

د. أحمد عبد العزيز محمد أبو الحسن

باحث بمركز أبحاث القانون/ كلية القانون

الجامعة البريطانية بمصر

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

■ **المراسلة:** د. أحمد عبد العزيز محمد أبو الحسن
باحث بمركز أبحاث القانون/ كلية القانون
الجامعة البريطانية بمصر

■ **معرف الوثيقة الرقمي (DOI):** jolets.v5i1.215/10.54873

■ **البريد الإلكتروني:** Ahmed.Aboualhasan@bue.edu.eg

■ **نسق توثيق البحث** أحمد عبد العزيز محمد أبو الحسن
حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة
وتأمين المنازل، المجلد الخامس، العدد الأول، أبريل ٢٠٢٥

الملخص

تعرض الطبيعة التقنية الخاصة والمعقدة للأنظمة الذكية المتصلة لإدارة وتأمين المنازل البيانات الشخصية لمخاطر جمة ، فاستخدام تلك الأنظمة لتقنيات "إنترنت الأشياء"، يمكنها من جمع كمية ضخمة ومتنوعة مستمرة من بيانات العابرين بنطاق مستشعراتها، وأيضاً فإن استخدامها لبرمجيات الذكاء الاصطناعي لمعالجة تلك البيانات وأداء المهام المطلوبة منها يعرض البيانات الشخصية لأنواع من المعالجة المتقدمة التي قد تعرض الأشخاص المعنية بها لمخاطر التنميط وأتمته اتخاذ القرارات المتعلقة بهم، كما أن استخدام تقنيات الحوسبة السحابية للربط بين أجزاء هذه الأنظمة الداخلية والخارجية يعرض البيانات الشخصية لمخاطر النقل والمتزامن والمستمر لها بشكل غير محدد ومعروف، واستخدام تقنيات التعرف على الوجه عن طريق مسح البيانات البيومترية للوجه يعرض الأشخاص المعنيين بالبيانات لمخاطر التتبع وقد ينجم عنه توجيه التهم الجنائية لهم بشكل خاطئ، ووجود الأجهزة المكونة لتلك الأنظمة في بيئة غير مؤمنة صناعياً قد يعرضها لمخاطر الاختراق الخارجي المستمر واستمرار عمل تلك الأجهزة طوال الوقت يعرض العابرين بنطاقها لجمع بياناتهم بدون موافقتهم أو وعيهم

وعليه يجب مراعاة تلك المخاطر المستحدثة أثناء تصنيع وتشغيل تلك الأنظمة الحديثة، وخصوصاً بعد أن ظهرت تطبيقات واقعية لمثل هذه الانتهاكات في مناسبات متعددة كفضيحة "شركة رينج التابعة لأمازون"، وقضية "وايس ضد شركة رينج"، وقضية "زيلمر ضد فيس بوك"، والتقارير الحقوقية المستمرة ضد شركات كشركة أمازون وخدماتها السحابية

Abstract

Smart and connected systems for managing and securing homes create risks related to personal data protection ,as The use of IoT technologies enables it to collect a huge ,diverse ,and continuous amount of data relating to the passers-by within its sensor range, also Its use of artificial intelligence software to process these data and perform the tasks required from it exposes personal data to advanced types of processing that may expose the data subject to the risks of profiling and the automation of decisions related to them ,And the use of cloud computing technologies to connect the different sections of these systems exposes personal data to the risks of unlimited ,simultaneous ,continuous ,and unknown transfer of personal data ,Using facial recognition techniques by scanning face biometric data exposes personal data subjects to tracking risks and may result in wrongful criminal charges ,and the presence of the devised that constitute those systems in an un-secure home environment may expose them to the contentious risks of external attacks ,and the continues operations of these systems ٧/٢٤ expose the passers-by to the risks of collecting their data without their consent or awareness.

Therefore ,those risks must be considered during the manufacturing and operating of these systems ,to avoid these risks.

مقدمة

أولاً: التعريف بالبحث

لم يقف التطور التقني على حدوده التي كان عليها منذ وقت قصير أثناء بدء الموجة الجديدة من قوانين حماية البيانات الشخصية، والتي استهلكتها اللائحة العامة الأوروبية لحماية البيانات الشخصية بما يعرف بـ «تأثير بروكسل»^١، فاليوم في ظل الانتشار الواسع للمنتجات والخدمات التقنية التي تتبني وتقوم على النقلة النوعية الجديدة لصناعات تقنية المعلومات والاتصالات الرقمية، ظهرت مخاطر مستحدثة والتي إن لم تثر قضايا جديدة في هذا المجال فقد عوّدت من المفاهيم المستقرة فيه

وهذا البحث يتناول بعضاً من هذه المخاوف، والتي أثارها فقه حماية البيانات الشخصية منذ فترة ما بعد إصدار الاتحاد الأوروبي للائحته الجديدة لحماية البيانات الشخصية وخصوصاً تلك المخاوف التي تتعلق بالتطبيقات الأحدث في تقنيات المعلومات والاتصالات الرقمية كـ: (الحوسبة السحابية، والذكاء الاصطناعي، وإنترنت الأشياء والقيمة، وتقنيات التعرف على الهوية بمسح نمط الوجه) وما يترتب عليها من مفاهيم فرعية، أظهرت الحاجة إلى إعادة النظر في بعض من المفاهيم الأساسية والأكثر استقراراً في فقه وقوانين حماية البيانات الشخصية

وهذا له اعتباره حيث أن اللائحة العامة لحماية البيانات الشخصية والتي مر عقد من الزمن منذ البدء في مداولاتها التشريعية، وست سنوات على سنّها، وأربعة على دخولها حيز النفاذ — وهي مدد قصيرة بالنسبة للمجال التشريعية — أصبحت بحاجة — للأسف — لتعديل في بعض موادها وفلسفتها لتتلاءم مع

١ يعرف تأثير بروكسل بأنه: التأثير الناجم عن قوة الاتحاد الأوروبي والسوق الأوروبية على باقي العالم نتاج حجم السوق وأهميته والمعايير الصارمة نسبياً والقدرات التنظيمية للاتحاد الأوروبي، لهذا تجد الشركات والدول على مستوى العالم أنه من المستحسن تبني المعايير والقوانين التي تضعها بروكسل أثناء اجرائها لأعمالها على مستوى العالم لا فقط داخل السوق الأوروبية الموحدة، وقد تمت صياغة مصطلح تأثير بروكسل في عام ٢٠١٢ من قبل البروفيسور أنو برادفورد من كلية الحقوق في كولومبيا.

University Oxford) World the Rules Union European the How :Effect Brussels The ,Bradford Anu Should :Effect in Is GDPR The ,Roberts John Jeff :See :أنظر : 2-3 (2020 Kingdom United ,Press .S.U :http://www.afraidbe.companies? :site web ,Fortune ,24 May ,2018 (Limited IP Media Fortune .bit/ :http://www.gdprfor/ly ، وفي مثال لهذا داخل مجال حماية البيانات الشخصية: قانون لخصوصية المستهلك لولاية كاليفورنيا بالولايات المتحدة في ٢٨ يونيو ٢٠١٨، والقانون البحريني لحماية البيانات الشخصية لعام ٢٠١٨، القانون المصري لحماية البيانات الشخصية لعام ٢٠٢٠، النظام السعودي لحماية البيانات الشخصية لعام ٢٠٢١

٢ دخلت اللائحة العامة بدائرة الاعتماد والتشريع الاتحادي كآلآتي: ٢٥ (يناير) ٢٠١٢: تم طرح الاقتراح الخاص باللائحة. ٢١ أكتوبر ٢٠١٣: أدلت لجنة البرلمان الأوروبي للحريات المدنية والعدل والشؤون الداخلية (LIBE) بصوتها التوجيهي، ١٥ ديسمبر ٢٠١٥: أسفرت المفاوضات بين البرلمان الأوروبي والمجلس والمفوضية (اجتماع ثلاثي رسمي) عن اقتراح مشترك، ١٧ ديسمبر ٢٠١٥: صوتت لجنة LIBE لجنة الحريات المدنية والعدل والشؤون الداخلية التابعة للبرلمان الأوروبي لصالح المفاوضات بين الأطراف الثلاثة. ٨ أبريل ٢٠١٦: اعتمدت اللائحة من قبل مجلس الاتحاد الأوروبي. وكانت الدولة العضو الوحيدة التي صوتت ضدها هي النمسا، التي جادلت بأن مستوى حماية البيانات في بعض النواحي أقل مقارنةً بتوجيه عام ١٩٩٥، ١٤ أبريل ٢٠١٦: اعتمدت اللائحة من قبل البرلمان الأوروبي، ٢٤ مايو ٢٠١٦: دخلت اللائحة حيز التنفيذ، بعد ٢٠ يوماً من نشرها في الجريدة الرسمية للاتحاد الأوروبي.

التقنيات الجديدة الآخذة في التسارع والتطور المستمر.

وسيتناول هذا البحث بعضاً من تلك المفاهيم انطلاقاً من تطبيق تقني حديث وهو «الأنظمة الذكية المتصلة لإدارة وتأمين المنازل»، والذي تم اختياره بالذات دوناً عن باقي الأنظمة التقنية الحديثة لأن البنية الحالية لها من حيث التصميم والتشغيل تعتمد مجموع التقنيات التي يهتم فقه حماية البيانات الشخصية بدراسة تأثيرها على منظومة حماية البيانات الشخصية الحالية، فهي تتبنى تقنيات إنترنت الأشياء في تصميم المنتجات المادية المكونة لها، و«الذكاء الصناعي وتطبيقاته» في أنماط معالجة للبيانات التي تنتهجها تحقيقاً لغاياتها، وأخيراً تقنيات «الحوسبة السحابية» لتحقيق التكاملية والاتصال بين مكوناتها الداخلية والخارجية، مما يجعلها نقطة انطلاقاً مثلى وتطبيقية لتناول المخاطر المستحدثة لتلك التقنيات الحديثة على الحق في البيانات الشخصية

ثانياً: أهمية الدراسة

تكمن أهمية الدراسة من حادثة موضوعها، كونها تبحث المخاطر الواقعة على البيانات الشخصية جراء معالجتها واستخدامها لأغراض الأنظمة الذكية لإدارة وتأمين المنازل، وقد اختار الباحث هذه الأنظمة بالتحديد لأنها تعطي فرصة فريدة لتناول تأثير مجموعة من أحدث التقنيات المعلوماتية على المفاهيم السائدة والمستقرة في فقه وتشريعات حماية البيانات الشخصية، وأيضاً تعرض تلك البيانات لمخاطر جديدة لم تتناولها التشريعات الحالية لحماية البيانات الشخصية بالتنظيم

هذه المخاطر التي ستكون مجموعها وأجزائها إشكاليات البحث، وسيكون تقديم توصيات وحلول لها هدفه

ثالثاً: إشكالية البحث:

تثير الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل بعض الإشكاليات التي تطول جميع جوانب المنظومة القانونية الحالية لحماية البيانات الشخصية، وسوف يحاول الباحث هنا تقديم حلول قانونية لبعض من تلك الإشكاليات، وهي:

- ١- ما المخاطر المستحدثة التي تثيرها التقنيات المستخدمة في إنشاء وتشغيل الأنظمة الذكية المتصلة لإدارة وتأمين المنازل «على الحق في البيانات الشخصية»؟
- ٢- ما هي الإشكاليات التي تثيرها تلك التقنيات المستحدثة على المفاهيم المستقرة في فقه حماية البيانات الشخصية؟

٣- ما هي الالتزامات الخاصة بحماية البيانات الشخصية التي يجب على

٢٥ مايو ٢٠١٨: أصبحت أحكامها قابلة للتطبيق مباشرة في جميع الدول الأعضاء، بعد عامين من دخول اللائحة حيز التنفيذ. ٢٠ يوليو ٢٠١٨: أصبح اللائحة سارية المفعول في بلدان المنطقة الاقتصادية الأوروبية (أيسلندا وليختنشتاين والنرويج)، بعد انعقاد اللجنة المشتركة للمنطقة الاقتصادية للبيئة ووافقت البلدان الثلاثة على اتباع اللائحة

- مقدمي تلك الأنظمة اتباعها أثناء تقديمهم وتشغيلهم لتلك الأنظمة؟
- ٤- ما هي حقوق الأشخاص المعنية بالبيانات أثناء استخدامهم أو تواجدهم في نطاق تلك الأنظمة الذكية الحديثة؟
- ٥- ماهية تأثير جمع ومعالجة البيانات الشخصية للأشخاص المعنية بالبيانات من العابرين في نطاق أنظمة إدارة وتأمين المنازل على القواعد القانونية الحالية لحماية البيانات الشخصية؟
- ٦- ماهية المسؤولية القانونية التي يثيرها تصنيع وتشغيل وإدارة تلك الأنظمة الذكية المتصلة؟
- ٧- كيفية الحفاظ على التوازن بين اعتبارات الأمن الخاص أثناء إدارة وتشغيل أنظمة المراقبة المنزلية الذكية المتصلة والحق في البيانات الشخصية؟
- ٨- ما هي حدود ومشروعية استخدام البيانات الشخصية المجمعة لأغراض الأمن الخاص والعام.

رابعاً: أهداف الدراسة

تهدف هذه الدراسة للتعريف بأحدث ما يتناوله فقه حماية البيانات الشخصية من قضايا من خلال تأصيل معالجة البيانات الشخصية لأغراض تشغيل الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل، تلك الأنظمة التي تمثل نقلة نوعية في المجال التقني وبنية مجتمع فيها أحدث التقنيات المستخدمة حالياً لتقديم خدمات استهلاكية تقنية حديثة

فهذه الأنظمة تمثل المرحلة الحالية لصناعات تقنية المعلومات والتي لا تركز على التواصل البشري كسابقها، ولكن على أهداف أكثر حداثة مثل تقديم خدمات متعددة تعتمد على الذكاء الصناعي من خلال مراكز حوسبة ضخمة تتصل فيما بينها عن طريق شبكات اتصالات سريعة وحديثة

لهذا فإن هذا البحث يتناول بعضاً من تلك المخاطر الحديثة كـ «الأنظمة الذكية المتصلة لإدارة وتأمين المنازل» واستخدامها لبعض التقنيات المستحدثة كإنترنت الأشياء والحوسبة السحابية والذكاء الصناعي، في محاولة لتقديم حلول وتوصيات تساهم في حل الإشكاليات القانونية التي تثيرها تلك التقنيات الحديثة والمخاطر التي يتعرض لها الحق في البيانات الشخصية جراء استخدام الأجهزة التقنية المعتمدة عليها

خامساً: منهجية البحث

نظراً لاقتران البحث على تناول مجموعة من أحدث التقنيات الحديثة، والتي لم تكن بالتطور الحالي وقت وضع اللائحة العامة لحماية البيانات الشخصية،

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

فلم تتعرض لها تلك اللائحة بالتنظيم الكافي وبالتالي لم تتناولها القوانين المستلهمة منها كالقانون المصري والبحريني والإماراتي والسعودي لحماية البيانات الشخصية ، فستقتصر منهجية البحث على المنهجية التحليلية، من حيث تحليل دورات واستخدامات ووسائل معالجة البيانات الشخصية لأغراض الأنظمة الذكية المتصلة لإدارة وتأمين المنازل، واستتزال القواعد الفقهية عليها لمحاولة الوصول لتنظيم قانوني أكثر ملاءمة للتطور الحالي لتلك التقنيات

مع ضرب والاستعانة ببعض النصوص التشريعية المختلفة حين تدعو الحاجة إليها وخصوصا من القانون المصري لحماية البيانات الشخصية، واللائحة العامة لحماية البيانات الشخصية

سادسا: خطة البحث

سيقسم هذا البحث إلى فصلين ومبحث تمهيدي يتناول المقدمة الفنية والتعريفية اللازمة للمفهوم التقني المستحدث لموضوع البحث وهو الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل، ثم سيتناول الفصل الأول جانب الإدارة والفصل الثاني جانب التأمين، كالآتي:

مبحث تمهيدي: ماهية معالجة البيانات الشخصية للأنظمة الذكية لإدارة وتأمين المنازل

المطلب الأول: تعريف وتصميم الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

المطلب الثاني: معالجة البيانات الشخصية داخل أنظمة المنازل الذكية المتصلة

الفصل الأول: معالجة البيانات الشخصية لأغراض الأنظمة الذكية لإدارة المنازل

المبحث الأول: أركان مشروع معالجة البيانات الشخصية

المطلب الأول: المراكز القانونية للمنخرطين في تشغيل «الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل»

المطلب الثاني: تأسيس مشروع معالجة البيانات الشخصية لأغراض تشغيل الأنظمة الذكية لإدارة وتأمين المنازل

المطلب الثالث: التبصير

المطلب الرابع: جمع البيانات الشخصية لغير مالكي الجهاز (نحو مفهوم محدودية التشغيل)

المطلب الخامس: أمن وسلامة البيانات الشخصية

المبحث الثاني: التزامات خاصة بأنواع معينة من المعالجة

المطلب الأول: معالجة البيانات الحساسة

المطلب الثاني: معالجة البيانات الشخصية بواسطة آليات الذكاء الصناعي

المطلب الثالث: نقل البيانات الشخصية لأغراض الحوسبة السحابية

الفصل الثاني: معالجة البيانات الشخصية لأغراض أنظمة الذكاء لتأمين

المنازل

المبحث الأول: المشاكل التي تثيرها معالجة البيانات

المطلب الأول: الشروط القانونية لإنشاء أنظمة التأمين

المطلب الثاني: تقنيات التعرف على الهوية من خلال مسح نمط الوجه

المبحث الثاني: إشكاليات استخدام البيانات الشخصية لأغراض أنظمة التأمين

المنزلي لأغراض الأمن العام

المطلب الأول: مخاطر استخدام أنظمة التعرف على الهوية من خلال بيانات

الوجه البيومترية لأغراض الأمن العام

المطلب الثاني: المخاطر التي يثيرها التعاون بين مشغلي أنظمة المراقبة

الذكاء للمنازل وبين جهات الأمن العام

المطلب الثالث: الجهود الدولية للحد من تدخل الحكومات في أنشطة معالجة

البيانات الشخصية لأغراض القطاع الخاص

مبحث تمهيدي

ماهية معالجة البيانات الشخصية للأنظمة الذكية لإدارة وتأمين المنازل

تعتبر «الأنظمة الذكية المتصلة لإدارة وتأمين المنازل» حالياً واحدة من أكثر قطاعات صناعات تقنيات المعلومات والاتصالات نمواً حالياً، نظراً لتهافت العديد من المستخدمين على اقتناء وتنصيب تلك الأنظمة في بيوتهم سواء بشكل كامل يشمل جميع أنواع تلك الأجهزة وفئاتها، أو على الأقل يشمل بعضها منها كأنظمة الأمن والمراقبة المنزلية

مما جعل شركات تقنية الاتصالات والحوسبة تتسابق لطرح تلك الأنظمة وتقديمها للمستخدمين طمعاً في الاستحواذ على سوقها، نظراً لطبيعتها الخاصة التي تتضمن طلبات شراء متعددة لأكثر من جهاز إلكتروني من قبل المستهلك الواحد، وقد أدى هذا إلى النمو المطرد لهذا القطاع في فترة صغيرة بما يقرب من ثمانية وثلاثون بليون دولار في ٢٠١٧ إلى معدل يقدره الخبراء بمائة وخمسة وعشرين بليون دولار في ٢٠٢٣.

وهذه الأنظمة تطرح العديد من المخاطر المستحدثة بالنسبة لحماية البيانات الشخصية مما يوجب تناولها بالبحث.

المطلب الأول

تعريف وتصميم الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

تتميز الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل بطبيعتها المعقدة، نظراً لاستخدام العديد من التقنيات المفتاحية الحديثة كـ «إنترنت الأشياء» و «الحوسبة السحابية» وأخيراً «الذكاء الاصطناعي» في تصميمها وتصنيعها وتشغيلها، مما يوجب التعريف بها وشرح آليات عملها، ودورات معالجة البيانات الشخصية بداخلها وأثناء عملها، كمقدمة لازمة لتحديد المخاطر الواقعة على البيانات الشخصية جراء استخدام وتنصيب تلك الأنظمة

وهذا في فرعين:

الفرع الأول: تعريف الأنظمة الذكية لإدارة وتأمين المنازل

الفرع الثاني: تصميم الأنظمة الذكية لإدارة وتأمين المنازل

3 Nadine Guhr ,Oliver Werth ,Philip Peter Hermann Blacha and Michael H .Breitner‘ ,Privacy concerns in the smart home context (2020) ’SN Applied Sciences.1

الفرع الأول

تعريف الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

أولاً: تعريف الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

وتعرف «الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل» على أنها «مجموعة من الأجهزة التي تؤتمت العمليات المنزلية، وتهدف لتحقيق راحة وأمن ورفاهية مستخدميها داخل منزله، من خلال قدرتها على إدارة نفسها وأتمتة العمليات المنزلية بأقل قدر من التدخل البشري، وهذا من خلال تقنيات مستحدثة كإنترنت الأشياء والأتمتة»^٤.

وقد أشار قانون الصمود السيبراني للاتحاد الأوروبي رقم ٢٨٤٧ لسنة ٢٠٢٤ للأجهزة المعروفة تسويقياً بالأجهزة الذكية بالأجهزة ذات المكون الرقمي وعرفها على أنها: «منتج برمجيات أو أجهزة وحلول معالجة البيانات عن بُعد، بما في ذلك مكونات البرمجيات أو الأجهزة التي يتم طرحها في السوق بشكل منفصل»^٥.

ثانياً: تعريف إنترنت الأشياء

وانترنت الأشياء هو «توليفة من الأجهزة المتصلة بشكل مباشر بالإنترنت وشبكات الاتصال المختلفة، ولها قدرات خاصة في جمع معلومات عن البيئة المحيطة حولها لأداء مهام خاصة، وهذا عن طريق عدد من المستشعرات وشرائح المعالجة المدمجة داخلها والتي تستطيع فهم ومعالجة البيانات الملتقطة بواسطة تلك المستشعرات المتعددة المرتبطة بها، مما يجعلها يطلق عليها أسماء أخرى كالمستشعرات الذكية»^٦.

وانترنت الأشياء هو مصطلح يشير إلى: «تلك الأجهزة التي تتصل بالإنترنت وتعمل بشكل مؤتمت، ولها القدرة على الاتصال ببعضها والعمل كوحدة متكاملة داخل نظام موحد، وهي في معظمها نسخ حديثة من أجهزة كهربائية صغيرة وتقليدية كجرس الباب والأجهزة المنزلية الأخرى»^٦.

4 Mehdi Rahmani-Andebili, Operation of Smart Homes ,Power Systems) Springer Nature ,united states .(2021

5 Regulation) EU 2024/2847 (of the European Parliament and of the Council of 23 October 2024on horizontal cybersecurity requirements for products with digital elements and amending Regulations) EU (No 168/2013 and) EU 2019/1020 (and Directive) EU) 2020/1828 (Cyber Resilience Act ,art' 3, product with digital elements 'means a software or hardware product and its remote data processing solutions ,including software or hardware components being placed on the market separately;

6 Nagender Kumar Suryadevara and Subhas Chandra Mukhopadhyay ,Smart Homes :Design ,Implementation and Issues Volume 14 of Smart Sensors ,Measurement and Instrumentation) Springer ,united

ويمكن تبسيط تعريف هذه الأنظمة بضرب أمثلة عليها، فهي ببساطة عبارة عن نسخة ذكية متصلة من كل جهاز منزلي موجود حالياً كالتلفاز ومبرد الطعام والموقد، ولكن يتم تصنيعها ليصبح بالإمكان التحكم بها صوتياً وعن بعد عن طريق تطبيقات خاصة بالهاتف المحمول الذكي ومتصلة بالإنترنت تمكن المستخدم من الوصول إليها من على بعد، وتقدم خدمات مضافة أو أتمتة لعمل تلك الأجهزة عن طريق مستشعرات وكاميرات مزودة بها بشكل خفي

الفرع الثاني

تصميم الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

وتصمم هذه الأنظمة على ثلاث أقسام قسم داخلي مادي يستطيع المالك شراؤه وتنصيبه في منزله، وقسم للاتصالات وهو قسم وسيط يعمل على ربط أجهزة القسم الأول الداخلي بالقسم الثالث الخارجي، وقسم خارجي يقع في حيازة الشركة المقدمة والمشغلة للنظام أو شركة أخرى تتعاقد معها تلك الشركة وهو يقع خارج سيطرة أو حتى اختيار المستخدم النهائي لهذا النظام، بل يمكن القول إن معظم المستخدمين لتلك الأنظمة لا يدركون حتى وجوده وكيونته

أولاً: القسم الداخلي المادي (الاستشعار والتفاعل):

ويقسم القسم الداخلي المادي هذا لثلاثة منظومات فرعية وهي: «أجهزة منزلية ذكية، محطة تنسيق واتصال ومساعدة رقمية ذكية، تطبيقات للهاتف المحمول الذكي والأجهزة اللوحية التي توفر اتصال عن بعد»^٧، هذه المنظومة بكاملها توفر حلاً متكاملاً لأتمتة الأعمال المنزلية من خلال أوامر يلقيها المالك عن طريق الصوت تنسقها محطات التنسيق المركزية وتنفذها الأجهزة المنزلية الذكية

وهذه الأجهزة تتنوع ابتداءً من مصابيح الإنارة الذكية المتصلة بالإنترنت ويمكن التحكم في تشغيلها من على بعد أو عن طريق مستشعر حركة، وأجهزة قياس واستشعار كأجهزة قياس حرارة المنزل، وأجهزة الأمن المنزلي والأقفال الذكية، الكاميرات الذكية، المكانس المؤتمتة الحركة والذكاء، الأجهزة المنزلية الذكية المتصلة كالثلاجات والتكييف وحتى أجهزة الطهي، كل هذا يطرح رؤية مستقبلية لمنزل ذكي متصل دوماً يمكن التحكم فيه ومراقبته من على بعد في أي مكان العالم، مما يجعله نموذجاً معيشياً مميزاً وجذاباً للمستخدمين لما يوفره من عوامل أمان وراحة^٨.

states.41 (2015)

7 Nick Vandome ,Smart Homes in easy steps :Master smart technology for your home In Easy Steps)In Easy Steps ,United Kingdom.5 (2018

8 ibid.6-9

ثانيا: القسم الأوسط (الاتصالات)

أما القسم الأوسط فإنه يعتمد إما على أجهزة اتصال رقمية أرضية منصبة، ويرتبط بها القسم الداخلي المادي، أو اتصال خلوي بياني عن طريق مثلا الهاتف الذكي للمستخدم

ثالثا: القسم الخارجي (المعالجة والذكاء الصناعي):

وأخيرا فإن القسم الخاص بالمعالجة الحقيقية للبيانات هو عبارة عن مخدمات حاسوبية عملاقة كالحواسيب الضخمة والخارقة والرئيسية، وهي أصرحه تقنية ضخمة تقدر تكاليف تشغيلها بملايين الدولارات، لذا فهي تملك حصرا للشركات التقنية العملاقة ك(أي بي أم) ميتا فيرس (المالكة لفيس بوك)، وألفبيت (المالكة لجوجل)، وأمازون مثلا، وهي تقدم خدماتها عن بعد لهذه الأنظمة، كون أن أنواع المعالجة التي تتطلبها أنظمة المنازل الذكية تعتمد على تقنيات مستحدثة للغاية تتطلب قدرة معالجة ضخمة لا تقدر عليها أجهزة الحاسب العادية ناهيك عن شرائح المعالجة المصغرة microchips المثبتة داخل العتاد المادي للأجهزة المادية المكونة للقسم الداخلي من «أنظمة المنازل الذكية»، وهذا عن طريق اتصالها وتزامنها مع تلك المكونات المادية الداخلية بما يعرف بالحوسبة السحابية، والتي بدونها لا تستطيع تلك الأنظمة أداء وظائفها المعلن عنها

ويمكن ضرب مثال توضيحي على هذه النقطة من خلال «المساعدات الصوتية المنصبة على الهواتف الذكية» كمساعد جوجل google asistant في أجهزة أندرويد، وسيري siri في أجهزة أبل، والتي بدون اتصال بالإنترنت لا تستطيع أداء مهامها، لحاجتها للمخدمات العملاقة التي تقوم بالعمل الحقيقي المطلوب منها وليس شرائح المعالجة المصغرة الموجودة ماديا داخل الهاتف الذكي⁹.

وقد أشار إليها قانون الصمود السيبراني بأنها المعالجة عن بعد للبيانات وعرفها بأنها: «تعني «معالجة البيانات عن بُعد» معالجة البيانات عن بُعد التي تم تصميم وتطوير البرمجيات من أجلها من قبل الصانع، أو تحت مسؤولية الصانع، والتي من شأن غيابها أن يمنع المنتج الذي يحتوي على عناصر رقمية من أداء إحدى وظائفه»¹⁰.

9 George Terzopoulos and Maya Satratzemi 'Voice Assistants and Smart Speakers in Everyday Life and in Education (3)19 (2020) 'Informatics in Education.473

10 Cyber resilience act ,article :3 definition 'remote data processing 'means data processing at a distance for which the software is designed and developed by the manufacturer ,or under the responsibility of the manufacturer ,and the absence of which would prevent the product with digital elements from performing one of its functions;

المطلب الثاني

معالجة البيانات الشخصية داخل أنظمة المنازل الذكية المتصلة

تعتمد الأنظمة الذكية المتصلة لإدارة وتأمين المنازل بشكل كامل على معالجة البيانات الشخصية، ولهذا تم تصميمها وتزويدها بكمية ضخمة ومتنوعة من المستشعرات التي تمكنها من جمع أنواع متعددة من البيانات الشخصية، ابتداء من البيانات الشخصية العادية كالاسم وأرقام الولوج وأكواده وبيانات حسابات التواصل الاجتماعي وبيانات وصفية ومؤتمنه كأرقام التعريف للأجهزة المتصلة mac addresses، وبيانات حساسة كالبيانات البيومترية من بصمة الصوت وقالب الوجه وبصمة الأصبع وقزحية العين، وبيانات صحية كنسبة السكر في الدم والأكسجين وغيرها

كما تقوم تلك الأنظمة بتمرير تلك البيانات الشخصية على دورات معالجة متعددة ومتزامنة ومختلفة بشكل لم يكن ممكنا في الأجيال الأسبق منها، ونظرا لتعدد وحدثة دورات المعالجة تلك وأهميتها المطلقة لعمل تلك الأنظمة لا يمكن الحكم على مشروعاتها بشكل مبدئي بدون شرحها وتأصيلها من الوجهة الفنية والقانونية، وهذا على فرعين :

الفرع الأول

أهمية معالجة البيانات الشخصية أثناء تشغيل الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

تمثل البيانات الشخصية أهمية كبرى ودورا محوريا في آليات عمل تلك الأجهزة، بل يمكن القول إنه بدون الأذن والقدرات الموجودة في تلك الأجهزة لاستخلاص ومعالجة البيانات الشخصية لا يمكن لتلك الأجهزة أن تؤدي أغراضها والمهام المطلوبة منها، لأن البيانات الشخصية تؤدي أدوارا متعددة داخل منظومة تشغيل تلك الأنظمة، وهي:

أولا: إتمام الأعمال المطلوبة والموكلة لتلك الأنظمة

تستعمل البيانات الشخصية كبيانات مساعدة في دورة عمل تلك الأجهزة من خلال توفير بيانات معينة تحتاجها هذه الأجهزة لأداء أعمالها كمثلا التعرف على الوجه والصوت والبيانات البيومترية الأخرى كبصمة الأصبع للسماح بالولوج ، التعرف على المكان والموقع الجغرافي لتحديد حالة الطقس مثلا ، التعرف على تفضيلات المشاهدة والتسوق لعمل قائمة باحتياجات ملاكها، التعرف على درجة الحرارة لضبط الأوامر الخاصة بدرجة حرارة المنزل التعرف على التفضيلات

والمحاذير الغذائية لتشغيل الأجهزة المنزلية الخاصة بتحضير الطعام، والتعرف على البيانات الشخصية الصحية للتعرف على احتياجات المالك وتوفير الرعاية الصحية له ، وغيرها من الأمثلة

ثانيا: تدريب برمجيات الذكاء الاصطناعي:

كما تلعب تلك البيانات تلعب دورا في تمرين وتدريب لو غاريتمات الذكاء الصناعي التي تدير تلك المنظومات لتحسين كفاءتها وتطوير قدرات ومميزات أكثر لمالكها، وللشركة المنتجة لتلك الأنظمة، ولهذا حديث آخر يفصل لاحقا

الفرع الثاني

دورة معالجة البيانات الشخصية في الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل

نظرا للطبيعة الخاصة لأنظمة الذكية والمتصلة لإدارة وتأمين المنازل، فإن البيانات الشخصية تمر على دورة معالجة تشترك فيها العديد من الأجهزة المكونة لهذه المنظومات وهي كالآتي:

أولا: التقاط الأوامر التشغيلية:

تبدأ دورة معالجة البيانات الشخصية أثناء قيام المستشعرات المتعددة الموجودة داخل أجهزة أنظمة المنازل الذكية بعملها، وهو ينقسم لقسمين أولهما هو التقاط الأوامر التشغيلية التي يلقها مالك النظام صوتيا أو كتابيا

فبالنظر لنموذج عملها فهي تجمع النمط الصوتي الخاص بمالكها، ورقم تعريف برتوكول الانترنت ip number لكي تستقي أوامرها من مالكها إما عن طريق الصوت أو جهاز حاسوبي يرتبط بها.

ولكي تعمل تلك الأجهزة وفق لإرادة مالكها فقط، فهي تكون عن طريق الحوسبة السحابية والذكاء الاصطناعي نمط صوتي خاص للتعرف على هوية مالكها، وأيضا فهي تملك مستشعرات بصرية وحركية لتحديد مكان مالكها، كما أنها متصلة بهاتفه الذكي وتمتلك القدرة على الولوج لحساباته الرقمية، وحتى أحيانا حسابات تواصله الاجتماعي، وأخيرا فهي تعمل على مدار الساعة ومتصلة بمصدر طاقة مستمر

فهذه المستشعرات توفر البيانات التشغيلية لوحدات المعالجة أو البيانات التي من خلالها تنفذ تلك الوحدات الحاسوبية سواء أكانت داخلية أو متصلة عن

طريق الحوسبة السحابية مهامها، وهذه الرقائق الحاسوبية تستخدم تقنيات حديثة كخوارزميات تعلم الآلة machine learning algorithms لمعالجة تلك البيانات واستخدامها في سيناريوهات معدة مسبقاً لتنفيذ مهام مخصصة ومؤتمتة من خلال تقنيات التعرف الصوتي واستخراج الأنماط¹¹.

ثانياً: النقاط البيانات الوصفية للبيئة المحيطة:

ثاني مهام المستشعرات الموجودة في الأجهزة المادية المكونة لمنظومة البيت الذكي هو جمع البيانات المساعدة للنظام والتي تمكنه من أداء عمله، وهذا عن طريق المسح المستمر للبيئة المنزلية المحيطة بها لتوفير بيانات وصفية عن تلك البيئة تساعد وحدات المعالجة الحاسوبية السحابية في أداء مهامها، فهذه الأنظمة تصمم وتزود بكمية ضخمة ومتنوعة من المستشعرات التي تمكنها من جمع كمية ضخمة ومتنوعة من البيانات عن البيئة المحيطة بها بما فيها البيانات الشخصية¹²، وهذا عن عمد فهي بدون تلك البيانات الشخصية المتنوعة لن تقوم بأداء مهامها المعقدة المطلوبة منها بالشكل الأمثل والمرضي لمالكها

فهي فمثلاً تقوم بالنقاط درجة الحرارة والرطوبة الداخلية للمساعدة في ضبط المستشعر لدرجة الحرارة، وتقوم بالنقاط تحركات الأشخاص المتواجدين في نطاقها لأتمتة الانارة، كما تقوم بالنقاط البيانات الصحية لهم بغرض توفير خدمات الرعاية الصحية، وأيضاً تقوم بالنقاط بنمط عاداتهم اليومية لتنظيم عمل الأجهزة المكونة لها بما يتناسب مع الأنماط الشخصية لهؤلاء، وتقوم أيضاً بالنقاط الصور والفيديوهات والأصوات لتوفير عوامل الأمان والمراقبة لطالبيها

ثالثاً: نقل البيانات الشخصية لوحدات المعالجة الرئيسية السحابية:

كما أسلفنا قبلاً فإن رقائق الحوسبة الموجودة في الأجهزة المكونة للقسم الداخلي لأنظمة إدارة وتأمين المنازل لا تقوم بمعالجة البيانات الشخصية التي تلتقطها وتجمعها مستشعراتها، بل ترسلها لمخدمات وحواشيب عملاقة خارجية لإتمام تلك المعالجة، وفي هذا تستخدم تلك الأنظمة نوعين من التقنيات أولهما تقنية الحوسبة السحابية لأغراض النقل والاتصال والمزامنة، وثانيهما تقنيات الذكاء الصناعي المختلفة لأغراض المعالجة والتشغيل

11 Athar Khodabakhsh and Sule Yildirim Yayilgan, 'Data Privacy in IoT Equipped Future Smart Homes' Unpublished paper, researcher gate August (2020 https://www.researchgate.net/publication_343626251/Data_Privacy_in_IoT_Equipped_Future_Smart_Homes accessed 15 September.2022

12 Abdelsalam Sumi (Helal and others, Smart Homes and Health Telematics6: th International Conference, ICOST 2008 Ames, IA, USA, June28 th July, 2008, 2 Proceedings Information Systems and Applications, incl. Internet/Web, and HCI Volume 5120 of Lecture Notes in Computer Science) Springer Science & Business Media, united states.137 (2008)

رابعاً: تغذية وتدريب برمجيات الذكاء الصناعي:

تعتمد تلك الأنظمة على توليفة فريدة من أحدث التقنيات في جميع مراحل عملها ابتداء من تلقي الأوامر التشغيلية وانتهاء بكيفية انفاذها لأوامر مالكيها وأيضاً الطرق التي تستخدمها للتواصل مع هذا المالك والتي في أغلب الأحوال تكون عن طريق الأوامر الصوتية، ولهذا يلجأ مشغلي ومصممي تلك الأنظمة للذكاء الصناعي وألياته المختلفة، وهذا من شأنه أن يعرض البيانات الشخصية لشتى أنواع المخاطر التي تتعدي حدود أغراض التشغيل، فغالبا ما يستغل مقدمي خدمات الذكاء الاصطناعي تلك البيانات في التغذية الرجعية لبرامجهم وتطوير خوارزميات الذكاء الصناعي خاصتهم من خلال تقنيات حصاد وتعيين البيانات ^{١٣} data mining and harvesting، ولهذا فإن البيانات الشخصية في هذه المرحلة لا تلعب دوراً فقط في تنفيذ أغراض المعالجة الرئيسية، بل يستفيد مشغل برمجيات الذكاء الصناعي سواء أكان متحكم أم معالج منها في تغذية وتطوير برمجياته الخاصة، مما يضيف على هذا شبهة التكبس غير المشروع من تلك البيانات الشخصية وتعدي حدود المعالجة المشروعة للبيانات الشخصية

خامساً: أغراض أخرى:

تولد تلك الأنظمة بيانات وصفية^{١٤} تستخدم البيانات الشخصية كعامل رئيسي لتوليدها، وهذه البيانات الوصفية لها أهميتها الخاصة وتستخدم للعديد من الأغراض، منها أغراض داخلية تتعلق بالنظام نفسه، كأغراض مراقبة النظام وجودته وتوفير تعليمات تساعد في صيانتها المستمرة وتطويره، ويمكن أن تستخدم تلك البيانات في أغراض أخرى داخلية لمصلحة مشغل تلك الأنظمة كتوفير إحصائيات الكفاءة والتشغيل والتي تستخدم إما لأغراض التدريب الداخلي أو التطوير للنسخ الأحدث من تلك الأنظمة أو حتى أغراض التسويق للتدليل على جودة تلك الأنظمة مقارنة بمنيلاتها

وأخيراً فإن تلك البيانات قد تستخدم في أغراض متعددة بالمخالفة لقواعد حماية البيانات الشخصية مثل التسويق المباشر، والهندسة الرجعية لإعادة توليد البيانات أو ربط البيانات ببعضها لتكوين حزم البيانات الضخمة

١٣ وهو قيام الشركات بمعالجة كتل البيانات الضخمة التي تحصل عليها لأغراضها الخاصة، وحصاد البيانات هو استخلاص البيانات الهامة من المصادر المختلفة (Harvesting Data, Privacy, Freedman Jeri, Per- and Promise the You and, Group Publishing Rosen The) Technology of ils (2019 States United, Inc, 13).

١٤ هي بيانات مخلفة حاسوبية لتصف البيانات الأصلية المدخلة بصورة عادية، وتستخدمها نظم المعلومات لفهم المدخلات البشرية بصورة حاسوبية، ويمكن استخدام هذه البيانات لإعادة تخليق واسترجاع البيانات الأصلية عن طريق ما يعرف بالهندسة العكسية، فإن كانت تلك البيانات الأصلية هي بيانات شخصية أصبح لدى البيانات الواصفة المتعلقة بها نفس الطبيعة حال هندستها عكسياً بالصورة الصحيحة راجع: W. Hon Kuan, Policy and Laws Localization Data: International Protection Data EU The (2017 Publishing Elgar Edward) ١٠٧.

ولهذا فإن الباحث يري أن دور البيانات الشخصية في دورة عمل أنظمة المنازل الذكية ينقسم إلى:

- ١- بيانات شخصية تستخدم من أجل تشغيل الأجهزة المتعددة المكونة في مجموعها لنظام البيت الذكي، وهي في معظمها تتكون من: بيانات شخصية أساسية تعريفية للمستخدم كـ «الاسم، البريد الإلكتروني، رقم تعريفى مميز للمستخدم، الموقع الجغرافي للمستخدم، الأرقام التعريفية للأجهزة المكونة لمنظومة البيت الذكي، رقم تعريف المستخدم على شبكة الانترنت، بيانات التعرف الصوتي كبصمة الصوت، بيانات التعرف البصري كبصمة الوجه والعين وأحيانا الأصبع».
- ٢- بيانات شخصية تستخدم من أجل مسح وجمع بيانات عن حاجات وظروف المنزل والمستخدم، كـ: «بيانات درجة الحرارة، بيانات الموقع الجغرافي، تغذية بصرية حية مستمرة، مسح لخريطة المنزل، معلومات متعددة أخرى كدرجة الرطوبة، نسبة نقاء الماء، الوقت، المتواجدين في المنزل ونمط حركتهم وغيرها».
- ٣- بيانات شخصية تستخدم لتغذية أنماط تعلم الآلة والذكاء الصناعي.
- ٤- توليد بيانات وصفية لأغراض متعددة.

الفصل الأول

معالجة البيانات الشخصية لأغراض الأنظمة الذكية لإدارة المنازل

تتعدد أنواع البيانات الشخصية التي تعتمد عليها الأنظمة الذكية لإدارة المنازل للقيام بمهامها، كما تتعدد وسائلها في معالجة تلك البيانات الشخصية، إلا أن الملاحظ حسب بنيتها التي تم شرحها سابقا أنها تستخدم وسائل قاطعة التقدم في هذه المعالجة، ولهذا يجب النظر في مشروعية هذه المعالجة وضوابطها، وهذا في مبحثين :

المبحث الأول

أركان مشروعية معالجة البيانات الشخصية

تنثير معالجة الأنظمة الذكية لإدارة وتأمين المنازل إشكاليات قانونية متعددة تتعلق بمدى مشروعية عملياتها المجراة على تلك البيانات التي تقوم بجمعها وتستخدمها لأغراضها الخاصة سواء أكانت تلك الأغراض تتعلق بتنفيذ الأوامر المطلوبة منها بواسطة مالكها، أو لأغراض أخرى قد لا يعرف هنا مالك النظام شيئا وتعلق بأغراض تخص مشغل تلك الأنظمة وصانعيها

وهذه الإشكاليات لها أسباب متعددة أولها الطبيعة المختلفة لتلك الأنظمة عن المعاملات الإلكترونية الأخرى القائمة في بيئة الإنترنت والمواقع الإلكترونية،

فهي ذات طبيعة مادية تعمل على مدار الساعة وتلازم مالكها طوال تواجده في محيطه المادي،

ثانيها الإمكانيات الضخمة المزودة بها تلك الأنظمة والتي تتيح لها جمع كم ضخم ومتنوع من البيانات الشخصية بشكل لا يتوفر في البيئة الإلكترونية لمواقع الإنترنت مثلاً، وثالثها قيامها بجمع بيانات العابرين بنطاقها مما يعقد من الطبيعة المعتادة لمشروعية معالجة تلك البيانات الشخصية والعلاقة القائمة بين الثلاثة أطراف من مشغل ومالك وعابرين

لذا وجب دراسة كل هذه النقاط من وجهة نظر قوانين حماية البيانات الشخصية، وهذا في خمسة مطالب

المطلب الأول المراكز القانونية للمخترطين في تشغيل «الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل»

تشكل الطبيعة الخاصة للأنظمة الذكية والمتصلة لإدارة وتأمين المنازل تحديات متعددة أثناء تكييف وتحديد المراكز القانونية للمخترطين في عمليات معالجة البيانات الشخصية الملازمة لعمل تلك الأنظمة، وهذا لعدة أسباب من أهمها ما يمكن تلخيصه في كلمة واحدة «التعددية»

فابتداءً من تعدد الأجهزة المتضمنة والمكونة لمنظومة واحدة من تلك المنظومات وبالتالي تعدد مصنعها ومشغليها، وما يثيره هذا من إشكاليات تتعلق بتحديد مراكز المتحكمين والمعالجين، والذين لا يمكن تحديدهم بشكل واضح وصريح مثلاً كحالات المتحكم في صفحة ويب أو مقدم خدمة ما يقوم عليها متحكم منفرد

وأيضاً الطبيعة الخاصة لدورة عمل تلك الأنظمة التي تفرض عليها القيام بالجمع المستمر والمتزامن لجميع من يمر بنطاقها، كونها أجهزة مادية متصلة ومزودة بالطاقة بشكل مستمر، مما يثير إشكالية تحديد من هو أو من هم الأشخاص المعنيين بالبيانات

وأخيراً اعتماد تلك الأنظمة على معالجة متطورة لهذا الكم الضخم من البيانات، مما قد يتطلب برمجيات وتقنيات خاصة قد لا تتوافر لمصنعي الأجهزة المادية المكونة لنظم إدارة وتأمين المنازل، مما يجعلهم يلجأون لحلول معقدة كالتعهيد والنقل السحابي المتزامن لتلك البيانات الشخصية لمراكز معالجة متخصصة غير

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

معلن عنها، وقد لا يعرف الشخص المعني بالبيانات أو حتى المستخدم النهائي لتلك الأنظمة شيئاً عن ماهيتها، مما يثير مشاكل خاصة بموضوع تحديد المعالجين والتزاماتهم

وسيبحث هذا المطلب ذلك في ثلاثة فروع، كالآتي:

الفرع الأول

تحديد الشخص المعني بالبيانات

عرف القانون المصري الشخص المعني بالبيانات على أنه «أي شخص طبيعي تنسب إليه بيانات شخصية معالجة إلكترونيا تدل عليه قانوناً أو فعلاً، وتمكن من تمييزه عن غيره»^{١٥}، وهذا يتفق مع ما جاء قبله من تعريفات تشريعية^{١٦}، ما عدا ما يتعلق بنطاق القانون المصري من اقتصاره على حالات المعالجة الإلكترونية

ويري الباحث تميز معالجة البيانات الشخصية لأغراض تقديم وتشغيل خدمات الأنظمة الذكية لإدارة وتأمين المنازل مثلاً عن حالات تقديم خدمات إلكترونية أكثر تقليدية كمثال تشغيل موقع إلكتروني، باحتوائها على حالتين لا حالة واحدة للشخص المعني بالبيانات، أولهما مالك النظام وثانيهما -وهو ما يثير الإشكاليات المستحدثة- حالات العابرين في نطاق هذه الأنظمة

أولاً: مالك النظام كالشخص المعني بالبيانات:

أول حالات الأشخاص المعنية بالبيانات في أطر «أنظمة إدارة وتأمين المنازل» هو مالك النظام، فهو الشخص الأساسي الذي يفترض أن يقوم النظام ومكوناته بجمع بياناته الشخصية

وهذا لا يثير أي إشكالية خاصة هنا فيتبع بشأنه القواعد العامة المحددة لطبيعة العلاقة بين الشخص المعني بالبيانات والمتحكم في البيانات، فالشخص المعني بالبيانات هو المستأثر بالحقوق والالتزامات الناجمة عن معالجة بياناته من قبل المتحكم في البيانات وغيره من المخاطبين بأحكام قانون حماية البيانات الشخصية^{١٧}.

١٥ مرجع سابق: القانون المصري لحماية البيانات الشخصية، م ١٥

١٦ ق بحريني م ١، ق مغربي م ١، ق تونسي م ٦، اللائحة العامة م ٤

١٧ مرجع سابق: احمد عبد العزيز أبو الحسن. النظام القانوني لحماية البيانات الشخصية الرقمية. ص: ٥٠

ثانياً: حالات الأشخاص المعنية بالبيانات من غير مالك الجهاز (مفهوم العابرين):

١/ إشكالية جمع بيانات العابرين أثناء تشغيل أنظمة إدارة وتأمين المنازل

يؤثر الجمع المتزامن والغير محدد لجميع البيانات الشخصية لكل من يدخل في نطاق هذه الأنظمة على تحديد المراكز القانونية للأشخاص المعنية بالبيانات، فعلى حين يمكن القول بواحديّة العلاقة بين الشخص المعني بالبيانات والمتحكم فيها لأغراض التصفح وتقديم الخدمات والتعاقد عليها، إلا أن هذا لا ينطبق على الأنظمة الذكية لإدارة المنازل وتأمينها، والتي تقوم بالجمع والمعالجة المستمرة للبيانات الشخصية لكل من يقع في نطاق مستشعراتها، لذا لا يمكن القول بواحديّة «الشخص المعني بالبيانات»، بل يجب افتراض تعدديتهم طوال الوقت

فالإشكالية الأساسية هنا هي قيام تلك الأجهزة بجمع بيانات كل من يدخل في نطاقها بشكل متزامن وعشوائي بدون تحديد أو اقتصار على بيانات مالكيها، فسواء كانوا أحد أفراد الأسرة أو غيرهم من الآخرين المتواجدين بشكل شرعي أو غير شرعي في نطاق هذه الأنظمة، وهذا لا يمكن حظره ابتداءً كونه أساسياً لقيام بعضها من مكونات تلك الأنظمة بعملها المتوقع منها أداءه كتأمين المنزل مثلاً أو الاستجابة الفورية لأوامر مالك النظام، ولهذا يرى الباحث ملائمة اقتصار التدخل التشريعي والقانوني عامة على تكييف مشروعية استخدامه وحدود رخصة المتحكم في معالجة بيانات هؤلاء العابرين والمتواجدين بنطاق تلك الأنظمة

ويمكن طرح مثال تطبيقي على هذا المفهوم الحديث من خلال عرض الدعوى الجماعية التي رفعتها المواطنة الأمريكية «ميشيل وايس» على شركة «رينج التابعة لأمازون» عام ٢٠٢٠ والتي مثلت فيها مجموعة من الأفراد الذين لا يملكون أجهزة تابعة لتلك الشركة^{١٨}، ولكن زعموا أنهم تعرضوا لانتهاك خصوصيتهم جراء مسح صورهم والتعرف على هوياتهم أثناء عبورهم في نطاق تلك الأجهزة، وهذا بدون إذنهم وموافقتهم مما نجم عنه امتلاك تلك الشركة لبياناتهم الشخصية وخصوصاً قوالب وجوههم والتي تستخدم في تقنيات التعرف على الهوية من خلال مسح قوالب الوجه التابعة للشركة بدون علمهم أو موافقتهم^{١٩}، واستعانت المدعية ببراءة الاختراع المملوكة للشركة والمتعلقة بتقنيات التعرف على الوجه والتي تملكها الشركة وقد طعنت الشركة على الدعوى تأسيساً على سابقة قضائية أخرى وهي «زيلمر ضد فيس بوك»^{٢٠}، وقد رفض طعن الشركة

18 Wise v Ring LLC W.D. Wash. ,No-2:20 .cv.8/3/22 ,01298-.

19 Samantha Hawkins' ,Ring Loses Bid to Dismiss Biometric Claims Over Doorbell Cameras' (Bloomberglaw 4 ,August (2022 <https://news.bloomberglaw.com/privacy-and-data-security/ring-loses-bid-to-dismiss-biometric-claims-over-doorbell-cameras> accessed 13 September.2022

20 Zellmer v Facebook ,Inc-3:18) cv (01880-District Court ,N.D .California ,March 2018, وسيتم 27، تقصّلها لاحقاً

وما زالت القضية معروضة أمام القضاء الأمريكي^{٢١}.

2/ تعريف "عابري المنازل الذكية":

مثل هذه الحالة وحالات أخرى قد دعت بعض الفقه لصك مفهوم جديد لهذه الفئة يدعى «عابري المنازل الذكية» وهم بتعريفهم: «الأشخاص الذين لا يملكون هذه الأنظمة أو الأجهزة ولكنهم يتعرضون لالتقاط بياناتهم بواسطة أو قد يشاركون في استخدامها بمحض الصدفة مثل باقي أفراد الأسرة غير المالك، المستأجرين لبيوت تحتوي على تلك الأنظمة، العمال والمهنيين الذين يترددون على تلك المنازل^{٢٢}»

لذا يمكن القول بأن تعريف الأشخاص المعنية بالبيانات في أطر «الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل» يشمل مالكيها والعابرين بنطاقها على حد سواء، ليكون «أي شخص طبيعي يتعرض لمعالجة بياناته الشخصية من خلال أي مكون من مكونات تلك الأنظمة سواء بموافقة وعلمه أو بدونها، وسواء أكانت تلك البيانات الشخصية تدل على نشاط مشروع أو إجرامي يقوم به هذا الشخص الطبيعي»

فعابري الأنظمة الذكية لإدارة وتأمين المنازل إذن هم أشخاص معنية بالبيانات، سواء تمت معالجة بياناتهم بعلمهم ومعرفةهم أو بدونها، وهذا يطرح عدد من الإشكاليات والأسئلة التي تؤثر بشكل كبير على مدار عملية المعالجة والمراكز القانونية المرتبطة بها، فمثلاً ماهية العلاقة بين مالك النظام وهؤلاء العابرين نتاج تكييفهم كأشخاص معنية بالبيانات وحدود وكيفية معالجة بياناتهم والتي يتم جمعها بدون موافقتهم المسبقة أو حتى علمهم بهذه المعالجة، وهو ما سيحاول الباحث الإجابة عليه أثناء بحثه لمركز المتحكم في البيانات في أطر معالجة البيانات الشخصية لأغراض أنظمة إدارة وتأمين المنازل

21 JOHN C .COUGHENOUR ,District Judge order on 3/8/2022 on Case No .C20-1298-JCC.

22 Wael S Albayaydh and Ivan Flechais' ,Exploring Bystanders 'Privacy Concerns with Smart Homes in Jordan) 'CHI :22' Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, April (2022 art.2, 446

الفرع الثاني

تحديد المتحكم في البيانات

يعد تحديد المتحكمين في البيانات الشخصية أصعب من تحديد الأشخاص المعنية بالبيانات، وهذا لتعدد مشغلي ومصنعي تلك الأنظمة سواء أكان العتاد المادي المكون لها أو شبكات معالجة البيانات الشخصية داخلها والتي عادة ما تكون مبنية على نظم الحوسبة السحابية

أولاً: تحديد حالات المتحكم المنفرد

فأنظمة المنازل الذكية قد تتكون من عدد من الأجهزة من ذات المُصنع أو عدد متعدد من الأجهزة التي تنتمي لمُصنعين مختلفين، ويتم الربط بينهم بواسطة منصة تحكم واحدة قد تكون عادة هاتف ذكي مملوك لمالك هذه المنظومة أو في أحيان أخرى جهاز مخصص لهذا الغرض، وفي الحالة الأولى – أي حالة المُصنع المنفرد- فإن تحديد المتحكم أقل صعوبة لانتفاء إشكالية التعددية حيث أن المتحكم المنفرد هو ذاته مصنع ومشغل النظام المنزلي الذكي^{٢٣}.

ثانياً: تحديد حالات المتحكمين المنفردين والمشاركين:

١/ تمييز المتحكمين المنفردين من المتحكمين المشاركين في إطار أنظمة إدارة

وتأمين المنازل:

هناك حالتان لمراكز المتحكمين في البيانات عند تعدد المصنعين وموردي خدمات وأجهزة نظام منزلي ذكي واحد ، أولهما هي تعدد المتحكمين المنفردين، وثانيهما هي اشتراك المتحكمين المتعددين في علاقة مشتركة أو ما يعرف بالمتحكمين المشتركين^{٢٤} joint controller، ومن الجدير بالذكر أن القانون المصري لم يتعرض لمثل هذا المفهوم على الرغم من إشارته لحالة تعدد المتحكمين^{٢٥}، ولكن لم يحدد حالات اشتراكهم كلهم في مفهوم مقابل لمفهوم المتحكم المشترك الموجود في اللائحة العامة الأوروبية على سبيل المثال والتي عرفتهم بأنهم «عندما يقرر متحكمون في البيانات أو أكثر أغراض وطرق المعالجة»^{٢٦}.

23 Olumide Babalola، 'Internet of things (IoT): (data security and privacy concerns under the general data protection regulation) gdpr10' (th International Conference on Natural Language Processing, Australia, December, 2021, 24 ~ 23 World Academy of Science, Engineering and Technology.315)

24 Jiahong Chen and others، 'Who is responsible for data processing in smart homes ?Reconsidering joint controllership and the household exemption (4)10 (2020) 'International Data Privacy Law.282

٢٥ القانون المصري ١٥١/ ٢٠٢٠: م ٤ وفي حال وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعني ممارسة حقوقه تجاه كل متحكم على حدة.

وتتحقق الحالة الأولى حين تقدم كل شركة خدماتها بشكل مستقل عن الشركة الأخرى، والحالة الثانية تتحقق حين تشترك الأطراف المقدمة لخدمات أنظمة منزلية ذكية شاملة في علاقة تحكم واحدة ويقرروا بشكل جمعي أغراض معالجة البيانات الشخصية فيعتبروا في هذه الحالة متحكمين مشتركين

٢/ موقف محكمة العدل الأوروبية من تحديد المتحكمين المشتركين:

ومن خلال استقراء التوالى القضائي لمحكمة عدل الاتحاد الأوروبي، نجد أن تحديد العلاقة بين مجموع المتحكمين على أنهم متحكمين فرديين أو مشتركين، يفسر تفسيراً واسعاً حسب كل حالة على حدة، ولا يجب وجود علاقة مؤسسية أو تعاقدية بين هؤلاء لتحولهم من متحكمين منفردين لمتحكمين مشتركين، بل يمكن أن تنشأ تلك الرابطة بصورة مؤقتة نتيجة شراء أو تنصيب أحد المستهلكين لمنظومة واحدة تجمع أجهزة هؤلاء

فقد فسرت تلك المحكمة العلاقة بين المتحكمين في سلسلة المعالجة الواحدة حسب الحالة المعروضة أمامها بدون التقيد بأي قيود صارمة أو مسبقة، وقد ظهر موقفها هذا في عدد من القضايا التي استندت في كل واحدة منها على سبب مختلف لتفسير العلاقة بين المتحكمين في البيانات بأنهم متحكمون مشتركون، فمثلاً فسرت المحكمة العلاقة بين المتحكمين في قضية «أكاديمية الأعمال شليسفيغ هولشتاين»^{٢٧}، وقضية «جوجل إسبانيا»^{٢٨}، أنها علاقة تحكم مشترك نشأت نتيجة سماح أحد المتحكمين لمتحكمين آخرين بالاستفادة من البيانات التي يجمعونها لأغراضهم الخاصة، أما قضية «شهود يهوه» ففسرت من خلالها المحكمة العلاقة بين جماعة شهود يهوه الدينية وأعضائها الذين يجمعون البيانات الشخصية أثناء قيامهم بأعمال التبشير لصالح الجماعة بأنهم يشكلون متحكم مشترك نتيجة وحدة الغرض والانتماء الديني المؤسسي بين الجماعة وأعضائها^{٢٩}، وأخيراً ففي قضية «فاشون أي دي fashion id» قررت المحكمة أن العلاقة بين شركة «فاشون أي دي» وبين شركة «فيس بوك» هي علاقة متحكمين مشتركة حيث أن شركة فيس بوك هي الأخرى تستفيد من البيانات الشخصية المجمعة بواسطة موقع الشركة من خلال إدماج الشركة لخدمات «زر أعجبنني» في موقعها وهذا حتى بدون وجود أي علاقة تعاقدية بين الطرفين ما دامت تلاقت مصالحهم على غرض واحد للمعالجة^{٣٠}.

27 Case C 210/16–Wirtschaftsakademie Schleswig-Holstein [2018] OJ C.268/3

28 Case C 131/12–Google Spain and Google [2014] OJ C.212/4

29 Case C 25/17–Jehovan todistajat [2018] OJ C.319/7

30 Case C 40/17–Fashion ID.

٣/ تحديد المسؤولية القانونية للمتحكمين المشتركين لأنظمة إدارة وتأمين المنازل:

ومن هنا يمكن القول إنه إذا اشتركت أكثر من شركة ومقدم خدمة في تقديم الخدمات والأجهزة المتعددة المكونة لمنظومة البيت الذكي المتصل الواحدة وتوحدت أهدافهم الكامنة وراء تقديمهم لمثل تلك المنتجات والخدمات فيعتبروا في هذه الحالة متحكمين مشتركين، ويجب عليهم أن يتأكدوا من التزامهم بكافة المعايير القانونية أثناء معالجتهم للبيانات الشخصية التي تقوم أجهزتهم وخدماتهم بجمعها، وأن يوضح كل متحكم من هؤلاء المتحكمين المشتركين التزاماته المحددة حيال الشخص المعنى بالبيانات بشكل واضح وشفاف^{٣١}.

أما عن مسئوليتهم حيال الأضرار التي قد تنجم عن معالجتهم للبيانات الشخصية بشكل جمعي فطبقا لللائحة العامة فإذا لم يحدد هؤلاء المتحكمين لمسئولياتهم بشكل منفرد، يرجع عليهم بالمسؤولية التضامنية عن أي ضرر يقع عن مجموع المعالجة في أي حالاتها أو أجزائها^{٣٢}، وطبقا للقانون المصري فإنه في حالات تعدد المتحكمين فإنهم يكونوا ملتزمين بكافة الالتزامات القانونية المنصوص عليها في القانون المصري بشكل فردي، وللشخص المعنى أن يمارس حقوقه ويرجع عليهم بالمسؤولية كل منهم على حده^{٣٣}، ويرى الباحث أن تنظيم اللائحة العامة أشمل وأضمن لعدم انفلات التفسير القضائي للعلاقة القائمة بين المتحكمين وبعضهم مما يخل بالمقصد الأساسي من وضع مفهوم المتحكم ألا وهو تسهيل عملية الإشراف والرقابة على أعمال هؤلاء من ناحية، ومن ناحية أخرى التسهيل على الشخص المعنى بالبيانات في ممارسة حقوقه والرجوع بالمسؤولية والتعويض على المتحكم القائم بالضرر، ومن ناحية ثالثة يساعد في عدم الخلط بين العلاقة القائمة بين المتحكمين المشتركين والمتحكمين والمعالجين

٣١ Guidelines EDPS ,EDPS and processor ,controller of concepts the on November 7 ,EDPS) 2018/1725 (EU) Regulation under controllership joint (2019) 24.

٣٢ General EU The ,Bussche dem von Axel and Voigt Paul ;26 art ,GDPR Switzerland ,Springer) Guide Practical A :(GDPR) Regulation Protection Data Developments Legal and Protection Data Personal ,Tzanou Maria ;36 (2017 Union European the in (2020 states United ,Global IGI) 68.

٣٣ القانون المصري ١٥١ / ٢٠٢٠: م ٤

الفرع الثالث

تحديد معالجي البيانات

أولاً: إشكالية التعددية المتزايدة لمعالجي البيانات الشخصية في إطار أنظمة إدارة وتأمين المنازل

على الرغم من إمكانية التحديد المبدئي للمعالجين بشكل أكثر سهولة من المتحكمين، من خلال تحديد طبيعة العلاقة بين مقدم الخدمة الرئيسي وأحد المتعاقدين معه لتزويده بخدمات تابعة لا ينتج عنها معالجة هذا المتعاقد للبيانات الشخصية لأغراضه الخاصة فمثلاً مزود لخدمة تخزين سحابية أو مزود لبرنامج تعرف على الوجه أو غيره من أشكال الذكاء الاصطناعي الذي تمر البيانات الشخصية على مخدماته دون أن يحتفظ بها أو يعالجها لأغراضه الخاصة، بل لأغراض المتحكم الرئيسي الخاصة³⁴.

ولكن مسألة تعددية هؤلاء المعالجين الناتجة عن تعدد حاجات أنظمة إدارة وتأمين المنازل لتقنيات مستحدثة كثيرة قد يوفرها عدد كبير من المعالجين إما لأسباب تتعلق بالملكية الفكرية أو المصالح التجارية للمتحكم صعوبة في حصر وتحديد المعالجين تثير صعوبة أثناء حصر معالجي البيانات لأغراض تقديم خدمات الأنظمة الذكية لإدارة وتأمين المنازل، فمثلاً يمكن أن يحتوي نظام بيت ذكي واحد على أكثر من منتج وخدمة يتبعوا أكثر من متحكم، ومن الممكن أن يتعاقد كل متحكم من هؤلاء مع أكثر من معالج للاستفادة من خدماتهم المختلفة بشكل يعقد الموضوع بشكل متسارع، ولهذا فقد رأى بعض الفقهاء أن الفارق بين المتحكم والمعالج في نطاق توفير وتشغيل أنظمة إدارة وتأمين المنازل هو أن المعالج لا يشارك في الإنشاء الرئيس للنظام والمنتج الرئيسي الذي يشتريه المستخدم النهائي³⁵.

ثانياً: الفارق بين العلاقة القانونية الناشئة بين المتحكمين المشتركين والمتحكم والمعالج:

وهناك فارق بين العلاقة الناشئة بين المتحكمين المشتركين، والعلاقة بين المتحكمين والمعالجين

34 ibid.314-315

35 ibid

١/ تمييز العلاقة بين المتحكمين المشتركين:

فالمتحكم المبدئي في البيانات أو منشئ فرضية المعالجة المبدئية التي على أساسها عولجت البيانات الشخصية أولا «مثلا شركة فاشون أي دي»، لم يتعاقد مع المتحكم الثاني «ومثلا هنا فيس بوك» لتقديم خدمات معينة لصالحه، بل إن المتحكم المبدئي «فاشون أي دي» استغلت خدمة مستقلة يقدمها المتحكم المنضم «فيس بوك» للاستفادة من خدمات هذا المتحكم، وبناء عليه استطاع هذا المتحكم المنضم أن يلج للبيانات الشخصية لموقع المتحكم الرئيسي ويعالجها لأغراضه الخاصة عند ضغطهم على زر أعجبني أثناء زيارتهم لموقع المتحكم المبدئي، وهذا العلاقة قد تكون واضحة للشخص المعنى للبيانات حيث أنه لديه القدرة على رؤية الزر واختيار الضغط عليه من عدمه - على الرغم من قلة معرفته بالآثار المترتبة على هذا - على عكس العلاقة بين المعالج والشخص المعنى بالبيانات حيث لا يكون للأخير وعي بهوية المعالج الذي يعمل بشكل خفي لصالح المتحكم ولأغراض المتحكم الخاصة

٢/ العلاقة بين المتحكم والمعالج:

ابتداء فإن الفارق الرئيسي هنا هو طبيعة العلاقة بين المتحكم والمعالج فالمعالج تابع للمتحكم، ويجب على المتحكم التأكد من استيفاء المعالج للشروط القانونية كالنزاهة والقدرة الفنية^{٣٦}، ويُسأل المتحكم عن أعمال المعالج الداخلة في الإطار التعاقدى بينهم مسئولية تضامنية، في حين يُسأل المعالج عن أعماله الخارجة عن الإطار التعاقدى مسئولية أصلية ولكن يمكن للمتحكم مطالبة المعالج بالتعويض عن الأضرار الناجمة عن تلك الأفعال طبقا لأحكام المسئولية العقدية المبينة على إخلال المعالج بشروط التعاقد بينهم^{٣٧}، كما يلاحظ أن بعضا من القوانين المقارنة كاللائحة العامة مثلا قد ألزمت المتحكم بكتابة عقد معالجة للبيانات الشخصية بينه وبين المعالج المزمع التعاقد معه وهذا العقد هو مجرد أداة قانونية لنقل الالتزامات القانونية للمعالجين المنصوص عليها باللائحة حال عدم انطباق اللائحة على هؤلاء المعالجين لوقوعهم خارج النطاق الانفاذي لللائحة على سبيل المثال^{٣٨}، كما يمكن أيضا الارتكان هنا للمسئولية التقصيرية المعتمدة على مخالفة المعالج للنص القانوني الملزم له بعدم معالجة البيانات لصالحه في القوانين المقارنة عدا القانون المصري الذي أباح له هذا^{٣٩}.

36 Manish Gupta ,Strategic and Practical Approaches for Information Security Governance :Technologies and Applied Solutions) IGI Global ,Pennsylvania ,United States ;192 (2012 Khaled El Emam ,Lucy Mosquera and Richard Hoptroff ,Practical Synthetic Data Generation :Balancing Privacy and the Broad Availability of Data) O'Reilly Media ,Inc ,Newton ,Massachusetts ,United States.127-128 (2020

٣٧ مرجع سابق: أحمد عبد العزيز أبو الحسن، النظام القانوني للبيانات الشخصية الرقمية، ص: ٥٤-٥٥

٣٨ مرجع سابق: احمد عبد العزيز أبو الحسن. النظام القانوني لحماية البيانات الشخصية الرقمية. ص: ١١٣

٣٩ مرجع سابق: أحمد عبد العزيز أبو الحسن، النظام القانوني للبيانات الشخصية الرقمية، ص: ٥٠

فباتفاق جميع القوانين المقارنة فالمعالج ليس له أن يستخدم البيانات الشخصية المرسله له من قبل المتحكم لأغراضه الخاصة^{٤٠}، ما عدا القانون المصري الذي أباح له تقرير أغراض المعالجة^{٤١} في موقف منافي لفكرة المتحكم نفسها ويعارضه الباحث للخلط الذي ينجم عنه بين المركز القانوني للمتحكم والمعالج، والذي يري الباحث أنه خلط ناجم عن عدم تقرير القانون المصري لمركز «المتحكمين المشتركين» فخلط بين العلاقة الناجمة بين المتحكمين المشتركين والمتحكم والمعالج، وما يؤكد هذا أن المشرع المصري خالف نفسه لاحقاً بتأكيد على التزام المعالج أثناء المعالجة بتعليمات المتحكم المكتوبة^{٤٢}، ولكن الباحث يري أنه طبقاً للقواعد التفسيرية فإن المادة التعريفية لها نطاق أوسع من المادة الموضوعية، ولهذا فيري أن أحكام المادة الخامسة من القانون المصري تنطبق فقط في حالات معالجة المعالج للبيانات الشخصية لصالح المتحكم لا لصالحه هو نفسه.

المطلب الثاني

تأسيس مشروعية معالجة البيانات الشخصية لأغراض تشغيل الأنظمة الذكية لإدارة وتأمين المنازل

اشتترطت قوانين حماية البيانات الشخصية على المتحكم تحديد غرضه من هذه المعالجة، واشتترطت اللائحة العامة أن يكون هذا التحديد قبل شروعه في هذه المعالجة، ولا يعدله أو يغيره أثناء قيامه بمعالجة هذه البيانات^{٤٣}، وهذا لضمان مشروعية المعالجة وعدم استغلال القائمين بالمعالجة لعدم وضوح غرض المعالجة^{٤٤}، و وافقها في هذا القانون المصري^{٤٥}.

ويلاحظ أنه أثناء تأسيس مشروعية معالجة البيانات الشخصية لأغراض تشغيل هذه الأنظمة يجب التفرقة بين حالتين، حالة بيانات المالكين لتلك الأنظمة

٤٠ قانون بحرين ٣٠ لسنة ٢٠١٨، م ١، article 7, gdpr

٤١ القانون المصري ١٥١ لسنة ٢٠٢٠، م ١ تعاريف

٤٢ القانون المصري ١٥١/٢٠٢٠ م ٥:١ - إجراء المعالجة وتنفيذها طبقاً للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقاً للحالات المشروعة والقانونية وبناءً على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية وافتاقها وكفايتها مع الغرض المحدد له.

43 Office of the Data Protection Ombudsman, 'Purpose limitation' (Office of the Data Protection Ombudsman, Helsinki 2019) <http://bit.ly/purilmposm> , Information Commissioner Office, 'Principle (b): Purpose limitation' (Information Commissioner Office, Wilmslow 2109) <http://bit.ly/purilmico> . , Justine Pila and Paul Torremans, European Intellectual Property Law (Oxford University Press, Oxford 2019) 503.

44 Office of the Data Protection Ombudsman, 'Purpose limitation' (Office of the Data Protection Ombudsman, Helsinki 2019) <http://bit.ly/purilmposm>; Information Commissioner Office, 'Principle (b): Purpose limitation' (Information Commissioner Office, Wilmslow 2109) <http://bit.ly/purilmico>; Justine Pila and Paul Torremans, European Intellectual Property Law (Oxford University Press, Oxford 2019) 503.

٤٥ القانون المصري لحماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠، م ٣

وحالة بيانات العابرين في نطاقها، وهذا في فرعين كالآتي:

الفرع الأول

تأسيس مشروعية معالجة البيانات الشخصية لمالكي الأنظمة

يمكن لمشغلي تلك الأنظمة تأسيس مشروعية معالجة بيانات المالكين على أسس تنفيذ التزاماتهم التعاقدية المبرمة مع هؤلاء المالكين ولصالح هؤلاء المالكين، والتي تقتضي قيام تلك الأنظمة بمهام معينة لا يمكنها القيام بها بدون معالجتها لتلك البيانات الشخصية، مع الأخذ في الاعتبار أن تكون تلك العقود وهذه المعالجة لصالح المالكين

وأیضا على أسس موافقة هؤلاء على معالجة بياناتهم الشخصية لتمكين تلك الأنظمة من أداء المهام المتوقعة أن تقوم بها، مع مراعاة حدود مبدأ الموافقة التي سيتم إيضاحها لاحقا

وقد نص كلا من القانون المصري واللائحة العامة وجميع قوانين حماية البيانات الشخصية على المشروعية المبتدئة لمعالجة البيانات الشخصية لتلك الأغراض^{٤٦}، كما يجب هنا الأخذ في الاعتبار أن هناك فارقا بين مشروعية ابتداء المعالجة ومشروعية استمرارها فالمشروعية مبدأ ممتد ومستمر طوال عملية المعالجة، والتي تفقد مشروعيتها بانتفاء أو انتهاء أحد شروط هذه المشروعية^{٤٧}، وهذا له تفصيله اللاحق

الفرع الثاني

مشروعية معالجة البيانات الشخصية للعابرين في نطاق تلك الأنظمة

تنثير البيانات المتعلقة بالعابرين في نطاق أنظمة إدارة وتأمين المنازل مشاكل ممتدة على طول خط المعالجة، تبدأ ببحث مدي مشروعية جمع تلك البيانات، فعلى حين يفترض واحدية أطراف عملية المعالجة في العديد من حالات معالجة البيانات الشخصية، وبالتالي يمكن الحكم على مشروعية المعالجة وأسباب البدء بها بسهولة، إلا أن طبيعة عمل أنظمة إدارة وتأمين المنازل تمكنها من الجمع العشوائي والكامل للبيانات الشخصية لكل من يعبر نطاقها، تعقد الحكم على مدى مشروعية معالجة البيانات الشخصية لأغراض أنظمة إدارة وتأمين المنازل بشكل كبير

٤٦ القانون المصري لحماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠، م ٦، GDPR، art ٦، and Wende Der Van Marijk
Oxford) Eurasia Across Universities Connecting :Road Silk New the on Europe and China ,others
Press University ,Oxford (٢٠٢٠) ٢٢٤.

٤٧ مرجع سابق: أحمد عبد العزيز أبو الحسن. النظام القانوني للبيانات الشخصية الرقمية. ص: ٢١

أولاً: العلاقة الثلاثية الناشئة بين العابرين ومالك النظام مشغله:

فأولاً : يلاحظ هنا تحول مالك النظام من شخص معني بالبيانات إلى متحكم في البيانات مشترك مع مشغل النظام، وهو مفهوم لم يتعرض له القانون المصري، ولكن تعرضت له اللائحة العامة بما يعرف المتحكمين المشتركين joint controller^{٤٩}.

١/ التمييز بين مركز مالك النظام كمتحكم في بيانات العابرين والمتحكمين المشغلين:

وعلى الرغم من هذا فيجب التفرقة بين المركز القانوني للمالك المتحكم في البيانات والمشغل المتحكم في البيانات، فالأول وإن ثبتت عليه صفة المتحكم في علاقته مع بيانات العابرين، ولكنه يتميز عنهم في عدة نقاط :

أولاً: من حيث طبيعته القانونية: فهو لا يعتبر حائزاً لها إلا في حالات التخزين الداخلي أو المحلي على وسائط تخزين مادية تقع في حوزته وله إمكانية الوصول إليها بالطرق المتاحة للمستخدم المعتاد

وثانياً: فهو غير مخاطب بأحكام قوانين حماية البيانات الشخصية: كونه يعالج البيانات الشخصية لأغراض المنزلية فقط وهذا باتفاق القوانين المقارنة^{٤٩}، وأيضاً كونه يعالجها لأغراضه الخاصة التي لا تتعارض مع حقوق الشخص المعنى بالبيانات المشروعة^{٥٠}، ولكن يجب ملاحظة أنه على الرغم من هذا يظل مخاطباً بالقواعد العامة للقانون وبالأخص بالقواعد العامة للحق في الخصوصية، فمثلاً هو ملزم بعدم مشاركتها وإتاحتها للغير، واقتصار معالجته لها على أغراضه المنزلية، حذفها بعد مضي فترة المعالجة، الالتزام بتأمينها وسريتها

ولهذا يري الباحث عدم التزام المتحكم المالك بنفس قواعد ونطاق مسؤولية المتحكمين المشتركين التجاريين المخاطبين بأحكام القانون كالحالات السابق ذكرها أثناء التعرض لمفهوم المتحكم المشترك، كونهم غير مخاطبين بأحكام القانون، كمشغلي النظام المخاطبين بأحكام قوانين حماية البيانات الشخصية

48 IBID: GDPR, article 26.

٤٩ كالقانون المصري رقم ١٥١ لسنة ٢٠٢٠ م ٣ اصدار، والقانون البحريني لحماية البيانات الشخصية م ٢
٥٠ القانون المصري ١٥١ لسنة ٢٠٢٠ م ٦

٢/ مركز مشغل النظام كمتحكم مشترك لبيانات العابرين:

أما في حالة المتحكم المصنع والمشغل لتلك الأنظمة، فلا يمكن تطبيق قاعدة الموافقة كسبب لمشروعية معالجة بيانات العابرين، ولكن يمكن تطبيق سبب آخر وهو تمكين المشغل والمصنع من القيام بالتزاماته المشروعة حيال المالك المشتري للنظام، وهو سبب اتفقت القوانين المقارنة عليه، ولكنه سبب مقيد بقيود أكثر من الموافقة والوفاء بالالتزامات التعاقدية، من حيث حدود المعالجة والرخصة التي يمنحها للمتحكم على البيانات الشخصية، والتي يجب ألا تتعارض مع حقوق الشخص المعني بالبيانات وهم هنا العابرين وليسوا المالك للنظام^{٥١}.

كما يجب عليه في هذه الحالة مراعاة الحدود الضيقة لمعالجة تلك البيانات الشخصية، والتي يجب أن تقتصر على حدود تقديم الخدمة لمالك النظام دون استغلالها لأغراض أخرى كتغذية برامج أو قواعد بياناته، فمثلا في حالة النقاط كاميرات التأمين لصور الأشخاص العابرين فلا يجب على المتحكم في البيانات الاحتفاظ بها أو تعريضها لأي نوع من أنواع المعالجة التي قد لا تتوافق مع حقوق هؤلاء الأشخاص المعنية بالبيانات

أي تكون حدود المعالجة بالنسبة لبيانات الأشخاص المعنية بالبيانات من العابرين هي فقط توفير البيانات الأساسية المجهولة اللازمة لإدارة وتشغيل خدمات أنظمة البيوت الذكية لمالك النظام، دون أن يحتفظ بها في أنظمتها أو يستعملها لتغذية أنظمة المعالجة الذكية الخاصة به (الذكاء الصناعي)

٥١ مرجع سابق: أحمد عبد العزيز أبو الحسن. النظام القانوني للبيانات الشخصية الرقمية، ص: ٢٨

المطلب الثالث

التبصير

أولاً: تأثير الشكل المادي للأجهزة الذكية لأنظمة إدارة المنازل على إدراك الشخص المعني بالبيانات:

تثير الأجهزة المكونة لأنظمة إدارة وتأمين المنازل والمصممة كأجهزة صغيرة أو أجهزة اعتاد المستخدم عدم قيامها بجمع البيانات الشخصية، إشكالية وعي مستخدمها بنطاق الجمع والمعالجة التي تقوم به تلك الأجهزة للبيانات الشخصية، سواء أكان هذا يتعلق بالعلم المبدئي بهذا الجمع أم حدود هذا الجمع الزمنية والنوعية⁵²، مما دعا العديد من الفقه الغربي للمناداة بتشديد قواعد الشفافية الخاصة بجمع البيانات الشخصية عن طريق تلك الأجهزة⁵³.

ثانياً: تأثير الطبيعة المادية لأجهزة أنظمة إدارة وتأمين المنازل على وصول الأشخاص المعنية بالبيانات لسياسة الخصوصية:

بالإضافة إلى هذا يجب على المتحكم المشغل والمصنع لتلك الأجهزة توفير وسيلة ثابتة لإنفاذ الالتزام بالإعلام والحق في العلم والتبصير، حيث إن تلك الأجهزة نظراً لطبيعة تصميمها لا توجد بها وسيلة ثابتة لعرض نسخة من سياسة الخصوصية⁵⁴، وهي الوسيلة الأعم لإنفاذ الالتزام بالإعلام والحق في العلم، فيجب إما توفير نسخة ورقية ثابتة مع هذا المنتج أو نسخة إلكترونية يمكن الاحتفاظ بنسخة ثابتة منها من موقع أو تطبيق المنتج، أو «كود سريع الاستجابة» موجود على الهيكل المادي لهذه الأجهزة يوفر وصولاً سريعاً لتلك السياسة

ثالثاً: خصوصية تأثير تحديث سياسات الاستخدام والخصوصية في حالات أنظمة إدارة وتأمين المنازل:

وأخيراً فإن تحديث سياسات الاستخدام للمنتج قد ينجم عنه تغيير في كمية أو نوع البيانات الشخصية التي تجمعها تلك الأجهزة، وكيفية وغرض معالجتها، مما قد يؤثر على طبيعة الموافقة المسبقة المطلوبة لمعالجة تلك البيانات الشخصية، فيري الباحث أنه في هذه الحالة يجب إعلام المستخدم بتلك التغييرات بشكل بسيط وواضح، وفي حالة رفضه لها لا يتم إيقاف عمل الجهاز أو التقليل من إمكانياته

52 Sanjay Goel and others ,Smart Grid Security) Springer ,United states.94 (2015

53 Thomas Pasquier and others, 'Viewpoint Personal Data and the Internet of Things It is time to care about digital provenance' (2019) 62(6) Communications of the ACM 32.

54 وهي «وثيقة قانونية نموذجية يصدرها المتحكم في البيانات طوعية أو استجابة لإلزام تشريعي أو عقدي، وتعمل على إبراء المتحكم من التزام الإعلام، واستيفاء الشرط الشكلي لموافقة الشخص المعني بالبيانات على معالجة بياناته»، مرجع سابق: أحمد عبد العزيز أبو الحسن، النظام القانوني للبيانات الشخصية الرقمية، ص: ١١٦

المفترضة أثناء شراؤه لمخافة هذا لحقوقه كمستهلك، وأيضا يعتبر هذا من وسائل الإكراه المخالفة لمبدأ حرية الموافقة

المطلب الرابع جمع البيانات الشخصية لغير مالكي الجهاز (نحو مفهوم محدودية التشغيل)

يلتزم المتحكمين في البيانات عموما بمبدأ محدودية الجمع وتناسبه مع الغرض، وهو من المبادئ المتفق عليها في جميع قوانين حماية البيانات الشخصية كالقانون المصري^{٥٥}، والقانون البحريني^{٥٦}، واللائحة العامة^{٥٧} التي قررت ضوابطه المختلفة، فنصت اللائحة علي أنه يجب ألا يجمع المتحكم في البيانات أي بيانات زائدة عن حاجته ولا تخدمه في الوصول للغرض النهائي من المعالجة^{٥٨}، ووضعت اللائحة مسؤولية إثبات هذا على عاتق المتحكم في البيانات، فيجب أن يكون قادرا على إثبات أن أي عملية من عمليات جمع البيانات التي يجريها أو أجراها متوافقة مع هذا المبدأ، أي يثبت أنه لم يجمع ولا يقوم بجمع بيانات شخصية أزيد من حاجته وما يقتضيه غرض المعالجة^{٥٩}.

وبالنسبة لحالة الأجهزة المتصلة المكونة لأجزاء «أنظمة إدارة وتأمين المنازل»، يلتزم مشغل هذه الأنظمة وتلك الأجهزة بهذا المبدأ، من حيث توفير وسائل مادية لضمان عدم الجمع المستمر للبيانات الشخصية، فلا يجب على مصمم الجهاز المتصل والمتحكم فيه أن يبقيه يقظا طوال الوقت ويقوم بجمع بيانات شخصية والتقاط أصوات وصور وأنشطة حتى في حالة عدم توجيه أوامر مباشرة له من مستخدمه^{٦٠}.

أولا: إشكالية حدود جمع بيانات العابرين

وفي حالة «أنظمة إدارة وتأمين المنازل» لا تقتصر البيانات الشخصية التي

٥٥ القانون المصري ١٥١ لسنة ٢٠٢٠، م ٢ / ٥

٥٦ القانون البحريني ٣٠ لسنة ٢٠١٨، م ٣

57 IBID :GDPR :Art 5 .GDPR – Principles relating to processing of personal data ,Art 25 .GDPR – Data protection by design and by default ,Art 47 .GDPR – Binding corporate rules ,Art 89 .GDPR – Safe-guards and derogations relating to processing for archiving purposes in the public interest ,scientific or historical research purposes or statistical purposes ,Recital.156

58 Office of the Data Protection Ombudsman, ‘Minimisation of data’ (Office of the Data Protection Ombudsman, Helsinki 2019) <http://bit.ly/moddposm>.

59 Information Commissioner Office, ‘Guide to Data Protection Guide to the General Data Protection Regulation (GDPR) For organisations, Principle (c): Data minimization’ (Information Commissioner Office, Wilmslow 2109) <http://bit.ly/dlimico>.

60 IoT European Large-Scale Pilots Programme, ‘personal data protection for internet of things deployments:lessons learned from the europeanlarge scale pilots of internet of things’ (V. 8.5, European union, brussle February 2020) 12; ibid 3.

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

تجمعها الأجهزة المكونة لمنظومة المنازل الذكية على بيانات مستخدمها ومالكها فقط، بل تشمل أيضا العابرين من (أعضاء الأسرة الآخرين، رواد المنزل من ضيوف ومهنيين، مخترقي المنازل من مرتكبي الأنشطة الاجرامية، المارين على حدود المنزل)، وهذا يطرح تحديات جديدة لمبدأ محدودية الجمع والمعالجة

فهنا يكون للالتزام بمحدودية الجمع مفهوم أوسع من المفهوم المعتاد في حالات المعالجة العادية التي تقتصر فقط على أنشطة الشخص المعنى بالبيانات^{٦١}، وطبقا لقوانين حماية البيانات الشخصية وأيضا طبيعة هذا الجمع فإن مالك الجهاز لا يعتبر متحكم في البيانات حيث أنه أولا في معظم الحالات لا يملك وصول للبيانات المعالجة ولم يبدأ في أي أنشطة معالجة لها، وثانيا، حتى لو أمكنه معالجتها وتخزينها فهو يخرج من نطاقها لمعالجته تلك البيانات للأغراض المنزلية والعائلية^{٦٢}.

ثانيا: مفهوم الالتزام بمحدودية التشغيل

وعليه يري الباحث ضرورة تقديم مفهوم جديد ألا وهو محدودية التشغيل بحيث يضمن مقدم خدمات المنزل الذكي ومنتج تلك الأجهزة عدم عمل الجهاز طوال الوقت، بل فقط عند توجه أمر صوتي أو مادي له فقط من صاحب الجهاز، ومثال على هذا كلمات مفتاحية مثل hey google الموجهة للمساعد الصوتي المقدم من شركة جوجل، وتكون هذه الطريقة هي الطريقة الأصلية لتشغيل تلك الأجهزة، مما يضمن عدم استراقها للسمع أو التقاطها لبيانات شخصية بطريقة عشوائية

وفي حالات أخرى عندما يختار مالك الجهاز أن يعمل الجهاز طوال الوقت أو تكون طبيعة عمل الجهاز تحتم هذا مثل حالات أنظمة الرقابة والأمن الذكية يجب التأكيد على محدودية الجمع وتناسبه مع الغرض بحيث لا تتجاوز مدة تخزين البيانات الشخصية مدة محددة بواسطة قانون أو قرار للجهة الرسمية المشرفة على عمليات معالجة البيانات الشخصية (كمثلا مركز حماية البيانات الشخصية المصري)، بشرط أن تتناسب مع غرض المعالجة المبني عليه مشروع معالجة البيانات الشخصية

61 Georg Borges and Christoph Sorge ,Law and Technology in a Global Digital Society :Autonomous Systems ,Big Data ,IT Security and Legal Tech) Springer Nature ,united states.143 (2022

٦٢ قانون رقم ١٥١ لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية: المادة رقم ٣ - اصدار: لا تسري أحكام القانون المرافق على ما يأتي : البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير ، ويتم معالجتها للاستخدام الشخصي. القانون البحريني: مادة (٢) نطاق التطبيق: ٤) استثناء من أحكام البند (١) من هذه المادة، لا تسري أحكام هذا القانون على ما يأتي أ) معالجة البيانات التي تتم من قبل أي فرد لأغراض لا تتجاوز الشؤون الشخصية أو العائلية، القانون المغربي: المادة ٢: ٤: لا يطبق هذا القانون على: - معالجة المعطيات ذات الطابع الشخصي من لدن شخص ذاتي لممارسة نشاطات شخصية أو منزلية بصفة حصرية؛ القانون التونسي: الباب الأول أحكام عامة: الفصل ٤ . تعتبر معطيات شخصية على معنى هذا القانون كل البيانات مهما كان مصدرها أو شكلها والتي تجعل شخصا طبيعيا معرّفا أو قابلا للتعريف بطريقة مباشرة أو غير مباشرة باستثناء المعلومات المتصلة بالحياة العامة أو المعتبرة كذلك قانونا، gdpr: recital ١٨.

المطلب الخامس

أمن وسلامة البيانات الشخصية

أولاً: المخاطر التقنية المستحدثة على البيانات الشخصية جراء معالجتها من قبل أنظمة إدارة وتأمين المنازل:

تعرض الطبيعة المتقدمة لأنظمة إدارة وتأمين المنازل البيانات الشخصية التي تجمعها لمخاطر عالية الخطورة، وهذا لحاجة تلك الأنظمة وأجهزتها المكونة لها للبقاء متصلة بشبكات المعلومات طوال الوقت من ناحية، ومن ناحية أخرى لإعتمادها على تقنيات مستحدثة تجعلها عرضة للاختراق بشكل أوسع، كما أن جمعها لأنواع حساسة من البيانات الشخصية يفرض ضرورة تأمينها بشكل أكثر جدية نظراً للأضرار الشديدة التي يمكن أن يسببها وقوع تلك البيانات الشخصية في حيازة الغير

وتتنوع هذه المخاطر من عوامل تتعلق بطبيعة تلك الأجهزة والتي لا تأتي بواجهة مستخدم مباشرة، بل تحتاج إلى ربطها بجهاز حاسوبي آخر كمثالاً هاتف أو لوحى ذكى وتنصيب برنامج مخصص للتعامل مع تلك الأجهزة ويتيح الوصول لإعداداتها، مما يعقد من عملية تغيير اعدادات الخصوصية والتأمين الافتراضية لكلمة السر الافتراضية والتي غالباً ما يسهل اختراقها بواسطة مخترقي الأنظمة hackers، أو تبني معايير أعلى من التأمين كمثالاً الولوج ثنائي الخطوات two way authentication، ويؤفف المستخدمين العاديين من الاقدام على تغييرها نظراً لصعوبتها أو عدم علمهم بطريقة تغييرها أو حتي بضرورة تغييرها، كما أن الحاجة الضرورية لتبني نماذج الحوسبة السحابية في تلك الأنظمة يجعل اتصالها المستمر بشبكات الاتصالات ضرورة حتمية مما يعرض البيانات الشخصية لمخاطر متزايدة نتيجة تواجدها الدائم على شبكة متصلة وشبه مفتوحة يمكن اختراقها من قبل أطراف خارجية

وعليه يقترح الباحث إرفاق تعليمات لكيفية تشغيل تلك الاعدادات مع الجهاز، وأيضاً وسيلة سريعة للوصول لصفحة تلك الاعدادات عن طريق كود استجابة سريع مرفق مع تلك التعليمات، وأيضاً قيام المشغل بتوفير اشعارات مخصصة لكيفية ووسيلة تغيير اعدادات الخصوصية والتأمين فور أن يقوم المالك بتشغيل النظام أو الأجهزة لأول مرة من خلال إشعار صوتي يخرج من الجهاز حال تشغيله لأول مرة باللغة التي يفهمها المالك، وفي حالة عدم توافر تلك الإمكانيات يمكن دفع رسالة مؤتمنة تظهر للمالك فور اقتران النظام أو أحد أجهزته بالهاتف المحمول الذكي لمالك النظام أو حاسوبه الشخصي مثلاً

لشبكات أنظمة المنازل الذكية من خلال مسح ومراقبة أنشطة الأجهزة المكونة لهذه الأنظمة وتحديد الأنماط الغريبة التي قد تحدث داخل تلك الشبكات⁶⁹.

وقد أكد قانون الصمود السيبراني للاتحاد الأوروبي في حيثته الرابعة والثلاثون على أهمية الأمن السيبراني للأجهزة ذات العنصر الرقمي وخاصة تلك الموضوعة في قائمة الأجهزة المهمة ذات العنصر الرقمي products Important digital with elements⁷⁰، والتي منها أي جهاز ذو عنصر رقمي يعالج البيانات الشخصية أو يقوم بعمليات معالجة للبيانات الشخصية قد تسبب أذى أو خطورة في قائمة الأجهزة المهمة ذات العنصر الرقمي Important elements digital with products والتي يجب أن تخضع لتقييم للمخاطر قبل طرحها في الأسواق حسب المادة السابعة من هذا القانون⁷¹.

69 Sandra Siby ,Rajib Ranjan Maiti and Nils Ole Tippenhauer' ,IoT Scanner:Detecting Privacy Threats in IoT Neighborhoods3) 'rd ACM International Workshop on IoT Privacy ,Trust ,and Security ,Abu Dhabi, 2April.24-25 (2017

70 Eu ,Cyber Resilience Act43) ,Products with digital elements should be considered to be important if the negative impact of the exploitation of potential vulnerabilities in the product can be severe due to ,inter alia ,the cybersecurity-related functionality or a function carrying a significant risk of adverse effects in terms of its intensity and ability to disrupt ,control or cause damage to a large number of other products with digital elements or to the health ,security or safety of its users through direct manipulation, such as a central system function ,including network management ,configuration control ,virtualisation or processing of personal data .In particular ,vulnerabilities in products with digital elements that have a cybersecurity-related functionality ,such as boot managers ,can lead to a propagation of security issues throughout the supply chain .The severity of the impact of an incident may also increase where the product primarily performs a central system function ,including network management ,configuration control ,virtualisation or processing of personal data.

71 Eu ,Cyber Resilience Act ,article :7 Important products with digital elements .1 ,Products with digital elements which have the core functionality of a product category set out in Annex III shall be considered to be important products with digital elements and shall be subject to the conformity assessment procedures referred to in Article (2)32 and (3) b (the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt ,control or cause damage to a large number of other products or to the health ,security or safety of its users through direct manipulation ,such as a central system function ,including network management ,configuration control ,virtualisation or processing of personal data

المبحث الثاني

التزامات خاصة بأنواع معينة من المعالجة

نظرا للطبيعة المعقدة لأنظمة إدارة وتأمين المنازل وقدراتها المتزايدة على جمع البيانات الشخصية المختلفة، فإن حدود جمعها لا تتوقف على نوع معين من البيانات الشخصية بل تتسع لجميع أنواع البيانات الشخصية ومن ضمنها أنواع خاصة من البيانات الشخصية أو ما أسمته قوانين حماية البيانات الشخصية بـ«البيانات الشخصية الحساسة»، وأيضا فهي تستخدم طرقا حديثة في أداء مهامها كالحوسبة السحابية لنقل البيانات لمراكز معالجتها باستخدام تقنيات الذكاء الصناعي، وهذا كله يطرح إشكالياته الخاصة التي تتطلب تنظيما خاصا لحماية البيانات الشخصية من تلك الطرق التي تعرضها

المطلب الأول

معالجة البيانات الحساسة

أولا: التنظيم القانوني لمعالجة البيانات الشخصية الحساسة:

البيانات الشخصية هي بيانات معنونة ومحددة حصرا في القوانين المقارنة لحماية البيانات الشخصية كبيانات حساسة، وهذا لفرض حماية أعلى عليها لما أرتاه المشرع من ضرورة حمايتها بشكل مشدد عن باقي البيانات لما تمثله دلالتها من حساسية مشددة لصاحبها^{٧٢}.

ويعتبر التوجيه الأوروبي لحماية البيانات الشخصية لعام ١٩٩٥، ثم اللائحة العامة خليفته هم المصدر الأول لما اعتبر بعد هذا «بيانات حساسة»، وقد وافقهم القوانين الأخرى كالقانون المصري بهذا التقسيم والذي شمل: «البيانات التي تفصح عن الصحة النفسية، أو العقلية، أو البدنية، أو الجينية، أو بيانات القياسات الحيوية «البيومترية» أو البيانات المالية، أو المعتقدات الدينية، أو الآراء السياسية، أو الحالة الأمنية»^{٧٣}، وأضاف عليها القانون المصري بيانات الأطفال^{٧٤}.

وتحظر القوانين المقارنة معالجة تلك البيانات الشخصية الحساسة إلا تحت ظروف معينة مشددة، فمثلا حظر القانون المصري معالجة تلك البيانات إلا بترخيص مسبق من مركز حماية البيانات الشخصية^{٧٥}، ونصت اللائحة العامة على بعض الأحوال التي من الممكن معالجة البيانات الشخصية الحساسة حصرا

٧٢ مرجع سابق: أحمد عبد العزيز أبو الحسن، النظام القانوني للبيانات الشخصية الرقمية، ص: ٦٩

٧٣ القانون البحريني ٣٠ لسنة ٢٠١٨، م ١، 9، article gdpr

٧٤ القانون المصري ١٥١ لسنة ٢٠٢٠، م ١

٧٥ القانون المصري ١٥١ لسنة ٢٠٢٠، فصل سادس م ٢٠

كالموافقة الحصرية على المعالجة، المعالجة اللازمة لمصلحة الشخص المعني بالبيانات، أغراض التوظيف والعمل، التشخيص الطبي وتقديم الخدمات الصحية، أغراض البحث العملي، كما اشترطت حذف البيانات الشخصية الحساسة فور الانتهاء من معالجتها^{٧٦}، ويلاحظ إضافة بعض القوانين الأخرى حالات أخرى على تلك المنصوصة في اللائحة العامة، كمثلاً القانون البحريني الذي أضاف المعالجة لأغراض التأكد من مدى توفر المساواة للأقليات^{٧٧}.

ثانياً: معالجة البيانات الحساسة لأغراض الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل:

أ: تنوع إمكانيات المعالجة والجمع وحاجتها

مع المهام المختلفة لأنظمة إدارة وتأمين البيوت تتنوع احتياجاتها لمعالجة البيانات الشخصية المختلفة، والتي في الواقع معظمها يندرج تحت تصنيف البيانات الشخصية الحساسة، ولكن يجب الأخذ في الملاحظة أن هذا الجمع لا تتساوي فيه جميع تلك الأنظمة نظراً لطبيعتها المرنة القائمة اتاحة الفرصة للمالك بتصميم نظامهم الذكي المنزلي ليتلاءم مع احتياجاته، فمثلاً تتوقف قدرة تلك الأنظمة على جمع أنواع خاصة من البيانات الإحيائية (البيومترية) على وجود أو غياب أجهزة خاصة تتمتع بأنواع من المستشعرات الإحيائية كمستشعرات قياس نسبة السكر في الدم وضغط الدم مثلاً كالساعات الذكية والأجهزة الطبية الذكية المتصلة

أما عن البيانات المعنوية الحساسة، كالبيانات الدينية والمتعلقة بالآراء الفلسفية فهي بيانات إن لم يعبر عنها الشخص المعنى بالبيانات أو يوفرها كتابة فمن الصعب معالجتها في مثل هذه المنظومات كونها تعبر عن اعتقادات داخلية، ولكن ليس من المستحيل استخلاصها فهي يمكن استخلاصها مثلاً من بث فيديو مباشر أو تسجيل صوتي ما، وهو في كل الأحوال تعدي مباشر على الحق في البيانات الشخصية لعدم الاحتياج الضروري لمثل هذا النوع من البيانات في ظل طبيعة تشغيل تلك المنظومات، إلا لو كان هذا التحليل للبيانات مبني على استثناء يتعدى حدود المشروعات العادية للمعالجة كالاحتياجات الأمنية العامة مثلاً^{٧٨}.

وهذه البيانات تجمع بالضرورة لتلبية احتياجات المالك، ولهذا فإن جمعها

٧٦ Kart Pormeister، 'Genetic data and the research exemption: is the GDPR going too far?' (2017) 7 International Data Privacy Law. 137

٧٧ القانون البحريني ٣٠ لسنة ٢٠١٨، م ٥
٧٨ القانون المصري ١٥١ لسنة ٢٠٢٠: م ٦ شروط المعالجة ٣ - تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً على حكم قضائي، م ٣ إصدار بند ٥:٥ - البيانات الشخصية لدى جهات الأمن القومي، وما تقدره لاعتبارات أخرى. ويجب على المركز، بناءً على طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال مدة زمنية محددة، وفقاً لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به.

مشروع ابتداء، أما عن بيانات العابرين فيمكن تطبيق نفس السبب عليها وهو تلبية الحاجات التعاقدية بين المشغل والمالك، لهذا يمكن معالجتها ما دامت تلك المعالجة لا تضر بالعبارين

ب: بيانات المقاييس الحيوية (البيانات البيومترية)

أما أكثر أنواع تلك البيانات والتي يتم معالجته بشكل خاص ومستمر داخل «منظومات الإدارة والتأمين الذكي المتصل للبيوت» فهو بيانات المقاييس الحيوية أو البيانات البيومترية^{٧٩}، وهي تعني «بيانات التعرف على الشخص بناء على بيانات مؤتمنة مستخلصة من خواصه الاحيائية كبصمة الاصبع وقزحية العين والطول أو خواصه الخارجية أو تصرفاته كطريقة مشيه^{٨٠}»، وأيضا طبقا للائحة العامة فهي «بيانات تستخلص من طرق معينة في المعالجة التقنية لخواص شخص طبيعي ما الفيزيائية والنفسية والتصرفات»^{٨١}.

وتتنوع قدرات الأجهزة المتصلة بأنظمة إدارة المنازل الذكية فيما يتعلق بجمع ومعالجة البيانات البيومترية، ولكن معظم النسخ الأحدث من تلك الأجهزة تمتلك قدرات كبيرة بالنسبة لمعالجة تلك البيانات كمثلا أجراس الباب الذكية من شركة «نكست هالو» تستطيع التعرف على هوية المتواجد أمامها، وأيضا جهاز المساعد المنزلي «مضخم للصوت ملحق به شاشة» من شركة «نيست» يستطيع التعرف على هوية المتواجدين بنطاقه بأي مكان في الغرفة ويعرض معلومات مخصصة لهم، وأجهزة تقديم خدمات الرعاية الطبية للمسنين ومراقبتهم تجمع كما ضخما من البيانات الشخصية الضرورية لأداء عملها^{٨٢}، كما أن أجهزة المراقبة المنزلية تستعمل البيانات البيومترية في التعرف على الأشخاص فمثلا تستخدم بصمة الأصبع وبصمة قزحية العين لتأمين الممتلكات وقوالب الوجه للتعرف على المجرمين مثلا^{٨٣}.

٧٩ تأتي كلمة biometric من جمع كلمتي bio وتعنى الحياة و matrix وتعنى قياس، See: Mikhail and Mitra Sinjini, Challenges and Trends in Biometrics, Gofman Press CRC) (2016 states United .xvii

80 Els J. Kindt, Privacy and Data Protection Issues of Biometric Applications :A Comparative Legal Analysis, Volume 12 of Law, Governance and Technology Series) Springer Science & Business Media, United states.1 (2013

81 Gloria González, Rosamunde Van Brakel and Paul De Hert, Research Handbook on Privacy and Data Protection Law :Values, Norms and Global Politics, Research Handbooks in Information Law series)Edward Elgar Publishing, United kingdom.385 (2022

82 Ming Hu, Smart Technologies and Design for Healthy Built Environments) Springer Nature, Switzerland.108 (2020

83 Vishal Goar, advances in information communication technology and computing :proceedings of Volume 392 of Lecture notes in networks and systems) Springer Nature, Singapore.312 (2021

ج: المخاطر الناجمة عن معالجة البيانات البيومترية:

تثير معالجة البيانات البيومترية مخاطر جمة وخصوصا في الشكل الذي تعالج به من قبل "أنظمة إدارة وتأمين المنازل"، فالكثير منها يعالج ويجمع بدون علم ومعرفة المستخدم أو الشخص المعنى بالبيانات، وهي ترسل عن طريق الحوسبة السحابية لمعالجتها للأغراض التشغيلية ولكنها يمكن إعادة استخدامها مرة أخرى لأغراض خاصة بالمتحكم تبتعد عن الغرض القانوني للمعالجة المشروعة، وهذا يمكن أن ينتهك مبدأ محدودية المعالجة وتناسبها حيث أنه من خلالها يمكن استخلاص العديد من أنواع البيانات الأخرى كالنوع والعرق، كما يكثر استخدام البيانات الشخصية البيومترية المتعلقة بالصحة لأغراض التأمين والأعمال البنكية والتوظيف، وقد تستخدم في تعقب الأشخاص، والتنمية والقبولة⁸⁴.

ويري الباحث أن الخطر الأكبر الواقع من معالجة البيانات الشخصية يكمن في طبيعتها الخاصة كونها بيانات متخصصة للغاية ولا يمكن تشفيرها والاستفادة منها إلا بوسائل خاصة، وأيضا فإن وسائل جمعها قد تكون غير واضحة للمستخدم العادي كباقي وسائل جمع أنواع البيانات الشخصية الأخرى بل أنه في أحيان كثيرة قد يجهل بجمعها وكيفية جمعها وطبيعته وكيفية الاستفادة منه، فهناك بعضا من البيانات البيومترية التي لا يدرك بوجودها حتى الأشخاص العادية ذات درجة المعرفة العالية كمثلا نمط المشي واستخدامه في ملاحظة وتتبع والتعرف على الأشخاص⁸⁵، وبالتالي فإن درجة حرره في استعمالها قد تقل بشكل كبير، وأخيرا فإن الطبيعة الثبوتية الكبرى لتلك البيانات تجعل إمكانية وصول أطراف متعددة لها له مخاطره الغير مشروعة كمثلا انتحال الهوية والتزييف وحتى الصاق التهم الجنائية بأشخاص أبرياء عن طريق استخدام تلك البيانات البيومترية

وقد وضع المشرع الأوروبي أي أجهزة ذات عنصر رقمي به حساس أو عنصر رقمي يتيح له قراءة البيانات البيومترية والتي عادة ما تستخدم لأغراض المصادقة والتأمين في فئة الأجهزة الرقمية المهمة ذات العنصر الرقمي⁸⁶، والتي تحتاج لإجراءات أكثر صرامة للتأكد من مطابقتها للمعايير الأوروبية الخاصة بالأمن السيبراني للأجهزة ذات العنصر الرقمي والتي أرساها هذا القانون والتي ستعرف بـ marking CE⁸⁷.

84 Patrizio Campisi ,Security and Privacy in Biometrics) Springer Science & Business Media ,United states.6 (2013

85 Yang Xu ,Wen Jung Li and Ka Keung Lee ,Intelligent Wearable Interfaces) John Wiley & Sons, united states.75 (2008

86 Eu Cyber Resilience Act ,ANNEX III IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS :class1: .1.Identity management systems and privileged access management software and hardware ,including authentication and access control readers ,including biometric readers

87 يهدف هذا إلى تعزيز الأمن السيبراني للمنتجات التي توزع ويتم بيعها في السوق الأوروبي المشتركة، وهي تمتد من المصنع للموزع للمستهلك، للمزيد انظر : marking CE ,Union European the :visited last 2024\12\15 ,https://sin-

المطلب الثاني معالجة البيانات الشخصية بواسطة أليات الذكاء الصناعي

أولاً: تعريف الذكاء الصناعي ودوره في أنظمة البيوت الذكية:

يعرف الذكاء الصناعي على أنه "فرع من فروع علوم الحاسوب والتي يعني بتطوير أليات حاسوبية يمكنها القيام بعمليات تشبه التفكير البشري مثل التعلم والمنطق والتصحيح الذاتي والتكيف وتطور هذا التعريف إلى "تقليد الذكاء والسلوك الصناعي"^{٨٨}، وهو فرع حديث من فروع العلوم التطبيقية له تطبيقاته المتعددة والمهمة للغاية في مسار التطور التقني الحالي^{٨٩}.

ويمكن القول بأن الذكاء الصناعي له درجتين أولهما ما يعرف بالذكاء الصناعي الحقيقي وهو ما عرف بأنه «الألة التي تستطيع أن تسلك وتفكر كالإنسان» وهي أعلى درجة للذكاء الصناعي، ثم الدرجة الأدنى من الذكاء الصناعي وهي الألة التي تستطيع أن تبين تقليدا للسلوك والتفكير البشري وهي ما يعرف بالمساعدات الآلية الشخصية مثل مساعد جوجل «جوجل اسيستنت» ومساعد أبل سيرري^{٩٠}.

وللذكاء الصناعي داخل أنظمة البيوت الذكية تطبيقات متعددة، ابتداء من عملية التشغيل التي تستعمل ما يطلق عليه فهم اللغة الطبيعية^{٩١}، وبها يمكن للأجهزة والمساعدات الصوتية التي تدير منظومة البيت الذكي فهم الأوامر المعطاة إليها من مالك النظام، وأيضا تستخدم للتعرف على الهوية عن طريق مسح البيانات البيومترية، وأتمتة العمليات، وفهم البيانات الشخصية وغير الشخصية المعطاة إليها من خلال مستشعرات الأجهزة المكونة للنظام لتنفيذ الأوامر المطلوبة منها

[en_marking-ce/market-single/eu.europa.ec.economy-market-gle](https://en.marking-ce/market-single/eu.europa.ec.economy-market-gle)

88Joost Nico Kok, ARTIFICIAL INTELLIGENCE, Volume 15 of Encyclopedia of life support systems (unesco, EOLSS Publications, united kingdom 2009) 2.

٨٩ تم صك المصطلح بواسطة العالم ألان تورينج من أباء علوم الحاسب بعام ١٩٤٧ بمقالة نشرت عام ١٩٥٠ بعنوان «هل يمكن للآلات التفكير»، واكتسب المصطلح شهرته في مؤتمر كلية دارموث عن التفكير الآلي بعام ١٩٥٦، وفيه تنبأ بقدرة الآلات على فعل كل ما يفعله البشر بحلول ١٩٨٥ : Bramer Max : Intelligence Artificial, Perspective International An : 5640 Volume, (Business & Science Springer) Survey Art-The-Of-State :Intelligence Artificial in Notes Lecture of

Media , 2009 kingdom united) 1.

90 Deepika Pandoi, 'Analysis of Implication of Artificial Intelligence on youth' in Vishal Goyal and others (eds), Proceedings of International Conference on Communication and Artificial Intelligence: ICCAI 2020, Volume 192 of Lecture notes in networks and systems (Springer Nature, Singapore 2021) 401-402.

٩١ فهم / معالجة اللغة الطبيعية هو فرع متراكب من عدد من العلوم يبحث في كيفية استخدام الحاسوب لمعالجة وفهم الكلام كما يتكلمه البشر الطبيعيون (اللسان المعنود) لأداء مهام نافعة. أنظر Li, Liu Yang and Deng Li Natural in Learning Deep, (Springer) Processing Language (Singapore, 2018) ١.

ثانيا: استخدام البيانات الشخصية في داخل أنظمة الذكاء الصناعي:

للبيانات الشخصية دورا حيويا في أنظمة الذكاء الصناعي وبرمجياته، فإن كان الهدف النهائي من هذه التقنيات هو أنسنه الآلة، فلا مرأى من الحاجة الشديدة والحيوية للبيانات الشخصية في جميع مراحل برمجة تلك البرمجيات، فهي تستخدم بشكل معتاد لتمرين وتطوير برمجيات محاكاة الذكاء والسلوك البشري^{٩٢}.

وثاني هذه الاستخدامات هو الاستخدام المباشر لتلك البيانات في تنفيذ المهام الموكلة للأجهزة القائم عملها على برمجيات الذكاء الصناعي، كمثلاً: التعرف على الوجه، المساعدات الصوتية الحديثة، الروبوتات المؤتمتة، فهم اللغة الطبيعية language natural، الرؤية الحاسوبية vision computer.

ثالثا: الشروط القانونية لمعالجة البيانات الشخصية لأغراض الذكاء الصناعي:

على الرغم من عدم تناول القانون المصري لمعالجة البيانات الشخصية لأغراض الذكاء الاصطناعي بأي تنظيم خاص، إلا أن هذا ليس الحال في باقي القوانين المقارنة والتي حرصت على تخصيص جزءا من موادها لهذا النوع من المعالجة، كالثلاثة العامة التي ألزمت المتحكم الذي يعالج البيانات الشخصية لأغراض الذكاء الاصطناعي بمعيار الشفافية والذي يلزمه بإعلام الأشخاص المعنية بالبيانات وأيضا لمستخدمي خدماته عموما أنه يستخدم برمجيات الذكاء الصناعي في عملياته الداخلية، وأن يوضح تلك العمليات، وأنه قد يستخدم بياناتهم الشخصية لأغراض تطوير تلك البرمجيات التي يستخدمها^{٩٣}.

وأیضا فإن الطبيعة الخاصة لاستخدام البيانات الشخصية لأغراض تدريب وتطوير أليات الذكاء الصناعي تتعارض بشكل مباشر مع مبدأ الالتزام بمحدودية المعالجة وتناسبها مع الغرض من المعالجة، وأيضا الالتزام بتقليل كمية البيانات الشخصية التي تعالج لأقصى حد ممكن، وأيضا فهي تتعارض أيضا مع معايير معالجة البيانات الحساسة وربط البيانات ببعضها^{٩٤}.

ولما كانت معالجة البيانات الشخصية لأغراض تطوير برمجيات الذكاء الصناعي لها أهميتها المطلقة في مجالات البحث والتطوير العلمي، فيمكن الاستناد إلى المعايير التي أتت في القوانين المقارنة – لا القانون المصري^{٩٥} - وخصوصا

92 European parliament, The impact of the General Data Protection Regulation (GDPR) on artificial intelligence, France: Scientific Foresight Unit, 2020, p: 1

93 Kaori Ishii, 'Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence: looking at functional and technological aspects' (2019) 34 AI & SOCIETY 515.

94 Ibid :European parliament ,p2 :

٩٥ القانون المصري لم يتناول معالجة البيانات الشخصية لأغراض البحث العلمي بأي نوع من التنظيم الخاص، مقارنة مثلا ببعض القوانين الأخرى كالقانون التونسي لحماية البيانات الشخصية والثلاثة العامة والتي أفردت مواد مخصصة لهذا النوع الخاص من المعالجة، راجع: مرجع سابق: احمد عبد العزيز أبو الحسن، النظام القانوني للبيانات الشخصية الرقمية، ص: ٢١٥-٢١٨

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

تجهيل البيانات واتاحتها فقط على هيئة إحصائيات عامة مجهلة بعد نزع المفاتيح الدلالية منها لإضفاء المشروعية على تلك المعالجة، وهي مشروعية مقيدة فقط بحدودها وشروطها الضيقة^{٩٦}.

والحقيقة أن الوضع التشريعي الخاص بمعالجة البيانات الشخصية لأغراض الذكاء الاصطناعي قد تطور كثيراً بعد إقرار النسخة النهائية لقانون الذكاء الاصطناعي الأوروبي، ولكن باختصار يتطلب القانون الأوروبي توازناً تاماً بين مصالح تطوير وتسويق نماذج الذكاء الاصطناعي والمتطلبات الخاصة بمعالجة البيانات الشخصية طبقاً لللائحة العامة لحماية البيانات الشخصية، على طول خط المعالجة وتشغيل نماذج الذكاء الاصطناعي^{٩٧}.

المطلب الثالث

نقل البيانات الشخصية لأغراض الحوسبة السحابية

كما أسلفنا فإن الأجهزة المادية المكونة للمنظومات الذكية للبيوت لا تملك بداخلها شرائح حاسوبية قوية بالقدر الكافي لتقوم بالمهام المطلوبة منها، لذا فإن تقنيات الحوسبة السحابية لها مكان مهم للغاية في تصميم هذه المنظومات، فهي حلقة الوصل بين قسمي المنظومة من القسم الداخلي القائم بالتقاط البيانات والأوامر والقسم الخارجي المعالج لتلك البيانات لتتمكن المنظومة من أداء مهامها، والحوسبة السحابية تعني «نقل عمليات الحوسبة من معالجة وتخزين لمنصات حاسوبية ضخمة موزعة عالمياً تتواصل عن طريق شبكة اتصالات سريعة، يمكن للعميل من خلالها أن يقوم بكافة متطلباته الحاسوبية كالتخزين والمعالجة والتصفح دون أن يملكها كجهاز واحد متكامل في يده أو حوزته بل يؤجر خدماتها فقط، وهي أيضاً تستخدم في عمليات الحوسبة العملية والذكاء الصناعي»^{٩٨}.

وعلى الرغم من قصر قانون الصمود السيبراني لنطاق الحوسبة السحابية فيما يخص تنظيمه لـ «الأجهزة ذات العنصر الرقمي» على مفهوم أطلق عليه «معالجة البيانات من على بعد» وهو ما ربطه بالبرمجيات أو الأجهزة التي صممت خصيصاً أو تحت إشراف أو تحت مسؤولية المصنع للجهاز ذو العنصر

96 Ann Bowling and Shah Ebrahim, Handbook of Health Research Methods: Investigation, Measurement And Analysis) McGraw-Hill Education) UK, (England; 167 (2005 EU Regulation 536/2014 on clinical trials on medicinal products for human use, arts.81, 56

97 See IAPP, 'A deep dive into Europe's approach on personal data processing in AI systems' <https://iapp.org/news/a/a-deep-dive-into-europes-approach-on-personal-data-processing-in-ai-systems> accessed 16 December.2024

٩٨ نجلاء أحمد يس، الحوسبة السحابية للمكتبات حلول وتطبيقات، القاهرة: العربي للنشر والتوزيع، ٢٠١٤، ص: ٢٠، طلال أبو غزالة، العالم المعرفي المتوقد، الأردن: طلال أبو غزالة للترجمة والتوزيع والنشر، ط٢، ٢٠١٩، ص: ٥٥، وأيضاً: «الحوسبة السحابية هي نموذج عمل يمكن من طلب منصات حاسوبية متعددة وقابلة للتخصيص حسب الطلب، تتكون من مخدمات وأجهزة اتصال وتخزين وتطبيقات وخدمات» B. Nayan, Ruparelia, Computing Cloud, (MIT Press, states United ٢٠١٦) ٤: «تقنية تحول الخدمات والتقنيات والتطبيقات التي تتاح على الانترنت وتحولهم أدوات خدمة ذاتية» Computing Cloud, Sosinsky Barrie

(Sons & Wiley John) Bible (٢٠١١) ٤

الرقمي، وبدونها لا يستطيع هذا الجهاز أداء مهامه، إلا أننا نرى أن هذا راجع لطبيعة هذا القانون ذاته من حيث تركيزه على التنظيم الصناعي لتلك الأجهزة، وهذا لا يعني أن أي جهاز ذكي أو ذو عنصر رقمي لا تخضع لقواعد معالجة البيانات الشخصية ونقلها خارج الحدود المنصوص عليها في اللائحة العامة لحماية البيانات الشخصية، وهي:

أولاً: الاشتراطات القانونية لنقل البيانات الشخصية:

١/ تزامن لا نقل

أول الإشكاليات التي تظهر أثناء نقل البيانات الشخصية طبقاً لأليات الحوسبة السحابية، هو عدم دقة كلمة النقل نفسها وعدم انطباقها على طبيعة العمليات المجرأة على البيانات أثناء معالجتها وتزامنها سحابياً، فالأحرى أن يطلق عليها المزامنة لا النقل كون أن البيانات تكون متواجدة بشكل لحظي في أكثر من مكان حول العالم، وهذا يرجع لكيفية تصميم تلك الأليات المستحدثة التي تفرض توزيع مكونات المنظومة الحاسوبية هذه في أكثر من نطاق قانوني فيمكن أن يتم التخزين في دولة والمعالجة في دولة أخرى والتعامل النهائي على البيانات الشخصية بدولة أخرى تماماً

٢/ حالة النقل السحابي المعتمد على منصة أمازون لخدمات الحوسبة السحابية:

وتتضح المخاطر المستحدثة على البيانات الشخصية من جراء استخدام تقنيات الحوسبة السحابية بما أثارته مجموعة حقوقية أمريكية من مخاوف تتعلق بسياسة نقل البيانات الشخصية الخاصة بشركة رينج التابعة لأمازون الأمريكية والمعتمدة على بنية الحوسبة السحابية التابعة لشركة أمازون والمسماة بأمازون ويب سيرفيس service web amazon^{٩٩}، وخصوصاً ما يتعلق بتحديد الولوج وتأمين البيانات أثناء نقلها عبر الحدود الوطنية وخارج حدود الولايات المتحدة^{١٠٠}،

99 Nick Barney and Alexander S. Gillis, 'Amazon Web Services (AWS) (Techtarget (<https://www.techtarget.com/searchaws/definition/Amazon-Web-Services> accessed 29 January.2023

١٠٠ تمتلك شركة أمازون الأمريكية شركة تدعى «رينج RING» وهي شركة تقدم خدمات أمنية منزلية من خلال بيع جهاز ينتمي لما يعرف بإنترنت الأشياء IOT عبارة عن جهاز تنبيه وجرس باب منزلي مزود بكاميرا ذكية متصلة بالإنترنت يعرف بـ «جرس الباب الذكي bell door smart»، Fang Zhigang, Technology Applied and Science Energy, the of Proceedings :Technology Applied and Science Energy on Conference International ٢nd (ESAT) (٢٠١٥) (٢٠١٥), Press CRC Kingdom United (٢٠١٥) ٢٦١ وهو يوفر وظائف جرس الباب التقليدي مع إمكانيات حديثة تتدرج من توفير بث مباشر وحى لما يحدث في نطاقه، وأيضاً إمكانية تواصل بين ماله ومن يتواجدون في نطاق الجهاز، ومتابعة ومراقبة وتتبع لكل الأحداث التي تحدث في نطاقه، كما أنه متصل بخدمات حوسبة سحابية تتيح له القيام بعمليات معالجة متقدمة على البيانات كنخزين مقاطع مراقبة أو تحليلها ومشاركتها كمقاطع تشبه ما يحدث في مواقع التواصل الاجتماعي، واستخدام برامج التعرف على الهوية وقوالب الوجه face pattern لمن يقعون في نطاقه، وهو برنامج تابع للشركة الأم «أمازون» ويدعى أمازون ريكognition AMAZON REKognition and Analytics, Management Data, Chakrabarti Amlan and Sharma Neha, Balas Emilia Valentina Systems Intelligent in Advances of ٨٠٨ Volume ١, Volume ٢٠١٨ ICDMAI of Proceedings :Innovation

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

فهذه السياسة تسمح لفريق الشركة الهندسي الواقع بأوكرانيا بالولوج لكافة البيانات الشخصية لعملاء الشركة الأمريكيين عن طريق خدمات الشركة الأم «أمازون» «خدمات أمازون للويب services web amazon» بدون تحديد للولوج أو تشفير وحماية لتلك البيانات، مما يعرض تلك البيانات الشخصية لمخاطر متزايدة، وخصوصا إذا تم الأخذ في الاعتبار الطبيعة المتقدمة للعمليات المجراة على تلك البيانات والتي تتضمن تقنيات الذكاء الاصطناعي والذي تعتمد عليه الشركة في جوهر أعمالها وتصميمها لكافة أجهزتها، لتستفيد من الإمكانيات الضخمة لبنية الحوسبة السحابية التابعة لشركة أمازون بما فيها تقنيات التعرف على الوجوه والرؤية الحاسوبية^{١٠١}.

٣/ المخاطر الناجمة عن عدم توافقية قوانين حماية البيانات الشخصية بين دول العالم:

وعلى الرغم من الأهمية المطلقة للانسياب الحر للبيانات الشخصية في المنظومة العالمية الحديثة^{١٠٢}، فإن عمليات النقل هذه تشكل مخاطر متعددة وجسيمة على البيانات الشخصية، ومن أهمها خروج عمليات المعالجة هذه والقائمين عليها من نطاق الانفاذ القانوني المحلي، وخضوعه لقوانين أخرى قد لا توفر نفس الحماية القانونية الممنوحة لمثل تلك البيانات في القانون المحلي، وعليه يجب الالتزام التام بقواعد نقل البيانات الشخصية أثناء استخدام مثل تلك التقنيات المستحدثة، حيث اتفقت قوانين حماية البيانات الشخصية على ضرورة أخذ تصريح مخصص من السلطات المحلية المختصة بحماية البيانات الشخصية قبل الشروع في نقل تلك البيانات الشخصية وهذا لضمان توافر مستوى كافي من الحماية للبيانات الشخصية التي يراد نقل البيانات الشخصية لها^{١٠٣}.

كما اتفقت هذه القوانين على وجوب تعيين ممثل وطني داخل دولة القانون للمتحكم الأجنبي ويخاطب هذا الممثل في جميع ما يخص عمليات معالجة البيانات الشخصية التي يجريها المتحكم على بيانات مواطني الدولة^{١٠٤}.

States United, Springer) Computing and ٢٠١٨ (٢٨٣.

101 sam biddle. for owners of amazon's ring security cameras, strangers may have been watching too, sources disclosed troubling privacy practices at a ring office in Ukraine, theintercept (web site), january10 2019, last visited: 12/9/2022, <https://theintercept.com/2019/01/10/amazon-ring-security-camera/>

102 The OECD Council 'Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data' THE OECD PRIVACY FRAMEWORK, Paris 23September (1980 <http://bit.ly2/t3QPnf>).

١٠٣ راجع القانون المصري رقم ١٥١ / ٢٠٢٠ لحماية البيانات الشخصية م ١٤-١٥-١٦، القانون البحريني ٢٠١٨٣٠ / لحماية

البيانات الشخصية م / ١٢-١٣، GDPR، arts ٤٠-٤٥، recitals ١٠١-١٠٤-١٠٦-١١٠; von Axel and Voigt Paul ; (GDPR) Regulation Protection Data General EU The, Bussche dem (Springer) Guide Practical A : (GDPR) Regulation Protection Data General EU The, Bussche dem

Germany /Berlin (٢٠١٧) ١١٦.

١٠٤ راجع القانون المصري رقم ١٥١ لسنة ٢٠٢٠، م ٤ بند ١١، القانون البحريني ٣٠ لسنة ٢٠١٨، م ٢ بند ٣، GDPR، art 27; United Press University Oxford) Business Online and Law Privacy Data European, Kuner Christopher

كما نصت اللائحة العامة على آلية تعاقدية تخدم كناقل للالتزامات القانونية المفروضة على المتحكم المخاطب بموجب اللائحة العامة إلى الجهة التي يتم نقل البيانات الشخصية إليها، وهي عقود نموذجية تضعها السلطات الإشرافية على البيانات الشخصية أو المتحكم الناقل للبيانات الشخصية، وتوافق عليها السلطة الإشرافية قبل إبرامها، ولها وظيفتان أولهما إباحة النقل العابر للحدود للبيانات من قبل المتحكم، وثانيهما إلزام الجهة التي تنتقل لها تلك البيانات بنفس الالتزامات التي يلتزم بها هذا المتحكم»^{١٠٥}، وهذا لضمان نفس مستوى الحماية والمسئولية القانونية.

ولهذه الآلية التعاقدية نوعان، أولهما القواعد التي تنظم نقل البيانات الشخصية داخل مؤسسة (شخص اعتباري خاص) واحد له صفة دولية (له أكثر من فرع عالميا) وهي قواعد تضعها الشركات وتلزم بها نفسها وتسري على جميع فروعها الدولية حتي لو لم تكن مقار تلك الفروع تلتزم بقواعد معينة للتعامل مع البيانات الشخصية، وتعرف ب (القواعد الملزمة للشركات rules binding coporate) والنوع الآخر وهو العقود النموذجية Standard Contractual Clauses (SCC) (((الموضوعة والموافق عليها من قبل السلطات الإشرافية، وهذه العقود هي صيغ جاهزة تم الموافقة عليها قبلا من قبل السلطات الإشرافية وتعمل على توفير ونقل الالتزامات التشريعية لهيئة عقدية تكون ملزمة للطرف الغير خاضع للالتزامات التشريعية^{١٠٦}.

111 (2003 Kingdom

105 John E. Steiner, Clinical Research Law and Compliance Handbook (Jones & Bartlett Learning, usa 2006) 251.

106 Santa Slokenberga, Olga Tzortzatou and Jane Reichel, GDPR and Biobanking: Individual Rights, Public Interest and Research Regulation Across Europe, Volume 43 of Law, governance and technology series (Springer Nature, Switzerland 2021) 57; Eleni Kosta, Consent in European Data Protection Law, Nijhoff Studies in European Union Law (Martinus Nijhoff Publishers, boston/ usa 2013) 181; Orla Lynskey, The Foundations of EU Data Protection Law, Oxford Studies in European Law (Oxford University Press, Oxford 2015) 42; Mor Bakhom and others, Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?, MPI Studies on Intellectual Property and Competition Law, Volume 28 (Springer, Germany 2018) 514.

107Andreas Bartosch and Jens-Daniel Braun, EC Competition and Telecommunications Law, International competition law series vol6 (Kluwer Law International B.V., the Netherlands 2009) 555; Deborah Ellis Timberlake, Payroll Answer Book: 2019 Edition (Wolters Kluwer Law & Business, new York 2019) 46.

الفصل الثاني

معالجة البيانات الشخصية لأغراض الأنظمة الذكية لتأمين المنازل

لا يقف دور الأنظمة الحديثة المؤتمتة لأعمال المنزلية على جانب الإدارة فقط، بل يلعب التأمين جانبا خطيرا في جذب الأشخاص لتشغيل وتنصيب تلك الأنظمة في منازلهم الخاصة

فعلى الرغم من قدم انتشار ما يعرف بـ «دوائر الرقابة التليفزيونية المغلقة CCTV»^{١٠٨}، إلا إن هناك صور أحدث من تلك الأنظمة القديمة تشكل جانبا كبيرا من الأنظمة الذكية لإدارة وتأمين المنازل، وهي كاميرات الفيديو الذكية المتصلة والتي تعرف بـ «أنظمة المراقبة الذكية المتصلة»^{١٠٩}، وقد تم تبني هذه الصورة الحديثة لكاميرات المراقبة والتأمين بشكل كبير للغاية على المستوي العالمي^{١١٠}، وأصبحت تتخذ صوراً متعددة ابتداءً من كاميرات وأنظمة فردية صغيرة داخل المنازل انتهاءً بأنظمة صناعية متطورة وضخمة تستخدم لتأمين الملكيات والمؤسسات الكبرى

وهذه الصورة الأحدث من هذه الأنظمة تتيح امكانيات أضخم لمالكها ازاء البيانات الشخصية التي تلتقطها وتعالجها، وكلما تقدمت هذه الأنظمة زادت امكانياتها لتتجاوز ما يمكن أن تقدمه هذه الوحدات الحاسوبية الصغيرة بمفردها، حيث أن صورها الأحدث تعتمد على ما يعرف بالحوسبة السحابية واتصالها المستمر بوحدات معالجة ضخمة تتيح لها استخدام تقنيات الذكاء الاصطناعي والرؤية الحاسوبية والتعرف على الأصوات واللغة الطبيعية وغيرها من الإمكانيات المتقدمة والتي وإن كانت تعظم من الفائدة العائدة على مالك تلك الأنظمة إلا أنها تزيد من المخاطر الواقعة على البيانات الشخصية بشكل مهول، وهو ما سيحاول الباحث تفصيله هنا على مبحثين

١٠٨ أنظمة المراقبة التليفزيونية المغلقة: هي أنظمة حيث يتم ربط عدد من كاميرات الفيديو ببعضها، ويتم بث الصور الملتقطة لعدد من شاشات المراقبة التليفزيونية ولا يتم بثها للعموم of Dictionary SAGE The ,Fleming Jenny and Wakefield Alison (SAGE) Policing (٢٠٠٨) ٢٨.

١٠٩ وقد عرف اتحاد التصوير المؤتمت الأمريكي هذا النوع من كاميرات التصوير بأنها كاميرات بها بعض الإمكانيات المتعلقة بمعالجة الصور والتصوير وأيضا بها وحدة معالجة حاسوبية تستخدم لأغراض التصوير ومعالجة الصور، تقوم ببعض أنواع العمليات بشكل مؤتمت مثل تتبع الحركة بدون الحاجة لتدخل بشري Ahmed Nabil Belbachir, Smart Cameras, London, Springer Science & Business Media, ٢٠٠٩, p: ٣

110 Jean-Yves Dufour, Intelligent Video Surveillance Systems) John Wiley & Sons, New Jersey, United States. 1 (2012

المبحث الأول المشاكل التي تثيرها معالجة البيانات لأغراض الأنظمة الذكية لتأمين المنازل

تنتشر اليوم في الشوارع والملكيات والأماكن التجارية استخدام أنظمة المراقبة الفيديوية التقليدية، وأحيانا الذكية منها، لما لها من دور مهم في تأمين الملكيـات الخاصة، كما توفر الإصدارات الأحدث منها عوامل أمان وامكانيات وراحة مستخدم أكثر^{١١١}، وهي تنتشر حتى بشكل أكبر في الخارج فقد قدر الخبراء أن المواطن الأمريكي العادي قد يتعرض للتصوير بواسطة ٢٣٨ كاميرا مراقبة أسبوعيا^{١١٢}.

وتثير هذه الأنظمة مشاكلها الخاصة التي تزيد عن باقي مكونات النظام المنزلي الذكي الحديث، نظرا لطبيعة المعالجة، ورغبة الجهات الأمنية العامة في استخدام البيانات الشخصية المولدة من خلالها لأغراض الخاصة

ولهذا نظمتها بعضا من القوانين المقارنة لحماية البيانات الشخصية، وعملت بعضا من المنظمات الدولية على تحديد أخطارها وتقديم توصيات لتنظيم استخدامها في مجال الأمن العام لما لهذا الاستخدام من مخاطر على حقوق وحريات الأفراد

المطلب الأول الشروط القانونية لإنشاء أنظمة التأمين

على الرغم من عدم تناول القانون المصري لحماية البيانات الشخصية لمثل هذا النوع من أنواع المعالجة بالتنظيم، إلا أن بعض القوانين الأخرى لحماية البيانات الشخصية نظمتها تنظيما خاصا

والملاحظ هنا أن هذه القوانين قد وضعت هذه المواد وفي نصابها أنظمة التأمين والمراقبة العادية دون الأنظمة الحديثة المتصلة التي تستعمل برمجيات الذكاء الصناعي لأغراض أكثر تقدما مثل تحديد الهوية عن طريق مسح ومعالجة البيانات البيومترية

كالقانون التونسي مثلا الذي اشترط ضرورة الحصول على تصريح مسبق من الجهة الاشرافية «الهيئة الوطنية لحماية المعطيات الشخصية التونسية» عند تركيب تلك الأنظمة وإدارتها، كما قصر نطاقها على الأماكن العامة وأماكن العمل

111 Yunqian Ma, Gang Qian, Intelligent Video Surveillance: Systems and Technology, united states, CRC Press, 2009, p: 4

112 Alexia Georgiou, AI :My Story ;The Story AI Tells ;Bias & Privacy) Life Betterment Through God, LLC ,united states102 (2020 .

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

الجماعية والمواصلات العامة، ويجب أن يراعي مشغلها (المتحكم في البيانات) معيار تحديد الغرض والتخزين والاعلام، ولا يتم نقل البيانات التي تولدها إلا بعد موافقة الشخص المعنى بالبيانات، أو في حالات المصلحة والأمن العام^{١١٣}، واتفق القانون البحريني مع مثيله التونسي في ضرورة الحصول على تصريح مسبق قبل البدء في تنصيب هذه الأنظمة^{١١٤} ولكنه لم يفصل شروطا خاصة لتنصيبها

ولم تخص اللائحة العامة هذا النوع من معالجة البيانات الشخصية بتنظيم خاص به، ولكنها أيضا لم تستثنها من أحكامها، ولهذا عملت بعض من الجهات الأوروبية المعنية بوضع إرشادات وتوجيهات للأفراد الراغبين في تنصيب وتشغيل تلك الأنظمة

كمثلا مفوض حماية البيانات البريطاني الذي أوضح حالتان لتلك الأنظمة: أولهما تنصيبها بحيث لا يتجاوز نطاق النقاطها حدود الملكية الخاصة، وفي هذه الحالة فهي لا تخضع لقانون حماية البيانات الشخصية (النسخة البريطانية لللائحة الأوروبية)، أما في حالة تعدي نطاق النقاطها للملكية الخاصة، فهي في هذه الحالة تخضع للقانون ويكون مالكة ملتزمة بكافة الالتزامات التي ينص عليها القانون، لذا فقد أوصى بتنصيبها بحيث لا يتجاوز نطاقها نطاق الملكية الخاصة تخفيفا للالتزامات القانونية التي يخضع لها مالكةا^{١١٥}.

كما نصت كل تلك القوانين على ضرورة الالتزام بالقواعد العامة للمعالجة المشروعة للبيانات من حيث الاعلام، ومحدودية الجمع، واقتصار استخدام البيانات على سبب مشروعية المعالجة، وأخيرا سرية وتأمين البيانات وعدم مشاركتها

ويجب الأخذ في الاعتبار هنا أنه على الرغم من خروج مالك نظام المراقبة من الأشخاص الطبيعية من نطاق اللائحة العامة، فإن هذا لا يعفيه من الالتزامات العامة والمشروعة للحق في الخصوصية، فلا يجوز به استخدام تلك البيانات وخصوصا الصور والفيديوهات التي تلتقطها تلك الأنظمة لأغراض الابتزاز أو التشهير أو أي غرض آخر غير تحقيق أمنه الخاص، وفي حالة التقاطه لأنشطة إجرامية يجب عليه اقتصار مشاركتها مع المعنيين بالأمر من جهات الأمن العام، وليس استخدامها في أفعال مجرمة كالابتزاز الإلكتروني^{١١٦}.

١١٣ القانون التونسي لحماية البيانات الشخصية ٦٣ لسنة ٢٠٠٤: القسم الرابع في معالجة المعطيات الشخصية لأغراض المراقبة البصرية

١١٤ القانون البحريني: مادة (١٥) التصريح المسبق/ هـ

١١٥ICO, 'Domestic CCTV systems – guidance for people using CCTV' <https://ico.org.uk/your-data-matters/domestic-cctv-systems-guidance-for-people-using-cctv>

١١٦ تامر محمد محمد صالح، الابتزاز الإلكتروني : دراسة تحليلية مقارنة، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، ع ١٤، الإسكندرية: جامعة الإسكندرية - كلية الحقوق، ٢٠١٨، ص: ٥٥٦، د/ داليا عبد العزيز، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة، المملكة العربية السعودية: مجلة جيل الأبحاث القانونية المعمقة العدد ٢٥، لبنان، مركز جيل البحث العلمي، ص: ٣٣

المطلب الثاني

تقنيات التعرف على الهوية من خلال مسح نمط الوجه

أولاً: تعريف تقنيات التعرف على الهوية من خلال مسح نمط الوجه:

لا يمكن انكار أهمية هذه التقنية وخصوصاً في قطاعات الأمن والتأمين، ولهذا فهي من أكثر تقنيات وأجهزة التأمين والأمن البيومترية جذبا لمطوري أجهزة ونظم المراقبة والتأمين^{١١٧}، وقد عرف التعرف على الوجه على أنه «المعالجة التلقائية للصور الرقمية التي تحتوي على وجوه الأفراد بغرض تحديد الهوية، التوثيق/التحقق أو التصنيف لهؤلاء الأفراد. وهي عملية تتكون من عدد العمليات الفرعية المنفصلة: الحصول على الصور التي تحتوي على وجوه الأشخاص، تحديد الوجه، مسح المتغيرات البسيطة وتحسين الوجه، تحديد النقاط المفتاحية للوجه، ادخال بيانات الوجه ضمن نظام التعرف على الهوية، المقارنة والتعريف^{١١٨}»

ثانياً: المخاطر الناجمة عن استخدام تلك التقنيات على الحق في البيانات الشخصية:

١/ المخاطر الناجمة من عدم وعي الشخص المعني بالبيانات بالتقاط بياناته والتعرف عليه:

ويري الباحث أن تقنيات «التعرف على الهوية من خلال مسح نمط الوجه» من أخطر تقنيات التعرف البيومترية من وجهة نظر حماية البيانات الشخصية، كونها لا تتطلب تفاعلاً واعياً بين الشخص المعني بالبيانات والآلة التي تتعرف عليه فالكثير من تلك الآلات يمكنها التعرف على هوية الشخص المعني بالبيانات بمجرد وجوده في نطاقها الذي يمكن أن يمتد لمئات الأمثال

وفي حالات أخرى يمكن مسح والتعرف على هوية الأشخاص بدون حتى أي تفاعل مادي بين الشخص المعني بالبيانات والآلة المعروفة للهوية، أو حتى علم الشخص المعني بالبيانات

117 Stan Z .Li and Anil K .Jain ,Handbook of Face Recognition) Springer Science & Business Media, United states ; 1 (2005 Asit Kumar Datta ,Madhura Datta and Pradipta Kumar Banerjee ,Face Detection and Recognition :Theory and Practice) CRC Press ,United States.4 (2015

118 Article 29 Data Protection Working Party' ,opinion 02/2012 on facial recognition in online and mobile services 22) 'March.2 (2012

وقد ظهر هذا في حالة قضية «زيلمر ضد فيس بوك» وهي «دعوى جماعية» رفعتها مجموعة من غير مستخدمي منصة التواصل الجماعي «فيس بوك» لزعيمهم أن الشركة قامت بانتهاك خصوصياتهم حين احتفظت بقوالب لوجوهم انتجتها باستخدام تقنيات الذكاء الصناعي لديها المفعلة ذاتيا أثناء مسح الشركة للصور التي يرفعها مستخدمي المنصة بالميزة المعروفة باسم «tagging»^{١١٩}.

وقد تداولت هذه الدعوى في أرجاء المحاكم الأمريكية منذ عام ٢٠١٥ وانتهت بأضخم تسوية في تاريخ القضاء الأمريكي فيما يتعلق بقضايا مخالفات الخصوصية حيث وافقت شركة فيس بوك على دفع ما يقرب من تسعة وسبعون مليون دولار أمريكي ونصف المليون كأجمالي نهائي للتسوية تقسم على المدعين بحيث يحصل كل مدعى على ثلاثمائة وخمسة وأربعون دولار، وهو على حسب الحكم النهائي بالموافقة على التسوية أقل من المقدار المفروض حال السريان في الدعوى وفرض غرامات جنائية على شركة فيس بوك لمخالفتها قانون ولاية إلينوى الأمريكية لخصوصية البيانات البيومترية لعام ٢٠٠٨ والتي تتراوح بين ألف دولار وخمسة آلاف دولار لكل مخالفة^{١٢٠}.

ثانيا: الانتهاكات الواقعة على البيانات الشخصية أثناء وتناج تطوير تلك البرمجيات:

١/ المخاطر الناجمة من اعتماد تقنيات كتل البيانات الضخمة

يعتمد مطوري تلك البرامج على تقنيات متعددة تستخدم ما يعرف بكتل البيانات الضخمة^{١٢١} لتغذية وتطوير برمجياتهم، وتعتمد هذه التقنيات على مطابقة ومعالجة كمية ضخمة من الصور للتعرف على أنماط للوجه يتم تخزينها واستخدامها لاحقا لتحديد الهوية، وهذا يتعارض مع عدد كبير من الضوابط القانونية للمعالجة المشروعة للبيانات الشخصية، مثل الموافقة المسبقة للمعنى بالبيانات الشخصية،

119 Kristin L. Bryan and David J. Oberly, 'Recent BIPA Opinion May Have Significant Implications on The Scope of Section 15 b (Claims Moving Forward)' The National Law Review 13, September (2022) <https://www.natlawreview.com/article/recent-bipa-opinion-may-have-significant-implications-scope-section15-b-claims> accessed 13 September, 2022

120 RE FACEBOOK BIOMETRIC INFORMATION PRIVACY LITIGATION Case No-15 .cv-03747-JD)United States District Court ,Northern District of California 26 ,February (2021 https://www.govinfo.gov/content/pkg/USCOURTS-cand-15_3-cv-03747-pdf/USCOURTS-cand-15_3-cv-03747-16-pdf.pdf.

١٢١ «البيانات الضخمة هي وسيلة لتخزين ومعالجة كمية ضخمة من البيانات، لإكتشاف أنماط ومعلومات مخفية، قد لا تظهر بطرق المعالجة العادية والمفردة للبيانات، بما يرفع قيمة هذه البيانات، وينتج عنه اتخاذ قرارات أفضل» أنظر Tzanou Maria, Health Research Routledge, Responses Regulatory and Challenges Data Big :GDPR the under Privacy Data (٢٠٢٠ states united ,Routledge) Technologies Emerging of Law the in preface ١.

٢/ قضية شركة كلير فيو الأمريكية

وقد ظهر البعد الحقيقي للمخاطر التي تمثلها تلك التقنيات في قضايا عدة كمثلاً قضية "كلير فيو view clear" الأمريكية التي تمتلك برنامجاً للتعرف على الهوية من خلال نمط الوجه، حيث تواردت تقارير تؤكد قيام مؤسس الشركة ومبرمج البرنامج «تون ذات ton that» بحصاد بيانات شخصية مجمعة من على الإنترنت لتدريب برنامج للتعرف على الوجوه خاصته، متجاوزاً جميع قواعد معالجة البيانات الشخصية التي تتعلق بمشروعية المعالجة ومحدوديتها وعلم الأشخاص المعنيين بالبيانات واستخدام البيانات الشخصية لأغراض الذكاء الصناعي والتربح^{١٢٢}،

وقد رفع المواطن الأمريكي الأمريكي متنيك MUTNICK VS CLEARVIEW AI INC^{١٢٣} ضد الشركة^{١٢٤}، دعوى جماعية تتعلق بهذا، والتي تم رفضها فقط لعدم وجود نص قانوني يجرم ممارسات تلك الشركة، ولكن رغم هذا فقد فسخت شركة «كلير فيو» كل تعاقداتها عدا هذه الموقعة مع قوات الأمن العام، والتي فسختها أيضاً داخل ولاية إلينوي لوجود قانون إلينوي لحماية البيانات البيومترية^{١٢٥}.

وهذا يؤكد ضرورة تناول هذا الموضوع بشكل تشريعي يحده ويحافظ على التوازن اللازم بين اعتبارات الأمن سواء العام أو الخاص، وبين الحق في البيانات الشخصية

122 Alexander L. Vuving, Hindsight, Insight, Foresight: Thinking About Security in the Indo-Pacific (Asia-Pacific Center for Security Studies, United States), 52 (2020) Martin Ford, Rule of the Robots: How Artificial Intelligence Will Transform Everything (Hachette UK, United Kingdom), 54 (2021) Ronald J. Deibert, Reset: Reclaiming the Internet for Civil Society (September Publishing, United Kingdom) (2020), 52.

123 Mutnick v Clearview AI, Inc Case No 20 .C.0512

124 Mutnick v Clearview AI, Inc et al No1:2020 .cv00512, Document) 86 N.D. Ill. (2020 . urt Description: MEMORANDUM Opinion and Order: The Court denies defendants' Rule 12(b)(2) and § 1404(a) motions [29, 45]. Signed by the Honorable Sharon Johnson Coleman on 8/12/2020. Mailed notice. (ym,)

125 Henry H. Perritt, Digital Communications Law) revised 2020 edn, Wolters Kluwer, United States; 13-170 (2010) ibid. 48

المبحث الثاني إشكاليات استخدام البيانات الشخصية لأغراض أنظمة التأمين المنزلي لأغراض الأمن العام

كما سبق أن أسلفنا فإن أنظمة تأمين المنازل تولد كمية من البيانات الشخصية تعتبر كنزاً لجهات الأمن العام فهي تسهل لها مهماتها من حيث مراقبة الممتلكات وحركة السير وتمكنها من تحديد هوية المجرمين، ولكن لاعتبارات كثيرة لا يمكن الاعتماد على تلك التقنيات في توجيه تهم جنائية لمتهمين معينين، ولهذا عملت عدد من الجهات الدولية لتنظيم العلاقة بين المصلحة العامة المتمثلة في اعتبارات تحقيق الأمن العام والحقوق الفردية، وهذا ما سنتناوله هنا في مطلبين

المطلب الأول مخاطر استخدام أنظمة التعرف على الهوية من خلال بيانات الوجه البومترية لأغراض الأمن العام

أولاً: انتقادات دولية ومخاطر على حقوق الأشخاص المعنية بالبيانات

على الرغم من الإمكانيات الهائلة التي توفرها هذه التقنية في مجال الأمن الخاص والعام، إلا أن العديد من الجهات الدولية قد وجهت انتقادات واسعة للتأثير الخطير لـ (تقنيات التعرف المؤتمت على الهوية من خلال تحليل البيانات البومترية للوجوه) على الحق في البيانات الشخصية، ابتداءً من الخطورة البالغة للاعتماد على مثل هذه التقنيات الحديثة في مجال انفاذ القانون والأمن العام، فقد أشارت «وكالة الاتحاد الأوروبي للحقوق الأساسية» أنه حتى مع نسبة خطأ تبلغ واحد في المائة فهذا يعني تعرض الآلاف للاحتجاز وتوجيه التهم الجنائية عن طريق الخطأ¹²⁶، كما أشار «المجلس الأوروبي للبيانات الشخصية» أن هذه التقنيات لا توفر نتائج موثوق بها، وهذا يرجع لحاجتها لصور متعددة الجوانب للوجه الواحد لزيادة دقة البيانات البومترية الناجمة عنها، وعليه فإنه من الخطر الاعتماد عليها في أعمال خطيرة كالتحقيقات الجنائية وتوجيه التهم الجنائية للأشخاص¹²⁷.

وإزاء هذه التحذيرات جاء قانون الاتحاد الأوروبي للذكاء الاصطناعي مانعاً لطرح نماذج ذكاء اصطناعي في السوق الأوروبي التي تنشئ أو توسع قواعد

126 The EU Fundamental Rights Agency, facial recognition technology: fundamental rights considerations in the context of law enforcement) FRA – European union agency for fundamental rights, Austria 9 (2019

127 The European Data Protection Board*, Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement 27) June.11 (2022

بيانات التعرف على الوجه من خلال الكشط غير المستهدف لصور الوجه من الإنترنت أو لقطات كاميرات المراقبة^{١٢٨}.

ثانياً: حالات تطبيقية

وبالرجوع مرة أخرى لحالة شركة كلير فيو «الرؤية الواضحة clear view» الأمريكية، التي توجر خدماتها بشكل حصري لقطاع الأمن العام، والذي يعتمد على مثل تلك التقنيات لسد حاجاته المتنامية لتحديد الهوية والتعرف على المتهمين، نجدها تقدم أبلغ مثال للمخاطر التي يمكن أن يتعرض لها الأبرياء جراء عدم تنظيم عمل هذه الشركات

ففي حيث تملك الشركة قاعدة بيانات تحتوي على ثلاثة بليون صورة، فإن قاعدة بيانات وكالة الاستخبارات الفيدرالية الأمريكية تحتوي على ستمائة وأربعون مليون صورة فقط، كونها مقيدة بمعايير قانونية أعلى من الشركة الخاصة بموجب قوانين الخصوصية الأمريكية التي تحكم القطاع العام، على عكس الشركات الخاصة كشركة «كلير فيو» الغير خاضعة لقوانين شاملة تنظم أعمالها فيما يتعلق بالخصوصية وحماية البيانات الشخصية^{١٢٩}، وهذا راجع لعدم وجود قوانين تخاطب القطاع الخاص فيما يتعلق بالخصوصية وحماية البيانات الشخصية بأمريكا^{١٣٠}، ولهذا اعتبر الكثيرون استخدام السلطات العامة الأمريكية لمقاولين من القطاع الخاص لتولي أعمال المراقبة وتحليل البيانات الشخصية تحايلاً على القواعد القانونية الحاكمة لها، وهو ما حدث بالضبط في حالة فضيحة برنامج «بريزم الأمريكية» الشهيرة والتي فضحها «سنودن»^{١٣١}.

128 Regulation) EU 2024/1689 (of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence) Artificial Intelligence Act, (art 5. Prohibited AI practices 1. The following AI practices shall be prohibited: a) the placing on the market, the putting into service for this specific purpose, or the use of AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

129 Roland Vogl, Research Handbook on Big Data Law, Research Handbooks in Information Law series) Edward Elgar Publishing, United States. 35 (2021)

130 Roberto J. Rodrigues, Petra Wilson and Stephen J. Schanz, The Regulation of Privacy and Data Protection in the Use of Electronic Health Information: An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases) Pan American Health Organization, Washington, D.C., United States; 38 (2001) Jacqueline Klosek, Data Privacy in the Information Age) Greenwood Publishing Group, Westport /Connecticut /United States; 190 (2000 United States. Congress. House. Committee on Energy and Commerce. Subcommittee on Commerce, Trade, and Consumer Protection, The EU Data Protection Directive: Implications for the U.S. Privacy Debate: Hearing Before the Subcommittee on Commerce, Trade, and Consumer Protection of the Committee on Energy and Commerce, House of Representatives, One Hundred Seventh Congress, First Session, March, 2001, 8 Volume) 4 U.S. Government Printing Office, Washington, D.C. /United States; 4 (2001 Curtis Frye, Privacy-enhanced Business: Adapting to the Online Environment) Greenwood Publishing Group, Westport /Connecticut /United States. 71 (2001)

131 T.C. Sottek and Janus Kopfstein, 'everything you need to know about prism, a cheat sheet for

المطلب الثاني

المخاطر التي يثيرها التعاون بين مشغلي أنظمة المراقبة الذكية للمنازل وبين جهات الأمن العام

أولاً: فضيحة شركة رينج التابعة لآمازون

أثارت مؤخراً فضيحة شركة رينج الأمريكية التابعة لآمازون بعد أن كشفت تلك الشركة في شهر يوليو الماضي عن سياسات تتبعها شركتها التابعة رينج فيما يتعلق بمقاطع الفيديو والبيانات الشخصية المولدة بواسطة أجهزة «جرس الباب الذكي» التي تبيعها، وتضمن هذا الكشف عن مشاركة مستمرة من قبل شركتي «آمازون» و «رينج» لهذه البيانات والمقاطع مع جهات انفاذ القانون المحلية في جميع أنحاء أمريكا^{١٣٢}.

جاء هذا التصريح بعد سلسلة من المخاطبات والتساؤلات بشأن هذا الموضوع^{١٣٣} وجهها السيناتور/ عضو مجلس الشيوخ الأمريكي «ادوارد جي ماركي» السيناتور الديموقراطي لولاية ماساتشوستس الأمريكية لشركة آمازون، حول سياسات شركة «رينج» فيما يخص البيانات الشخصية التي تجمعها أجهزتها والتي تقدر ب عشرة ملايين جهاز حول أمريكا^{١٣٤}.

والذي اقلق العامة في أمريكا حول هذا التصريح أنه أولاً يأتي بدون علم أو موافقة ملاك تلك الأجهزة، فطبقاً لتصريحات شركة «آمازون» فهي تشارك الصور ومقاطع الفيديو مع قوات انفاذ القانون بدون علم أو موافقة عملائها، أو طبقاً لتصريح أو اذن قضائي^{١٣٥}، وأيضاً بالمخالفة لسياساتها المعلنة حول شراكتها مع جهات انفاذ القانون المحلية^{١٣٦}، والذي أعلنت فيه أنها تشارك البيانات الشخصية مع جهات الأمن العام بناء فقط على ما أسمته دواعي الطوارئ والمحافظة على حياة وأمن الأفراد

the nsa's unprecedented surveillance programs) 'The Verge 17, July (2013 <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>.

132 Alfred Ng 'amazon gave ring videos to police without owners 'permission' Politico 13, July (2022 <https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission> 00045513-accessed 11 September.2022

١٣٣ وهذه المخاطبات استمرت من سنة ٢٠١٩ حتى الآن نتيجة للسمعة المسبقة حول شراكة آمازون مع جهات انفاذ القانون المحلية وسيتم تفصيلها لاحقاً

134 Edward J. Markey, a letter to Andrew jassy, united states, June , 2022, p: 1, you can download the letter from, <https://www.markey.senate.gov/download/senator-markey-letter-to-amazon-on-ring-audio-and-law-enforcement>

135 Edward J .Markey 'a letter to Andrew jassy) 'united states ,June 1 (2022 <https://www.markey.senate.gov/download/senator-markey-letter-to-amazon-on-ring-audio-and-law-enforcement>.

136 'Weird' Amazon Handed Ring Data to Police Without Warrants ' <https://www.wired.com/story/amazon-ring-police-videos-security-roundup> /accessed 11 September.2022

د. أحمد عبد العزيز محمد أبو الحسن

وقد أثار هذا التصريح استياء العديد من عملاء الشركة، وخصوصا في ظل الاطارين القانوني والثقافي الأمريكي الذي لا يحبذ على الاطلاق فكرة تدخل جهات انفاذ القانون المحلية في شئون المواطنين وخصوصياتهم بدعوى توفير الخدمات الأمنية

ثانيا: حالة تقديم برامج التعرف على الهوية من خلال مسح بيانات الوجه (أمازون ريكوجنشن)

لم تقتصر شراكة شركة أمازون مع أجهزة الأمن الأمريكية على ما أثير في فضيحة شركة رينج، ولكن للشركة تاريخ قديم في تقديم خدمات التعرف على الوجه التابعة لها "أمازون ريكوجنشن" لهذه الأجهزة، وهي جزء من خدمات الحوسبة السحابية التابعة أيضا لأمازون والمعروفة بـ "خدمات أمازون المقدمة عبر شبكة المعلومات العالمية (AWS amazon web services)"، وهذا البرنامج من المعروف عنه استخدامه لقاعدة واسعة من الصور المخزنة حاسوبيا للتعرف بسرعة ودقة على الوجوه والهويات، وهو يقدم عددا من الخدمات الفرعية تتنوع بين التعرف على العمر والنوع من خلال البحث عن بعض العلامات المميزة في تركيبة الوجه وتدعى "تحديد الوجه DEDECT FACE" و التعرف على الوجه من خلال مطابقته بقاعدة بيانات ضخمة يحتويها البرنامج ترتبط بخدمات أمازون السحابية^{١٣٧} "FACE AND SEARCH FACES" INDEX.

حيث خصصت أمازون جزءا من تلك البيئة الحاسوبية الحوسبية للقطاع الأمني ابتداء من أواخر عام ٢٠١٧، مما أثار حفيظة عدد من المنظمات الحقوقية الأمريكية، وجعلهم يطالبوا «أمازون» بإيقاف هذا التعاون متعللين باستخدام جهات الأمن العام لتلك التقنيات بشكل غير قانوني يهدد مصالح وحقوق الأفراد^{١٣٨}، بما يتنافى مع القيم الدستورية الأمريكية^{١٣٩}، وأيضا ردا على عدد من الدراسات التي أكدت على خطورة الاعتماد على هذه التقنيات الحديثة في أعمال شديدة الخطورة كالتحقيقات الجنائية^{١٤٠}.

واستجابة لتلك الدعوات أوقفت شركة أمازون تعاونها مع قوات الأمن المحلية منذ عام ٢٠٢٠ حتى تاريخه، داعية الحكومات لتقديم قوانين أكثر

137 IBID283

138 Stephen J.A. Ward ,Handbook of Global Media Ethics) Springer Nature ,Switzerland.525 (2021

139 Elizabeth Dwoskin' ,Amazon is selling facial recognition to law enforcement — for a fistful of dollars) 'The Washington Post 22 ,May (2018 <https://www.washingtonpost.com/news/the-switch/wp/2018/05/22/amazon-is-selling-facial-recognition-to-law-enforcement-for-a-fistful-of-dollars/> accessed 13 September.2022

140 Karen Hao' ,The two-year fight to stop Amazon from selling face recognition to the police) 'MIT Technology Review 12 ,June (2020 <https://www.technologyreview.com/2020/06/12/1003482/amazon-stopped-selling-police-face-recognition-fight/> /accessed 13 September.2022

صرامة لاستخدام تلك الجهات لبرامج التعرف على الوجوه وتحديد الهوية بالذكاء الاصطناعي^{١٤١}.

وقد كشفت بعض المنظمات الحقوقية كمنظمة الحقوق الأمريكية الرائدة «مؤسسة الحدود الإلكترونية» في عام ٢٠٢١ أن قسم شرطة ولاية لوس انجلوس بكاليفورنيا أمريكا طلب من خلال برنامج «الضواحي» صور تتعلق بمظاهرات «حياة السود تهم black live matters» المشهورة الموجهة ضد عنف الشرطة تجاه أصحاب البشرة الملونة من الأمريكيين ذوي الأصول الأفريقية^{١٤٢}، مما صعد من حدة الانتقادات الموجهة لهذا النوع الجديد من المراقبة الأمنية، بعد ظهور استخدامها بشكل يقمع الأفراد من ممارسة حقوقهم الدستورية كالحق في التظاهر

ومن ناحية أخرى فقد أظهرت العديد من الدراسات والأبحاث عدم معصومية تلك البرامج من ارتكاب الأخطاء وخصوصا في حالات معينة تتعلق بالتعرف على أصحاب البشرة الملونة كالأمركيين من أصل أفريقي وغيرهم من أصحاب الخلفيات الإثنية، وأيضا النساء والصغار^{١٤٣}، كما نادى «اتحاد الحريات المدنية الأمريكي» بوقف استخدام هذا البرنامج لأغراض الأمن العام بواسطة قوات إنفاذ القانون الأمريكية بناء على هذه الدراسات واستشهد بالذات بدراسة قام بها هذا البرنامج بالتعرف على ٢٨ نائب كونجرس أمريكي على أنهم مجرمين^{١٤٤}.

ولهذا فيري الباحث عدم إمكانية استخدام تلك التقنيات الحديثة وخصوصا في حالتها الراهنة من التطور التقني كأدلة ضد شخص ما، أو في مجال الأمن العام عموما، فتوجيه التهم الجنائية الخاطئة ضد الشخص المعني بالبيانات الشخصية له أثاره وأضراره الخطيرة التي قد لا يمكن التعويض عنها أو تلافي أثارها

141 Amazon 'We are implementing a one-year moratorium on police use of Rekognition 10) 'June(2020 <https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition> accessed 13 September.2022

142 Matthew Guariglia and Dave Maass' ,lapd requested ring footage of Black Lives Matter protests' (Electronic Frontier Foundation ,February (2021 <https://www.eff.org/deeplinks/2021/02/lapd-requested-ring-footage-black-lives-matter-protests> accessed 13 September.2022

143 Rosario Girasa ,Artificial Intelligence as a Disruptive Technology :Economic Transformation and Government Regulation) Springer Nature ,Switzerland.114-115 (2020

144 Danny Caine ,How to Resist Amazon and Why :The Fight for Local Economics ,Data Privacy ,Fair Labor ,Independent Bookstores ,and a People-Powered Future) !Microcosm Publishing ,United states 152 (2022

المطلب الثالث

الجهود الدولية للحد من تدخل الحكومات في أنشطة معالجة البيانات الشخصية لأغراض القطاع الخاص

نتاج لهذه المخاوف المتزايدة^{١٤٥}، قامت العديد من المنظمات الدولية بدعوة الحكومات للحد من تدخلها في أنشطة معالجة البيانات الشخصية التي يجريها القطاع الخاص، ومطالبتها للشركات بتسليم تلك البيانات للجهات الحكومية سواء كانت أمنية أم غير أمنية لتستخدمها لأغراضها الخاصة

أولاً: قرار الجمعية العامة للأمم المتحدة «الحق في الخصوصية في العصر الرقمي» لعام ٢٠١٨

ومن ضمن هذا الجهود المتواصلة التي قامت به الأمم المتحدة بعد فضيحة التجسس الأمريكية المشهورة بـ «بريزم prism» في عام ٢٠١٢، والذي انتهت بإصدار قرار الجمعية العامة للأمم المتحدة «الحق في الخصوصية في العصر الرقمي» لعام ٢٠١٨^{١٤٦}، والذي أوصت فيه الأمم الأعضاء بـ: (احترام واتخاذ التدابير اللازمة لاحترام الحق في الخصوصية وخصوصاً في قطاع الاتصالات الرقمية، وإعادة النظر في إجراءات جمع ومعالجة البيانات الشخصية ومراقبة الاتصالات الرقمية، وإنشاء وتعزيز آليات الرقابة البرلمانية والقضائية والمستقلة وتزويدها بالموارد والقدرات اللازمة لممارسة عملها، وإتاحة تعويض مناسب للمتضررين، سن تشريعات مناسبة ومتخصصة تضمن احترام المبادئ الدولية بهذا المجال، وغيرها من التوصيات)^{١٤٧}.

وأهاب القرار الشركات (المؤسسات التجارية) بالعمل على تنفيذ معايير إطار الأمم المتحدة المعنون «الحماية والاحترام والانتصاف»^{١٤٨}، وأن توفر لمستخدميها قواعد الشفافية والانتصاف اللازمين لحمايتهم وحماية بياناتهم الشخصية ضد

145 Aurelia Tamò-Larrieux, Designing for Privacy and its Legal Framework :Data Protection by Design and Default for the Internet of Things ,Volume 40 of Law ,Governance and Technology Series) Springer, Germany.8 (2018

١٤٦ الأمم المتحدة - الجمعية العامة , قرار الجمعية العامة للأمم المتحدة رقم (١٧٩١٧٣) للعام ٢٠١٨ الحق في الخصوصية في العصر الرقمي, (نيويورك: الأمم المتحدة - الجمعية العامة, الدورة الثالثة والسبعون/ الجلسة العامة ٧٠, ٢١ January ٢٠١٩), وثيقة

رقم RES/A/٧٣/١٧٩, مستخرج من الموقع الرسمي لوثائق الأمم المتحدة: <http://unrtpidage١٨/ly.bit//http> ١٤٧ من التقرير صفحة ٧ من البند السادس يرجى مراجعة: (ن) أن تتظر في وضع التشريعات والتدابير الوقائية ووسائل الانتصاف اللازمة لمعالجة الضرر الناجم عن تجهيز البيانات الشخصية أو استخدامها أو بيعها أو إعادة بيعها لمرة متعددة أو تداولها بشكل آخر بين المؤسسات التجارية دون موافقة صريحة يعطيها الفرد بحرية وعن بيئة من الأمور ، أو في مواصلة تنفيذ تلك التشريعات والتدابير ووسائل الانتصاف؛ ص ٦-٧ بند ٦ خاص بالدول

١٤٨ الأمم المتحدة - الجمعية العامة , تقرير الممثل الخاص للأمين العام المعني بمسألة حقوق الإنسان والشركات عبر الوطنية وغيرها من مؤسسات الأعمال، جون روغي مبادئ توجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون «الحماية والاحترام والانتصاف»، (نيويورك: الأمم المتحدة - الجمعية العامة, الدورة السابعة عشرة/ الجلسة العامة ٧٠, ٢١ March ٢٠١١), مستخرج من الموقع الرسمي لوثائق الأمم المتحدة: unarc١٧٣١/ly.bit//http

حماية البيانات الشخصية من مخاطر الأنظمة الذكية لإدارة وتأمين المنازل

المخاطر التي قد تتعرض لها، وأن تعمل على دمج آليات عمل رقابية وفنية وإدارية تضمن تجهيز البيانات، وأن تحترم الحق في الخصوصية أثناء تصميمها لتكنولوجيات أتمتة اتخاذ القرارات والذكاء الصناعي وتشغيلها وتقييمها والرقابة عليها، ومعالجة انتهاكات حقوق الإنسان التي تكون قد تسببت أو أسهمت فيها^{١٤٩}.

ثانياً: قضية شيرمس ضد فيس بوك أيرلندا

وأيضاً الرأي الذي حكمت به محكمة عدل الاتحاد الأوروبي في قضية المواطن الاستيري شيرمس ضد فيس بوك أيرلندا الخاصة بعدم قانونية نقل البيانات الشخصية الصحية للولايات المتحدة بناء على اتفاقية درع الخصوصية بين الاتحاد الأوروبي والولايات المتحدة، لأسباب تتعلق بالسلطات الممنوحة قانوناً للأجهزة الأمنية الأمريكية^{١٥٠}، وفي هذا الرأي حكمت المحكمة العليا للاتحاد الأوروبي بعدم قانونية أي نقل للبيانات الشخصية خارج حدود الاتحاد الأوروبي إذا كان سيعرض البيانات الشخصية لأي انتهاكات أو استخدامات غير مصرح بها حتى لو كانت للأغراض الأمنية^{١٥١}.

وعليه نرى أن استخدامات البيانات الشخصية المولدة لأغراض القطاع الخاص لأغراض الأمن العام هو أمر تتفاوت القوانين فيه، فمن التجربة الأمريكية التي لا تجرمه إلى التجربة الأوروبية التي تشدد في تجريمه

والحقيقة أن موقف الباحث في هذا الموضوع يقف في المنتصف بين الاتجاهين بالقول بالسماح باستخدام البيانات الشخصية لأغراض الأمن العام، ولكن يجب مراعاة القواعد العامة لمثل هذه الاستخدام مثل محدودية المعالجة واقتصارها على الحفاظ على الأمن العام ومكافحة الجريمة، ووجود سبب فعلى لحيازة البيانات الشخصية المعالجة لأغراض القطاع الخاص

^{١٤٩} مرجع سابق، ص ٧-٨، بند خاص بالشركات

^{١٥٠} European Parliament, 'The CJEU judgment in the Schrems II case' (2020) [https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA\(2020\)652073_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf)

^{١٥١} Dara Hallinan and others, 'International transfers of personal data for health research following Schrems II: a problem in need of a solution' [2021] European Journal of Human Genetics <https://www.nature.com/articles/s41431-021-00893-y#ref-CR3>.

خاتمة

على الرغم من حداثة اللائحة العامة الأوروبية لحماية البيانات وما نجم عنها من قوانين حول العالم، إلا أن التطور التقني لبعض التطبيقات المستحدثة في صناعات الاتصالات وتقنية المعلومات قد ألقى بظلال التقادم على بعض من القواعد الأساسية التي أرسنها تلك القوانين

فالأنظمة الذكية لإدارة وتأمين المنازل والتي تعتمد في تصميمها على بعض من أكثر تلك التقنيات حداثة خير مثال على هذا، فاعتماد تلك الأنظمة على أجهزة تعتمد في تصميمها على انترنت الأشياء والتي تزود بمستشعرات تلتقط كمية ضخمة ومتنوعة من البيانات الشخصية، واستخدامها لتطبيقات الذكاء الصناعي والتي تمكن المتحكمين في البيانات من تعريض الشخص المعنى بالبيانات لأنواع خطيرة من معالجة بياناته كالتمييط والقبولة والتمييز الغير قانوني وأتمتة القرارات وتحديد الهوية والتتبع المستمر، وتتصل أقسامها الداخلية والخارجية ببعضها باستخدام الحوسبة السحابية والتي تمثل شكلا أكثر خطورة من النقل العادي الخطي للبيانات الشخصية، لتزامن عمليات معالجة البيانات داخل نظمها بين أكثر من دولة

وأیضا فإن المفاهيم المستقرة في قوانين وفقه حماية البيانات الشخصية كمن هو الشخص المعنى بالبيانات ومن هو المتحكم وأيضا من هو المعالج قد تواجه بعض الصعوبات، وخصوصا في ظل عدم خطية المعاملة بين هؤلاء حيث إن مستشعرات الأجهزة المكونة لهذه الأنظمة تجمع أي بيانات شخصية تقع في نطاقها مما يطرح مشكلة العابرين وأفراد الأسرة غير المالکین وموقفهم من جمع بياناتهم الشخصية، وأيضا تشارك العديد من المتحكمين في نفس المنظومة لتتووع مقدمي ومشغلي الأجهزة والخدمات التي تكون النظام المنزلي الذكي الواحد

وأخيرا فإن تقنيات التعرف على الهوية من خلال مسح البيانات البيومترية لقلب الوجه والتي يتزايد استخدامها في كاميرات التأمين والمراقبة الفيديوية الحديثة، قد تثير مشاكل تتعلق بطبيعتها الخاصة نتاج لقدراتها الغير مسبقة على تتبع الأشخاص من العابرين بمجالها وغيرهم وتحديد هويتهم بدون معرفة هؤلاء أو تفاعلهم مع هذه الأنظمة وعدم دقتها الكاملة أثناء قيامها بهذا مما قد يسبب أضرارا كبرى للشخص الذي تحدد هويته بشكل خاطئ، وأيضا بسبب حاجة مطوريها ومشغليها لكتل ضخمة من البيانات بشكل مستمر لتطوير أنظمتهم مما قد يدفعهم إلى جمع هذه البيانات بشكل غير مشروع عن طريق المسح والحصاد الغير مشروع لشبكات الحوسبة المتصلة

وأخيرا فإن الرغبة المستمرة لجهات الأمن العام لحيازة والاستعانة بهذه الثروة الرقمية المكونة من البيانات الشخصية المعالجة لأغراض منظومات التأمين الذكية للمنازل والممتلكات الخاصة، قد تؤثر بشكل سلبي على حقوق الأشخاص المعنية بالبيانات إن لم يراعى التوازن بين حاجات الأمن العام والحقوق للصيقة بالشخصية كالحق في البيانات الشخصية

النتائج:

انتهى الباحث لبعض النتائج عن المخاطر التي يمكن أن يسببها استخدام الأنظمة الذكية والمتصلة لإدارة وتأمين المنازل على البيانات الشخصية، وهي كالآتي:

- ١- قد ينجم عن الأنظمة الذكية المتصلة لإدارة وتأمين المنازل مخاطر متنوعة على البيانات الشخصية، وهذا نتيجة لاستخدام تلك الأنظمة لتوليفة متنوعة من التقنيات المستحدثة التي تتيح لها جمع مستمر وغير مسبوق القدرات للبيانات الشخصية.
- ٢- قد تجمع هذه الأنظمة البيانات الشخصية للعابرين في نطاقها، وأيضا قد تتعرض لاختراقها بسهولة نتيجة لعدم احترافية مالكيها، ووجودها في بيئة عادية غير مؤمنة، وتعدد وتنوع مكوناتها مما قد يشكل نقط ضعف في جدار حمايتها ضد الاختراقات الخارجية.
- ٣- قد ينجم عن النقل المستمر وتزامن البيانات الشخصية خارج الحدود الوطنية في ظل أنظمة الحوسبة السحابية تواجد هذه البيانات في دول لا تقدم معايير كافية لحماية تلك البيانات الشخصية.
- ٤- قد ينجم عن معالجة البيانات الشخصية ببرمجيات الذكاء الصناعي مخاطر مستحدثة على الأشخاص المعنية بالبيانات نتيجة لتعرضهم للقبول أو التمييز أو حتى اتخاذ المؤتمت للقرارات وأيضا التعرف على الهوية والتتبع المستمر.
- ٥- قد ينجم عن استخدام تقنيات التعرف على الهوية باستخدام مسح البيانات البيومترية لقالب الوجه مخاطر متنوعة على الأفراد تتبع إما من الطبيعة غير الدقيقة لمثل هذه التقنيات، والتي قد تؤدي لتوجيه التهم الجنائية الخاطئة للأشخاص الأبرياء، أو التتبع المستمر والملاحقة غير المشروعة لهؤلاء من قبل الأشخاص الطبيعية والاعتبارية العامة والخاصة، وأخيرا وجود هويتهم في مخدمات مجهولة بالنسبة إليهم.

يوصي الباحث ببعض التوصيات لتقليل المخاطر الناجمة من استخدام الأنظمة الذكية المتصلة لإدارة وتأمين المنازل، وهي كالآتي:

١- يجب وضع أليات خاصة للإعلام والتبصير وإيفاء الالتزام بالإعلام الواقع على المتحكم في البيانات الشخصية داخل الأنظمة الذكية المتصلة لإدارة وتأمين المنازل، كمثلاً توفير نسخة ورقية أو اليكترونية ثابتة من سياسة الخصوصية يمكن الوصول إليها بسهولة عن طريق التقنيات الحديثة كتقنية مسح الاكواد السريعة QR codes.

٢- في حالة تغيير المتحكم لسياسات الخصوصية الخاصة به يجب اعلام الشخص المعنى بالبيانات فوراً، وفي حالة عدم موافقة هذا الشخص على هذا التغيير لا يجب إيقاف المميزات المعلنة أثناء تسويق الأجهزة المشتراة، بل يمكن فقط إيقاف الميزات الإضافية التي قد تعتمد على تلك التغييرات.

٣- يجب أن يعمل المتحكم في البيانات على إتاحة أنواع معالجة بسيطة وأساسية داخل الرقائق الحاسوبية الداخلية الموجودة مادياً في الأجهزة المكونة للنظام الذكي للبيوت، دون الحاجة المستمرة لنقل تلك البيانات أو تعريضها للمعالجة بواسطة تقنيات الذكاء الصناعي والحوسبة السحابية والتي قد تعرض البيانات الشخصية لمخاطر أكثر جسامة من مجرد معالجتها داخلياً.

٤- يجب أن يعمل موفري تلك الأنظمة وأجهزتها على تحقيق التكاملية بين أجهزتهم في مجال تبني تقنيات التصميم المراعي لقواعد الخصوصية design by privacy وتقييم المخاطر بالنسبة للبيانات الشخصية personal assessment risk data قبل طرح أنظمتهم للمستهلكين (نمذجة وقياسية الأنظمة standardization).

٥- يجب على المتحكمين توفير تقنيات توفر محدودية التشغيل والجمع بحيث تقتصر كمية البيانات الشخصية المجمعة من قبل الأجهزة وخصوصاً البيانات الحساسة والتي تتضمن بيانات بيومترية أو بث فيديو أو صور للعابرين على بيانات مالك الجهاز دون العابرين.

٦- يجب في حالة التقاط بيانات العابرين أن يتم معالجتها بشكل محدود للغاية، وأن يتم تدميرها فور انتهاء الغرض المباشر منها، وعدم استخدامها لأي أغراض أخرى ولو حتى أغراض تطوير برمجيات وأنظمة المتحكم المشغل للأنظمة الذكية.

٧- يجب على المتحكمين في البيانات من موفري تلك الأنظمة، مراعاة جهل المستخدمين وهشاشة تلك الأنظمة لتواجدها المادي في بيئة غير مؤمنة تقنياً (المنازل العادية) وخطورة العمليات التي تجريها تلك الأنظمة على البيانات الشخصية، وعليه يجب عليهم تبني أكثر أنظمة التأمين حداثة كتقنيات "صندوق

البيانات box data “و” الدفاع ضد الآثار المظلمة Dark Against Defense “Artefacts”.

٨- يجب على المتحكمين عدم استغلال كتل البيانات الضخمة التي توفرها لهم مثل تلك الأنظمة لأغراضهم الخاصة، وفي حالة استخدامها لتدريب وتطوير أليات الذكاء الصناعي يجب تجهيل ومسح البيانات المفتاحية المحددة للهوية قبل استخدامها.

٩- يوصي الباحث بعدم الاعتماد على التقنيات الأكثر حداثة في مجال التعرف على هويات الأشخاص كالتعرف على الهوية من خلال مسح البيانات البيومترية لقلالب الوجه في الأعمال الأكثر خطورة كتوجيه التهم الجنائية أو أعمال الأمن العام والبحث الجنائي بشكل عام، وهذا لعدم دقة تلك التقنيات بشكل كافٍ متناسب مع الآثار والأضرار الخطيرة التي قد تنجم عن الخطأ في مثل هذه الحالات.

١٠- يوصي الباحث بمراعاة التوازن بين الحق في البيانات الشخصية واستخدامات البيانات الشخصية لأغراض الأمن العام حال رغبة القائمين عليه باستخدام البيانات الشخصية المولدة من تلك الأنظمة لأغراضهم الخاصة.

١١- يوصي الباحث بتنظيم تركيب وتشغيل هذه الأنظمة تشريعياً، وخصوصاً أنظمة مراقبة تأمين للمنازل والممتلكات الخاصة لما تمثله هذه الأنظمة من مخاطر شديدة على الحق في البيانات الشخصية.

المراجع

أولاً: المراجع باللغة العربية

١ / الكتب

- ١- طلال أبو غزالة، العالم المعرفي المتوقد، الأردن: طلال أبو غزالة للترجمة والتوزيع والنشر، ط٢، ٢٠١٩، ص: ٥٥
- ٢- مني الأشقر جبور، محمود جبور، البيانات الشخصية والقوانين العربية- الهم الأمني وحقوق الأفراد، بيروت: المركز العربي للبحوث القانونية والقضائية، مجلس وزراء العدل العرب، جامعة الدول العربية، ٢٠١٨
- ٣- نجلاء أحمد يس، الحوسبة السحابية للمكتبات حلول وتطبيقات، القاهرة: العربي للنشر والتوزيع، ٢٠١٤

٢ / دوريات

- ١- تامر محمد محمد صالح، الإبتزاز الإلكتروني : دراسة تحليلية مقارنة، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، ع١٤، الإسكندرية: جامعة الإسكندرية - كلية الحقوق، ٢٠١٨
- ٢- داليا عبد العزيز، المسؤولية الجنائية عن جريمة الابتزاز الإلكتروني في النظام السعودي دراسة مقارنة، المملكة العربية السعودية: مجلة جيل الأبحاث القانونية المعقدة العدد ٢٥، لبنان، مركز جيل البحث العلمي

٣ / اصدارت رسمية

- ١- الأمم المتحدة - الجمعية العامة، تقرير الممثل الخاص للأمين العام المعني بمسألة حقوق الإنسان والشركات عبر الوطنية وغيرها من مؤسسات الأعمال، جون روغي مبادئ توجيهية بشأن الأعمال التجارية وحقوق الإنسان: تنفيذ إطار الأمم المتحدة المعنون «الحماية والاحترام والانتصاف»، (نيويورك: الأمم المتحدة - الجمعية العامة، الدورة السابعة عشرة/ الجلسة العامة ٧٠، ٢١ March ٢٠١١)، مستخرج من الموقع الرسمي لوثائق الأمم المتحدة: <http://unarc1731/ly.bit/>
- ٢- الأمم المتحدة - الجمعية العامة، قرار الجمعية العامة للأمم المتحدة رقم (١٧٩/٧٣) للعام ٢٠١٨ الحق في الخصوصية في العصر الرقمي، (نيويورك: الأمم المتحدة - الجمعية العامة، الدورة الثالثة والسبعون/ الجلسة العامة ٧٠، ٢١ January ٢٠١٩)، وثيقة رقم RES/A/٧٩/٧٣، مستخرج من الموقع الرسمي لوثائق الأمم المتحدة: <http://unrtpidage18/ly.bit/>

٣- الهيئة الوطنية للأمن السيبراني، الضوابط الأساسية للأمن السيبراني، الإمارات: الهيئة الوطنية للأمن السيبراني، ٢٠١٨

English references

1 /books

1. Ahmed Nabil Belbachir ,Smart Cameras ,London ,Springer Science & Business Media2009 ,
2. Alexander L .Vuving .Hindsight ,Insight ,Foresight :Thinking About Security in the Indo-Pacific .United states ,Asia-Pacific Center for Security Studies2020 ,
3. Alexia Georgiou ,AI :My Story ;The Story AI Tells ;Bias & Privacy ,united states ,Life Betterment Through God ,LLC2020 ,
4. Andreas Bartosch ,Jens-Daniel Braun ,EC Competition and Telecommunica- tions Law , International competition law series vol6 ,the Netherlands :Kluwer Law International B.V2009 ,.
5. Ann Bowling ,Shah Ebrahim ,Handbook of Health Research Methods :Inves- tigation ,Measurement And Analysis ,England :McGraw-Hill Education) UK,(2005
6. Anu Bradford .The Brussels Effect :How the European Union Rules the World. United Kingdom .Oxford University Press2020 ,
7. Asit Kumar Datta ,Madhura Datta ,Pradipta Kumar Banerjee .Face Detection and Recognition :Theory and Practice .United States ,CRC Press2015 ,
8. Barrie Sosinsky .Cloud Computing Bible .United states ,John Wiley & Sons, 2011
9. Christopher Kuner .European Data Privacy Law and Online Business .United Kingdom ,Oxford University Press2003 ,
10. Curtis Frye ,Privacy-enhanced Business :Adapting to the Online Environment, Westport /Connecticut /United States :Greenwood Publishing Group2001 ,
11. Daniel J .Solove ,Paul M .Schwartz ,Consumer Privacy and Data Protection, Aspen Casebook Series3 ,rd edition ,united states :Wolters Kluwer Law& Business2020 ,
12. Deepika pandoi ,Analysis of Implication of Artificial Intelligence on youth ,Vishal Goyal ,Manish Gupta) Computer scientist ,(Aditya Trivedi ,Mohan L .Kolhe, Proceedings of International Conference on Communication and Artificial Intel- ligence :ICCAI ,2020 Volume 192 of Lecture notes in networks and systems, Singapore :Springer Nature2021 ,
13. Eleni Kosta ,Consent in European Data Protection Law ,Nijhoff Studies in Eu- ropean Union Law ,boston /usa :Martinus Nijhoff Publishers2013 ,
14. Els J .Kindt .Privacy and Data Protection Issues of Biometric Applications :A Comparative Legal Analysis ,Volume 12 of Law ,Governance and Technology Series .United states ,Springer Science & Business Media2013 ,
15. Georg Borges ,Christoph Sorge .Law and Technology in a Global Digital Society :Autonomous Systems ,Big Data ,IT Security and Legal Tech .united states ,Springer Nature2022 ,

16. González ,Gloria ,Van Brakel ,Rosamunde ,De Hert ,Paul .Research Handbook on Privacy and Data Protection Law :Values ,Norms and Global Politics ,Research Handbooks in Information Law series .United kingdom .Edward Elgar Publishing2022 ,
17. Henry H .Perritt .Digital Communications Law .Revised .2020 / United states, Wolters Kluwer 2020 ,2010 ,edition
18. Jacqueline Klosek ,Data Privacy in the Information Age ,Westport /Connecticut/ United States :Greenwood Publishing Group2000 ,
19. Jean-Yves Dufour ,Intelligent Video Surveillance Systems ,New Jersey ,United States ,John Wiley & Sons2012 ,
20. Justine Pila ,Paul Torremans ,European Intellectual Property Law ,Oxford: Oxford University Press2019 ,
21. Khaled El Emam ,Lucy Mosquera ,Richard Hoptroff ,Practical Synthetic Data Generation :Balancing Privacy and the Broad Availability of Data ,Newton, Massachusetts ,United States :O'Reilly Media ,Inc2020 ,
22. Kaori Ishii ,Comparative legal study on privacy and personal data protection for robots equipped with artificial intelligence :looking at functional and technological aspects ,AI & SOCIETY ,34 ,Germany :Springer Verlag2019 ,
23. Li Deng ,Yang Liu .Deep Learning in Natural Language Processing .Singapore ,Springer2018 ,
24. Manish Gupta ,Strategic and Practical Approaches for Information Security Governance :Technologies and Applied Solutions :Technologies and Applied Solutions ,Premier reference source ,Pennsylvania ,United States :IGI Global, 2012
25. Maria Tzanou ,Health Data Privacy under the GDPR :Big Data Challenges and Regulatory Responses ,Routledge Research in the Law of Emerging Technologies ,united states :Routledge2020 ,
26. Martin Ford .Rule of the Robots :How Artificial Intelligence Will Transform Everything .United Kingdom ,Hachette UK .2021 ,P ,54 :Ronald J .Deibert. Reset :Reclaiming the Internet for Civil Society .United Kingdom .September Publishing2020 ,
27. Max Bramer ,Artificial Intelligence :.An International Perspective ,LNCS sublibrary :Artificial intelligence ,Volume 5640 of Lecture Notes in Artificial Intelligence :State-Of-The-Art Survey ,united kingdom :Springer Science & Business Media2009 ,
28. Mehdi Rahmani-Andebili ,Operation of Smart Homes ,Power Systems ,united states ,Springer Nature2021 ,
29. Ming Hu .Smart Technologies and Design for Healthy Built Environments. Switzerland ,Springer Nature2020 ,
30. Mor Bakhoun ,Beatriz Conde Gallego ,Mark-Oliver Mackenrodt ,Gintarė Surblytė-Namavičienė ,Personal Data in Competition ,Consumer Protection and Intellectual Property Law :Towards a Holistic Approach , ?MPI Studies on Intellectual Property and Competition Law ,Volume ,28 Germany :Springer2018 ,
31. Nadine Guhr ,Oliver Werth ,Philip Peter Hermann Blacha ,Michael H .Breitner. Privacy concerns in the smart home context .SN Applied Sciences ,springer. 2020
32. Nagender Kumar Suryadevara ,Subhas Chandra Mukhopadhyay ,Smart Homes :Design ,Implementation and Issues Volume 14 of Smart Sensors,

- Measurement and Instrumentation ,united states ,Springer2015 ,
33. Nayan B .Ruparelia .Cloud Computing .United states ,MIT Press2016 ,
34. Nick Vandome ,Smart Homes in easy steps :Master smart technology for your home In Easy Steps ,United Kingdom ,In Easy Steps2018 ,
35. Orla Lynskey ,The Foundations of EU Data Protection Law ,Oxford Studies in European Law ,Oxford :Oxford University Press2015 ,
36. Patrizio Campisi .Security and Privacy in Biometrics .United states ,Springer Science & Business Media2013 ,
37. Paul Voigt ,Axel von dem Bussche ,The EU General Data Protection Regulation) GDPR :(A Practical Guide ,Berlin /Germany :Springer2017 ,
38. Paul Voigt ,Axel von dem Bussche .The EU General Data Protection Regulation) GDPR :(A Practical Guide .Switzerland ,Springer2017 ,
39. Richard Mortier ,Jianxin Zhao ,Jon Crowcroft ,Liang Wang ,Qi Li ,Hamed Haddadi ,Yousef Amar ,Andy Crabtree ,James Colley ,Tom Lodge ,Anthony Brown ,Derek McAuley ,Chris Greenhalgh .Personal Data Management with the Databox :What's Inside the Box .?California 12 ,December2016 ,2016 ACM Workshop on Cloud Assisted Networking
40. Roberto J .Rodrigues ,Petra Wilson ,Stephen J .Schanz ,The Regulation of Privacy and Data Protection in the Use of Electronic Health Information :An International Perspective and Reference Source on Regulatory and Legal Issues Related to Person-identifiable Health Databases ,Washington ,D.C .,United States :Pan American Health Organization2001 ,
41. Roland Vogl .Research Handbook on Big Data Law ,Research Handbooks in Information Law series .United States ,Edward Elgar Publishing2021 ,
42. Rosario Girasa .Artificial Intelligence as a Disruptive Technology :Economic Transformation and Government Regulation .Switzerland ,Springer Nature, 2020
43. Sanjay Goel ,Yuan Hong ,Vagelis Papakonstantinou ,Dariusz Kloza .Smart Grid Security .The United States ,Springer2015 ,
44. Santa Slokenberga ,Olga Tzortzatou ,Jane Reichel ,GDPR and Biobanking: Individual Rights ,Public Interest and Research Regulation Across Europe, Volume 43 of Law ,governance and technology series ,Switzerland :Springer Nature2021 ,
45. Sinjini Mitra ,Mikhail Gofman .Biometrics in a Data Driven World :Trends, Technologies ,and Challenges .The United States ,CRC Press2016 ,
46. Stan Z .Li ,Anil K .Jain .Handbook of Face Recognition .United States, Springer Science & Business Media2005 ,
47. Stephen J.A .Ward .Handbook of Global Media Ethics .Switzerland ,Springer Nature2021 ,
48. Thomas Pasquier ,David Eysers ,Jean Bacon ,Viewpoint Personal Data and the Internet of Things It is time to care about digital provenance ,Communications of the ACM ,(6)62 ,united states :University of Bristol2019 ,
49. Tzanou ,Maria .Personal Data Protection and Legal Developments in the European Union ,Advances in Information Security ,Privacy ,and Ethics .United states ,IGI Global2020 ,
50. Valentina Emilia Balas & ,others .Data Management ,Analytics and Innovation, Switzerland ,Springer Nature2021 ,
51. Valentina Emilia Balas ,Neha Sharma ,Amlan Chakrabarti .Data Management,

- Analytics and Innovation :Proceedings of ICDMAI ,2018 Volume ,1 Volume 808of Advances in Intelligent Systems and Computing .United States ,Springer2018 ,
52. vishal goar .advances in information communication technology and computing :proceedings of Volume 392 of Lecture notes in networks and systems. Singapore ,Springer Nature2021 ,
53. Yang Xu ,Wen Jung Li ,Ka Keung Lee ,Intelligent Wearable Interfaces ,united states ,John Wiley & Sons2008 ,
54. Zhigang Fang ,Energy Science and Applied Technology :Proceedings of the 2nd International Conference on Energy Science and Applied Technology)ESAT ,(2015 United Kingdom ,CRC Press2015 ,

2 /periodical's

- 1- Abdelsalam) Sumi (Helal ,Sumi Helal ,Simanta Mitra ,Johnny Wong ,Carl K .Chang ,Mokhtari Mounir ,Smart Homes and Health Telematics6 :th International Conference ,ICOST 2008 Ames ,IA, USA ,June28 th July ,2008 ,2 Proceedings Information Systems and Applications ,incl .Internet/Web ,and HCI Volume 5120 of Lecture Notes in Computer Science ,united states ,Springer Science & Business Media2008 ,
- 2- Heleen Janssen ,Jatinder Singh .Personal Information Management Systems .Germany ,Internet Policy Review ,Alexander von Humboldt Institute for Internet and Society 11 .April2022
- 3- Kart Pormeister ,Genetic data and the research exemption :is the GDPR going too far ,?Oxford ,England :International Data Privacy Law ,Oxford University Press ,2017 ,Vol ,7 .No2 .
- 4- olumide Babalola .internet of things) iot :(data security and privacy concerns under the general data protection regulation) gdpr.(Australia10 ,th International Conference on Natural Language Processing .December ,2021 ,24 ~ 23 World Academy of Science ,Engineering and Technology.
- 5- Wael S Albayaydh ,Ivan Flechais .Exploring Bystanders 'Privacy Concerns with Smart Homes in Jordan .CHI :٢٢' Proceedings of the ٢٠٢٢ CHI Conference on Human Factors in Computing Systems ,April, ٢٠٢٢ Article No٤٤٦ :

c /case law

- 1- Case C 131/12-Google Spain and Google [2014] OJ C212/4 .
- 2- Case C 210/16-Wirtschaftsakademie Schleswig-Holstein [2018]OJ C268/3 .
- 3- Case C 25/17-Jehovan todistajat [2018] OJ C319/7 .
- 4- Case C - 40/17-Fashion ID
- 5- European parliament ,The CJEU judgment in the Schrems II case ,2020 ,[https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA_652073\(2020\)EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA_652073(2020)EN.pdf)
- 6- JOHN C .COUGHENOUR ,District Judge order on 3/8/2022 on Case No .C20-1298-JCC.
- 7- Mutnick v .Clearview AI ,Inc .et al ,No1:2020 .cv00512-Document) 86 N.D .Ill (2020 .urt Description :MEMORANDUM Opinion and Order :The Court denies defendants 'Rule)12 b (2)(and)1404 §a (motions .[45 ,29] Signed by the Honorable Sharon Johnson Coleman on .8/12/2020 Mailed notice) .ym(,
- 8- Mutnick v .Clearview AI ,Inc .,Case No 20 .C0512
- 9- Wise v .Ring LLC ,W.D .Wash .,No-2:20 .cv8/3/22 ,01298-
- 10- Zellmer v .Facebook ,Inc-3:18) .cv (01880-District Court, N.D .California ,March2018 ,27

d /official releases

- 1- article ٢٩ data protection working party .opinion02/2012 on facial recognition in online and mobile services .Brussels22 , March2012
- 2- Article 29 Working Party ,Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive/95/46 EC) WP) ,(217 Brussel 9 :April ,2014 the European Commission Justice and Consumers(
- 3- European parliament ,The CJEU judgment in the Schrems II case ,2020 ,[https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA_652073\(2020\)EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA_652073(2020)EN.pdf)
- 4- European Data Protection Supervisor .Opinion 9/2016 EDPS

Opinion on Personal Information Management Systems ,towards more user empowerment in managing and processing personal data. Marrakesh ,European Data Protection Supervisor2016 ,

5- European parliament ,The impact of the General Data Protection Regulation) GDPR (on artificial intelligence ,France :Scientific Foresight Unit2020 ,

6- the EU fundamental rights agency .facial recognition technology :fundamental rights considerations in the context of law enforcement .Austria ,fra – European union agency for fundamental rights2019 ,

7- The European Data Protection Board .Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement .Brussel 27 ,June2022

8- The International Association of Privacy Professionals .Personal information management systems :A new era for individual privacy ..?last visited .16/9/2022 :<https://iapp.org/news/a/personal-information-management-systems-a-new-era-for-individual-privacy/>

9- the OECD Council ,Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Trans-border Flows of Personal Data) Paris ,THE OECD PRIVACY FRAMEWORK ,23/9/1980,OECD ,(accessed from oecd website: <http://bit.ly2/t3QPnf>

10- United States .Congress .House .Committee on Energy and Commerce .Subcommittee on Commerce ,Trade ,and Consumer Protection ,The EU Data Protection Directive :Implications for the U.S .Privacy Debate : Hearing Before the Subcommittee on Commerce ,Trade ,and Consumer Protection of the Committee on Energy and Commerce ,House of Representatives ,One Hundred Seventh Congress ,First Session ,March ,2001 ,8 Volume ,4 U.S ,.Washington ,D.C /.United States :Government Printing Office 2001.