في تعطيل خاصية الاتصال بالشبكة:** يعتبر الاعتراف بهذا الحق، وفقًا للخبراء، دعامة إضافية للحماية المقررة للخصوصية، وفق التصميم، أي من يوم تصميم الشيء الذكي وصنعه. وقد أقرَّت المفوضية الأوروبية بما تم تسميته «بالحق في صمت الرقاقة»، في توصيتها بتاريخ 12 مايو 2009. ويهدف هذا الإجراء إلى استعادة التحكم

(95) Règlement de UE n°2016-679 du 27 avril 2016, Art 83.

(96) Sandra Wachter, Normative Challenges of Identification in the Internet of Things: Privacy, Profiling, Discrimination, and the GDPR, Computer Law & Security Review, 34, (2018), p.443.

في الأشياء المتصلة من قِبل المُسْتَخْدِم؛ وذلك من خلال العودة إلى الاستخدام «العادي» للكائن، من دون تفاعل إلكتروني، بواسطة الاحتفاظ بحق المستهلك في تعطيل اتصال الجهاز ومشاركة البيانات.

وبتفعيل هذه الخاصية، في الأشياء المتصلة، ووفق الغرض من الشريحة المُثبّتة في الشيء المتصل، يجب أن يظل المستهلك، أو المُسْتَخْدم، قادرًا على طلب تعطيل وإلغاء تنشيطه من دون مقابل، وبصفة مجانية. ويتعيَّن على الشركات المُصنِّعة إدراج هذه الخاصية، منذ مرحلة تصميم الكائن((97).

ب- الإقرار بحق المُسْتَخْدِم في محو أو تصحيح البيانات غير الدقيقة:

أقرت المادة (16) من التنظيم الأوروبي بإمكان الحق في تصحيح، أو محو البيانات غير الدقيقة، وإكمال البيانات غير الكاملة، وهي أداة أساسية لتقرير المصير المعلوماتي لهذه البيانات، أو التخفيف من استخدام البيانات غير المرغوب فيها. وأعطت المادة (17) إمكان محو هذه البيانات، عندما لا تصبح غير ضرورية للأغراض المُسطَّرة عند جمعها ومُعَالَجَتها.

وتأثرًا بالحكم السالف، أقرَّ القانون الإماراتي لحماية البيانات الشخصية في المادة (17)، بالحق في تصحيح، أو محو، البيانات الشخصية غير الدقيقة، أو استكمالها، أو طلب محوها في أيٍّ من الحالات المُحدَّدَة قانونًا، وهي: عندما تصبح البيانات الشخصية غير ضرورية، وفي حال عدول صاحب البيانات عن الموافقة التي بُنيت عليها المُعَالَجَة، واعتراضه على المُعَالَجَة، أو غياب الأسباب المشروعة للمُتَحَكِّم في المواصلة في استغلالها. كما أقر المُشَرِّع – كذلك – بحق المُستخدِم في إيقاف المُعَالَجَة؛ إذا كانت المُعَالَجَة لأغراض التسويق المباشر، بما في ذلك التنميط ذو العلاقة بالتسويق المباشر.

ج- تشديد الحماية بشأن البيانات الشخصية للمستهلك المتعلقة بالصحة والرفاه:

ظهر – في الآونة الأخيرة – جيل جديد من المنتجات والخدمات يسعى إلى التقييم الذاتي لعادات مُسْتَخْدِميها، وكذا نمط حياتهم. وتعرف بأجهزة التقدير الذاتي

(97) Règlement de UE n°2016-679 du 27 avril 2016 art. 80. règlement (UE) 2016/ 679 du Parlement Européen Et Du Conseil - du 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, et abrogeant la directive 95/ 46/ CE (règlement général sur la protection des données) (europa.eu) (19.04.2022).

للصحة والرفاه، مثل الساعات والعدادات التي تقيس خطى المُسْتَخْدِم، وفرشاة الأسنان، وأشياء أخرى متصلة تستقي البيانات الشخصية المتعلقة برفاه الفرد وصحته، علمًا بأن مثل هذه المعلومات الحساسة التي تستخدمها الشركات المُصنِّعة لتطوير منتجاتها وخدماتها، تتطلب مزيدًا من الحرص والتشديد للحفاظ على خصوصية الأفراد.

وقد أقر المُشَرِّع الإماراتي الطابع الخاص لهذه البيانات الشخصية، وأطلق عليها تسمية «البيانات الشخصية الحساسة»، وأدرج فيها القياسات الحيوية البيوميترية الخاصة به، أو أي بيانات خاصة بصحة هذا الشخص، وتشمل حالته الجسدية، أو النفسية، أو الذهنية، أو العقلية، أو البدنية، أو الجينية، أو الجنسية، بما في ذلك المعلومات المتعلقة بتوفير خدمات الرعاية الصحية له، وتكشف عن وضعه الصحي[98].

كما اعترفت المادة (4) من النظام الأوروبي لحماية البيانات بخصوصية هذه البيانات باعتبارها «أي معلومات تتعلق بالصحة الجسدية، أو العقلية، لشخص ما، أو تقديم الخدمات الصحية لذلك الشخص»، مع التأكيد على إخضاعها لنظام قانوني خاص؛ لأنها تشكل بيانات حساسة، يحظر قانون حماية البيانات مُعَالَجَتَها وجمعها مبدئيًّا، ما لم يكن الشخص المعني قد أعطى موافقته الصريحة على ذلك.

من جهته أقر التقنين الفرنسي الخاص بالصحة العامة، في مادته (L.1111-8)، بوجوب الحصول على موافقة مسبقة من وزير الصحة المُكلَّف، لتداول بيانات شخصية متعلقة بالصحة من طرف مضيفها. من هنا أقر الفقه الفرنسي أنه يمكن مستقبلًا، وفقًا لهذا الحكم، إخضاع الشركة المُصنِّعة للأشياء المتصلة، والتي تستضيف بيانات شخصية تخص رفاه المستهلك وصحته، للالتزامات المتعلقة بالبيانات الصحية؛ وفقًا لقانون الصحة العامة سابق الذكر[99].

وفي نظر الباحثَين يبقى القانون الأمريكي المحلي لولاية إيلينوي Illinois الأمريكية، المُخصَّص لحماية البيانات البيومترية لسنة 2015، والمعروف بقانون BIPA [100]، من أكثر التشريعات التي أبانت عن حماية ممتدة للمُسْتَخْدِم، حيث أعطى مفهومًا واسعًا للبينات البيومترية، ولم يحصرها في خدمة إنترنت الأشياء[101]، كما أن هذا القانون

(98) المادة الأولى من المرسوم بقانون اتحادي رقم 45 لسنة 2021، بشأن حماية البيانات الشخصية.

(99) Caroline Laverdet, op. cit, pl. 1154.

(100) 740 ILCS 14/ Biometric Information Privacy Act. (ilga.gov).

(101) Art. 14 (10): «Biometric information» means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

يلزم بحفظ هذا البيانات الحساسة وتخزينها بطريقة مكتوبة، مع ضرورة موافقة المستهلكين قبل جمع هذه المعلومات، وقد أعطى هذا القانون، في الولاية، فرصة مقاضاة الهيئات المستَغلّة لهذا النوع من البيانات الشخصية الحساسة، برفع دعاوى جماعية ضدها، بتهمة جمع بيانات بيوميترية، مثل: بصمة الوجه، وبصمات الأصابع.

كما أتاح فرصة ممارسة الدعاوى الجماعية لجمعيات حماية المستهلكين، في حال انتهاك الحق في الخصوصية، وهذا ما أقرَّه التنظيم الأوروبي الخاص بحماية البيانات الشخصية، بحيث أتاح للدول الأعضاء فرصة تفعيل الدعاوى الجماعية من طرف جمعيات حماية المستهلكين، مع ترك هذا الخيار بيد السلطة التقديرية للدول في الاعتراف بها.

ويعتبر هذا الإجراء بمنزلة إعادة بعث للوظيفة الوقائية لدعاوى المسؤولية المدنية ودعاوى التعويض، والذي يظل الخيار الوحيد لردع المهنيين عن ارتكاب أخطاء يجنون من خلالها أرباحا طائلة Fautes lucratives، خاصة لما لها من آثار وخيمة عندما يقع المساس على بيانات شخصية، وحقوق وحريات أساسية للأفراد[102].

ويرى الباحثان، فيما يتعلق بالتشريع الإماراتي، أنه يمكن لجمعيات حماية المستهلكين، مستقبلًا، إثارة مثل هذه الدعاوى في حالة المساس بالرغبات المشروعة لمُسْتَخْدِمي الأشياء المتصلة والذكية، من إعمال حكم المادة (7) من القانون الاتحادي لحماية المستهلك رقم 15 لسنة 2020[103]، على أساس إخلال المُزَوِّدين ومُصنِّعي هذه الخدمات والمنتجات بالتزامهم بوجوب تنبيه المستهلك وتنويره؛ بشأن كل استخدام ينطوي على خطورة بشكل واضح ودقيق، وفقًا لما تقرُّ به اللوائح التنفيذية الموضِّحَة لذلك.

كما يقع على عاتق المُزَوِّدين، وجميع المهنيين المساهمين في طرح الأشياء الذكية، وفقًا لنص المادة (11) من القانون ذاته، إبلاغ الوزارة، أو السلطات المحلية المختصة، فور اكتشاف أي عيوب من المُحْتَمَل أن تضر بالمستهلكين، وبيان كيفية الوقاية منها، ولو اقتضى الأمر سحبها من السوق على وجه السرعة، أو إعلان خطورتها[104].

(102) Caroline Laverdet, op. cit., pp.1154-1155.

(103) المادة (7) من القانون الإماراتي الاتحادي رقم 15، بشأن حماية المستهلك.

(104) المادة (11) من القانون الإماراتي الاتحادي رقم 15، بشأن حماية المستهلك.

المطلب الثاني
ضمان حق المستهلك في التعويض
عن أضرار إنترنت الأشياء

وتتمثل الصعوبة الأخرى، المرتبطة باستخدام إنترنت الأشياء، في خطر الأضرار التي تُعرِّض مستخدميها – بصفة مُطوَّلة – للموجات الكهرومغناطيسية التي يولِّدها؛ حتى إن كانت عواقب التعرُّض المفرط للأمواج ثابتة بالكامل من الناحية العلمية، غير أن هذا لا يمنع – بعد التشريعات – من إعمال مبدأ الحيطة والحذر، وهذا ما أقرَّته الحكومة الفرنسية مكرِّسةً هذا المبدأ في المادة (5) من ميثاق البيئة، والذي تم منحه قيمة دستورية بقرار من مجلس الدولة في عام 2008، وهو يُخوِّل السلطات العامة اتخاذ تدابير وقائية دون الحاجة إلى إظهار جدية المخاطر على صحة وسلامة الأشخاص بشكل كامل. وهذه الخطوة من المحبَّذ إعمالها من طرف السلطات العامة؛ لصياغة معايير صناعية ستُفرَض على مُصنِّعي الأشياء المتصلة مستقبلا[105].

كما تكمن خصوصيات أضرار إنترنت الأشياء في طبيعتها الخاصة، وصعوبة تحديد المسؤول عنها، بحيث يبدو من الصعب تطبيق القواعد العامة للمسؤولية المدنية وفقًا للنهج الكلاسيكي بصددها، لاسيما فيما يتعلق بمبدأ المسؤولية المشتركة؛ كونه غير مناسب لأضرار إنترنت الأشياء؛ لذلك يبدو من الضروري تكييف الإطار التنظيمي، مع الأخذ بعين الاعتبار هذه الخصوصية التي يتصف بها الضرر الذي تتسبب فيه الأشياء المتصلة بالشبكة العنكبوتية.

ويمكن هنا إيجاد ثلاث طوائف رئيسية من الأضرار، هي:

أ- الأضرار التقليدية الناجمة عن استخدام إنترنت الأشياء، والماسة بالجسد أو المال.

ب- لانتهاكات الماسة بالبيانات الشخصية للمُسْتَخْدِمين وخصوصيتهم.

جـ- الأضرار الماسة بالمصالح الاستهلاكية لمُسْتَخْدِم إنترنت الأشياء، في حال عدم استجابة الخدمة أو المُنتَج المقدَّم لرغباتهم وتوقعاتهم المشروعة.

(105) Sabine Bernheim-Desvaux, Objets connectés: L'objet connecté sous l'angle du droit des contrats et de la consommation, Contrats Concurrence Consommation, Lexis Nexis, n° 1, Janvier 2017, étude 1, pp.1-13.

ومن المُحْتَمَل جدًّا – في مجال الانتهاكات الماسة بسلامة الأشخاص، في مجال إنترنت الأشياء ـ أن تنصب بمناسبة استخدام بالسيارات ذاتية القيادة، والتي على الرغم من برمجتها، يمكن أن تتورط في حوادث مرورية، يصعب معها تطبيق القواعد الكلاسيكية لتعويض ضحايا هذه الحوادث، في ظل انسحاب السائق البشري.

ويشهد الواقع العملي على حصول عدة انتهاكات – تسببت فيها إنترنت الأشياء والكيانات المتصلة – أدت إلى إلحاق أضرار جسدية أو مالية بالمستهلك، وهذا ما حصل تحديدًا مع امرأة، في مقتبل عمرها، في كوريا الجنوبية، في العام 2015، وفق ما أوردته تقارير صحافية؛ إذ تعرضت للهجوم من قبل مكنسة كهربائية متصلة، تعمل بالروبوت، والتي مصت شعرها عن غير قصد، في أثناء نومها.

ولايزال النقاش حادًّا بين الفقهاء، بشأن مدى إمكان تطبيق أحكام مسؤولية المنتجين المستوحاة من التوجيه الأوروبي لسنة 1998، في وقت شككت فيه مفوضية الاتحاد في قدرة تمديد أعمال المسؤولية المشدَّدَة والصارمة للتوجيه الأوروبي، بصدد إنترنت الأشياء؛ لاعتبار هذه الأخيرة أقرب إلى الخدمة أكثر من المُنتَج؟ مؤكدةً أن أحكام هذا التوجيه كانت ثمرة تحكيم بين المصالح المتضاربة للمستهلكين والمهنيين، ولا يصلح مع معطى إنتاج واستخدام تكنولوجيا إنترنت الأشياء(106).

والخصوصية الأخرى التي تمثلها أضرار إنترنت الأشياء، هي صعوبة تحديد المسؤول بشكل قطعي ودقيق؛ إذ غالبًا ما يتم تجريد الضرر الناشئ من الكيان المادي للشيء، ليتجسد – في الغالب – في سلسلة المتدخلين في تصميم الشيء الذكي، أو في كيان مستقل مُزَوَّد بخاصية الذكاء الاصطناعي، كما تزيد صعوبة تحديد المسؤولية عن الأضرار كلما وقع الانتهاك على البيانات الشخصية للمستهلك، ويمكن التساؤل عن طريقة التعويض العادل والجابر لهذا النوع من الأضرار.

(106) Nathalie Martial-Braz, Objets connectés et responsabilité, Revue Dalloz IP/IT, Paris, 2016, pp.399-403.

الخاتمة

اتضح للباحثين، في ظل دراسة التحديات القانونية المعاصرة لاستخدامات إنترنت الأشياء، ودراسة النظام القانوني الإماراتي والمقارن، مجموعة من النتائج والتوصيات، يمكن إيجازها في الآتي:

أولًا: النتائج

- أحسن المُشَرِّع الإماراتي بوضع سياسة تنظيمية لخدمات إنترنت الأشياء، تضمنت جوانب مهمة، تركز على تحديد المفاهيم، مثل: مفهوم إنترنت الأشياء، والبيانات وتصنيفها، وتطبيقاتها المختلفة، ونطاق العمل، وضوابط الاستخدام، والجزاء المترتب على مخالفة هذه الضوابط.
- يشكل تزايد استخدام إنترنت الأشياء الحاجة إلى المقدرة على إدارة هذا التحول، وجاهزية البنية التحتية لإنترنت الأشياء، بواسطة التكنولوجيا القادرة على ربط الكم الضخم من البيانات والأجهزة بعضها ببعض، والجاهزية التكنولوجية لارتباطها بالإنترنت، وتوفير الخبرات اللازمة للتعامل مع تعقيد الأنظمة المُسْتَخْدَمة لإدارة هذا التحول في أنماط الحياة والعمل.
- اتضح للباحثين، على الرغم من الاستخدام الإيجابي لإنترنت الأشياء، وجود مخاطر قانونية مظلمة، تمس الحياة الخاصة، أو الحق في الخصوصية والرقابة السرية للأشخاص، وإفشاء الأسرار، وأخرى تقنية، مثل: الأخطاء غير المتوقعة والمُحْتَمَلة.
- تجلى للباحثين ضرورة أن تتعامل السلطات العامة بالحيطة والعقلانية، بعدم ترك الهيمنة المطلقة للشركات المُصنِّعة لهذه التكنولوجيا من دون رقابة كافية، من خلال وضع خطة ممنهجة يجتمع فيها رجال القانون والتقنية على حد سواء.
- إن القواعد العامة في المسؤولية المدنية لا تحقق حماية وقائية من مخاطر إنترنت الأشياء، في ظل التطور التكنولوجي، خاصة في ضوء عدم قيام المسؤولية المدنية إلا بتحقق الضرر وثبوته، الأمر الذي يشكل قصورًا تشريعيًا، كما أن الشخص في حاجة إلى الحماية قبل حدوث الضرر.
- يحسب للمُشَرِّع الإماراتي التحديث الذي جاء به القانون رقم 15، المؤرخ في نوفمبر 2020، والخاص بحماية المستهلك، بحيث جعل من الحقوق الأساسية التي يملكها المستهلك في المادة (4)، حقه في حماية خصوصيته، وأمن بياناته،

وعدم استخدامها في أغراض الترويج والتسويق، وهو ما يشكّل حماية لمُسْتَخْدِمي الأشياء الذكية والمتصلة، والتي تعتمد في الأساس على استغلال بياناته الشخصية لأغراض تجارية بحتة.

ثانيًا: التوصيات

- العمل على عقد اتفاقيات عربية تنظمُ إنترنت الأشياء في ظل الذكاء الاصطناعي، وتُحققُ الحماية الوقائية المنشودة من مخاطرها، وقبل حدوث الضرر.
- تعميم الالتزامات على الصناع ومصممي الأشياء الذكية، بضرورة وضع لافتات وتنبيهات إلزامية على جميع الأشياء المتصلة؛ لمحاربة جمع البيانات السرية والتجسس، في صورة التوجيهات التي تضمنها التنظيم الأوروبي حول حماية البيانات الشخصية للأفراد، مع مراعاة مبدأ الشفافية، من خلال تزويد جمهور المستهلكين بمعلومات كافية تُعرِّفهم بما ستؤول إليه بياناتهم الشخصية المتداولة.
- تعزيز سياسة التعريف باستخدامات إنترنت الأشياء، من خلال تزويد ملصقات وشهادات تدل على موثوقية استعمالها؛ بالإضافة إلى تطوير المعايير التي يمكن للمنتجين استخدامها لضمان حق الأفراد في خصوصية بياناتهم الشخصية، وجلب ثقة أكبر لدى المستهلكين؛ لتسويق أشياء متصلة آمنة وعالية الجودة.
- يرى الباحثان ضرورة التدخل التشريعي المتأني، بإصدار قانون خاص بإنترنت الأشياء في دولة الإمارات العربية المتحدة خاصة، والدول العربية عامة، وصولًا إلى حماية الأشخاص من الجوانب المظلمة، ومن مخاطرها القانونية والتقنية، مثل: الرقابة السرية، وحفظ البيانات أو المعلومات، من دون الاعتداء عليها من الغير كحيازتها، وإفشائها، والأخطاء التقنية المتوقعة والمُحْتَمَلة، بما يكفل حماية وقائية من الضرر قبل حدوثه.
- الاستفادة من التوجيه الأوروبي، والتشريع الفرنسي، والقوانين الخاصة بأمن وحماية البيانات، وقوانين حماية المستهلك، عند إصدار القانون المرتقب، لمواجهة التحديات الحالية والمستقبلية المتعلقة باستخدام إنترنت الأشياء.
- ضرورة تثقيف المستهلك وتوعيته، وحماية حقه في الإعلام والتبصير، بأنجع الطرق التي تضمن الاستعمال الآمن والعقلاني لهذه التكنولوجيا، والاستفادة من إيجابياتها في أنماط الحياة والعمل المرتقبة، من خلال إجراءات الوسم والتعريف بالمنتجات والخدمات المطروحة، وضوابط استخدام هذه التقنية.

- ويرى الباحثان أن قانون حماية البيانات الشخصية الإماراتي، لسنة 2021م، وإن كان خطوة محمودة قطعها المُشَرِّع لوضع إطار عام لصون حقوق مُسْتَخْدِم النظم المعلوماتية بشكل عام، لكن الأمل في سن تشريع خاص يضمن أمان خدمات إنترنت الأشياء، واستخدامات الأجهزة المتصلة لما تحمله من مخاطر أعلى بمصالح المستهلك، مع الأخذ بعين الاعتبار الأسس التالية:

- ضرورة التشديد على المتعاملين الاقتصاديين بالسهر على تطبيق مبدأ تخصيص استغلال البيانات، بالوقوف عند حدود الغرض الذي تم تحصيل البيانات تحقيقًا له، وعدم استغلالها لأغراض أخرى من دون ترخيص.
- إقرار مبدأ التقليل من استخدام البيانات الشخصية؛ بإلزام المُزَوِّد بالتقليل من جمع البيانات، والاقتصار على البيانات الكافية، وذات الصلة بالأغراض التي تتم مُعَالَجَتُها لأجلها.
- ضرورة التأكد من توفير الإمكانات اللوجستية التي تسمح بضمان استخدام آلية التشفير، وضمان خاصية إغفال هوية المُسْتَخْدِم، لمنع إمكان التتبُع والربط وتنسيب هذه البيانات بصاحبها ضمانًا للخصوصية.
- ضرورة تشديد الحماية بشأن استخدام البيانات الشخصية للمستهلك، والمتعلقة بالصحة والرفاه، في ظل الطابع الحساس لهذه البيانات، والتي تتطلب الرفع من الحماية للحفاظ على خصوصية الأفراد.
- النظر في إمكان السماح لجمعيات حماية المستهلكين بممارسة دعاوى جماعية؛ ضمانًا لتعويض الانتهاكات التي تمس بخصوصية المستهلك، وحرمة بياناته الشخصية.

قائمة المراجع

أولًا: باللغة العربية

1- الكتب

- حسام الدين الأهواني، الحق في احترام الحياة الخاصة (الحق في الخصوصية): دراسة مقارنة، دار النهضة العربية، القاهرة، 1978.

2- البحوث

- أكمى تكيوكا تشاتفيلد، إطار عمل الحكومة الذكية الممكنة بإنترنت الأشياء: دراسة حالة لسياسات الأمن السيبراني لإنترنت الأشياء وحالات الاستخدام في الحكومة الفيدرالية الأمريكية، معهد الإدارة العامة، الرياض، س60، ع3، مارس 2020.
- إبراهيم حسن الملا، الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون، أكاديمية شرطة دبي، س26، ع (19 يناير 2018).
- بشار طلال المومني ومنذر طلال المومني، الحماية المدنية من مخاطر الذكاء الاصطناعي في التشريع الإماراتي، مجلة الحقوق، كلية الحقوق، جامعة البحرين، مج17، ع2، سنة 2021.
- هاري سوردين، الذكاء الاصطناعي والقانون: لمحة عامة، مجلة معهد دبي القضائي، ع11، السنة الثامنة، أبريل لسنة 2020.
- حسام الدين الأهواني، حماية الحق في الخصوصية في ظل قانون دولة الإمارات العربية المتحدة، مجلة الأمن والقانون، أكاديمية شرطة دبي، مج16، ع2، لسنة 2008.
- مارية الحصين، نظام تشريعي مقترح لأنظمة إنترنت الأشياء في المملكة العربية السعودية: دراسة استشرافية، مجلة الدولية للمعلوماتية والإعلام وتكنولوجيا الاتصال، جامعة بني سويف، مصر، مج3، ع2، 2021.
- محمد حسن علي، النظام القانوني لحماية البيانات الشخصية المعالجة إلكترونيًا: دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة، مجلة العلوم القانونية، كلية القانون، جامعة عجمان، الإمارات، مج7، ع14، يوليو 2021.

- محمد مالك، المعلومات والأمن: رهان استراتيجي وأدوات جديدة للصراع، مجلة الحكمة، مركز الحكمة للبحوث والدراسات، الجزائر، ع27، لسنة 2013.
- نهى بنت عوض الدارودي، كيف تحدد البيانات الضخمة مستقبلنا، أوراق عمل المؤتمر السنوي الخامس والعشرين لجمعية المكتبات المتخصصة، فرع الخليج العربي، إنترنت الأشياء: مستقبل الأشياء المتصلة، أبوظبي، 2009.
- سعيد عبداللطيف إسماعيل، رؤية وتحليل للتحديات المستجدة للحق في الخصوصية الناتجة عن الثورة الرقمية وتطور الاتصالات والإنترنت، مجلة كلية القانون الكويتية العالمية، السنة الثالثة، ع12، ديسمبر 2015.
- عبدالرحمن الدراجي خلفي، الحق في الحياة الخاصة في التشريع العقابي الجزائري: دراسة تحليلية مقارنة، مجلة جامعة الملك سعود – الحقوق والعلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة الملك سعود، الرياض، مج24، ع2، يوليو 2012م/ 1433هـ، 237.
- علي بن ذيب الأكلبي، العائد من تطبيقات إنترنت الأشياء على العملية التعليمية، المجلة الدولية للبحوث في العلوم التربوية، المؤسسة الدولية لآفاق المستقبل، تالين–أستونيا، مج2، ع3، لسنة 2019.
- عماد عبدالرحيم دحيات، إشكالية العلاقة بين البشر والآلة، مجلة الاجتهاد للدراسات القانونية والاقتصادية، جامعة تامنراست، الجزائر، مج8، ع5، لسنة 2019.
- فيصل عقلة خطار وآخرون، الحماية الدستورية والقانونية للحق في الحياة الخاصة، مجلة دراسات، علوم الشريعة والقانون، الجامعة الأردنية، مج4، ع1، لسنة 2020.

3– المقالات:

- براند مار، «أهم عشر حالات استخدام في الذكاء الاصطناعي والتَّعلُّم الآلي التي يجب على الجميع التعرف عليها»، 30 سبتمبر 2016.
- بتول عتوم ، من سيتحكم في إنترنت الأشياء، 24 يونيو 2020، من سيتحكم في إنترنت الأشياء؟ – ibara3e – إي عربي (20/02/2022).

- يوسف العربي، 4,2 مليار درهم الإنفاق على إنترنت الأشياء في الإمارات العربية المتحدة خلال 2019، جريدة الاتحاد، 17 أغسطس 2019.
- منى الأشقر جبور ومحمود جبور، البيانات الشخصية والقوانين العربية: الهم الأمني وحقوق الأفراد، ط1، المركز العربي للبحوث القانونية والقضائية، جامعة الدول العربية، بيروت، لبنان، 2018.
- مركز محمد بن راشد للابتكار الحكومي، ابتكر، دبي، «إنترنت الأشياء لخدمات حكومية أفضل»، بتاريخ 30 سبتمبر 2020.

ثانيًا: باللغة الأجنبية

- Anaëlle Grondin, Quand les objets connectés aident la police à résoudre des affaires criminelles, Journal les Echos, Paris, 26 avr. 2017.
- Caroline Laverdet, Les enjeux juridiques de l'Internet des objets, La semaine juridique - édition générale, Dalloz, Paris, n° 23 - 9 juin 2014.
- Emad Dahiyat, Intelligent agents and liability: is it a doctrinal problem or merely a problem of explanation? Artificial Intelligence and Law 18 (1), (2010), p.113.
- Imad Saleh, Internet des Objets (IdO): Concepts, Enjeux, Défis et Perspectives, Revue Internet des objets, ISTE Open Science, London, UK, 2017, 1.
- Jean- Paul Crenn, Les objets connectés décryptée pour les juristes, Revue Dalloz IP/IT, Sept. 2018, p.389.
- John Fruehe, The Internet of things is about Data, not Things, Fobes, 30 June. 2018. The Internet Of Things Is About Data, Not Things (forbes. com) (20.02.2022).
- Luigi Atzori, Antonio Iera, Giacomo Morabito, The Internet of Things: A Survey, Computing Networks, 54, 2010.
- Matthieu Bourgeois et Marion Moine, Internet des objets (IOT): Quand l'inerte s'anime, Revue pratique de la prospective et de l'innovation, Commission Prospective du Conseil national des barreaux and LexisNexis, Paris, N°2, oct. 2019.

- Myriam Quéméner, Objets connectés et cybercriminalité:risques et réponses juridiques, ENI, 2016.
- Nathalie Martial-Braz, Objets connectés et responsabilité, Revue Dalloz IP/IT, Paris, 2016.
- Overview of the Internet of things, Recommendation ITU-T Y.2060, 2012. https://academy.itu.int/sites/default/files/media/file/IoT%20TP%20Report.pdf#:~:text=In%202012%20the%20ITU%20defined%20IoT%20in%20Recommendation,existing%20and%20evolving%20interoperable%20information%20and%20communication%20technologies. (20.02.2022).
- Sabine 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.
- Sandra Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, Computer Law & Security Review, 34, 2018.
- Stéphane Larrière, Internet des objets, le droit à l'envers du décor?, 27 Juin 2016, https://laloidesparties.fr/internet-des-objets-droit.
- Terrell MC Sweeny, Consumer Protection in the Age of Connected Everything, Exploring the Things on the Internet of Things: Implications for Business, Consumers, and the Law, Volume 62 Issue 2, Jan. 2018.
- The Parrot Flower Power user guide, Parrot S.A, flower-power_user-guide_uk.pdf (parrot.com) (19.02.2022).
- Xavier Caron, Rachelle Bosua, Sean B. Maynard, Atif Ahmad, The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective, computer law & security review 32, 2016.
- Yaël Cohen-Hadria, Le véhicule connecté : Un objet connecté comme les autres? Revue Dalloz IP/IT, Paris, Mars. 2018.

المحتوى