Spring 6-2022

حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي ((دراسة تحليلية مقارنة

ريم غريب الشامسي

جامعة الإمارات العربية المتحدة
United Arab Emirates University

رقم أطروحة الماجستير 2022: 56

كلية القانون

قسم القانون الخاص

حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي
(دراسة تحليلية مقارنة)

ريم غريب علي حمدان الشامسي

2022 يونيو

جامعة الإمارات العربية المتحدة

كلية القانون

قسم القانون الخاص

حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي
(دراسة تحليلية مقارنة)

ريم غريب علي حمدان الشامسي

أطروحة مقدمة لاستكمال متطلبات الحصول على درجة الماجستير في القانون الخاص

يونيو 2022

جامعة الإمارات العربية المتحدة أطروحة ماجستير 2022: 56

الغلاف: صورة توضح تسارع ظهور تطبيقات الذكاء الاصطناعي مقترنة بازدياد فرص المساس بخصوصية الأفراد.
(تصوير: ريم غريب علي حمدان الشامسي)

المطبعة: خدمة طباعة الجامعة. جامعة الامارات العربية المتحدة 2022

إقرار أصالة الأطروحة

أنا **ريم غريب علي حمدان الشامسي،** الموقعة أدناه، طالبة دراسات عليا في جامعة الإمارات العربية المتحدة ومقدمة الأطروحة الجامعية بعنوان **"حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي (دراسة تحليلية مقارنة)"**، أقر رسميا بأن هذا هو العمل البحثي الأصلي الذي قمت بإعداده تحت إشراف **الأستاذ الدكتورعلاءالدين عبدالله الخصاونة، أستاذ في كلية القانون** وأقر أيضاً بأن هذه الأطروحة لم تقدم من قبل لنيل درجة علمية مماثلة من أي جامعة أخرى، علماً بأن كل المصادر العلمية التي استعنت بها في هذا البحث قد تم توثيقها والاستشهاد بها بالطريقة المتفق عليها. وأقر أيضاً بعدم وجود أي تعارض محتمل مع مصالح المؤسسة التي أعمل فيها بما يتعلق بإجراء البحث وجمع البيانات والتأليف وعرض نتائج و/أو نشر هذه الأطروحة.

توقيع الطالب: ___Reem_____

التاريخ: _____22/06/2022____

لجنة الإشراف

1) المشرف الرئيسي: أ.د. علاءالدين عبدالله الخصاونة

الدرجة: أستاذ

قسم القانون الخاص

كلية القانون

2) عضو مناقش الداخلي: أ.د. أسامة أحمد بدر

الدرجة: أستاذ

قسم القانون الخاص

كلية القانون

إجازة أطروحة الماجستير

أجيزت أطروحة الماجستير من قبل أعضاء لجنة المناقشة المشار إليهم أدناه:

1) المشرف (رئيس اللجنة): الأستاذ الدكتور / علاء الدين الخصاونه

الدرجة : أستاذ

قسم القانون الخاص

كلية القانون – جامعة الإمارات العربية المتحدة

التوقيع: _____ التاريخ: 19.06.2022

2) عضو داخلي: الأستاذ الدكتور / أسامه بدر

الدرجة : أستاذ

قسم القانون الخاص

كلية القانون – جامعة الإمارات العربية المتحدة

التوقيع: _____ التاريخ: 19.6.2022

3) عضو خارجي: الدكتور / عمرو طه

الدرجة : أستاذ مشارك

جامعة زايد

التوقيع: _____ التاريخ: 19/6/2022

اعتمدت الأطروحة من قِبل:

عميد كلية القانون : الأستاذ الدكتور محمد حسن على محمد

التاريخ: _____2022/06/29_____

التوقيع: __ _____

عميد كلية الدراسات العليا: الأستاذ الدكتورعلى المرزوقي

التاريخ: _____

التوقيع: _____August 31,2022

الملخص

مع بزوغ عصر الثورة الصناعية الرابعة (4IR)، تزامن ذلك مع وجود حقبة جديدة في التطور التقني و التحول الرقمي و التي أصبحت فيها التكنولوجيا جزءاً لا يتجزأ من المجتمعات، مما أدى إلى ازدياد ظهور تطبيقات الذكاء الاصطناعي بشكل كبير و التي دخلت في مجالات كثيرة في حياتنا اليومية، فأصبح الاستغناء عنها ضرباً من الخيال، فنرى استخدامات الطائرات بدون طيار في مجال التجارة الإلكترونية في إيصال السلع و الخدمات، و الروبوتات الجراحية في العمليات الدقيقة، و الاستشارات المهنية و القانونية عن بعد، و الحكومة الذكية في استخدام التطبيقات الحكومية المؤتمتة - من بينها حكومة الإمارات بوضع استراتيجية الحكومة الرقمية لدولة الإمارات 2025 واستراتيجية الإمارات للذكاء الاصطناعي-،حتى وصولها للتعليم التفاعلي في جائحة كورونا.

لكن بالرغم من كل هذه الإيجابيات لتطبيقات الذكاء الاصطناعي إلا أنها قد تمس أحد الحقوق الأساسية للأفراد ألا و هو الحق في الخصوصية أو الحق في الحياة الخاصة، و التي كفلته الشرائع السماوية و دساتير الدول الوضعية بالإجماع احتراماً لقدسيته إذ أنه من الحقوق التي تمس كرامة الفرد و لا يجوز انتهاكها أو الاعتداء عليها، فكان لابد من وضع الأطر القانونية لعدم انتهاك عناصر الخصوصية في تطبيقات الذكاء الاصطناعي.

و ظهرت العديد من التشريعات في هذا الشأن و لعل أشهرها اللائحة الأوروبية العامة لحماية البيانات رقم 679 لسنة 2016، و سارت على النهج ذاته العديد من القوانين كالقانون المصري رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية ومؤخراً صدور المرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، و في هذه الدراسة سنرى مدى كفاية و شمولية هذه الأطر القانونية لتوفير الحماية المرجوة لخصوصية الأفراد، و هل نحن بحاجة لقواعد قانونية جديدة لحماية الخصوصية في ظل تطبيقات الذكاء الاصطناعي في ظل عدم وجود قانون مستقل لحماية الخصوصية وعدم وجود قانون أو قواعد قانونية متعلقة بالذكاء الاصطناعي.

كلمات البحث الرئيسية: الخصوصية الرقمية، البيانات الشخصية، تطبيقات الذكاء الاصطناعي، صاحب البيانات الشخصية، مشغلي تطبيقات الذكاء الاصطناعي، المسؤولية المدنية.

العنوان والملخص باللغة الإنجليزية

Protecting Digital Privacy Under Implementation of Artificial Intelligence Applications (A Comparative Analytical Study)

Abstract

With the rise of the Fourth Industrial Revolution (4IR), a new era in technical development and digital transformation in which technology has become an integral part of societies. This led to a significant increase in the emergence of artificial intelligence applications that have entered many areas in the world became integral part of our daily lives. Living without technology has become delusional and almost impossible. We see the uses of drones in the field of e-commerce in the delivery of goods and services, surgical robots in precise operations, professional and legal advice remotely, and smart government in the use of automated government applications -The UAE government is among the governments who adopted smart technology, the UAE government is developing the UAE digital government strategy 2025 and the UAE strategy for artificial intelligence – the real life result can be seen through the interactive education during the COVID-19 Pandemic.

But despite all these advantages of artificial intelligence applications, it may affect one of the basic rights of individuals, which is the right of personal privacy or the right to a private life. This is guaranteed by heavenly laws and the constitutions of the positive countries unanimously out of respect for its sanctity as it is one of the rights that affects the dignity of the individual. Moreover, it may not be violated or assaulted, so it was necessary to put in place legal frameworks not to violate the elements of privacy in artificial intelligence applications.

Several legislations appeared in this regard, perhaps the most famous of which is the European General Data Protection Regulation No. 679 of 2016, and many laws followed the same approach, such as Egyptian Law No. 151 of 2020 issuing the Personal Data Protection Law and recently the issuance of Federal Decree Law No. 45 of 2021 regarding Protection of personal data. In this study we will see the adequacy and comprehensiveness of these legal frameworks to provide the desired protection for the

privacy of individuals. Additionally, this study will explore the need of new legal rules to protect privacy, especially while dealing the artificial intelligence applications in the absence of an independent law to protect privacy and the absence of a law or legal rules related to artificial intelligence.

Keywords: Digital privacy, Personal data, Artificial intelligence applications, Personal data owner, Artificial intelligence application operators, Civil liability.

شكـــــر وتقدير

بادئ ذي بدء أشكر الله تعالى وأحمده على تيسيره طريق العلم وتوفيقي لنيل ما أصبو إليه في إنجاز هذا البحث العلمي، فله الحمد تبارك و تعالى على هذه النعم.

أود أن أتوجه بالشكر الخالص لأستاذي ومشرفي أ.د.علاءالدين الخصاونة، على عطائه اللامحدود لي في النصح والإرشاد والتوجيه طوال فترة إعداد الأطروحة، فلم يبخل علي بوقته الثمين و علمه الوفير، فأسأل الله أن يجزيه خير الجزاء و يذلل له الصعاب.

و أتقدم بالشكر الجزيل لكل من مد يد العون لي و شجعني و لو بكلمة بشكل مباشر أو غير مباشر من أساتذة الجامعة الأفاضل أو الإداريين فيها.

كما أتقدم بالشكر الوافر للجنة المناقشة الموقرة.

الإهداء

إلى من لا تصفه كلمات العالم أجمع، ملجئي ..... أبي الحبيب

إلى من وضع الله -سبحانه وتعالى -الجنة تحت قدميها .... أمي الغالية

إلى ركائز القوة في حياتي .... عائلتي

إلى كل من أخذ بيدي وساندني ودفعني وامدني بالعزيمة لإكمال مسيرتي العلمية...

إلى كل عاشقٍ للتطوير و النجاح ...

أهديكم ثمرة جهدي المتواضع ...

قائمة المحتويات

الفصل الأول: المقدمة

أولاً: نظرة عامة

أحدثت تطبيقات الذكاء الاصطناعي ثورة ضخمة في الوقت الحالي في مجال تخزين ومعالجة وتبادل المعلومات بسرعة واتقان، ولعبت دوراً مهماً في تعزيز العلوم المختلفة والتجارة والاستخدامات الطبية وجميع مناحي الحياة، بحيث مثلت ثورة صناعية رابعة (Fourth Industrial Revolution) ساهمت ولا زالت تساهم في نمو التجارة والصناعة وغيرها من القطاعات. وتتعدد تطبيقات الذكاء الاصطناعي بصورة كبيرة ومتسارعة وتندرج في مختلف مجالات الحياة المعاصرة، بعد أن أصبح العالم قرية صغيرة في ظل ظهور العولمة، وأضحت الحياة أسهل في جوانب كثيرة ومختلفة، حيث استخدمت هذه التطبيقات الذكية في تنشيط معاملات التجارة الإلكترونية، والحكومة الذكية، بالإضافة إلى المساعدة في عالم الطب عبر التطبيقات الذكية التي تساعد في تشخيص الأمراض و وصف الأدوية وإجراء العمليات الجراحية الدقيقة، وقد ظهر ذلك بشكل جلي خلال الأزمة الصحية الناتجة عن وباء كورونا[1].كما ظهرت أهمية تطبيقات الذكاء الاصطناعي بشكل جلي في تقديم الاستشارات القانونية والمهنية عن بعد، وما شهده العالم من تسارع استخدام تطبيقات الذكاء الاصطناعي في مجال التعليم التفاعلي بسبب جائحة كورونا.

وبالرغم من الإيجابيات الكثيرة لتطبيقات الذكاء الاصطناعي إلا أن استخدامها ما زال بلا شك محفوفاً بالمخاطر ويثير العديد من المشاكل التي تمس الحقوق الأساسية للأفراد ويترتب عليها العديد من الآثار القانونية، فمع ازدياد استخدام تطبيقات الذكاء الاصطناعي في الآونة الأخيرة زادت فرص المساس بخصوصية الأفراد وظهرت صور جديدة لانتهاك خصوصية البيانات المتعلقة بهم والمساس بحقهم في الصورة وغيره من عناصر الحق في الخصوصية. فقد أصبح شائعاً أن استخدام هذه التطبيقات للوصول إلى السلع والخدمات المقدمة مشروط بتقديم المستخدم معلومات شخصية عن نفسه، بحيث لن يستطيع الدخول إلى هذا التطبيقات واستخدامها بدون تقديم هذه البيانات، والمستخدم حين يعلن عن موافقته على بنود ما يسمى بسياسة الخصوصية لهذه المواقع أو التطبيقات فغالباً ما يتم ذلك دون قراءة شروط هذه السياسات. كما قد تتضمن أحد بنود هذه السياسات إمكانية استخدام البيانات الشخصية لهذا المستخدم من قبل طرف ثالث سعياً وراء أغراض تجارية وإعلانية معينة قد يكون لها تأثير على حياة المستخدمين. كذلك، فإن العديد من التطبيقات تتضمن الحصول على صور الشخص وخصائصه "البيومترية" (Biométrie) ومشاركتها مع جهات مختلفة مما يمثل مساسا بالحق في الصورة والخصوصية الجسدية، كما سنرى لاحقا، بالإضافة إلى ما تمثله تطبيقات التتبع وبرامج الكوكيز (Cookies) من مراقبة لتصفح المستخدم للمواقع الالكترونية وتكوين ملف عن اهتماماته ورغباته دون إذنه. كذلك، يجب الإشارة إلى تطبيقات تحديد الموقع الجغرافي (Géolocalisation) التي تسمح بتحديد موقع المستخدم في أي لحظة. وبالرغم من أن الحق في الخصوصية من الحقوق المكفولة بنص في

1 تطورات الذكاء الاصطناعي ومقتضيات حماية الحقوق والحريات الأساسية، تقرير عن منظمة الايسيسكو (منظمة العالم الإسلامي للتربية والعلوم والثقافة)، تحت إشراف الأستاذ محمد الهادي السهيلي، 2019/12/31، ص10، منشور على:

http://www.icesco.org/wp-content/uploads/2019/12/تطورات-الذكاء-الاصطناعي-مقتضيات-حماية-الحقوق-الحريات-الأساسية.pdf, Access date: 19/06/2022.

الدستور في العديد من الدول، إلا أن هناك قيوداً قد تترتب على هذا الحق مما يجعل منه حقاً مباحاً لمشاركته من قبل أطراف معينة، ويؤدي إلى تعدد صور المساس به.

ولا يخفى على أحد أن العديد من الدول لجأت في السنوات الأخيرة إلى استخدام كاميرات المراقبة الذكية (Vidéosurveillance) التي تقوم بتسجيل الفيديوهات وتحليل كل الصور ومقاطع الفيديو الملتقطة للأفراد، وهذا لا شك أنه يساهم في التخفيف من الجرائم والمخالفات وضبطها، لكنه قد يشكل مساساً بخصوصية الأفراد. كذلك لا بد من الإشارة إلى تأثير استخدام الطائرات الذكية بدون طيار للمراقبة، و التاكسي الطائر[1]، وتطبيقات التنبؤ الشرطي على حق الخصوصية للأشخاص. وقد أثار البعض مسألة تحيز تطبيقات الذكاء الاصطناعي ضد فئات معينة بناء على ما تم تخزينه من معلومات. وفي الوقت الحالي، تستخدم مواقع التواصل الاجتماعي بعض تطبيقات الذكاء الاصطناعي للحد من الممارسات غير السليمة وتقوم بتحليل بيانات مواقع التواصل، كما تقوم بعض الجهات باستخدام تطبيقات الذكاء الاصطناعي التي لها القدرة على التعلم الذاتي والتنبؤ (Algorithmes prédictifs) في مجال التعرف على السلوك، عن طريق تحليل البيانات الضخمة للأفراد للوقوف على التطورات التي تطرأ على أنماط سلوك الإنسان وتفاعلاته، الأمر الذي يُتيح مزيداً من القدرة على مراقبة السلوك البشري الجمعي والفردي، والتنبؤ بتوجهاتها المستقبلية.

ونلاحظ أن كل هذه القدرات لتطبيقات الذكاء الاصطناعي قد تثير أسئلة مهمة حول تأثيرها على الحق في الخصوصية. كما أنه في ظل هذا التقدم في تطبيقات الذكاء الاصطناعي، كان لابد من الاستفادة من هذه التطبيقات في ظل إطار قانوني منضبط يضمن فعالية هذه التطبيقات وحماية الحقوق الأساسية للأفراد. وقد دشنت دولة الإمارات العربية المتحدة وزارة متخصصة للذكاء الاصطناعي وعلوم المستقبل. و في سبتمبر 2017، أطلقت حكومة دولة الإمارات استراتيجية الإمارات للثورة الصناعية الرابعة، ضمن أعمال الاجتماعات السنوية لحكومة دولة الإمارات بهدف تعزيز مكانة دولة الإمارات كمركز عالمي للثورة الصناعية الرابعة. والتي جاء فيها من ضمن أسس المستقبل في القطاعات الحيوية "بيئة متكاملة و آمنة للبيانات" من خلال تأسيس بيئة بيانات ضخمة متكاملة و آمنة إلكترونياً و ربطها بالذكاء الاصطناعي و وضع البروتوكولات الكفيلة بحمايتها على نطاق واسع[2]. كما تم اعتماد الرؤية الخاصة بمشروع الحكومة الإلكترونية تحت شعار: "التحول نحو حكومة على مستوى عالمي قائمة على المعرفة"، ووضعت إستراتيجية للذكاء الاصطناعي تجسد رغبة دولة الإمارات العربية المتحدة على الاستفادة من تطبيقات الذكاء الاصطناعي في كافة المؤسسات والإدارات تحقيقا المصلحة العامة، ومؤخرا صدور المرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، والقانون الاتحادي رقم 44 بشأن إنشاء مكتب الإمارات للبيانات، وكذلك القانون الاتحادي رقم 15 لسنة 2020 بشأن حماية المستهلك، بما في ذلك خصوصية وأمن بيانات المستهلك، بحيث يمنع استخدامها لأغراض الترويج والتسويق. وعلى المستوى الدولي، بالإضافة إلى وضع مبادئ لأخلاقيات الذكاء الاصطناعي فأحد المبادئ المهمة التي ارستها اليونسكو في التوصية الخاصة بأخلاقيات الذكاء الاصطناعي في دورته

1 للمزيد انظر. شويكي، شوق حسين و محمود إبراهيم، فياض (2019). المسؤولية المدنية عن حوادث التاكسي الطائر في دبي: دراسة استشرافية. مجلة جامعة الشارقة للعلوم القانونية. *17*(2)، ص297-338.

2 https://u.ae/ar-ae/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/the-uae-strategy-for-the-fourth-industrial-revolution , Access date:06/06/2022.

الحادية و الأربعين بنوفمبر/2021م، مبدأ الحق في الخصوصية و حماية البيانات و الذي ينص على وجوب احترام الخصوصية و صونها طوال دورة حياة نُظم الذكاء الاصطناعي، بالإضافة إلى وضع أطر ملائمة لحماية البيانات و أية آليات مرتبطة بها سواء كان ذلك على الصعيد الوطني أو الدولي[1]، كما صدرت العديد من المواثيق الدولية والتوجيهات الأوروبية لضمان حماية الخصوصية المعلوماتية، من أهمها: اللائحة العامة لحماية البيانات رقم 679 لسنة 2016 والتي صدرت عن الاتحاد الأوروبي عام 2016 وبدأت بالنفاذ عام 2018[2]، بالإضافة للتشريعات الأخرى في هذا المجال، وهو ما سنبحثه في إطار تحليلي مقارن في هذه الدراسة.

ثانياً: أهمية الموضوع

تتمثل أهمية موضوع حماية الخصوصية في ظل تطبيقات الذكاء الاصطناعي من ناحيتين: فمن الناحية النظرية (العلمية) تتمثل أهمية حماية الخصوصية في ظل تطبيقات الذكاء الاصطناعي في تعزيز وعي كل فرد بحقه في حماية خصوصيته من أي انتهاكات من قبل أطراف ثالثة قد تستخدمها أو تعالجها أو تجري عليها دراسات دون موافقة صاحب الحق فيها. بالإضافة إلى ما يمثله هذا الموضوع من مسائل جديدة وإشكاليات قانونية حيوية بحاجة للإجابة. أما من الناحية التطبيقية (العملية) فتتمثل في التطور السريع وازدياد ظهور تطبيقات للذكاء الاصطناعي في الوقت الحالي مما يؤدي إلى ازدياد حالات انتهاك خصوصية الأفراد، مما يوجب وضع تشريعات قانونية لمجابهة صور انتهاك هذا الحق، وتبرز هذه الأهمية في ظل عدم وجود قانون للذكاء الاصطناعي حتى هذه اللحظة في دولة الإمارات.

ثالثاً: أسباب الدراسة

- مواكبة التشريعات الإماراتية التي صدرت مؤخراً فيما يخص حماية البيانات الشخصية.
- زيادة الاعتداءات على عناصر الخصوصية الرقمية.
- قلة القضايا المعروضة في الموضوع.
- ظهور أشكال جديدة لتطبيقات الذكاء الاصطناعي.

رابعاً: أهداف الدراسة

- تهدف هذه الدراسة إلى التعرف على:

1 UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, Retrieved November,2021 from https://unesdoc.unesco.org/ark:/48223/pf0000380455 , Access date: 23/05/2022.

2 Regulation (EU) 2016/679 of the European Parlimant and of the council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, https://eur-lex.europa.eu/legalcontent/EN/TXT/

- مفهوم الحق في الخصوصية الرقمية وتحديد طبيعة هذا الحق وبيان النظريات التي تساهم في تحديد نطاق الخصوصية.
- التعرف على القيود التي ترد على الحق في الخصوصية.
- التعرف على المخاطر التي يثيرها الذكاء الاصطناعي في مجال الخصوصية وكيفية مواجهتها تشريعياً.
- تحديد كيفية حماية الحق في الخصوصية في ظل تطبيقات الذكاء الاصطناعي من خلال الضمانات القانونية في القانون الإماراتي والمقارن.

خامساً: إشكالية الدراسة

قد تثير تطبيقات الذكاء الاصطناعي مخاطر عدة منها انتهاك خصوصية الفرد من قبل الجهة المخول لها الاطلاع على هذه البيانات، و بالرغم من صدور المرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية إلا أن موضوع الحماية المقررة للحق في الخصوصية مازال بحاجة إلى مزيد من الدقة ذلك أن هذا القانون يتضمن العديد من الثغرات التي قد تحول دون توفير الحماية الفعالة للحق في الخصوصية المعلوماتية، وينتج عن هذه المشكلة الرئيسية عدة تساؤلات، هي:

ما المقصود بالحق في الخصوصية المعلوماتية، وما هي مظاهره في ظل تطبيقات الذكاء الاصطناعي؟ ما مدى كفاية القواعد القانونية التقليدية العامة المتعلقة بحق الفرد في حماية خصوصيته في ظل تطبيقات الذكاء الاصطناعي والتي توجد في عدة قوانين متفرقة؟ وهل نحن بحاجة لقواعد جديدة لحماية الخصوصية في ظل تطبيقات الذكاء الاصطناعي في ظل عدم وجود قانون مستقل لحماية الخصوصية وعدم وجود قانون أو قواعد قانونية متعلقة بالذكاء الاصطناعي؟.

سادساً: المنهج المتبع

اتبعت الباحثة في هذه الرسالة المنهج الوصفي التحليلي، حيث سيتم وصف المشكلة وبيان مفهوم الحق في الخصوصية المعلوماتية ومخاطر الذكاء الاصطناعي على عناصر الحق في الخصوصية وكيفية وضع حلول تقنية وتشريعية لها، كما سيتم تحليل القواعد القانونية الخاصة بالحق في الخصوصية وكيفية حماية هذا الحق، لإعطاء وصف وتحليل موضوع البحث من مختلف جوانبه وكافة أبعاده، إبراز التطورات العامة للحق في الخصوصية في ظل تطبيقات الذكاء الاصطناعي. وتعتمد هذه الدراسة على المنهج المقارن أيضاً من خلال مقارنة القواعد القانونية الخاصة بحماية الخصوصية في القانون الإماراتي والقوانين المقارنة ودراسة الأحكام القضائية الصادرة واستعراض موقف الفقه المقارن في هذا المجال. وقد تم التركيز على ثلاثة قوانين في هذا المجال وهي اللائحة العامة لحماية البيانات باعتبارها الإطار العام لحماية البيانات الشخصية على المستوى الدولي، والقانون الإماراتي وكذلك القانون المصري، وقد يتم الإشارة إلى بعض التشريعات الأخرى إن اقتضت الحاجة. و من أجل ذلك فقد تم تقسيم الدراسة إلى فصلين رئيسين:

- الفصل الثاني: ماهية الحق في الخصوصية المعلوماتية في ظل تطبيقات الذكاء الاصطناعي
- الفصل الثالث: مضمون الحماية القانونية للحق في الخصوصية المعلوماتية في تطبيقات الذكاء الاصطناعي.

الفصل الثاني: ماهية الخصوصية المعلوماتية في ظل تطبيقات الذكاء الاصطناعي

تمهيد و تقسيم

لقد فرض موضوع الخصوصية والبيانات الشخصية نفسه في ظل انتشار وسائل التواصل الاجتماعي والعالم الافتراضي المعزز بسبب التفاعل بين وسائل الإعلام ووسائل الاتصال والتقنيات الالكترونية، وقد زاد ذلك مع ظهور تطبيقات الذكاء الاصطناعي التي بدأت تمس كل جوانب الحياة في الوقت الحالي. ونشير هنا إلى أن الحق في الخصوصية يعتبر أحد أهم الحقوق التي يتمتع بها الإنسان في الوقت الحالي، ولا يخفى على أحد ما تمثله الخصوصية وحرمة الحياة الخاصة من أهمية كبيرة وحاجة ماسة لكل شخص يعيش في المجتمع وخصوصاً في ظل العولمة وانتشار وسائل التواصل الاجتماعي وتطبيقات الذكاء الاصطناعي والتطور العلمي والتكنولوجي الذي أفرز صوراً جديدة للمساس بالحق في الخصوصية لم تكن شائعة من قبل كان آخرها الحديث عن تقنيات الميتافيرس، حيث بدأ موضوع خصوصية البيانات يجسد موضوعاً مهماً ويشغل بال المشرعين ومستخدمي تطبيقات الذكاء الاصطناعي في السنوات الأخيرة، وتزايدت المطالبات بمزيد من الشفافية في عملية جمع البيانات وتخزينها واستخدامها ونقلها للغير وإعطاء المستخدمين السيطرة عليها. وقد أصبحت هذه التطبيقات تمثل خطراً كبيراً على خصوصية الأفراد وسرية بياناتهم الشخصية وحقهم في الصورة أكثر من أي وقت مضى، فمع تزايد استخدام هذه التطبيقات وسهولة حفظ البيانات بكميات هائلة وسرعة نقلها وتداولها، بدأت المخاوف حول البيانات الشخصية تتزايد خصوصاً مع بروز القيمة التجارية للبيانات الشخصية في ظل تطور التجارة الالكترونية، مما أثار التساؤلات حول تأثير هذه التطبيقات على الحق في الخصوصية. وهذا ما دفع الدول والهيئات الدولية ومواقع التواصل الاجتماعي نفسها إلى التنبه لضرورة وضع إطار قانوني ينظم الحق في الخصوصية بجميع صوره وتحديد حقوق الأفراد والتزامات الدولة والمؤسسات والهيئات والأفراد للحيلولة دون المساس بهذا الحق. من أجل ذلك، فقد كرست هذا الحق دساتير الدول وقوانينها، بالإضافة إلى المواثيق الدولية وإعلانات حقوق الإنسان جنبا إلى جنب مع الاهتمام القضائي الوطني والدولي بهذا الحق. فقد اعتنت التشريعات الإماراتية بهذا الحق من جوانبه المختلفة وفي تشريعات متعددة لتأكيد هذا الحق وتكريس صوره المختلفة بدءاً من الدستور الإماراتي في المادة (31) منه التي تتطرق لحماية سرية المراسلات ووسائل الاتصال بجميع أشكالها، والمادة (36) التي تتناول حرمة المساكن وعدم جواز دخولها بأي شكل من الأشكال إلا وفقاً لأحكام القانون، وقوانين العقوبات والمعاملات المدنية والجرائم الإلكترونية والمعاملات الالكترونية وصولاً إلى المرسوم بالقانون الاتحادي الجديد الخاص بحماية البيانات الشخصية لسنة 2021، ويأتي البحث في حماية الخصوصية في ظل الذكاء الاصطناعي لبيان أحكام هذا الحق في التشريع الإماراتي ومقارنته بالتشريعات الوطنية والدولية لضمان تكريس هذا الحق وبيان صور الاعتداء عليه وتحديد أهم الضمانات والوسائل المتاحة للأفراد لمنع وقوع أي مساس بهذا الحق ومجابهة كل صور الاعتداء وضمان حق الفرد بالحصول على التعويض عما أصابه من أضرار بسبب انتهاك هذا الحق. ونتناول في المبحث الأول مفهوم الحق في الخصوصية المعلوماتية ثم نتطرق لنطاق ومضمون هذا الحق في المبحث الثاني.

المبحث الأول: مفهوم الحق في الخصوصية المعلوماتية

تمهيد و تقسيم

يرتبط الحق في خصوصية المعلومات بالحق في الخصوصية المعلوماتية الرقمية، فالحق في الخصوصية يتضمن ثلاثة مكونات أساسية تتعلق بالجانب المكاني لهذا الحق، كحق المسكن، وجانب آخر يتعلق بذات الشخص، كحرمة حياته الخاصة وكرامته وحرية التنقل، وجانب ثالث يتعلق بحماية معلوماته وسريتها[1]. ولتحديد مفهوم الحق في الخصوصية المعلوماتية لابد لنا إذا من التعريف بهذا الحق في المطلب الأول، ثم تحديد طبيعته القانونية وتمييزه عن غيره من الحقوق في المطلب الثاني.

المطلب الأول: التعريف بالحق في الخصوصية المعلوماتية

ونتطرق في هذا المطلب إلى المقصود بالحق في الخصوصية وطبيعته القانونية، والإطار القانوني له.

الفرع الأول: المقصود بالحق في الخصوصية المعلوماتية

يعتبر وضع تعريف منضبط للحق في الخصوصية بشكل عام مهمة صعبة في ظل عدم وجود تعريف تشريعي واختلاف الإتجاهات الفقهية في تحديده من حيث اختلاف الزاوية التي ينظر فيها إلى هذا الحق، بالإضافة إلى الطبيعة النسبية للحق في الخصوصية واختلافها في الزمان والمكان. أما لغة، فيقصد بالخصوصية حالة الخصوص، والخصوص نقيض العموم، والخاصة خلاف العامة، ويقال خصه الشيء يخصه خصاً وخصوصية، والفتح أفصح وخاصة الشيء ما يختص به دون غيره أي ينمو به، ويقال اختص فلان بالأمر وتخصص له إذا انفرد وخص غيره ببره، ويقال فلان يخص بفلان أي خاص به وله به خصيصة، والخاصة ما تخصه لنفسك.[2]

وفي الاصطلاح، فقد اختلف الفقه والقضاء والقانون المقارن في تحديد المقصود بالحق في الخصوصية، فذهب بعضهم إلى التوسع في المقصود بالحق في الخصوصية، بينما ذهب آخرون إلى تضييق نطاق هذا الحق، وسنتطرق إلى توضيح هذين الاتجاهين.

أولا: التعريف الواسع

يرتبط مفهوم الخصوصية وفقا لهذا الاتجاه بمفهوم الحرية[3]، ولا يقيد أصحاب هذا الاتجاه عناصر الحق في الخصوصية، بل أن صاحب الحق هو من يحدد نطاق خصوصيته، وقد تم تبني هذا الاتجاه في التعريف الذي وضعه معهد القانون الأمريكي، وقد أصبح يتمتع بقيمة هامة في الولايات المتحدة الأمريكية وهو يشير إلى الخصوصية من زاوية المساس بها قائلاً: "كل شخص ينتهك بصورة جدية وبدون وجه حق،حق شخص آخر في أن تصل أُمُوره

1 الأهواني، حسام الدين (2000). الحق في احترام الحياة الخاصة، الحق في الخصوصية (ص132). الطبعة الثانية. القاهرة: دار النهضة العربية.

2 أنيس، إبراهيم و آخرون (1972). المعجم الوسيط (ص237-238). الطبعة الثانية (الجزء الأول). مصر : دار المعارف.

3 راجع، بحر، ممدوح خليل (2011). حماية الحياة الخاصة في القانون الجنائي- دراسة مقارنة – (ص213). القاهرة : دار النهضة العربية، و كذلك عرب، يونس (2002م). الخصوصية وحماية البيانات في العصر الرقمي- الجزء الثاني– منشورات اتحاد المصارف العربية-، ص54.

وأحوالِه إلى علم الغير، و تكون صورته عرضة لأنظار الجمهور يعتبر مسؤولا أمام المعتدى عليه"[1]. ونلاحظ أن التعريف الذي وضعه معهد القانون الأمريكي للخصوصية أفرد أحد عناصر الخصوصية فقط (الصورة)، ولم يتطرق لذكر العناصر الأخرى، فقد ذهب إلى أن الخصوصية تنتهك عندما يقوم أحد الأفراد بجعل صورة فرد آخر عرضه لأنظار الجمهور دون علم صاحب الصورة بذلك. كما ذهب مؤتمر رجال القانون المنعقد في استكهولم في مايو سنة 1967 إلى أن الحق في الخصوصية يعني "حق الفرد في ان يعيش حياته بمنأى عن الأفعال الآتية: التدخل في حياة أسرته أو منزله، التدخل في كيانه البدني أو العقلي أو حريته الأخلاقية أو العقلية، الاعتداء على شرفه أو سمعته، وضعه تحت الأضواء الكاذبة، إذاعة وقائع تتصل بحياته الخاصة، استعمال اسمه أو صورته، للتجسس والتلصص، التدخل في المراسلات، سوء استعمال الاتصالات الخاصة المكتوبة أو الشفوية، إفشاء المعلومات التي تصل إليه بحكم الثقة في المهنة"[2]. ونلاحظ أن تعريف الخصوصية الذي تم وضعه من قبل مؤتمر رجال القانون لم يفرد هذه الفكرة في ما يخص الفرد ذاته بل تعدى ذلك إلى أسرته ومنزله، من تدخل بدني أو عقلي أو حريته الأخلاقية أو العقلية، الاعتداء على شرفه أو سمعته بالإضافة إلى إذاعة وقائع تتصل بحياته الخاصة، و استعمال اسمه أو صورته، والتجسس والتلصص، و التدخل في المراسلات، وسوء استعمال الاتصالات الخاصة المكتوبة او الشفوية، وإفشاء المعلومات التي تصل إليه بحكم الثقة في المهنة.

ثانيا: التعريف الضيق

ويرتبط مفهوم الخصوصية وفقا لهذا الاتجاه بحق الشخص بالاحتفاظ بسرية حياته الخاصة، وحقه في أن يعيش وحيداً في عزلة وألفة وسكينة[3]. كما عرفه الفقيه الفرنسي كاربونييه بأنه: "حق الشخص في المجال الخاص لحياته بحيث يستطيع أن يعيش بمنأى عن الآخرين،أي الحق في احترام الخصوصية الطبيعية للفرد، والحق بأن يعيش بهدوء"، كما عرفه الأستاذ كابان بأنه: "حق كل شخص بأن يعيش في سلام وسكينة"[4]. وذهب القاضي COOLEY إلى تعريفه بأنه: "أن يترك الإنسان وشأنه"[5]. وبالرغم مما ذكر سابقاً من تعريف واسع وضيق للحق في الخصوصية، إلا أن فكرة الحق في الخصوصية تتميز بكونها فكرة مرنة، تتغير حسب تغير المجتمع، باختلاف العادات والتقاليد من مجتمع لآخر، لذلك فمن الصعب وضع تعريف دقيق ومحدد وشامل لها، وبالرغم من اتفاق الدساتير[6] والتشريعات الحديثة على أهمية حماية هذا الحق إلا أنه لم يرد تعريف لهذا الحق في الدساتير أو التشريعات الخاصة التى قررت

1 تعريف معهد القانون الأمريكي موجود لدى ساجت، شاكر (2016). الحق في الخصوصية كحق من حقوق الإنسان. بحث مقدم إلى مركز النماء لحقوق الإنسان، جمهورية العراق. ص2.

2 تعريف مؤتمر رجال القانون موجود لدى المقاطع، محمد عبدالمحسن (1992). حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسب الآلي (ص29). الكويت : دار ذات السلاسل للطباعة و النشر.

3 انظر، العبهجي، عصام (2005). حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية (ص58). الإسكندرية: دار الجامعة الجديدة للنشر.

4 مرجع سابق.

5 منشور لدى المقاطع، محمد عبدالمحسن. مرجع سابق. ص19.

6 راجع في ذلك الدساتير العربية الآتية:

الدستور المصري المواد (57، 58)، الدستور اللبناني (م 15)، الدستور الكويتي (م30، 38)، الدستور التونسي (فصل 9 حرمة المساكن و المراسلات)، الدستور الأردني (م 7،10،18).

حماية هذا الحق بما فيها التشريع الإماراتي[1]. فلم يعرف التقنين المدني الفرنسي ولا القانون الفرنسي الخاص بالمعلوماتية والحريات لسنة 1978 المقصود بالحق في الخصوصية أو بالحياة الخاصة، كما لم يعرف هذا الحق في كل من التشريع الإماراتي والمصري.

ونشير أخيراً، إلى وجود اتجاه يميل إلى تعريف الحق في الخصوصية بصورة سلبية، وذلك بالقول إن الحياة الخاصة هي كل ما لا يدخل في نطاق الحياة العامة[2]. ولاتساع نطاق الحياة العامة وصعوبة حصر الحياة الخاصة لجأ هذا الاتجاه لمعيار الزمان وطبيعة الأشخاص وشهرتهم وبعض المظاهر والسلوكيات التي يمارسها الشخص لمحاولة حصر مظاهر الحياة الخاصة،حيث لا تدخل ضمن نطاق حياته الخاصة نشاطه المهني، وممارسة الأنشطة القيادية والسياسية [3]. كما أن المعيار المكاني، يفيد أن كل ما يتم داخل نطاق المسكن يعتبر من قبيل الحياة الخاصة التي لا يجوز المساس بها، وما يدور خارجها من أفعال علنية يعتبر من قبيل الحياة العامة.

مما سبق يتضح لنا تباين آراء الفقه في بيان المقصود بالحق في الخصوصية، وعدم الاتفاق على تعريف جامع مانع لهذا المصطلح، ويرجع ذلك – في رأينا – إلى ما تتسم به فكرة الحق بالخصوصية من المرونة التي قد تتغير بتغير المجتمعات والأزمنة، بل وقد ترجع إلى الظروف الخاصة بكل شخص إذا ما كان شخص عادياً أم مشهوراً، بالإضافة إلى أن مسألة التعريف ليست من مهام المشرع الذي غالباً ما يتركها للفقه و القضاء. ويمكن القول إن للخصوصية جانب آخر معنوي في حياة الشخص، فلكل شخص الحق في حماية الجانب المعنوي الخاص به كسمعته وأفكاره ومشاعره واحاسيسه وآرائه التي يجب ألا تنتهك. فنحن نرى أنه من الصعب وضع تعريف موحد للحق في الخصوصية وذلك بسبب أنه حق يعتمد في تحديده على عادات وظروف كل مجتمع وقيمه وأخلاقه، لذا قد يختلف مفهوم الخصوصية من مجتمع لآخر، فالأفضل إعطاء تعريف مرن وترك تحديد مفهوم الخصوصية لكل مجتمع على حده وفقا لقيمه وأخلاقه وظروفه.

ونتفق مع الرأي القائل بأن الحق في الخصوصية له العديد من المظاهر منها؛ الخصوصية المعلوماتية والخصوصية الجسدية، خصوصية الاتصالات، وأخيراً الخصوصية الإقليمية[4]. ونركز في دراستنا هذه على الحق في الخصوصية المعلوماتية، حيث اختلط مفهوم الخصوصية وارتبط بمفهوم حماية البيانات الشخصية، وأن حماية البيانات الشخصية هي جزء من الحق في الخصوصية والحياة الخاصة. وبخصوص مصطلح الحق في الخصوصية المعلوماتية[5]، فقد عرفها الأستاذ ويستن بأنه: "حق الأفراد و المجموعات و المؤسسات في أن يحددوا لأنفسهم متى و

1 انظر أمين، محمد و إبراهيم، سليمان. (2016). الحماية الجنائية في حرمة الحياة الخاصة في قانون العقوبات الإماراتي. مجلة جامعة الشارقة للعلوم الشرعية و القانونية. 13(1)، ص64.

2 بادنتر، مقالته "الحق في احترام الحياة الخاصة"، الأسبوع القانوني– 1986م- 2136 – رقم 12، مشار إليه لدى الأهواني، حسام الدين. مرجع سابق. ص53.

3 أنظر في عرض هذا الرأي، الأهواني، حسام الدين. مرجع سابق. ص54.

4 بدوي، عمرو طه (2020). التنظيم القانوني لمعالجة البيانات الشخصية – دراسة تطبيقية على معالجة تسجيلات المراقبة الصوتية – (ص28).الطبعة الأولى. مصر : دار النهضة العربية، الإمارات: دار النهضة العلمية، أنظر كذلك، الغافري، د. حسين (2-4 يونيو 2008). الحماية القانونية للخصوصية المعلوماتية في مشروع قانون المعاملات الالكترونية العماني، مؤتمر أمن المعلومات و الخصوصية في ظل قانون الانترنت (ص6). القاهرة.

5 أنظر في هذا المفهوم، كريكط، عائشة (2019). حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات. مجلة الحقيقة للعلوم الاجتماعية والإنسانية. *18* (02)، جوان، ص258.

كيف و إلى أي مدى يمكن للمعلومات الخاصة بهم أن تصل إلى الآخرين"[1]. و يعرفه الأستاذ (ميلر) بأنه: "قدرة الأفراد على التحكم في دورة المعلومات التى تتعلق بهم".[2]

وفي ظل انتشار التقنيات الرقمية وتطبيقات الذكاء الاصطناعي، بدأ الحديث عن الخصوصية المعلوماتية الرقمية[3]، وهي ذات الخصوصية المعلوماتية بمعناها التقليدي، لكن الاختلاف يكمن فقط في الوسائل[4]، حيث أن الخصوصية المعلوماتية الرقمية تكون من خلال الوسائل الحديثة والتطبيقات المتطورة بحيث يستطيع الأفراد والشركات التحكم في معلوماتهم المحتفظ بها من قبل مزودي الخدمة. نستخلص من كل ذلك أن الحق في الخصوصية المعلوماتية غير محدد المعالم وليس من السهل تعريفه وتحديد نطاقه، وهو ما يثير التساؤلات حول جدوى وجود نظام قانوني واحد يقدم حماية فعالة له.

وفي سياق متصل لا بد من تحديد المقصود بالبيانات الشخصية، فقد تم تعريفها بموجب الفقرة الأولى من المادة الرابعة من اللائحة العامة للبيانات الصادرة عن الاتحاد الأوروبي رقم 679 لسنة 2016 بأنها: "أي معلومة تتعلق بشخص طبيعي محدد identified أو قابل للتحديد identifiable". وقد عرفت المادة (2) من القانون الفرنسي رقم 801 لسنة 2004[5]، البيانات الشخصية بأنها: "يعتبر بيانا شخصيا أي معلومة تتعلق بشخص طبيعي محدد هويته أو من الممكن تحديد هويته بأي شكل كان، وبطريقة مباشرة أو غير مباشرة سواء تم تحديد هويته بالرجوع إلى رقمه الشخصي أو بالرجوع إلى أي شيء يخصه". وقد جاء المشرع المصري في الفقرة الأولى من المادة الأولى من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020[6] بتعريف أكثر تفصيلاً، حيث ورد فيها أن البيانات الشخصية هي: "أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية". نلاحظ أن هذه القوانين ركزت على كون البيانات الشخصية تتعلق بشخص طبيعي وليس معنوياً[7]. بالمقابل، فقد كان المشرع المصري أكثر توسعاً في تحديد صور البيانات الشخصية كما يظهر جلياً من التعريف المشار إليه سابقاً.

وفي التشريع الإماراتي، لم يتطرق المشرع لتعريف الحق في الخصوصية في الدستور أو القوانين الأخرى ذات الصلة لاتساع المقصود بهذا المصطلح بالإضافة إلى الأسباب التي تم ذكرها سابقاً. بالمقابل، فقد تطرق لوضع تعريف للبيانات الشخصية وفرق بينها وبين البيانات الشخصية الحساسة والبيانات الشخصية البيومترية في المرسوم بقانون اتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية، فقد عرف الأولى في المادة الأولى بأنها: "أي

---

1 موجود لدى عبدالرحمن، محمود (2020). التطورات الحديثة لمفهوم الحق في الخصوصية المعلوماتية. مجلة كلية القانون الكويتية العالمية. *8*(8)، ص105.

2 انظر، الذهبي، خدوجة (ديسمبر 2017). حق الخصوصية في مواجهة الاعتداءات الإلكترونية – دراسة مقارنة -. مجلة الأستاذ الباحث للدراسات القانونية و السياسية.1(8)، ص143.

3 كريكط، عائشة. مرجع سابق. ص260.

4 عاطف، كريم. الخصوصية الرقمية بين الانتهاك والغياب التشريعي (2013). القاهرة، مصر. مركز دعم تقنية المعلومات. ص2.

5 Loi n 2004-801 du 6 aout 2004 relative a la protection des personnes physique a la regard des traitements des donnes a caractere personel et modifiant la loi n 78-17 du 6 Janvier 1978 relative a linformatique aux fishier et aux liberties, J.o n 182 du 7 aout 2004, www.legifrance.gouv.fr

6 الجريدة الرسمية ، العدد 28 مكرر (ه) في 2020/7/15.

7 التهامي، سامح (2020). ضوابط معالجة البيانات الشخصية - دراسة مقارنة بين القانون الفرنسي والكويتي -. بحث منشور في مجلة كلية القانون الكويتية العالمية. السنة 8. العدد 8. ص401.

بيانات تتعلق بشخص طبيعي محدد، أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر من خلال الربط بين البيانات، من خلال استخدام عناصر التعريف كاسمه، أو صوته، أو صورته، أو رقمه التعريفي، أو المعرف الإلكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية، أو الاقتصادية، أو الثقافية، أو الاجتماعية، و تشمل البيانات الحساسة و البيانات الحيوية البيومترية"[1]. ويتضح لنا من المادة السابقة أن المشرع عرف البيانات الشخصية تعريفاً واسعاً و أكثر شمولية من خلال عبارة "ي بيانات تتعلق بشخص طبيعي محدد،أو تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر"، فقد أورد البيانات الشخصية على سبيل المثال و ليس الحصر فكل معلومة تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه تعتبر بيانات شخصية يشملها القانون بالحماية، بالإضافة إلى جعله البيانات الحساسة و البيومترية جزءاً من البيانات الشخصية، و بمفهوم المخالفة إذا كانت البيانات لا تتعلق بشخص محدد أو لا توجد إمكانية لتحديده بشكل مباشر أو غير مباشر لا يمكن اعتبارها بيانات شخصية، فالمشرع وضع ضابطاً لاعتبار البيانات شخصية من غيرها. و بالرغم من ذلك فقد اقتصر تعريف المشرع للبيانات الشخصية على الشخص الطبيعي دون الاعتباري، فقد جعل الشخص الاعتباري يخرج من نطاق تطبيق المرسوم بقانون اتحادي فيما يتعلق بالبيانات الشخصية التي تكون محمية بقوانين أخرى فقد عرف المشرع الإماراتي صاحب البيانات في المادة الأولى من المرسوم بأنه: "الشخص الطبيعي موضوع البيانات الشخصية"، والحكمة من ذلك، هي أنه لا يتصور تطبيق البيانات الشخصية أو البيانات الشخصية الحساسة أو البيانات الشخصية البيومترية على الشخص الاعتباري، لأنها تتصل بذات الشخص و تعبر عن مكنوناته و تمس ذاته و كيانه، بذلك يمكن أن نصل إلى نتيجة مهمة وهي أن المشرع الإماراتي احترم حق البيانات الشخصية كحق من الحقوق اللصيقة بالشخصية والتي لها قدسيتها واحترامها وبالتالي عدم جواز انتهاكها. كما يستخلص من هذا النص أنه يعتبر بيانات شخصية (IP) أو المعرف الرقمي لكل جهاز الكتروني مرتبط بشبكة الانترنت[2]، كذلك يدخل في مفهوم البيانات الشخصية عنوان البريد الالكتروني وأرقام البطاقات البنكية وحساباته الشخصية على مواقع التواصل الاجتماعي.

أما البيانات الحساسة بحسب قانون حماية البيانات الشخصية المصري، فهي تلك المتصلة بالمعلومات العرقية أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو الطائفية أو غير ذلك من المعتقدات، والصحة، والحياة الجنسية، والإدانة الجنائية، والقياسات الحيوية وعلم الوراثة. وقد نصت المادة الرابعة من اللائحة الأوروبية العامة لحماية البيانات صراحة على نوعين من هذه البيانات وهما البيانات الجينية والبيانات البيومترية، وأعطتهما مستوى حماية عال يفوق ذلك المخصص للبيانات الشخصية العادية. بالإضافة لذلك، فقد جعل المشرع الاماراتي البيانات الحساسة والبيانات الحيوية البيومترية جزءاً من البيانات الشخصية بالرغم من إفراده تعريفاً خاصاً بكل من البيانات الحساسة و البيانات البيومترية في المادة ذاتها، لكن جعل الاختلاف في وصف البيانات الحساسة بأنها البيانات التي تكشف عن الأمور الحساسة التي تتصل بالشخص الطبيعي، كالبيانات التي تكشف عن عائلة الشخص أو أصله العرقي أو سجل سوابقه

1 عرف المشرع الإماراتي البيانات و المعلومات الشخصية في المادة الأولى من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية المنشور في الجريدة الرسمية العدد سبعمائة و اثنا عشر (ملحق)، السنة الواحدة و الخمسون الموافق 26/09/2021م، بأنها: "المعلومات أو البيانات الخاصة بالأشخاص الطبيعيين متى كانت مرتبطة بحياتهم الخاصة أو تحدد هويتهم أو يمكن من خلال ربط هذه المعلومات و البيانات بطريقة مباشرة أو غير مباشرة تحديد و معرفة هوية الشخص".

2 أو العنوان البروتوكولي للشبكة المعلوماتية و الذي عرفه المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية بأنه: "معرف رقمي يتم تعيينه لكل وسيلة تقنية معلومات مشاركة في شبكة معلومات، و يتم استخدامه لأغراض الاتصال".

الجنائية أو آرائه السياسية أو الفلسفية أو معتقداته الدينية، و غيرها من البيانات التي تكشف عن الأمور الحساسة للشخص، أما فيما يتعلق بالبيانات الحيوية البيومترية فهي ما يتصل بالخصائص الجسدية أو الفيسيولوجية أو السلوكية للشخص،وحسناً فعل المشرع الإماراتي عندما أفرد نصوصاً خاصة بالأنواع المختلفة للبيانات[1] سواء البيانات الشخصية بشكل عام و البيانات الشخصية الحساسة و البيانات الحيوية البيومترية لكنه أغفل تعريف البيانات و المعلومات الشخصية المصرفية و الائتمانية التي لديها تشريع ينظم حمايتها حتى و إن كانت تخرج عن نطاق هذا القانون و التي قد تخضع للعديد من التساؤلات من القانونيين دون تعريف خاص بها أو ضوابط، فقد استثنى المشرع الإماراتي أيضاً البيانات الشخصية الصحية التي لديها تشريع ينظم حمايتها لكنه أورد ذكرها في تعريف البيانات الشخصية الحساسة.

أما عن مصطلح تطبيقات الذكاء الاصطناعي الذي يعتبر أحد محددات دراستنا، فلا بد من الإشارة إلى أن تطبيقات الذكاء الاصطناعي تعتبر تقنية مهمة تستخدم التكنولوجيا لاتخاذ أي تخطيط وقرار استراتيجي، وتساعد في تحليل البيانات والمعلومات لمساعدة رجال الأعمال في اتخاذ قرار عمل فعال. يتألف الذكاء الاصطناعي من استخدامات الأدوات والأساليب المختلفة التي تمكن وتنظم في جمع البيانات والمعلومات ذات الصلة من المصادر المختلفة. وحاليا، يتم استخدام إنترنت الأشياء (ITO)[2]، على نطاق واسع في عملية الذكاء الاصطناعي لاتخاذ قرار استراتيجي والتخطيط الفعال. يتيح إنترنت الأشياء للموظفين الاتصال بأجهزة متعددة تعمل على نفس الشبكة، ويوفر استخدام أجهزة إنترنت الأشياء في قطاع الأعمال ميزة كبيرة في إدارة وتخطيط الأعمال. بالنظر إلى مزايا إنترنت الأشياء، فقد لوحظ أن تطبيقاته تعتبر فعالة للغاية في تقدير وتقييم المبيعات وفهم استراتيجية السوق عبر استخدام البيانات والمعلومات لمساعدة الموظفين في الحصول على البيانات لعمل أي خطة أو استراتيجية عمل. وتُستخدم البيانات الضخمة والحوسبة السحابية على نطاق واسع في تطبيقات الذكاء الاصطناعي وقد أحدثت تأثيرًا كبيرًا على تحسين الأداء.

ويعرف الذكاء الاصطناعي بأنه: "علم وهندسة صنع الآلات الذكية، وخاصة برامج الحاسوب الذكية وإنه مرتبط بالمهام المماثلة لاستخدام أجهزة الحاسوب لفهم الذكاء البشري والتفاعل مع البيئة المحيطة ومعطياتها مثل البشر.[3]

حيث يمكننا من ناحية أن نتعلم شيئًا ما حول كيفية جعل الآلات تحل المشكلات من خلال مراقبة الأشخاص الآخرين أو من خلال مراقبة أساليبنا الخاصة. كما يتضمن العمل في الذكاء الاصطناعي دراسة المشكلات التي يقدمها العالم للذكاء بدلاً من دراسة الأشخاص أو الحيوانات من ناحية أخرى. ويتمتع باحثو الذكاء الاصطناعي بحرية استخدام الأساليب التي لم تتم ملاحظتها عند الأشخاص أو التي تتضمن حوسبة أكثر بكثير مما يمكن للأشخاص القيام به.

وقد بدأ عدد من الأشخاص العمل بشكل مستقل على آلات ذكية بعد الحرب العالمية الثانية. وقد يكون عالم الرياضيات الإنجليزي آلان تورينج هو الأول،وقد ألقى محاضرة عن ذلك في عام 1947. وربما كان أيضًا أول من قرر أن البحث عن الذكاء الاصطناعي أفضل من خلال برمجة أجهزة الكمبيوتر بدلاً من بناء الآلات. بحلول أواخر

1 البيانات: "مجموعة منظمة أو غير منظمة من المعطيات، أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات تكون على شكل أرقام أو حروف أو كلمات أو رموز أو صور أو فيديوهات أو إشارات أو أصوات أو خرائط أو أي شكل آخر ، يتم تفسيرها أو تبادلها أو معالجتها، عن طريق الأفراد أو الحواسيب".

2 Internet Of Things.

3 John McCarthy, Stanford University, Retrieved March, 2022 from http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html

الخمسينيات من القرن الماضي، كان هناك العديد من الباحثين في مجال الذكاء الاصطناعي، وكان معظمهم يعتمدون في عملهم على برمجة أجهزة الكمبيوتر. ويعتقد عدد قليل من الناس أنه يمكن تحقيق الذكاء على مستوى الإنسان من خلال كتابة أعداد كبيرة من البرامج من النوع الذي يكتبه الناس الآن ويجمعون قواعد معرفية واسعة للحقائق باللغات المستخدمة الآن للتعبير عن المعرفة. ومع ذلك، يعتقد معظم الباحثين في مجال الذكاء الاصطناعي أن هناك حاجة إلى أفكار أساسية جديدة، وبالتالي لا يمكن التنبؤ بموعد تحقيق الذكاء على المستوى البشري.

ومنذ عام 2010، شهد العالم طفرة كبيرة في مجال الذكاء الاصطناعي. هذا يرجع إلى الطريقة التي نمت بها قوة الحوسبة وسعة التخزين بشكل كبير على مر العقود، ناهيك عن تحسين المنهجية[1]. على سبيل المثال: تعتبر تقنية "LSTM" للذاكرة طويلة المدى التي طورها علماء ألمان عنصراً حاسماً في التعرف على الكلام هذه الأيام. وقد وفرت شبكة الإنترنت ووسائل التواصل الاجتماعي وأجهزة الاستشعار الصناعية المدمجة امكانية الوصول إلى كميات هائلة من البيانات. بفضل أساليب الذكاء الاصطناعي وقوة الحوسبة، يمكن تحليل كميات ضخمة من البيانات في أي وقت من الأوقات. وظهرت التطبيقات المشهورة عالميًا في تتابع سريع، فقد وصلت الشركة الألمانية الناشئة دايبل dipel إلى مستوى جديد تمامًا من البراعة في الترجمة الآلية. وتعد أنظمة التعلم الذاتي بجلب مجموعة واسعة من التطبيقات وزيادة الإنتاجية. وفي الوقت نفسه، تنتج بعض أنظمة الذكاء الاصطناعي نتائج لا يستطيع البشر فك رموزها للعديد من المهام اليومية، وأنظمة الذكاء الاصطناعي ليست موثوقة بشكل كافٍ حتى الآن. بعض الناس لا يخافون من الروبوتات لأن زملاء العمل والبعض الآخر يمكن أن يخرج الذكاء الاصطناعي عن السيطرة. ما هو مؤكد هو أنه ليس كل ما هو ممكن تقنيًا يجب السماح بوضعه موضع التنفيذ، ولكن علينا أيضًا التعرف على الفرص. يعد الذكاء الاصطناعي بتقديم تشخيصات طبية أكثر دقة وتحسين العلاج للمرضى. يمكن أن يساعدنا الذكاء الاصطناعي في التغلب على حواجز اللغة ويمكنه تحسين تدفق حركة المرور في المدن الكبيرة وتقليل الازدحام ومنع الحوادث وحماية البيئة. لذلك فإن المهمة هي تشكيل الذكاء الاصطناعي من أجل الصالح العام للمجتمع.

الفرع الثاني: الإطار القانوني لحماية الخصوصية المعلوماتية

كفلت الشرائع السماوية حق الفرد في حماية خصوصيته، فقبل أن يعرف الحق في الخصوصية من قبل القوانين الوضعية نص عليها التشريع الإسلامي في عدة مواضع، ويعتبر حرمة المسكن من أهم تطبيقات الحق في الخصوصية وحرمة الحياة الخاصة الذي اهتمت به الشريعة الإسلامية، حيث نجد على سبيل المثال قول المولى عز و جل : "يَا أَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ (27) فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ (28)"[2]، فمن خلال هذه الآية يتضح لنا التأكيد على مبدأ حرمة المساكن و خصوصيتها، و عدم جواز دخولها إلا بالاستئذان لما فيه من كشف للعورات و فضح للمستور. و في موضع آخر، فقد أكد الإسلام على وجوب احترام الحياة الخاصة للإنسان، من خلال بيان الإثم الذي قد يقع على عاتق الشخص إذا ما قام بفعل يراد منه كشف ما يحتفظ

1 https://www.plattform-lernende-systeme.de/startseite.html, Access date: 11/01/2022.

2 سورة النور، آية 27 – 28.

به الإنسان سراً لنفسه و ذلك في قوله تعالى :"يَا أَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِّنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلا تَجَسَّسُوا وَلا يَغْتَب بَّعْضُكُم بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَن يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَّحِيمٌ"[1]. كما نجد اهتماماً بالحق في الخصوصية في الحديث النبوي، ومن ذلك قول الرسول "صلى الله عليه وسلم": "من حسن إسلام المرء تركه ما لا يعنيه". ولم يستخدم الفقهاء المسلمون صراحة لفظ الخصوصية أو الحياة الخاصة لكن ذلك لا يعني أنهم لم يتطرقوا إليه، بل على العكس حيث يظهر الاهتمام به عند تفسير ما ورد في القرآن الكريم من آيات تحث على عدم التجسس وضرورة الاستئذان وما ورد من أحاديث في هذا المجال.

وقد اهتمت المواثيق الدولية والتشريعات الوطنية بحماية هذا الحق، من ذلك: الإعلان العالمي لحقوق الإنسان لسنة 1948 في المادة (12) منه التي تنص على أنه: "لا يعرض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات"[2]. والمادة (17) من العهد الدولي للحقوق المدنية والسياسية، والمادة (8) من الاتفاقية الأوروبية لحماية حقوق الإنسان والحريات الأساسية لسنة 1950. وعلى مستوى الإتحاد الأوروبي، فقد صدرت العديد من التوجيهات الأوروبية في هذا المجال لكن أهمها صدر مؤخرا وهو اللائحة العامة لحماية البيانات الصادرة في 2016 وبدأت بالنفاذ عام 2018.

وفي فرنسا، فقد صدر قانون رقم 1978/17 بتاريخ 6 كانون الثاني 1978 والخاص بالمعلوماتية والملفات والحريات ووضع أسس ومبادئ التعامل مع البيانات الشخصية ومعالجتها، بالإضافة إلى قانون الثقة في الاقتصاد الرقمي لسنة 2004. وقد نظم دستور دولة الإمارات العربية هذا الحق في العديد من النصوص، كنص المادة (31) من الباب الثالث الخاص بالحريات والحقوق والواجبات العامة حول حرمة المراسلات وسريتها، والمادة (36) حول حرمة المساكن. وهو ذات الأمر في الدستور المصري لسنة 2014، حيث أكدت المادة (75) على أن "للحياة الخاصة حرمة وهي مصونة لا تمس، وللمراسلات البريدية والبرقية والالكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو رقابتها إلا بأمر قضائي مسبب ولمدة محددة وفي الأحوال التي يبينها القانون". كما أكدت المادة (92) من الدستور المصري على أن: "الحقوق والحريات اللصيقة بشخص المواطن لا تقبل تعطيلا أو انتقاصا". كذلك، فقد ورد في قانون العقوبات الاماراتي الاتحادي عدة نصوص تنظم جوانباً من الحق في الخصوصية وتضع العقوبات لكل من يرتكب أفعالاً جرمية تمس إحدى صور هذا الحق، كنص المادة (431) بشأن الاعتداء على حرمة الحياة الخاصة أو العائلية للأفراد، والمادة (433) والمادة (474). كما يمكن الإشارة إلى نص المادة (51-79) قانون الإجراءات الجزائية التي تنظم عملية تفتيش المنازل والأشخاص وجمع الأدلة وتشدد على ضرورة عدم المساس بخصوصية الشخص وحرمة حياته ومسكنه بدون إذن وكرس حرمة مراسلاته. أما قانون المعاملات المدنية الإماراتي الاتحادي، فقد نصت المادة (90) منه على أنه: "لكل من وقع عليه اعتداء غير مشروع وفق حق من الحقوق الملازمة لشخصيته أن يطلب وقف هذا الاعتداء مع التعويض عما يكون قد لحقه من

1 سورة الحجرات، آية 12.

2 انظر الإعلان العالمي لحقوق الإنسان المعتمد من قبل الجمعية العامة في 10 ديسمبر 1948، المنشور على:

https://www.un.org/ar/universal-declaration-human-rights/ Access date: 28/03/2022.

ضرر". حيث يمكن للأفراد الذي تم انتهاك خصوصيتهم وحرمة حياتهم الخاصة ملاحقة المعتدي واللجوء لهذه المادة للمطالبة بالتعويض ولطلب وقف الاعتداء على الحق في الخصوصية. كذلك، يمكن الإشارة إلى النصوص الواردة في قانون المعاملات المدنية والمتعلقة بالجوار والمظلات التي تضع قيوداً يجب مراعاتها للحفاظ على خصوصية الجيران. بالإضافة إلى قانون حماية البيانات الشخصية الاماراتي الاتحادي لعام 2021.

وعلى مستوى التشريعات العربية، فقد أصدرت العديد من الدول العربية تشريعات تنظم حماية البيانات الشخصية، حيث نشير إلى انه في تونس صدر القانون رقم (63) لسنة 2004 المتعلق بحماية المعطيات الشخصية، كذلك، فقد أصدر المشرع المغربي القانون رقم (8) لسنة 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة البيانات ذات الطابع الشخصي[1]، ونجد أيضا القانون العماني بمرسوم سلطاني رقم 2022/6 بإصدار قانون حماية البيانات الشخصية[2] ، والقانون الأردني الخاص بحماية البيانات الشخصية لعام 2022، والقانون القطري رقم (13) لسنة 2016 بشأن حماية خصوصية البيانات الشخصية[3]، و لائحة حماية خصوصية البيانات الكويتية[4]، و نظام حماية البيانات الشخصية في التشريع السعودي[5]، و قانون رقم (81) للمعاملات الالكترونية والبيانات ذات الطابع الشخصي في التشريع اللبناني[6]، وقانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية المصري.[7]

المطلب الثاني: الطبيعة القانونية للحق في الخصوصية وتمييزه عن غيره

من المعلوم أن القوانين المدنية ومنها قانون المعاملات المدنية الإماراتي تقسم الحقوق إلى حقوق شخصية وحقوق معنوية وحقوق عينية، وقد كان هناك اختلاف في تصنيف الحق في الخصوصية بين هذه الحقوق، حيث أن جانبا من الفقه يدخل الحق في الخصوصية ضمن طائفة الحقوق العينية، كحق الملكية. ويعتبره جانب آخر من الحقوق اللصيقة بالشخصية، ولا شك أن إدخال الحق في الخصوصية في أي من هذه التصنيفات يترتب عليه أثر مضمون الحق ذاته، من هنا تنبع أهمية تحديد الطبيعة القانونية لهذا الحق، فكان لابد من بيان هاتين النظريتين وتحديد نتائجها بالإضافة

1 للمزيد انظر، الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009، المنشور على الرابط:

https://www.cndp.ma/images/lois/Loi-09-08-Ar.pdf Access date: 23/03/2022.

2 لمزيد من المعلومات انظر، الجريدة الرسمية الصادرة من وزارة العدل و الشؤون القانونية. العدد (1429) . السنة (51). 13 فبراير 2022م، المنشور على الرابط:

https://qanoon.om/p/2022/rd2022006/ Access date: 23/03/2022.

3 المنشور في الجريدة الرسمية. العدد (15). 29 ديسمبر 2016، على الرابط:

https://almeezan.qa/LawView.aspx?opt&LawID=7121&language=ar Access date: 24/03/2022.

4 للمزيد انظر لائحة حماية خصوصية البيانات أنشئت في 27/06/2021، منشورة على موقع الهيئة العامة للاتصالات و تقنية المعلومات. على الرابط:

https://www.citra.gov.kw/sites/ar/Pages/regulations.aspx Access date: 24/03/2022.

5 للمزيد انظر، نظام حماية البيانات الشخصية 1443 هـ بناءً على المرسوم الملكي رقم (م/ 19) بتاريخ 1443/2/9هـ. المنشور على موقع هيئة الخبراء بمجلس الوزراء. على الرابط:

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/b7cfae89-828e-4994-b167-adaa00e37188/1 Access date: 23/03/2022.

6 للمزيد انظر، قانون رقم 81 المعاملات الالكترونية و البيانات ذات الطابع الشخصي، المنشور في الجريدة الرسمية. العدد (45). السنة (158). 18 تشرين الأول 2018، المنشور على الرابط:

https://smex.org/wp-content/uploads/2018/10/E-transaction-law-Lebanon-Official-Gazette-Arabic-.pdf Access date: 23/03/2022.

7 قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية. المنشور في الجريدة الرسمية - العدد 28 مكرر (هـ) - في 15 يوليه سنة 2020.

إلى عرض النقد الذي ورد عليهما، وبيان رأي الباحثة في ذلك (الفرع الأول)، وتمييز هذا الحق عما يتشابه معه من حقوق في (الفرع الثاني)، كما سيأتي معنا.

الفرع الأول: الطبيعة القانونية للحق في الخصوصية

انقسم الفقه القانوني في تحديد الطبيعة القانونية للحق في الخصوصية إلى اتجاهين، أحدهما يرى أن الحق في الخصوصية يعد من قبيل حق الملكية، بينما يرى الآخر أن هذا الحق يعتبر من قبيل الحقوق الشخصية، وسنستعرض هذين الاتجاهين بشيء من التفصيل:

أولاً: الحق في الخصوصية يعتبر من قبيل حق الملكية

ذهب أنصار هذا الرأي[1] إلى أن الحق في الخصوصية يعد من قبيل حق الملكية، وأن الشخص يعتبر مالكاً لحياته الخاصة، واستندوا في ذلك إلى أن خصائص حق الملكية تتشابه مع خصائص الحق في الخصوصية من حيث التصرف و الاستعمال و الاستغلال، وأوجدوا مثالاً على ذلك في فكرة الحق في الصورة والتي تعتبر جزءاً من جسمه، حيث يستطيع الشخص بحسب هذا الاتجاه بيع شكله أو ملامحه من خلال الصورة، و ينتج عن ذلك عدم جواز تصوير الشخص أو استعمال صورته إلا بعد أخذ الموافقة من صاحب الصورة، حتى لو كان في مكان عام[2]. ومن النتائج التى تترتب على اعتبار الحق في الخصوصية من قبيل الحق في الملكية أن الشخص يستطيع التصرف بحقه بالخصوصية كما هو الحال في حق الملكية، كما يحق له رفع دعوى لوقف الاعتداء على حياته الخاصة دون الحاجة لإثبات الضرر الذي وقع عليه سواء كان هذا الضرر مادياً أو معنوياً، فهذا ما يخوله حق الملكية للمالك.

وقد كان هذا الرأي محلاً للنقد من جانب بعض الفقه [3]، فذهبوا في هذا النقد إلى أن خصائص الحق في الملكية تتعارض مع خصائص الحق في الخصوصية، فضلاً عن اختلاف طبيعة الحق في الملكية عن الحق في الخصوصية، فطبيعة الحق في الملكية يتوجب (اختلاف–انفصال) صاحب الحق عن محل الحق الذي يمارسه عليه صاحب الحق سلطاته، فإذا اتحد صاحب الحق ومحله يستحيل ممارسة صاحب الحق لسلطاته الذي منحه القانون إياها، وهو ما ينطبق على الحق في الخصوصية. من جانب آخر، فقد ذهب معارضوا هذا الرأي إلى أن الإنسان لا يدخل في دائرة المعاملات القانونية، ولا يمكن أن يكون موضوع حق عيني. [4]

ثانيا: الحق في الخصوصية يعد من قبيل الحقوق الشخصية

ذهب أنصار هذا الرأي[5] إلى أن الحق في الخصوصية يعد من الحقوق اللصيقة بالشخصية، إذ أنه حق غير مالي ، فارتباطه ليس بالذمة المالية إنما بالكيان الشخصي للإنسان، فلا تنفصل عنه و يترتب على ذلك أن صاحب الحق

1 أسامة عبدالله قايد، بشر أحمد صالح، حسام الأهواني. أحمد محمد حسان.

2 حسان، أحمد محمد (2001). نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة و الأفراد "دراسة مقارنة" (ص41-42). القاهرة: دار النهضة العربية.

3 خالد مصطفى فهمي.

4 حسان، أحمد محمد. مرجع سابق. ص43.

5 العاني، ممدوخ خليل. مرجع سابق. ص317.

يستأثر به وحده، فيجب أن يحترم من قبل الكافة، إذ لا يجوز لأحد غير صاحب الحق القيام بالإطلاع أو بنشر (ما يدخل في خصوصيته من عناصر) إلا بإذنه، فإذا وقع عكس ذلك فقام أحد الأفراد بنشر صورة أو صوت لفرد آخر دون اذنه فيستطيع الأخير اللجوء إلى القضاء بمجرد وقوع الاعتداء مطالباً بوقف الاعتداء، دون الحاجة لإثبات ذلك. وهذا الحق غير قابل للتصرف فيخرج عن دائرة التعامل، فلا يجوز إنشاء أي تصرف عليه كالبيع أو الهبة أو التأجير وغيره من التصرفات، كما أنه لا يمكن التنازل عنه ولا ينقضي بالاستعمال فلا تسقط بعدم الاستعمال مهما طالت مدت عدم استعمالها ولا يجوز التنازل عنها للغير[1]. وفي هذا الإطار، فقد جاء قرار الجمعية العامة للأمم المتحدة حول "الحق في الحياة الخاصة في العصر الرقمي" الصادر في 27 نوفمبر 2013 باعتبار هذا الحق كحق أصيل من حقوق الإنسان[2]، و على مستوى التشريعات نرى أن الفقه الفرنسي من أنصار هذه النظرية، فقد ذهب المشرع الفرنسي في المادة (9) من القانون المدني الفرنسي إلى أن للشخص الحق في احترام حياته الخاصة، كما منح صاحب الحق من اللجوء إلى القضاء بمجرد الاعتداء عليه.[3]

وبعد عرض الاتجاهين السابقين وبيان نتائجهما والانتقادات الموجهة لهما، ترى الباحثة أن الحق في الخصوصية حق ذو طبيعة خاصة، فلا يعتبر حق ملكية ولا يعتبر حق من الحقوق اللصيقة بالشخصية، ويأتي ذلك من أنه يمكن اعتباره أقرب ما يكون إلى الحق اللصيق بالشخصية ولكن هنالك بعض الخصائص التي يختلف فيها الحق في الخصوصية عن الحقوق اللصيقة بالشخصية، مما يجعلها غير منسجمة أو متفقة مع هذه الخصائص للحقوق اللصيقة بالشخصية، فيمكن اعتبارها من الحقوق المستقلة القائمة بذاتها.

الفرع الثاني: تمييز الحق في الخصوصية عن غيره من الحقوق

يتشابه الحق في الخصوصية مع بعض الحقوق، وفي نفس الوقت فإنه يختلف عنها في بعض الأمور وهذه الحقوق هي (الحق في الصورة – الحق في الشرف والاعتبار – الحق في الدخول في طي النسيان) وهو ما نعرضه فيما يلي:

أولا: التمييز بين الحق في الخصوصية والحق في الحياة الخاصة

لم يميز الفقهاء بين الحق في الخصوصية والحق في الحياة الخاصة، بل أنهم اعتبروا أن كلا المصطلحين مترادفين ويمثلان وجهان لعملة واحدة. حيث يقوم بعضهم بتعريف الخصوصية على اعتبار أنها الحق في الحياة الخاصة والعكس صحيح.

وعلى مستوى التشريعات نلاحظ أن نص المشرع الإماراتي في المادة (431) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم والعقوبات على أنه: "يعاقب بالحبس والغرامة كل من اعتدى على حرمة

---

1 حسان، أحمد محمد. مرجع سابق. من ص44 إلى 47.

2 أنظر بن صغير فؤاد ،الحق في حماية الحياة الخاصة الرقمية: مسألة قانونية أم حقوقية، منشور على الموقع الالكتروني، https://www.hespress.com/الحق-في-حماية-الحياة-الخاصة-الرقمية-م-411211.html تاريخ الزيارة 25 مايو 2022.

3 انظر في عرض هذه الآراء الزبير، حايف سالم (2018). الاعتداء على الحياة الخاصة عن طريق الإنترنت في التشريع العراقي و اللبناني – دراسة مقارنة – (ص40) الطبعة الأولى. القاهرة : دار النهضة العربية للنشر و التوزيع.

الحياة الخاصة أو العائلية للأفراد وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه"[1]. كذلك، فقد نصت المادة (44) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية على أنه: "يعاقب بالحبس مدة لا تقل عن ستة أشهر والغرامة التي لا تقل عن (150,000) مائة وخمسين ألف درهم ولا تزيد على (50,000) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين كل من استخدم شبكة معلوماتية، أو نظام معلومات إلكتروني، أو إحدى وسائل تقنية المعلومات، بقصد في الاعتداء على خصوصية شخص أو على حرمة الحياة الخاصة أو العائلية للأفراد من غير رضا و في غير الأحوال المصرح بها قانونا بإحدى الطرق الآتية ..... ".

باستعراض النصوص القانونية أعلاه من قانون العقوبات الاتحادي و من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية، فقد نص المشرع الإماراتي في المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم و العقوبات على عبارة (الاعتداء على حرمة الحياة الخاصة) في أحوال معينة ذكرت في المادة المشار إليها سابقا، و في المرسوم بقانون أعاد ذكر بعض الأحوال التي ذكرت في المادة (431) من قانون العقوبات لكن بتغيير الصيغة إلى عبارة (الاعتداء على خصوصية شخص)، نستنتج من ذلك أن المشرع الإماراتي لم يفرق بين الحق في الحياة الخاصة و الحق في الخصوصية، حيث أنه اعتبرها حق واحد لا يقبل التجزئة.

وباستعراض النظم المقارنة، نرى أن المشرع المصري استعمل لفظ (الحياة الخاصة) في المادة (57) من الدستور التى نص فيها على أنه: "للحياة الخاصة حرمة، وهي مصونة لا تمس. وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفي الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك". وقد استخدم المشرع المصري اللفظ ذاته في القانون في المادة (309) من القانون رقم 37 لسنة 1972م والتي نصت على أنه: "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية فى غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه".[2]

ثانيا: التمييز بين الحق في الخصوصية والحق في الصورة

انقسم الفقه إلى قسمين في هذا الشأن، فاعتبر بعضهم الحق في الصورة مظهر من مظاهر الحق في الخصوصية، بينما ذهب الآخر إلى اعتبار الحق في الصورة حقاً مستقلاً عن الحق في الخصوصية، كما سنوضح لاحقاً:

1 المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم و العقوبات، المنشور في الجريدة الرسمية، العدد (712)، السنة (2021)، الموافق 2021/09/26.

2 قانون رقم 37 لسنة 1972 بتعديل بعض النصوص المتعلقة بضمان حريات المواطنين فى القوانين القائمة (تعديل قوانين العقوبات والإجراءات الجنائية وحالة الطوارئ) وبإلغاء القانون رقم 119 لسنة 1964 - بشأن بعض التدابير الخاصة بأمن الدولة - والقانون رقم 50 لسنة 1965 - فى شأن بعض التدابير الخاصة بأمن الدولة - وبإلغاء بعض مواد قوانين الإجراءات الجنائية وإعادة تنظيم الرقابة الإدارية وحالة الطوارئ.

1- اعتبار الحق في الصورة مظهر من مظاهر الحق في الخصوصية

ذهب بعض الفقه الفرنسي[1] إلى الأخذ بفكرة أن الحق في الصورة أحد أهم وأبرز مظاهر الحق في الخصوصية، فقد اعتبره عنصر من عناصر الحياة الخاصة شأنه شأن الصوت والمعلومات الشخصية. وقد استند أصحاب هذا الرأي إلى أن قيام شخص بتصوير و نشر صورة لشخص آخر بغير أخذ اذن من صاحب الصورة أو موافقة سابقة للنشر منه يعتبر انتهاكاً للخصوصية، وينطوي في أغلب الأحيان على المساس بالحق في حماية حياته الخاصة، و يمكن القول هنا أن الحق في الخصوصية يستغرق الحق في الصورة، فكلاهما لهما الطبيعة ذاتها.

وبالرجوع للقوانين المقارنة، نرى أن المشرع المصري نص على ذلك في المادة (309) مكرر والتي جاء فيها أنه: "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه: (أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت فى مكان خاص أو عن طريق التليفون. (ب) التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص فى مكان خاص".[2]

"فإذا صدرت الأفعال المشار إليها فى الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين فى ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضا. ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتماد على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة، كما تحكم التسجيلات المتحصلة عنها أو بمحو إعدامها"[3]. فالمشرع المصري لا يحمي الصورة ذاتها هنا، بل يحميها تحت طائلة الحياة الخاصة، أي أنه يعتبرها جزء لا يتجزأ من الحياة الخاصة، فهذا تعبير ضمني باعتبار الحق في الصورة عنصراً من عناصر الحياة الخاصة.

و بالرجوع للقانون الإماراتي، نرى أن المشرع الإماراتي نص في المادة (431) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم و العقوبات على عقوبة الاعتداء على حرمة الحياة الخاصة بالحبس و الغرامة و ذكر من بين حالات الاعتداء (ب- كل من التقط أو نقل بجهاز أياً كان نوعه صورة شخص في مكان خاص)، كما نص المشرع في المادة (44) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية على عقوبة الحبس و الغرامة لكل من استخدم شبكة معلوماتية أو نظام معلوماتي بقصد الاعتداء على خصوصية شخص أو حرمة الحياة الخاصة من غير رضا و في غير الأحوال المصرح بها قانوناً، و ذكر من بين هذه الطرق:"[2]. التقاط صور الغير في أي مكان عام أو خاص أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها"[4]، وهذا ما أكدته محكمة النقض في الحكم الصادر منها في نزاع والذي أرسى مبدأً هاماً وهو أن صورة الإنسان تعتبر من الأمور الملازمة لشخصية الإنسان، وأي استعمال كالنشر أو التداول دون أخذ موافقة صاحبها يشكل

1 بادنتير، مقالته (الحق في احترام الحياة الخاصة). مشار إليها لدى حسان، أحمد محمد . مرجع سابق. ص92.

2 راجع المادة "309" من قانون العقوبات المصري طبقاً لأحدث التعديلات بالقانون 95 لسنة 2003م، القانون رقم 58 لسنة 1937 بإصدار قانون العقوبات (1).

3 مرجع سابق.

4 انظر المادة (44) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية.

اعتداءً على حرمة الحياة الخاصة، مما يعرض المعتدي للمساءلة القانونية التي توجبه على وقف اعتداءه والتعويض حسب المادة 90 من قانون المعاملات المدنية الإماراتي.[1]

و ذهبت محكمة باريس إلى أن الصورة تعتبر من مظاهر الحياة الخاصة كالحق في الاسم و الصوت.[2]

2- استقلال الحق في الصورة عن الحق في الخصوصية

ذهب اتجاه آخر [3] إلى تبني فكرة ضرورة التفرقة بين الحق في الصورة والحق في الخصوصية، فاعتبر هذا الرأي أن كل حق من هذه الحقوق مستقل وقائم بذاته عن الحق الآخر. وقد استند أصحاب هذا الرأي إلى أن الفعل الواحد قد يشكل مساساً بأكثر من حق في الوقت ذاته، فالاعتداء إذا أصاب أكثر من حق فلا يعني ذلك بالضرورة أننا بصدد حق واحد، فقد يقترن المساس بالحق في الخصوصية بالمساس بالحق في الصورة، وبالرغم من ذلك فإن ذلك لا يمنع استقلال كل حق عن الآخر، فقد يقع المساس بالحق في الصورة دون المساس بالحق في الخصوصية، فالصورة ليست إلا امتداداً للشخصية، يمكن أن يقع الاعتداء عليها في الحياة العامة والعلنية دون أدنى مساس بالحق في الخصوصية.

وترى الباحثة أن الحق في الصورة مظهر من مظاهر الحق في الخصوصية، فالحق في الصورة جزء لا يتجزأ من الحق في الخصوصية كما أشرنا لذلك سابقاً، ولا يمكن أن يستقل عنه بأي شكل من الأشكال، وما يترتب على ذلك أن انتهاك الصورة فيكون معه انتهاك للخصوصية.

ثالثا: الحق في الخصوصية والحق في الشرف والاعتبار

بمناسبة التمييز بين هذين الحقين، يمكننا القول إن الحق في الخصوصية يحمي الجانب الشخصي للفرد، كالجانب الذي يتمتع بالهدوء والسكينة ولا يجوز لأي فرد آخر تسليط الضوء عليه إلا بعد أخذ الأذن من صاحب الحق، بينما يحمي الحق في الشرف والاعتبار الجانب المعنوي للفرد، وقد تم النص عليه في عدة قوانين، كقانون العقوبات والقانون المدني، وقد يحدث تداخل أحياناً بين الحق في الخصوصية والحق في الشرف والاعتبار، كما سنوضح فيما يلي:

1- أوجه الشبه بين الحق في الخصوصية والحق في الشرف والاعتبار

يتشابه الحق في الخصوصية مع الحق في الشرف والاعتبار في عدة صور من أهمها أنهما يشتركان في وحدة الفعل المكون للجريمة، كما يتشابهان في الإجراءات التى يجوز للقضاء المدني اتخاذها لحماية كلا الحقين، وسنتحدث بالتفصيل عن كل منهما فيما يلي:

---

1 راجع، محكمة النقض أبوظبي، الدائرة الإدارية، الطعن رقم (7) لسنة (2013)، الصادر في جلسة 2013/05/20، موقع محامو الإمارات، تاريخ الدخول: 17/01/2022 على الرابط:

https://www-mohamoon-uae-com.uaeu.idm.oclc.org/uaeu/default.aspx?Action=IntrDisplayJudgmentFile&PageNumber=1&Type=5&ID=21463&strSearch=20%الحياة الخاصة

2 نقلاً عن البهجي، عصام أحمد. مرجع سابق. ص217.

3 حسام الدين الأهواني.

أما عن وحدة الفعل المكون للجريمة، فلا بد من الإشارة إلى أن قد يؤدي ارتكاب فعل واحد إلى انتهاك حق الخصوصية والمساس بالحق في الشرف والاعتبار على حد سواء، و يحدث ذلك في حال قيام أحد الأطراف بنشر مكالمة هاتفية تمس خصوصيات أطراف أخرى دون رضاهم على العلن، ففي هذه الحالة يكون قد انتهك حق الخصوصية مع قيامه بالمساس بالحق في الشرف والاعتبار، و هذا ما أكدته محكمة النقض المصرية بوحدة السبب في الدعويين – الجنائية و المدنية – و نشوئهما عن الفعل ذاته و وجود ارتباط بينهما في وقائع القذف و السب، لكن يجب إثارة هذا الدفع أمام محاكم الموضوع، فلا يجوز إثارته لأول مرة أمام محكمة النقض باعتبارها محكمة قانون و دفع غير متعلق بالنظام العام.[1]

أما عن تشابه الإجراءات التي يجوز للقضاء المدني اتخاذها لحماية كلا الحقين، فيتضح تشابه الإجراءات عند المساس بالحق في الخصوصية أو الحق في الشرف و الاعتبار، إذ يجوز لقاضي الأمور المستعجلة في كلا الحالتين الأمر بوقف نشر المطبوعات التى تتضمن المساس بهما، أو وضعها تحت الحراسة. قانون الصحافة الفرنسي لا يسمح إلا بوقف نشر أربع نسخ فقط من المطبوعات في حالة ارتكاب جريمة القذف.[2]

وبالرغم من أن كلا الحقين ينبعان من مصدر واحد ألا وهو نص المادة (90) من قانون المعاملات المدنية الإماراتي وأن كليهما من الحقوق اللصيقة بالشخصية، كما أن معظم الانتهاكات التي تقع على الحق في السمعة تشكل مساسا بالحق في الخصوصية، إلا أن هناك عدة اختلافات كبيرة تقتضي التمييز بينهما.

2- أوجه الاختلاف بين الحقين

بعد بيان أوجه الشبه بين الحق في الخصوصية و الحق في الشرف و الاعتبار، كان لابد من بيان الشق الثاني و هو أوجه الاختلاف بين الحقين، فتندرج تحت أوجه الاختلاف بين الحق في الخصوصية و الحق في الشرف و الاعتبار أربعة أوجه رئيسية و هي: المصلحة المحمية، تحريك الدعوى الجنائية، الخطأ و الضرر، و كذلك تختلف أيضاً في مدة تقادم الدعوى، كما سنوضح فيما يلي هذه الأوجه:

أما بخصوص المصلحة المحمية، فيمكن القول إن المصلحة التى يحميها الحق في الشرف و الاعتبار هي تحقيق السلام الاجتماعي للشخص من خلال الروابط الإجتماعية للفرد مع باقي أفراد مجتمعه، فهي تختلف عن المصلحة التى يحميها الحق في الخصوصية و التى تتمثل في تحقيق السلام الشخصي للإنسان، فإذا كان هدف الأول حماية الحياة العامة، فهدف الثاني حماية الحياة الخاصة، حيث أنه يمكن المساس بالحق في الشرف و الاعتبار دون المساس بالحق في الخصوصية، فالحق في الخصوصية يتعلق بالحياة الخاصة فقط، بينما يتعلق الحق في الشرف و الاعتبار بالحياة العامة و الخاصة معاً.[3]

1 راجع، محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (2257) لسنة (56) القضائية، الصادر في جلسة 1992/05/24، منشور على موقع محكمة النقض المصرية، تاريخ الدخول: 17/01/2022، على الرابط:

https://www.cc.gov.eg/judgment_single?id=111144531&&ja=149781

2 انظر حسان، أحمد محمد. مرجع سابق. ص99-100.

3 راجع حسان، أحمد محمد. مرجع سابق. ص100-101.

أما فيما يتعلق بتحريك الدعوى الجنائية، فقد ذهب القانون المصري إلى أن تحريك الدعوى في جريمة القذف يتوقف على شكوى من المجني عليه، بينما في جريمة المساس بالخصوصية فلا يتوقف رفع الدعوى على شكوى من المجني عليه، بينما في القانون الفرنسي فيتوقف تحريك الدعوى الجنائية في الجريمتين على شكوى المجني عليه[1]، أما القانون الإماراتي فيتوقف تحريك الدعوى في جرائم سب الأشخاص و قذفهم على شكوى خطية أو شفهية من المجني عليه أو من يقوم مقامه.[2]

وعند الحديث عن الخطأ و الضرر في كلا الحقين، فإن الملاحظ أن الخطأ و الضرر في جريمة الاعتداء على الشرف و الاعتبار يختلف عنه في جريمة الاعتداء على الخصوصية، فيشترط لتحقق الخطأ في جريمة الاعتداء على الشرف و الاعتبار توفر القصد الجنائي بعنصريه العلم و الإرادة، بينما لا يشترط ذلك في جريمة الاعتداء على الخصوصية حتى أنه لا يشترط سوء النية في الكشف عن الخصوصية كذلك، بل يتحقق حتى لو كان المراد هو الإشادة بالشخص المجني عليه. و في الحديث عن اختلاف الضرر الناتج عن الخطأ في الجريمتين، فيتمثل الضرر في جريمة الاعتداء على الشرف و الاعتبار على حالة الاحتقار التى تلحق بالشخص بين أهله و أقرانه، بينما يتمثل الضرر في جريمة الاعتداء على الخصوصية في انتهاك أسوار حياته الخاصة في عرض مقتطفات من حياته التى لا يريد إظهارها للعامة.[3]

وأخيراً، فإن طلب التعويض عن الضرر الناشيء عن جريمة التعدي عليهما، فقد نص القانون الإماراتي على أن الشكوى لا تقبل في جرائم القذف و السب بعد ثلاثة أشهر من تاريخ علم المجني عليه بالجريمة و مرتكبها ما لم ينص القانون على خلاف ذلك[4]. و هذا ما استقرت عليه محكمة النقض في حكمها "بأن الشاكي يجب عليه رفع الشكوى خلال ثلاثة أشهر من تاريخ علمه بالجريمة"، فقد جعل الشارع أنه من أمضى هذه الأجل قرينة قانونية لا تقبل إثبات العكس على التنازل لما قدره أن سكوت المجني عليه هذه المدة يعد بمثابة نزول عن الشكوى لأسباب أرتآها الشاكي. عندما قام الجاني بقذف المجني عليها بألفاظ ماسة بالعرض و خادشة لسمعة العائلة، باستعمال وسيلة من وسائل تقنية المعلومات.[5]

يتبين لنا مما سبق أن المجني عليه لا يستطيع رفع الدعوى الجنائية على الجاني بعد مرور 3 أشهر من تاريخ علم المجني عليه بالجريمة و مرتكبها ما لم ينص القانون على خلاف ذلك، و كذلك لا يستطيع المضرور طلب التعويض عن الضرر الناشيء بعد مرور ثلاث سنوات من وقت علم المضرور بالحادث وبالشخص المسؤول عنه، باعتبار الضرر ضرر أدبي[6] يدخل تحت طائلة المسؤولية التقصيرية.

---

1 مرجع سابق، ص102.

2 انظر المادة 10 من قانون رقم 35 لسنة 1992م بشأن إصدار قانون الإجراءات الجزائية وفقاً لآخر التعديلات.

3 راجع حسان، أحمد محمد. مرجع سابق. ص102.

4 المادة 10 من قانون رقم 35 لسنة 1992م بشأن إصدار قانون الإجراءات الجزائية وفقاً لآخر التعديلات.

5 راجع، محكمة النقض أبوظبي، الدائرة الجزائية، الطعن رقم (22) لسنة (2020)س14 ق.أ، الصادر في جلسة 2020/02/04، موقع محامو الإمارات، تاريخ الدخول: 20/01/2022، على الرابط:

https://www-mohamoon-uae-com.uaeu.idm.oclc.org/uaeu/default.aspx?Action=IntrDisplayJudgmentFile&PageNumber=1&Type=5&ID=52814&strSearch=القذف

6 المادة (293) تنص على أن التعدي على حرية الغير أو مس الشخص في كرامته وعرضه وشرفه ومركزه الاجتماعي واعتباره المالي أو في سمعته، كلها تعد من أنواع الضرر الأدبي.

رابعا: الحق في الخصوصية والحق في الدخول في طي النسيان

لم يعد يخفى على أحد الدور الذي تلعبه شبكة الانترنت في نشر المعلومات بسرعة وإلى أي مكان في العالم، وهي تسمح أيضا ببقاء المعلومات المنشورة لفترات طويلة ويمكن استرجاع هذه المعلومات في أي وقت، مما طرح مشكلة نسيان الماضي بالنسبة للأفراد الذين يرغبون بمحو هذه المعلومات التي تضرهم أو تزعجهم، وبدأ الحديث عن إعطاء المستخدم الحق بطلب سحب أو إزالة أو محو ما قام بنشره أو ما نشر عنه من معلومات على شبكة الانترنت أو جعل الوصول إليها صعباً. هذا الحق يطلق عليه الحق في النسيان الرقمي أو الحق في الدخول في طي النسيان، وهو يعتبر بذلك جزءاً من الحياة الخاصة التي نصت عليها المادة (9) من التقنين المدني الفرنسي بقولها: "لكل فرد الحق في احترام حياته الخاصة"، وقد اعترف المشرع الفرنسي بالحق في النسيان في المادة 35 من قانون الصحافة الصادر في 1881م. وقد أشارت له المادة (6) و (40) من قانون المعلوماتية والحريات الفرنسي لسنة 1978 المعدل بموجب القانون رقم 1321 لسنة 2016 والمادة (6) من القانون الفرنسي حول الثقة في الاقتصاد الرقمي والمادة (27) من قانون الحماية الجزائية للملكية الأدبية والفنية عبر الانترنت لسنة 2009. كما نظمته اللائحة العامة لحماية البيانات رقم (679) لسنة 2016 والتي حلت محل التوجيه الأوروبي رقم (46) لسنة 1995. ويستثنى من نطاق الحق في النسيان ما إذا كانت المعلومات ضرورية لغايات تاريخية أو إحصائية أو علمية أو أن يشكل الوصول إليها مصلحة للجمهور لكونه شخصية عامة. ويكون للمستخدم أن يوجه طلبه مباشرة إلى الموقع الذي نشر البيانات، أو أن يوجه طلب إزالة الفهرسة أو الإشارة إلى محركات البحث لتجعل الوصول إلى هذه المعلومات صعباً.

وقد انقسم الفقه في تمييز هذا الحق عن الحق في الخصوصية إلى فريقين، فذهب البعض إلى اعتبار الحق في الدخول في طي النسيان جزءاً من الحق في الخصوصية، بينما ذهب الفريق الآخر إلى اعتبار الحق في الدخول في طي النسيان مستقلاً عن الحق في الخصوصية، كما سنوضح فيما يلي:

1- استقلال حق الإنسان في الدخول في طي النسيان عن الحق في الخصوصية

ذهب جانب من الفقه الفرنسي[1] إلى فكرة وجوب استقلال حق الإنسان في أن يدخل في طي النسيان عن الحق في الحياة الخاصة، استناداً إلى اختلاف مضمون ونطاق الحماية القانونية لهذين الحقين، فالحق في النسيان يختص فقط بكتمان وعدم الإفصاح عن الوقائع التي ظهرت مسبقاً بشكل علني، فقد تكون الوقائع المراد حمايتها قد اعلنت للناس عن طريق المحاكم مثلاً، مما يجعلها تتنافى مع صفة الخصوصية، بالإضافة لذلك قد تتعلق هذه الوقائع الخاصة بأحد الشخصيات المشهورة و العامة كالشخصيات التاريخية، فلا يصمد الحق في الحياة الخاصة أمام نشر الوقائع الخاصة المرتبطة بالشخصيات التاريخية لأغراض الفهم والتدوين التاريخي و لابد من الخوض في التفاصيل والتى قد تعتبر من قبيل الخصوصية، بخلاف الحق في طي النسيان الذي يبدو مفيداً في هذا الشأن. ومن هنا لا بد من الفصل بين الحق في الخصوصية والحق في الدخول في طي النسيان.

1 ليون كاري، موجود لدى حسان، أحمد محمد. مرجع سابق. ص107.

2- الحق في النسيان يدخل في نطاق الحق في الخصوصية

ذهب جانب آخر من الفقه[1] إلى أن الحق في النسيان يدخل في نطاق الحق في الخصوصية، واستند هذا الجانب إلى أن حرمة الحياة الخاصة تشمل خصوصيات الإنسان بصفة عامة في حاضرها وماضيها[2]. فقد أكدت المحاكم الأمريكية من خلال عدة أحكام قضائية على فكرة أن الحق في الخصوصية يشمل دخول الشخص في طي النسيان ويشترط في ذلك أن يكون الماضي بغيض ومهين للشخص العادي، فقد قضت بعدم وجود مساس بالحق في الخصوصية في قضية طالب نابغ في الرياضيات تخرج من جامعة هارفارد و تمتع بشهرة واسعة مما جعله يصبح من الشخصيات الشهيرة، و من ثم أصيب بأزمة نفسية جعلته يهجر الرياضيات، و عمل في وظيفة أمين مكتبة و درس تاريخ الهنود الحمر، و بعد ذلك قامت إحدى الصحف بالكشف عن ماضي هذا الشخص فتعرض لأزمة نفسية شديدة أدت إلى وفاته.[3]

المبحث الثاني: نطاق الحق في الخصوصية المعلوماتية

تمهيد و تقسيم

الحق في الخصوصية من الحقوق المكفولة فيجب عدم انتهاكها و التعدي عليها، لكن في ظل زيادة تطبيقات الذكاء الاصطناعي زادت صور انتهاك الحق في الخصوصية، و بالرغم من عدم جواز التعدي على الحق في الخصوصية إلا أنه ليس حقاً مطلقاً فهناك حالات محددة على سبيل الحصر يجوز فيها الاطلاع على عناصر الخصوصية وفق ضوابط معينة، فسنبحث في المطلب الأول من هذا المبحث عناصر الحق في الخصوصية ومخاطرها في تطبيقات الذكاء الاصطناعي، ثم نتطرق للقيود الواردة على الحق في الخصوصية في المطلب الثاني.

المطلب الأول: عناصر الحق في الخصوصية ومخاطرها في ظل تطبيقات الذكاء الاصطناعي

كما أشرنا سابقا فإن مفهوم الحق في الخصوصية يتسع ليشمل العديد من الصور وبرزت بمناسبة كثرة استخدام الوسائل التقنية وتطبيقات الذكاء الاصطناعي صور جديدة للحق في الخصوصية، وقد تمثلت مظاهر انتهاك الحق في الخصوصية في ظل تطبيقات الذكاء الاصطناعي بعدة طرق، لذلك نتناول عناصر الحق في الخصوصية في الفرع الأول، ثم نتحدث عن مخاطر تطبيقات الذكاء الاصطناعي على الحق في الخصوصية في الفرع الثاني.

الفرع الأول: عناصر الحق في الخصوصية في تطبيقات الذكاء الاصطناعي

وفقاً لبعض النظريات القانونية، فإن الحق في الخصوصية له ثلاثة عناصر أساسية: أحدها يتعلق بالجانب المادي للحق، مثل الحق في السكن، و آخر يتعلق بذات الشخص، مثل قدسية حياته الخاصة وكرامته وحرية التنقل،

1 الأهواني، حسام الدين. مرجع سابق. ص95، أنظر أيضا ليندون موجود لدى، حسان، أحمد محمد. مرجع سابق، ص107.

2 العوضي، عبد الهادي فوزي (2014). الحق في الدخول في طي النسيان على شبكة الإنترنت (ص74). الطبعة الأولى. القاهرة: دار النهضة العربية.

3 منشور لدى حسان، أحمد محمد. مرجع سابق. من ص110.

والثالث يتعلق بحماية وسرية معلوماته[1]. ويمكن الإشارة إلى أن هنالك العديد من عناصر ومظاهر الحق في الخصوصية والتي تجد لها تطبيقاً بارزاً في الذكاء الاصطناعي، نوردها في الآتي:

أولاً: انتهاك حرمة المسكن في ظل تطبيقات الذكاء الاصطناعي

فقد أظهر استخدام بعض الأجهزة التقنية الحديثة وتطبيقات الذكاء الاصطناعي، كالأجهزة المنزلية الذكية وانترنت الأشياء (Internet of Things)، كشاشات التلفاز الذكية التي من الممكن أن تستخدم للتجسس على الشخص، والطائرات بدون طيار (Drone)، إلى ظهور صور جديدة لانتهاك حرمة المسكن، وشكلت خطراً على الحق في الخصوصية وخاصة حرمة المسكن نظراً لمقدرتها على التحليق فوق المساكن مع أجهزة التصوير أو التجسس، وقد وضع المشرع الإماراتي قواعد خاصة لتنظيم استخدام هذه الطائرات وتحليقها فوق البيوت والأسطح لضمان الخصوصية وعدم خرق حرمة المساكن، حيث تشترط المادة (69) والمادة (70) من قانون الطيران المدني[2] تسجيل الطائرات دون طيار لدى هيئة الطيران المدني ووضع عقوبات مالية وسالبة للحرية على من جعل طائرته تطير دون تسجيل. كما اشترطت هيئة الطيران المدني أن تعمل تلك الطائرات في نطاق رؤية المستخدم مع الحفاظ على ارتفاع أقل من 400 قدم فوق سطح الأرض، وعدم جواز تركيب أية معدات تصوير عليها، بالإضافة إلى عدم جواز اقترابها من أية مبان أو منازل أو ممتلكات خاصة.

ثانياً: انتهاكات الواقع الافتراضي المعزز (Agumented Reality)

التي تستخدم الترميز الجغرافي للمسكن لتحقيق هدف البرنامج الإلكتروني للمستخدم، كخرائط قوقل وأجهزة الملاحة البرية، وتطبيقات وسطاء العقارات التي تستخدم الخرائط والمواقع لعرض العقارات المتاحة للبيع أو الإيجار، وبعض الألعاب الالكترونية، كلعبة بوكيمون[3] وببجي[4]. فقد أدت أتمتة النشاطات اليومية التي يطلبها المستخدم عن طريق الأوامر الصوتية أو الإشارات الحركية وغيرها من الوسائل، حيث تستقبل تلك الأجهزة تلك المدخلات بطرق مختلفة، ومن ثم تبدأ بتنفيذها حسب طبيعة الطلب. وأصبحت تلك الأجهزة الذكية تجمع المعلومات الشخصية وتسمح الشركات المصنعة أو القراصنة للولوج لتلك الأجهزة والاستفادة من المعلومات المدخلة.[5]

1 الأهواني، حسام الدين. مرجع سابق. ص132.

2 انظر القانون الإتحادي رقم (20) لسنة 1991 م بإصدار قانون الطيران المدني المنشور في الجريدة الرسمية، العدد (226)، الموافق 1991/06/24.

3 Kacurove, D (25/12/2020). Pokemon Go Palyers Report of Stolen Account. from: https://www.futuregamereleases.com/2020/12/pokemon-go-players-report-of-stolen-accounts/, Access date:16/05/2022.

4 https://tencentgames.helpshift.com/hc/en/3-pubgm/faq/365-account-hack---linked-social-media-account-email-address-has-been-hacked/ , Access date:16/05/2022.

5 Bartneck, C., Lutge, C., Wager, A. & Welsh, S. (2021). An Introduction to Ethics in Robotics and AI. 63-64. E Book: https://link.springer.com/book/10.1007/978-3-030-51110-4. Access date:20/06/2022.

ثالثاً: انتهاك سرية المراسلات والمحادثات الخاصة في تطبيقات الذكاء الاصطناعي

المراسلات الخاصة عبر مواقع التواصل الاجتماعي بأنواعها وبرامج المراسلات الخاصة مثل (WhatsApp) أو البريد الإلكتروني – و قد أورد القضاء المصري تعريفاً للبريد الإلكتروني بأنه: "وسيلة لتبادل الرسائل الإلكترونية بين الأشخاص الذين يستخدمون الأجهزة الإلكترونية من أجهزة كمبيوتر أو هواتف محمولة أو غيرها، تتميز بوصول الرسائل إلى المرسل إليهم في وقت معاصر لإرسالها من مُرسِلها أو بعد برهة وجيزة، عن طريق شبكة المعلومات الدولية (الإنترنت) أياً كانت وسيلة طباعة مستخرج منها في مكان تلقي الرسالة، و سواء اشتملت هذه الرسائل على مستندات أو ملفات مرفقة attachment أم لا"[1]، كما اكسبها المشرع المصري حجية إثبات مساوية للمفرغة ورقياً و المذيلة بتوقيع[2]، و يخضع لمبدأ سرية المراسلات بين الأطراف دون الحاجة أن يفصح المرسل بسريتها[3]، وتتميز تلك الوسائل الإلكترونية بمرور جميع المراسلات المتداولة عبر طرف ثالث يسمى مزود الخدمة، والذي يقوم بالاحتفاظ بتلك الرسائل في خوادم شبكة خاصة ليتيح للمستخدم الولوج إلى الخدمة والاطلاع على تلك المراسلات عند الحاجة. وعلى الرغم من أن المستخدم مرغم على قبول شروط واتفاقية استخدام الخدمة والتي بالعادة تضع شرط تبيح لمزود الخدمة الاطلاع على الرسائل الالكترونية وإفشاء مضمونها متى تم طلبها لأغراض أمنية أو بناء على أمر قانوني صادر من الهيئات القضائية دون الحاجة إلى موافقة صاحب الحساب. المراسلات الخاصة والتي تكون بين المرسل أو المرسل إليه فأكثر كالمجموعات، فتلك المراسلات – بوجهة نظرنا – تتمتع بالحق في الخصوصية كون أن المرسل قد قصد بإرسال المراسلة لفئة محدودة من الأشخاص، ومتى انطوى محتوى المراسلة على معلومات خاصة أو سرية، فيقع على المرسل لهم التزام بعدم إفشاء محتويات المراسلة للغير حفاظاً على خصوصية المرسل أو من تتعلق به المعلومات المرسلة.[4]

رابعاً: الحق في البيانات الشخصية

ويتضمن هذا الحق منع تجميع البيانات الشخصية من منافذ البيع وبيعها لجهات تجارية أخرى، أو تأسيس هوية رقمية للشخص عن طريق مراقبة وتعقب سلوكه على شبكة الإنترنت وعرض إعلانات تجارية أو سياسية وغيرها من الإعلانات بما يتناسب مع هذه الميول لجذب المستخدم إلى التعاقد أو تحقيق غرض معين[5]، عبر ملفات تعريف الارتباط أو "كوكيز Cookies" حيث أن جمع المعلومات الشخصية بواسطة الملفات الارتباطية لأغراض الإعلانات بدون موافقة المستخدم تعتبر من قبيل مساس بالحق في الخصوصية، و في هذا الشأن قام مدعون برفع قضية على

1 راجع، محكمة النقض المصرية، الدائرة التجارية، الطعن رقم (17689) لسنة (89) القضائية، الصادر في جلسة 2020/03/10، موقع محكمة النقض المصرية، تاريخ الدخول: 02/02/2022، على الرابط:

https://www.cc.gov.eg/judgment_single?id=111398859&&ja=297180

2 انظر المواد (18,15) من القانون المصري رقم 15 لسنة 2004 بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.

3 عائشة كركيط، مرجع سابق، ص262-263.

4 Manheim, K & Lyric, K (2019). Article of Artificial Intelligence: Risks to Privacy and Democracy. *The Yale Journal of Law and Techonlogy*. *21*(106). 182-184.

5 سيد، أشرف جابر (2013). الجوانب القانونية لمواقع التواصل الاجتماعي (ص57– 58). القاهرة: دار النهضة العربية.

شركة فيسبوك/ميتا وذكروا بأن شركة فيسبوك تقوم باستخدام ملفات تعريف الارتباط (cookies) ومكونات إضافية مختلفة من أجل تتبع وحفظ المعلومات حول زيارات المستخدمين إلى مواقع ويب الجهات الخارجية ثم بيعها للمعلنين. تم إثبات التهم على فيسبوك و اضطرت شركة فيسبوك لدفع مبلغ 90 مليون دولار أمريكي لإنهاء القضايا (21 قضية) التي تم رفعها ضد الشركة منذ 2012.

تُعد هذه التسوية بمثابة عظة و عبرة و تحذير للشركات التي تجمع بيانات المستخدم أو تتعقبها أو تستخدم أشكالًا أخرى من تتبع المستعرض (Browsers like google). تضمن هذه الشركات أن برامج الخصوصية الخاصة بها تواكب الامتثال لجميع القوانين ذات الصلة. نظرًا لأن قوانين الخصوصية تتغير باستمرار، فمن المهم بنفس القدر مواكبة التطورات القانونية الجديدة ومراقبة مشكلات الامتثال بعناية[1]، بالإضافة لذلك ملفات التجسس (Spyware) التي تتجسس على أنشطة المستخدم بطريقة لا يمكن حصرها، وبإمكانها أن تسجل كلمات المرور الإلكترونية والوصول إلى الملفات الحاسوبية ونقلها من جهاز المستخدم لطرف آخر دون موافقته أو علمه بها بطرق مختلفة. الابتزاز الإلكتروني، حيث يتم مساومة البيانات الشخصية الحساسة بمقابل مادي، متصيّدي كلمات السر على كلمة سر البريد الإلكتروني Phishing، ونشير هنا إلى قضية "Cambridge Analytica".

خامساً: الحق في الصورة

الذي نظمته المادة (431) من المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم و العقوبات واعتبرت التقاط صورة الشخص أو نشرها دون إذنه جريمة اعتداء على الحياة الخاصة. كذلك تعاقب المادة (44) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الالكترونية ذات الفعل سواء كان المكان عام أم خاص كون أن النص لم يخصص طبيعة المكان، و في هذا الشأن قضت محكمة النقض ببراءة المتهمة من تهمة الاعتداء على الحياة الخاصة عند قيامها بتصوير مكان مطروق للعامة و هو الشاطئ و ظهور المجني عليها فيها،حيث أوضحت المحكمة "أن الخصوصية تستمد من المكان المتواجد فيه الشخص الواقع عليه الاعتداء بأن يكون مكاناً خاصاً لا يسمح بدخوله للخارجين عنه أو يتوقف دخوله على أذن دائرة محددة ممن يملك الحق فيه فإذا تخلف هذا الشرط انتفى قيام الجريمة"[2]، و من الأحكام التي تؤكد ذلك أيضاً ما قضت به محكمة النقض بعدم وجود حالة انتهاك للخصوصية بالرغم من تركيب شركة معينة لكاميرات مراقبة في مكان لخدمة النساء، حيث قررت المحكمة

1 Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, (2022) Facebook to Pay $ 90 Million to Settle Data Privacy Lawsuit, The National Law Review, XII (49), Posted on the site:

https://www.natlawreview.com/article/facebook-to-pay-90-million-to-settle-data-privacy-lawsuit#:~:text=Facebook's%20parent%20company%20Meta%20has,of%20the%20social%20media%20platform , Access date:16 / 05/ 2022.

2 راجع، محكمة نقض أبوظبي، الدائرة الجزائية، الطعن رقم (1106) لسنة (2018) القضائية، الصادر في جلسة 2019/01/22، موقع شبكة قوانين الشرق، تاريخ الدخول: 02/02/2022، على الرابط:

https://eastlaws-com.uaeu.idm.oclc.org/data/ahkam/details/1195672

أن المكان مكان عام و لا يمثل ذلك انتهاك للخصوصية[1]، و في حكمٍ مماثل أصدرت المحكمة حكماً ببراءة أحد الأشخاص من تهمة الاعتداء على الخصوصية عند قيامه بتصوير مقطع فيديو في سوبرماركت لمنتجات غذائية بها حشرات لإرسالها للجهات المختصة، فهنا يقوم واجب المصلحة العامة فضلاً عن أن السوبرماركت مكان يقصده العامة[2]. وقد استخدمت بعض تقنيات الذكاء الاصطناعي في تعديل الصور وتركيبها والتقاطها واستخدامها بدون إذن صاحبها والتشهير به أحيانا.

سادساً: الحق في التخفي الرقمي

و مضمون هذا الحق أن لمن يتصفح مواقع الانترنت الحق في التواجد على شبكة الإنترنت باستخدام اسم مستعار وباللجوء للتشفير الالكتروني ودون إلزامه بالكشف عن هويته الحقيقية، ولكن يجب ألا يؤدي ذلك للإضرار بالنظام العام وحقوق وحريات الغير.[3]

سابعاً: الحق في الهوية الرقمية

ويتضمن هذا الحق إمكانية تمتع الشخص بهوية رقمية إلى جانب هويته الحقيقية، وتشمل هويته على البريد الالكتروني، وحساباته على مواقع التواصل الاجتماعي كتويتر وفايسبوك وانستغرام وسناب شات وغيرها، أي أن بإمكان مستخدم المواقع الالكترونية التواجد كشخص رقمي، وله الدفاع عن هذا الحق ضد انتحال هويته الرقمية أو بريده الالكتروني أو حساباته الالكترونية الأخرى.[4]

ثامناً: الحق في الدخول في طي النسيان.

وقد تم الحديث عنه سابقا، فنحيل إليه.[5]

الفرع الثاني: مخاطر استخدام تطبيقات الذكاء الاصطناعي على الحق في الخصوصية

تعتبر تطبيقات الذكاء الاصطناعي أحد أبرز نتائج الثورة التكنولوجية والرقمية وأخطرها لما له من أثر على مختلف جوانب الحياة الإنسانية، وهذا ينبع من قدرة هذه التطبيقات على تحليل البيانات والقدرة على التعلم الذاتي

1 راجع، محكمة نقض أبوظبي، الدائرة الجزائية، الطعن رقم (1182) لسنة (2015) القضائية، الصادر في جلسة 2016/02/22، موقع شبكة قوانين الشرق، تاريخ الدخول: 02/02/2022، على الرابط:

https://eastlaws-com.uaeu.idm.oclc.org/data/ahkam/details/416868

2 المحكمة الإتحادية العليا، الدائرة الجزائية، الطعن رقم (950) لسنة (2019) القضائية، الصادر في جلسة 2020/02/04، موقع شبكة قوانين الشرق، تاريخ الدخو : 04/02/2022، على الرابط:

https://eastlaws-com.uaeu.idm.oclc.org/data/ahkam/details/1195065

3 عائشة كركيط، مرجع سابق، ص261. أنظر أيضا، بن صغير فؤاد، الحق في حماية الحياة الخاصة الرقمية:مسالة قانونية أم حقوقية، منشور على الموقع الالكتروني، https://www.hespress.com/411211 تاريخ الزيارة 10 مارس 2022.

4 بن صغير مراد، مرجع سابق.

5 انظر في ذلك الفرع الثاني، من المطلب الثاني، من الفصل الأول.

والتفكير والإدراك والفهم من التجارب والخبرات السابقة، وإمكانية جمع وتحليل هذه البيانات والمعلومات، والقدرة ربطها مع بعضها لاتخاذ القرارات الصائبة وتوظيف خدمات الإنترنت، والروبوتات، والطباعة ثلاثية الأبعاد، والواقع الافتراضي، والبيانات الضخمة والقدرة على الاستجابة السريعة للمواقف والظروف الجديدة. فقد ظهر دور تطبيقات الذكاء الاصطناعي في تطوير الأدوية ودعم المركبات ذاتية القيادة ومساعدة مديري الموارد البشرية على إنجاز عمليات التوظيف بفاعلية أكبر. وباتت الشركات والحكومات قادرة على تحليل كميات ضخمة من البيانات بسرعة أكبر. ولكن مخاطر اختراق السرية تزداد أيضاً بازدياد حجم البيانات. فبالرغم من كل هذه الإيجابيات التي قدمها الذكاء الاصطناعي للبشرية فإنه في المقابل توجد العديد من التداعيات الأخلاقية السلبية، تتضح من القدرة على توليد الصوت والصورة والكلمة، الأمر الذي سهل القدرة على تزييف البصمة الصوتية لأي شخص. كما أن الشكوك بدأت تحوم بشكل أكبر حول حماية الخصوصية الشخصية مع انتشار تطبيقات الذكاء الاصطناعي، وتداول البيانات وتتبع السلوكيات الرقمية للبشر لحظة بلحظة، كما سيتيح الذكاء الاصطناعي إمكانية مراقبة العملاء والموظفين والمستهلكين بطريقة فاعلة والتعرف على سلوكياتهم والاطلاع على أسرارهم مما يمثل خرقاً لخصوصياتهم وبياناتهم. فتطبيقات الذكاء الاصطناعي التي تقدم الخدمات للمستخدمين تطلب من المستخدم السماح لها باستخدام البيانات الشخصية لتوفير الخدمات، وإذا لم يسمح العميل باستخدام بياناته الشخصية فلن يحصل على المميزات التي يحصل عليها العملاء الآخرين، مما يشكل ضغطاً من أجل التخلي عن الخصوصية وتزويد الشركة ببياناته الشخصية من أجل راحته.

وتشكل تطبيقات الذكاء الاصطناعي العديد من المخاطر الأمنية والعسكرية، والمخاطر الاجتماعية، والمخاطر الاقتصادية، والأخلاقية. ومن أهم هذه المخاطر:

أولاً: تقنية التعرف على الوجه

المستخدمة في العديد من الدول كالصين وأمريكا وعدد من الدول الأوروبية، وتتجسد هذه التقنية عبر إدخال صورة شخص ما ثم يقوم النظام بالبحث عن هذه الصورة بين مليارات الصور، ومن ثم تحديد الصفحات أو المواقع التي يظهر فيها هذا الشخص مثل مواقع التواصل الاجتماعي. وعلى الرغم من أن الشركات لا تستخدم بيانات كاميرات المراقبة المباشرة كما يحصل في الصين، فلا شك ان بناء قاعدة بيانات بهذا الحجم يعدُّ انتهاكًا مباشرًا لخصوصية الأفراد. ونشير أيضا إلى مخاطر استخدام برامج توليد صور جديدة لوجوه بشر بناء على تزويده بصور لبشر آخرين، بحيث يصبح من الممكن توليد صورة لبشر حقيقيين يتم توليدها بالكامل من خلال الاعتماد على الذكاء الاصطناعي دون قص ولصق من وجوه أخرى، ولم يتوقف الأمر عند حد توليد صور الوجوه البشرية فقط، بل تم توليد صور لديكورات داخلية للمنازل، وصور لأشخاص في داخل غرف النوم.[1]

1 Monique, M & Marcus, S (2017). Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *University of New South Wales Law Journal*. *40*(1). 121-145.

ثانياً: خطر الانحياز

تُستعمل المخاوف من إساءة استعمال الذكاء الاصطناعي للتحذير من الانحياز في أنظمة الذكاء الاصطناعي الذي سيؤدي بطبيعة الحال إلى انحياز في المخرجات والقرارات التي تنتج عنها وفي تطبيق القانون، أو تقديم الخدمات المصرفية، أو التوظيف أو الإعلانات ضد النساء مثلاً أو الأشخاص ذوي اللون بسبب البيانات المعيبة، والافتراضات الخاطئة، إلى جانب الافتقار إلى عمليات التدقيق الفني[1]. كما أن هذه البيانات تتركز بشكل أكبر في الأحياء التي ينتشر فيها العنف، ويقل جمع البيانات من الأحياء التي تعتبر آمنة، ليصير من الطبيعي أن يستنتج النظام وجود معدلات جرائم أعلى في تلك الأحياء التي يملك عنها بيانات أكبر. وقد أثير الجدل بشكل كبير حول انحياز أنظمة الشرطة الأميركية، حيث تستخدم العديد من أقسام الشرطة في أميركا أنظمة التعرف على الوجه المقدمة من الشركات التقنية، مثل نظام Recognition من أمازون، لشتى الأغراض مثل توقع الجريمة أو التعرف على الصور. كما نشير إلى مشاكل تطبيقات تحليل العواطف في النصوص، حيث تبين أن أنظمة تحليل المشاعر تختلف مخرجاتها إذا احتوى النص على أسماء شائعة بين الأميركيين السود مقابل الأميركيين البيض. كما أن معظم التطبيقات تنقل البيانات إلى شركات الإنترنت الكبرى من خلال «متتبعات البيانات» لأغراض إعلانية أو تجارية.[2]

ثالثا: تطبيقات الذكاء الاصطناعي القادرة على خلق الصوت لتعديل الكلام

يعني هذا أنه يمكن التلاعب بمقاطع الصوت لأي لشخص حتى صارت مقاطع الصوت عبارة عن عجين تصنع منه ما تشاء وبالنبرة التي تريدها، بل أن هناك تطبيقات متقدمة تجعلك قادراً على تعديل مخارج الحروف لتطابق الحقيقة، فهي بمثابة الفوتوشوب الصوتي الذي يمكن لأي شخص استعماله دون الحاجة لمعدات باهظة الثمن، ومن مخاطر هذه التطبيقات أنها قادرة على تزييف البصمة الصوتية لأي شخص كان، حيث أنه ولفترة قريبة كانت البصمة الصوتية تستخدم كنوع من الحماية أو التوثيق، لكن يبدو أن مستقبلها إلى زوال بعد أن أصبح من الممكن استنطاق أي شخص نريده وأن يتم نسب كلام لم يقله.

رابعاً: تطبيقات قادرة على خلق الفيديو من خلال تقنية تسمى Deep fake

وهي طريقة يتم فيها تجميع صور وفيديوهات لشخص ما ويتم تلقيمها لذكاء اصطناعي ليتعلم منها كيف يتحرك ويتكلم ذلك الشخص ثم يبدأ في توليد ما تريد له أن يولده فتجعل ذلك الشخص يتحرك ويقول ما تريد له أن يفعل بشكل طبيعي جداً لدرجة مخيفة. ولعل أكثر الأشخاص المستهدفين من هذه التطبيقات هم المشاهير والسياسيين، حيث تم تزييف مقاطع لهم (سياسية وإباحية) نظراً لتوفر مقاطع وصور لهم على الإنترنت بشكل واضح، ومن الواضح أن

1 Fuchs, D (2018). The dangers of human-like Bias in machine-learning algorithms. *Missouri University of Science and Technology*. *2*(1), 1.

2 Howard, A., Zhang, C. & Horvitz, E. "Addressing bias in machine learning algorithms: A pilot study on emotion recognition for intelligent systems," 2017 IEEE Workshop on Advanced Robotics and its Social Impacts (ARSO), 2017, 1-7.

الأمر يتطور بشكل سريع جداً وربما سيأتي يوم يستحيل فيه التمييز بين الحقيقة والتزييف في هذا المجال، فالصورة والصوت والفيديو صارت أشياء قابلة للتزييف.

تتيح هذه التقنية إنشاء صوت وفيديو لأشخاص حقيقيين يقولون ويفعلون أشياء لم تقال أو تفعل مطلقًا مما يزيد مقاومة اكتشاف التزييف، و قد يتم استخدامها بطريقة تسبب ضرراً على الخصوصية كسرقة هويات الأشخاص للحصول على منفعة مالية أو بعض المنافع الأخرى، كما يمكن أيضًا استخدام التزييف العميق لتصوير شخص ما، بشكل خاطئ على أنه يؤيد منتج أو خدمة أو فكرة سياسية، و قد يتعدى ذلك إلى جعل الموظف العام يتقاضى رشاوى باستخدام التزييف العميق.[1]

خامساً: مخاطر تتعلق بالبيانات الشخصية

و التي تتمثل في مجموعة من التطبيقات الخبيثة التي تستند إلى برمجيات الذكاء الاصطناعي والتي يمكنها القرصنة وكشف الشفرات وتهديد الحسابات الخاصة بالشركات والأفراد والبنوك[2]، فهناك عدداً هائلاً من البرمجيات الخبيثة المتخصصة في القرصنة واختراق الحسابات تتوفر عبر آلاف المنصات المنتشرة على المواقع الإلكترونية الخاصة ببرمجيات الاختراق، بل إن غالبية هذه البرمجيات أصبح من السهل شراؤها من خلال عدة مواقع إلكترونية، تماماً كما هو الأمر بالنسبة للتسوق عبر الإنترنت لشراء الكتب أو الملابس، وتتضمن البرمجيات الخبيثة حالياً وحدات متنوعة تعتمد على الطرف الثالث والمصادر المفتوحة، وهي متخصصة في مجالات التشفير أو فك التشفير، وأنظمة المدفوعات والبنية التحتية لمراكز التحكم والسيطرة وغيرها. وقد حذرت شخصيات عامة ورجال أعمال من مخاطر الذكاء الاصطناعي الخارج عن السيطرة، ولذلك لابد من البحث عن منظومة أخلاقية تسهم في الحد من تلك المخاطر الأخلاقية من منطلق أنها لا تقل أهمية عن البحث في مكاسب وإيجابيات الذكاء الاصطناعي.

عند استخدام وسائل التواصل الالكتروني وزيارة المواقع الالكترونية والبرامج والتطبيقات الحديثة يقدم الشخص بياناته ومعلوماته طواعية ويفقد السيطرة عليها دون أن يكون محيطا بمن تخزن لديه وكيف يعالجها وهل ينقلها للغير أو يتاجر بها، توجد العديد من التطبيقات الذكية التي يستخدمها المستهلك بشكل مستمر وتقوم بحفظ بياناته وتخزينها. من أهمها: وسائل التواصل الاجتماعي والدردشة، وأجهزة التتبع وتحديد المواقع الجغرافية التي تحتوي عليها أغلب الهواتف الذكية والتطبيقات التي بتنا نستخدمها بشكل يومي، حيث تساهم في معرفة تحركات وموقع المستخدم لها، كذلك مخاطر استخدام البريد الالكتروني، حيث يمر البريد الالكتروني بعملية تقنية قبل وصوله للمستقبل، و من خلال هذه العملية قد يتعرض لأحد المخاطر التالية، و التي يجب أن توضع في عين الاعتبار سواء من قبل المرسل بإن رسالته قد تتعرض لأحد هذه المخاطر، أو حتى مستقبل الرسالة عندما يتلقاها من قبل المرسل، فقد يتنكر ليبدو كأنه من شركة معروفة مثل مصرف أو بريد إلكتروني شخصي من صديق. وقد تحتوي حتى التنزيلات من المواقع الشرعية في بعض الأحيان على برامج ضارة مرفقة. ما يعني أنه حتى المستخدم الأكثر حرصًا يتعرض للخطر ما لم يتخذ إجراءات إضافية. كما قد تحتوي بعض رسائل البريد الالكتروني على معلومات سرية لا يجب الاطلاع

1 Chesney, B. & Danielle, C. (2019). Deep Fakes: A Looming Challenge for Privacy. *California Law Review.107*(6), 1771-1776.

2 عائشة كركيط، مرجع سابق، ص262.

عليها إلى من قبل الأطراف المسؤولة عن محتوى الرسالة. وقد يتلقى المستقبل بريد الكتروني من أحد الأصدقاء المقربين أو شركة معروفة يطلب فيها فتح الرابط لأي هدف كان، و بعد التحدث هاتفياً مع الصديق أو الشركة (مرسل الرسالة) يخبره بأنه ليس المرسل لهذه الرسالة و أن هناك منتحل لشخصية هذا المرسل ليتم من خلال ذلك سحب المعلومات الشخصية للمرسل، فيجب على المستقبل أن يعي و يتأكد من أي رسالة قد يساوره الشك فيها و الابتعاد عن فتح الروابط. كما يجب على المرسل الذي قام بإرسال البريد الالكتروني أن يضع في عين الاعتبار أن رسالته قد لا تصل بالمحتوى الذي قام بكتابته، و كذلك المستقبل أيضاً فعليه أن يضع نصب عينيه أن هذه الرسالة قد تصل إليه بعد تغيير في محتواها و ليس بالشكل أو المقصود الذي قام بإرساله المرسل له، فقد يتم تغيير المحتوى من قبل طرف ثالث قام بالاطلاع على محتوى الرسالة.

وفي بعض الأحيان، قد يحصل و أن يصل لشخص ما على بريده الالكتروني رسائل مزعجة و مؤذية فيمكن أن يكون محتوى الرسالة عبارة عن رابط يحتوي على نوع معين من الفايروسات[1] التى تمكن المرسل من سحب البيانات الشخصية للمستقبل الذي لم يعِ خطورة هذا البريد الالكتروني ليس بسبب الجهل في أغلب الأحيان، فقد تكون هذه الرسالة عبارة عن رابط يطلب فيه تحديث البيانات الشخصية أو يطلب تنزيل أحد البرامج لجهة معروفة فيظن المستقبل أن مرسل هذه الرسالة هي هذه الجهة التى جاء ذكرها في عنوان الرسالة، و هذا ما حدث فعلاً عندما تفاجأ الجمهور ببريد الكتروني صادر من مكتب التحقيقات الفيدرالي يصل إليهم يحتوي على تنبيه من أنهم أهداف لهجوم الكتروني [2]، فوصول انتهاكات البريد الالكتروني على مستوى الحكومات يقرع ناقوس الخطر بشأن وضع عقوبات مشددة على كل من تسول له نفسه بانتهاك حرية المراسلات.

وقد اتهمت جوجل وهي أحد أهم شركات البحث حول العالم بأنها تقوم بالاستيلاء التدريجي على بيانات الأفراد حول العالم، فعند استخدام جوجل للبحث عبر المواقع على شبكة الانترنت سنرى أنه يتعقب الأسئلة و الكلمات البحثية و يسجلها، فضلاً عن كل رابط الكتروني يتم النقر عليه من قبل المستخدم، و لم تقف جوجل عند هذا الحد بل تطور الأمر إلى إطلاق خدمة البريد الالكتروني (Gmail) و الذي من خلاله استطاعت الاطلاع على رسائل المستخدم الشخصية أو رسائل العمل و اكتشاف معلومات جديدة يمكن عرضها على المعلنين، بالإضافة إلى إتاحة الفرصة للمستخدم لحفظ أسماء و عناوين الأهل و الأصدقاء الكترونياً مما يمكنها من معرفة دائرة المعارف للمستخدم و قوتها الشرائية. و قد سبق مقاضاة جوجل في أكثر من دولة حول العالم بسبب انتهاكها خصوصية المستخدمين و اختراقاتها الأمنية، و إساءة استخدام البيانات، و الاعتداء على الملكية الفكرية. وقد اقيمت دعوى جماعية أمام المحكمة الفيدرالية في سان خوسيه – كاليفورنيا – تتهم فيها شركة جوجل بانتهاك خصوصية مستخدمي محرك البحث بالرغم من استخدامهم للمتصفح الذكي (smart browser) على APP STORE و المتصفح الخاص على GOOGLE PLAY ، فمن خلال ذلك تقوم جوجل بجمع بيانات المستخدمين بالإضافة إلى بيانات الأصدقاء و هواياتهم و عاداتهم اليومية كذلك في برنامج Google Analytics و Google Ad Manager و من خلال التطبيقات الأخرى على

1 كأحصنة طروادة، روتكيت، أسلوب الأبواب الخلفية، أسلوب البرامج المراوغة، الديدان: و جميعها برامج خبيثة تعمل بذات الآلية.

2 Kevin, C., Hacker sends spam to 100,000 from FBI email address, 14 Nov 2021, on: https://www.nbcnews.com/tech/security/hacker-takes-fbi-email-server-blasts-spam-thousands-rcna5530 Access date:6/5/2022.

الهواتف المتحركة، و قد طالب المدعوون بمبلغ 5 ملايين دولار لتعويض الأضرار التي لحقت كل مستخدم بسبب انتهاكات قوانين التنصت الفيدرالي و قوانين الخصوصية في كاليفورنيا.[1] و من جانب آخر فقد قامت لجنة حماية المنافسة والمستهلك الأسترالية في عام 2019م بمقاضاة جوجل أمام محكمة فيدرالية في سيدني، بسبب استخدام معلومات المستخدمين الشخصية الحساسة و القيمة حول أماكن تواجدهم دون أخذ الأذن منهم خارج عن إرادتهم[2]. فيما ذهب النائب العام هيكتور بالديراس في نيو مكسيكو إلى مقاضاة جوجل كذلك بتهمة انتهاك قانون"COPPA[3] قانون حماية خصوصية الأطفال عبر الإنترنت" وقانون الممارسات غير العادلة في نيو مكسيكو، فقد زعم النائب العام بأن جوجل تقوم بجمع بيانات المواقع و كلمات المرور و التسجيلات الصوتية من الأطفال دون إعطاء الحق لذويهم بالقبول أو الرفض.[4]

وقد اتهمت شركة فيسبوك بالاستخدام غير العادل للمعلومات و مشاركة معلومات مستخدمي فيسبوك مع مطوري برامج وشركاتٍ خارجية، إضافةً إلى السماح للمعلنين بجمع معلوماتٍ عن المستخدمين بمجرد ضغطهم على أي إعلانٍ من خلال موقع فيسبوك، وفقاً لما نشرته صحيفة "نيويورك تايمز" بتاريخ 29 تشرين الثاني (نوفمبر) 2011. ثم عادت صحيفة "نيويورك تايمز" من جديد، لتنشر تقريراً حول مشكلة شركة "كامبريدج أناليتيكا" المختصة بجمع وتحليل البيانات، التي حصلت على معلومات ما لا يقل عن 87 مليون مستخدم، مستخدمة إياها بطريقةٍ غير مشروعة، مستغلةً المعلومات في الحملة الرئاسية للرئيس السابق دونالد ترامب في 2016.

أما عن التصيد الاحتيالي (Phishing) والتجسس الالكتروني والفيروسات والتزوير الالكتروني، فيقصد بذلك انتهاك المعلومات و البيانات المصرفية للمتعاملين من خلال سرقة بياناتهم المالية بطرق احترافية عن طريق تصنع هوية المصرف بطرق احتيالية، و يتم ذلك عن طريق الحصول على الأرقام السرية لبطاقات الائتمان و بطاقات الدفع الإلكتروني[5]، و ذلك بأحد الطرق التالية: يقوم المعتدي بإرسال رسائل دعائية عن طريق البريد الإلكتروني، و يحتوي هذا البريد الإلكتروني على موقع وهمي شبيه بالموقع الحقيقي للشركة أو المؤسسة التي يودع فيها متلقي البريد الالكتروني أمواله، يطلب فيها تحديث البيانات الشخصية لمتلقي البريد الالكتروني، فبمجرد قيام متلقي البريد الالكتروني بالانصياع لذلك و قيامه بتحديث البيانات الشخصية السرية يأخذها صاحب الموقع الوهمي و يقوم باستغلالها للحصول على البيانات المالية، و قد يقوم المعتدي باستخدام ذلك في المشاريع الوهمية أو طلب القروض أو من الممكن أن يقوم ببيعها في السوق.

---

1 انظر جلال، أحمد (يونيو 2020)، جوجل تواجه دعوى قضائية بقيمة 5 مليارات دولار بتهمة انتهاك خصوصية المستخدمين، منشور على:

https://cutt.us/0H2m9 Access date:10/02/2022.

2 أستراليا تقاضي جوجل بسبب انتهاك خصوصية المستخدمين.أكتوبر 2019، على الرابط:

https://cutt.us/o3YvL Access date:10/02/2022.

3 Children's Online Privacy Protection Act.

4 جمال، منة الله (فبراير 2020)، جوجل أمام النائب العام بتهمة انتهاك خصوصية الأطفال، منشور على:

https://cutt.us/Fkmhz Access date: 10/02/2022.

5 عائشة كركيط، مرجع سابق، ص268-270.

ومن الطرق الأخرى في التصيد الاحتيالي قيام المعتدي باستخدام جهاز مشابه لأجهزة الدفع، وبمجرد تمرير مالك البطاقة لبطاقته الائتمانية على هذا الجهاز يقوم بنسخ جميع البيانات المالية المتعلقة بالبطاقة وذلك دون أن يشعر مالكها بذلك، ومن ثم قد يقوم بإصدار بطاقة مزيفة يشتري بها على حساب مالك البطاقة. كما قد يحصل التصيد الاحتيالي عبر البحث عن الثغرات في الأنظمة المالية أو إطلاق برامج تجسس في عدة مواقع، أو وضع برامج تجسس في أحد الملفات أو التطبيقات؛ لتتبع كلمات المرور والتقاط الأرقام السرية لصاحب الجهاز عند تسجيل دخوله لهذا الملف أو التطبيق الذي سبق وإن وضع فيه برنامج للتجسس، وقد يكون ذلك أيضاً من خلال الاعتراض للبريد الالكتروني الذي يتضمن معلومات العميل المالية والتقاط الأرقام السرية منها. وقد يحصل هذا التصيد عبر استخدام معادلات وخوارزميات رياضية للبحث والكشف عن أرقام البطاقات الائتمانية الخاصة بالعملاء، ونشرها عبر مواقعهم الخاصة على الانترنت، أو في حال حدوث عطل في جهاز العميل الذي سبق وأن قام بتسجيل الدخول من خلاله لهذا التطبيق فيتم سرقة الأرقام السرية.[1]

مما سبق نرى أن التصيد الالكتروني قد يحدث بعدة صور وطرق احتيالية يقوم من خلالها المعتدي بانتهاك البيانات المالية المصرفية للعميل والتي هي أساساً بيانات لا يجب الاطلاع عليها إلا من قبل صاحب البيانات والمخول له بالاطلاع عليها، وقد يصل في أغلب الحالات إلى عدم شعور صاحب البيانات بانتهاك بياناته المصرفية، إذ يستكمل المعتدي اعتداءه الآثم بطرق خبيثة بعد ذلك، فقد يقوم المعتدي بالشراء من البطاقة الالكترونية بشكل قليل وغير ملحوظ لدى صاحب البيانات.

أما عن المساس بسرية البيانات الصحية، فبالرغم من أن التطبيقات الخاصة بمراقبة الحالة الصحية والتي تقوم بحفظ السجل المرضي للفرد تساهم في الحد من انتشار الأوبئة، إلا أن هذه المعلومات الصحية لا يجوز لطرف ثالث غير الطبيب والمريض من الاطلاع عليها، إذ أنها تعتبر من المعلومات الشخصية والتي لها قدسية لا يجوز المساس بها أو انتهاكها. وذهبت بعض الدول إلى منع أرباب العمل من استغلال البيانات الصحية للعامل، كقيام رب العمل ببيع بيانات العامل الصحية لشركات التأمين مثلاً، وفرض عقوبات تعويضية بذلك[2]. وفي وقتنا الحالي يتم استخدام الروبوتات في كثير من مجالات الحياة المختلفة، كالمجالات العسكرية و الصناعية و الخدمات الترفيهية و المجال الطبي، و بالتركيز على المجال الطبي نرى استخدام الروبوت الطبي بشكل كبير في العمليات الجراحية والتي لا يمكن أن تحصل إلا بتخزين المعلومات الصحية للمريض في قاعدة البيانات الخاصة بهذا الروبوت الطبي، فقد يتمكن من خلال ذلك طرف ثالث بالاطلاع على معلومات المريض الشخصية و الحساسة وقد لا يكون هذا الطرف من الأطراف المخول لها بمعرفة هذه البيانات كالشركة المصنعة لهذا الروبوت أو الشركة المبرمجة له، فهذا يعد انتهاكاً للخصوصية، و في ذلك فقد عد المشرع الإماراتي انتهاك البيانات أو المعلومات الصحية التي تتعلق بالفحوصات أو التشخيص أو العلاج أو الرعاية أو السجلات الصحية ظرفاً مشدداً.[3]

1 انظر العمروسي، غادة علي (2021). موقف الفقه الإسلامي من التعدي على البيانات المالية. مجلة كلية الدراسات الإسلامية و العربية. 6 (4)، ص600-601، منشور على: https://jcia.journals.ekb.eg/article_220358.html Access date: 23/03/2022.

2 انظر مقال هل تطبيقات مراقبة الحالة الصحية تنطوي على انتهاك للخصوصية (نوفمبر 2020)، المنشور على: https://www.bbc.com/arabic/vert-cap-54923302 Access date: 20/02/2022.

3 انظر البند الثاني من المادة (6) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية.

وبخصوص البيانات المالية في ظل التطبيقات الخاصة بالبنوك وطرق الدفع الالكترونية[1] Apple pay وبطاقات السحب الممغنطة، فقد يتم التعدي على البيانات المالية باختراق الثغرات الأمنية (Security Bugs)، وتتمثل هذه الصورة في قيام المعتدي باختراق أنظمة البنك من خلال وسائل يتبعها للاستيلاء على الموقع الخاص بالبنك يتمكن فيها من فك الشفرة الخاصة بنظام البنك، و من ثم التوصل لشبكة المعلومات الخاصة بالعملاء و الاتصال بهم عن طريق الهاتف، و بالتالي القيام بتحويل الأموال من حسابات العملاء الخاصة لحساب المعتدي الشخصي، و من الطرق التي يتبعها المعتدي للاستيلاء على المواقع: قيام المعتدي بالبحث عن الثغرات التي قد تكون موجود على الموقع، أو البحث العشوائي عن الثغرات دون تحديد الهدف، أو البحث عن الثغرات التي سبق الإعلان عنها و لم يقم الموقع باتخاذ الإجراءات لسدها، و بمجرد الحصول على هذه الثغرة يتمكن من التحكم بالموقع عن طريق الحصول على اسم المستخدم و كلمة المرور و من ثم قيامه بإدارة الموقع.

وقد يتم ذلك عبر حجب الخدمة عن طريق قيام المعتدي بإغراق الشبكات بالبيانات و الرسائل الغير مهمة من أجل تعطيل الموقع عن العمل، باستخدام عدة برامج كبرامج Tear Drops و Ping of Death، يتم تحميل هذه البرامج على الأجهزة و من ثم يقوم المعتدي بإدخال بيانات الموقع المراد استهدافه و وقت البدء في عملية الهجمات، فقد تتعطل بعض المواقع لفترة و قد لا يتعطل بعضها لقوة إجراءات الحماية. كما قد يتمثل ذلك بطريقة البحث الجماعي من خلال الاتفاق الجماعي لعدة اشخاص على الاعتداء على موقع معين في الوقت ذاته، فعند البدء في الاعتداء يقوم المعتدون بالبحث عن أكثر كلمة تستعمل في الموقع، مما يؤدي لتعطل الموقع وبالتالي قد يؤثر على السمعة العامة للموقع بين المستخدمين. وقد يقوم المعتدي بتخمين كلمة المرور عن طريق تجربة احتمالات عدة ومن ثم إيجادها.[2]

سادساً: المركبات ذاتية القيادة

و في هذا الشأن ذهب البعض إلى اقتراح تضمين نظام العلبة السوداء "Boîte noire" في السيارات ذاتية القيادة، ليتتابع و يشمل جميع الآلات التي تعمل بالذكاء الاصطناعي، بما يمكن من التعرف على المسؤول عن الفعل الضار، لكن هذا الاقتراح قد يمس بالحياة الخاصة و البيانات الشخصية للأفراد.[3]

سابعاً: الطائرات بدون طيار

تعرف الطائرات بدون طيار بأنها:"طائرات توجه وتبرمج عن بعد يتحكم فيها خبراء متخصصون على الأرض، وتكون مجهزة بأدوات تسمح لها بأداء المهام المطلوبة، وتكون مزودة بأجهزة وكاميرات، وبقذائف وصواريخ لاستخدامها ضد أهداف معينة. كما جاء بأنها طائرات تطير في الفضاء الجوي بدون شخص على متنها"[4]. بالرغم من

1 جعل المشرع الإماراتي الاعتداء على البيانات و المعلومات المتعلقة بوسائل الدفع الإلكترونية ظرفاً مشدداً. انظر البند الثاني من المادة (6) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية.

2 انظر، العمروسي، غادة علي. مرجع سابق، ص602-603، منشور على:

https://jcia.journals.ekb.eg/article_220358.html Access date: 23/03/2022.

3 للمزيد، راجع، الخطيب، محمد عرفان (2020). المسؤولية المدنية و الذكاء الاصطناعي ... إمكانية المساءلة؟!. مجلة كلية القانون الكويتية العالمية. 8 (1). ص141-140-.

4 راجع، مؤمن، طاهر شوقي (2017). النظام القانوني للطائرات بدون طيار "الدرونز Les Drones" (ص311). القاهرة: دار النهضة العربية.

التوجه الكبير للدول لاستخدام الطائرات بدون طيار (الدرونز) لما لها من إيجابيات كثيرة مقارنة بالطائرات التقليدية بأنها بدون طيار و صديقة للبيئة و تكلفتها المعقولة و توفيرها للوقود، وتعد الطائرات بدون طيار أحد اهم تطبيقات الذكاء الاصطناعي والتي انتشرت انتشاراً واسعاً لما لها من أهداف عديدة يتم تحقيقها بأسهل الطرق، فلو عدنا قليلاً للقرن الماضي لرأينا أن أول استخدام للطائرات بدون طيار كان في عدة حروب كحرب فيتنام و حرب أكتوبر 1973م و حرب سهل البقاع بين سوريا و القوات الإسرائيلية عام 1982م، فالهدف من استخدامها آنذاك هو تحقيق الأغراض العسكرية كالتجسس على العدو لمعرفة مدى قوة إمكانياتها للتغلب عليه، و فضلاً عن استخدام الطائرات بدون طيار في المجالات العسكرية فقد استخدمت كذلك في المجالات المدنية من خلال قيام عدة شركات مبيعات بتنفيذ عملياتها من خلال هذه الطائرات كشركة علي بابا[1] التى تقوم بتوصيل منتجاتها للمستهلكين من خلال الطائرات بدون طيار منذ فبراير 2014م[2]، و هذا ما قامت به أيضاً شركة أمازون الأمريكية [3] من خلال استخدام الطائرات بدون طيار لإيصال السلع لعملاء/ زبائن / مستهلكين الشركة و التى قد تم تزويدها بنظام تحديد المواقع GPS (Global Positioning System) و ذلك في زمن قياسي مما يعكس توفير الوقت على الشركة و المستهلك، و بالرغم من سهولة ذلك الأمر بالنسبة للشركة و المستهلك إلا أن هذه الطائرات بدون طيار التى قد تكون مملوكة لطرف ثالث قد لا يعلم به المستهلك، فخطورة الأمر في ذلك تكمن في إمكانية جمع كم هائل من البيانات الشخصية للمستهلك و موقع سكنه بالإضافة إلى ميوله الاستهلاكية، مما قد يجعل الشركة تقوم ببيع هذه البيانات لأطراف منتجة لبضائع معينة تستهوي هذا المستهلك أو الأشخاص القاطنين في منطقة معينة.

ثامناً: تقنيات العالم الإفتراضي كتقنية الميتافيرس (Metaverse)[4]

عبارة عن شبكة مترابطة من البيانات الاجتماعية و الشبكات الغامرة في الأنظمة الأساسية متعددة المستخدمين المستمرة[5]، و هي بيئة رقمية ثلاثية الأبعاد والتي تدعم العالم الافتراضي و الواقع المعزز بشكل واسع النطاق، و هو يعمل على دمج بيئتين حقيقية و رقمية[6] فكل ما يحتاجه الشخص للدخول لهذه التقنية سماعات و نظارات الواقع المعزز و كذلك التطبيقات التي تدعم هذه التقنية، و بمجرد التمكن من الدخول لهذه التقنية يستطيع المستخدم ممارسة هواياته أو عقد اجتماعات العمل و لا يقف الأمر عند ذلك بل ذهب البعض إلى شراء الأراضي بالعملات الرقمية عن طريق منصات عدة توجد في هذه التقنية، و لا يلزم ذلك انتقال الشخص من مكانه، بالإضافة إلى إعطاء المستخدم كافة البيانات المتعلقة بالمستخدمين الآخرين الذين يشاركونه التقنية لكي يتمكن من التفاعل معهم، و هذا ما قد يؤثر على إتاحة بيانات

1 تم تأسيسها في 1999م، تعد أكبر متجر تجزئة في العالم، واحدة من أكبر شركات الإنترنت وشركات الذكاء الاصطناعي، واحدة من أكبر شركات رأس المال الاستثماري، واحدة من أكبر شركات الاستثمار في العالم.

2 مؤمن، طاهر شوقي. مرجع سابق. ص308.

3 موقع للتجارة الإلكترونية و الحوسبة السحابية تأسس في 5 يوليو 1994، من قبل جيف بيزوس و يعد من أكبر متاجر التجزئة القائمة على الإنترنت في العالم.

4 يتكون مصطلح الميتافيرس Metaverse من مقطعين هما Meta و تعني ما وراء، و المقطع الثاني Verse و هو مأخوذ من Universe بمعنى عالم، و بذلك فإن Metaverse تعني "ما وراء العالم". انظر بريك، أيمن محمد (مارس 2022). تطبيقات الميتافيرس و علاقتها بمستقبل صناعة الصحافة الرقمية–دراسة استشرافية خلال العقدين 2022:2042 -. المجلة المصرية لبحوث الإعلام. 2022 (78)، ص58.

5 Mystakidis, S. (2022). Metaverse. *Encyclopedia2022*, *2*(1), 486.

6 فرجون، خالد محمد (2022). تكنولوجيا "ميتافيرس" و مستقبل تطوير التعليم. المجلة الدولية للتعليم الإلكتروني. 5 (3)، ص77.

المستخدمين الخاصة لبعضهم البعض و بالتالي انتهاك خصوصيتهم و سرية معلوماتهم الشخصية. كما تتيح أجهزة الواقع (XR) التقاطًا أكثر شمولاً وواقعية لكمٍ هائل من المعلومات بدءًا من البيانات البيومترية للمستخدمين إلى البيانات المكانية، كما أنها تحتوي أجهزة استشعار لمسح و مراقبة محيط المستخدم فضلاً عن شاشات العرض المثبتة على الرأس (HMDs) يمكن أن تجمع بعض البيانات الحيوية كحركة الرأس وتتبع العين للمستخدم، لذلك يجب أن تتعامل هذه الأجهزة مع البيانات وفقًا لبعض المبادئ التي تحمي خصوصية المستخدمين. كما دعى وزير الدولة للذكاء الاصطناعي في المنتدى الاقتصادي العالمي في دافوس إلى وضع قوانين جديدة لمنع الناس من ارتكاب جرائم القتل في الميتافيرس.[1]

و في هذا الصدد دخلت إمارة دبي (MetaHQ) ميتافيرس عن طريق قيام هيئة تنظيم الأصول الإفتراضية في دبي بشراء قطعة أرض في Sandbox Metaverse لتسهيل المشاركة بين مزودي خدمات الأصول الافتراضية، جاء ذلك بعد الإعلان عن هيئة تنظيم الأصول الإفتراضية (VARA) الخاص بإنشاء إطار قانوني و نظام متقدم للأصول الإفتراضية، مما يجعلها أول سلطة حكومية تستثمر في الميتافيرس.[2]

و بالرجوع للقانون رقم (4) لسنة 2022 بشأن تنظيم الأصول الافتراضية في إمارة دبي نرى أن المشرع نص في البندين (2,3) من المادة (10) على التزام الرئيس التنفيذي و موظفي السُّلطة بالمحافظة على سرية المعلومات و البيانات التي يتم الإطلاع عليها أو التي وصلت إلى علمهم بمناسبة العمل في السلطة، و الالتزام كذلك بعدم نشر أو إفشاء أو كشف أو نقل أي معلومات أو بيانات أو الاحتفاظ بأي مستندات أو وثائق سرية تتعلق بمُقدِمي خدمات الأصول الافتراضية أو المستفيدين أو تداولات منصات الأصول الافتراضية دون الحُصول على موافقة السُّلطة الخطية المسبقة، و يستمر هذا الالتزام حتى بعد انتهاء عملهم في السُّلطة.[3]

المطلب الثاني: القيود التي ترد على الحق في الخصوصية

هنالك عدة اعتبارات وقيود ترد على نطاق الحق في الخصوصية، فحق الخصوصية وإن كان مقدسا إلا أنه ليس مطلقا، وتتمثل القيود الواردة عليه، بالأمن الوطني، والمصلحة العامة والغايات التاريخية، وغيرها، ونتطرق لهذه القيود فيما يأتي:

1 Shead, S (May 2022), Serious crime in the metaverse should be outlawed by the U.N, UAE minister says. CNBC.com, published in; https://www.cnbc.com/2022/05/25/metaverse-murders-need-to-be-policed-says-uae-tech-minister.html. Access date: 26/05/2022.

2 Pymnts (May 2022). Dubai's Virtual Assets Regulatory Authority Opens Sandbox-Based Metaverse HQ, PYMNTS.com, published in https://www.pymnts.com/metaverse/2022/dubais-virtual-assets-regulatory-authority-opens-sandbox-based-metaverse-hq/ Access date: 06/06/2022.

3 انظر المادة (10) من قانون رقم (4) لسنة 2022 بشأن تنظيم الأصول الافتراضية في إمارة دبي، المنشور في الجريدة الرسمية لحكومة دبي، السنة 56، في العدد 559، 11 مارس 2022م، المنشور على:

https://dlp.dubai.gov.ae/Legislation%20Ar%20Reference/2022/الأصول%20تنظيم%20بشأن%20202022%20لسنة%20(4)%20رقم%20قانون%20افتراضية.pdf , Access date: 19/06/2022.

الفرع الأول: الأمن القومي

حددت التوصية الأوروبية في العام 2002 الأمن القومي بأنه: "أمن الدولة، و الدفاع و السلامة العامة"، و قد تطور مفهوم الأمن القومي ليشمل السلامة المادية للشخص أو الوطن و الأمن الاقتصادي و الأمن الاجتماعي، و سنتطرق هنا إلى المراقبة الإلكترونية كإجراء استدلالي، و كذلك كعقوبة بديلة:

المراقبة الإلكترونية كإجراء استدلالي[1]، و من أهم التقنيات التي برزت في شأن المراقبة البرمجية:

أ) تقنية برنامج كارنيوز.[2]

ب) تقنية تعقب المواد الإباحية.[3]

المراقبة الإلكترونية كعقوبة بديلة:

ونشير هنا إلى المراقبة الالكترونية كعقوبة بديلة للعقوبة السالبة للحرية، أو ما يطلق عليها (السوار الالكتروني)، أو (القبض تحت المراقبة الإلكترونية)[4]، وهي نظام حديث لتنفيذ العقوبة السالبة للحرية بطريقة مبتكرة خارج السجن في الوسط الحر بين أفراد المجتمع حيث يتقيد فيها المحكوم عليه أو الخاضع للمراقبة فتواجده في مكان معين خلال أوقات محددة غالباً ما تكون خلال الفترة من السابعة مساءً إلى السابعة صباحاً لليوم التالي، و تكون هذه المراقبة لفترة زمنية بناءً على حكم قضائي، و قد نص على ذلك المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم و العقوبات في المادة (80) على أنه: "من حكم عليه بالسجن المؤبد أو المؤقت في جريمة ماسة بأمن الدولة الخارجي أو الداخلي أو في جريمة تزييف نقود أو تزويرها أو تقليدها أو تزوير طوابع أو مستندات مالية حكومية أو محررات رسمية أو في جريمة رشوة أو اختلاس أو سرقة أو قتل عمد، يوضع بحكم القانون بعد انقضاء مدة عقوبته تحت مراقبة الشرطة وفقا للقواعد التي يحددها وزير الداخلية مدة مساوية لمدة العقوبة على أن لا تزيد على خمس سنوات".

ومع ذلك يجوز للمحكمة في حكمها أن تخفف مدة المراقبة أو أن تأمر بإعفاء المحكوم عليه منها أو أن تخفف قيودها[5]. ويعاقب المحكوم عليه الذي يخالف شروط المراقبة بالحبس مدة لا تزيد على سنة وبغرامة لا تزيد على

---

1 أو المراقبة البرمجية، و يعني ذلك قيام المراقب–شخص ذو خبرة و كفاءة عالية في الأمور التقنية – باستخدام التقنية في جمع المعلومات و البيانات للمشتبه به سواء كان ذلك شخصاً أو مكاناً أو موقعاً إلكترونياً مما اساؤا استخدام الوسائل التقنية بصور غير مشروعة كإجراء أمني، و يتمثل ذلك في مراقبة الهكر ممن استطاع الولوج إلى الحاسب الآلي للمجني عليه مما ترتب على ذلك انتهاك للخصوصية، و لا يجوز إجراء المراقبة البرمجية إلا بعد استخراج إذن من النيابة.

2 تقنية تابعة لإدارة المعلومات في مكتب التحقيقات الفيدرالي، تهدف إلى تعقب و فحص رسائل البريد الالكتروني الصادرة و الواردة لجميع الشركات و التي يشتبه أنها تحمل معلومات عن الجرائم الجنائية، و لا يتم تنفيذها إلا بعد صدور إذن من المحكمة المختصة بالولايات المتحدة الأمريكية بوضع أجهزة تلك الشركة تحت المراقبة، و قد حققت هذه التقنية النجاح الكبير في تعقب المجرمين و رصدهم للقبض عليهم في القضايا المتعلقة بالأمن القومي، كالأدلة التي قدمت لمكتب التحقيقات الفيدرالي لإدانة قائد ميلشيات قامت باستخدام شبكات الانترنت للمراسلة و التخطيط للدخول إلى منشآت عسكرية و تفجير محطات للطاقة في جنوب شرق الولايات المتحدة الأمريكية.

انظر، فاطمة، مرنيز (2016). المراقبة الإلكترونية كإجراء استدلالي في مواجهة الحق في الخصوصية. *مجلة الحقيقة*. (38)*15*، ص109، منشور على الموقع:

https://el-hakika.univ-adrar.edu.dz/index.php?journal=JLS&page=article&op=view&path%5B%5D=334 Access date:6/5/2022.

3 أو ما يسمى ببرنامج "نوبد شرطة الإنترنت"، الهدف من هذه التقنية هو البحث عن الصور الجنسية المخلة على أجهزة الحاسب الآلي، و من ثم إبلاغ الهيئات الحكومية عنها.

انظر، فاطمة، مرنيز. مرجع سابق. ص109.

4 أسبانيا، سويسرا، بلجيكا، الولايات المتحدة الأمريكية.

5 انظر المادة (115) من المرسوم بقانون اتحادي رقم (31) لسنة 2021م بإصدار قانون الجرائم و العقوبات.

(50,000) خمسين ألف درهم أو بإحدى هاتين العقوبتين[1]، كما نص المشرع في القانون ذاته على نظام المراقبة الشرطية في المادة رقم (423) على أنه: "في حالة الحكم بالإدانة في إحدى الجرائم المنصوص عليها في هذا الفرع بعقوبة مقيدة للحرية لمدة سنة فأكثر يوضع المحكوم عليه تحت مراقبة الشرطة مدة مساوية لمدة العقوبة المحكوم بها".[2]

بالرغم مما تم استعراضه سابقاً باعتبار الأمن القومي أحد الاستثناءات الواردة على خصوصية الشخص، إلا أن القانون أعطى الجهة المنفذة سلطة مقيدة لا يجوز تجاوزها من قبل من يقوم بالإشراف على تنفيذ العقوبة، ففي نظام المراقبة الشرطية أعطى القانون الجهة التنفيذية سلطة مراقبة المحكوم عليه فترة معينة، مع الاحتفاظ بكامل الحق في الخصوصية للمحكوم عليه، فلو أتى المحكوم عليه بفعل مخالف للسلوك الذي يجب أن يكون عليه في هذه الفترة فلا تستطيع السلطة التنفيذية التعدي على خصوصيته–كالتنصت على الكالمات أو الإطلاع على المحادثات بين المحكوم عليه و أطراف أخرى–إلا بعد استخراج أذن من النيابة العامة أو السلطة المخولة بذلك في بعض الحالات، و هذا ما أكدته المادة (356) من المرسوم بقانون اتحادي رقم (17) لسنة 2018م و التي تنص على أنه: "..... و في جميع الأحوال، يجب أن يراعي في الوسائل الإلكترونية المنصوص عليها في الفقرة السابقة، احترام كرامة و سلامة و خصوصية الخاضع لها"[3]، هذا بالإضافة للبند الرابع من المادة الخامسة من قرار مجلس الوزراء رقم (53) لسنة 2019 في شأن تنفيذ المراقبة الإلكترونية التي أكدت الشأن ذاته فقد نصت على أنه: "من مواصفات الوسيلة الإلكترونية الخاصة بالمراقبة 4. ضمان الخصوصية و حرمة الحياة الخاصة"[4] بالنسبة للشخص الخاضع للمراقبة الإلكترونية.

و في الشأن ذاته عند النظر للقوانين المقارنة، نرى أن المشرع الأمريكي سن قانون باتريوت (The USA PATRIOT Act) و الذي تم إصداره في 26 أكتوبر 2001، بهدف مكافحة الإرهاب و قد نصت أحد مواده على السماح للحكومة بتوسيع صلاحيات المخابرات في أعمال المراقبة للأفراد الذين يتبعون جهات أجنبية في الولايات المتحدة دون ضوابط تتعلق بالشخص أو المكان، مما قد يخالف ما نص عليه الدستور الأمريكي. أما المشرع الفرنسي فقد ذهب إلى وضع عدة قوانين لمكافحة الإرهاب من أهمها قانون مكافحة الإرهاب الصادر في 2006م، و الذي يوسع من صلاحيات رجال الأمن في المراقبة و التتبع و الترصد على شبكة الانترنت.[5]

الفرع الثاني: الصحة العامة

من القيود الأخرى على حماية الحق في الخصوصية الحفاظ على صحة أفراد المجتمع، فالمصلحة العامة تقدم على المصلحة الخاصة، ففي حال انتشار أحد الأوبئة أو الأمراض المعدية في أحد الدول أو العالم ككل، في هذه الحالة يمكن للجهة المعنية بالحفاظ على الصحة من الاطلاع على البيانات الصحية لأي فرد يعيش على أرض الدولة التى انتشر فيها الوباء. و هذا ما حدث فعلياً عند انتشار فايروس كورونا المستجد، فوزارة الصحة و وقاية المجتمع بالتعاون

1 انظر مادة (80) من المرسوم بقانون اتحادي رقم (31) لسنة 2021م بإصدار قانون الجرائم و العقوبات.

2 المادة (423) من المرسوم بقانون اتحادي رقم (31) لسنة 2021م بإصدار قانون الجرائم و العقوبات.

3 المادة (356) من المرسوم بقانون اتحادي رقم (17) لسنة 2018م بتعديل بعض أحكام قانون الإجراءات الجزائية الصادر بالقانون الإتحادي رقم (35) لسنة 1995م، المنشور على موقع وزارة العدل.

4 البند الرابع من المادة الخامسة من قرار مجلس الوزراء رقم (53) لسنة2019م في شأن تنفيذ المراقبة الإلكترونية، المنشور في العدد 660 من الجريدة الرسمية.

5 انظر النمر، وليد سليم (2017). حماية الخصوصية في الإنترنت (ص355). الطبعة الأولى. الإسكندرية: دار الفكر الجامعي.

مع الهيئة الوطنية لإدارة الطوارئ و الأزمات و الكوارث في دولة الإمارات العربية المتحدة يمكنها الإطلاع على الملف الصحي لأي فرد من الأفراد المقيمين على أرض الدولة بدون طلب أذن من ذلك الفرد و بدون الرجوع إليه أيضاً، و السبب في وضع هذا القيد هو الحد من انتشار هذا الوباء من خلال إمكانية عزل المصابين لحماية الصحة العامة، و قد أعطى القانون الإتحادي رقم 14 لسنة 2014 في شأن مكافحة الأمراض السارية صلاحية الإطلاع على الملفات الطبية لجميع الأفراد من قبل الوزارة و الجهة الصحية في حالة تفشي أحد الأوبئة و الأمراض الخطيرة و التى قد تهدد سلامة الجميع، و هذا ما نصت عليه المادة (7) من القانون أعلاه بإعطاء صلاحية اتخاذ الإجراءات اللازمة بالتنسيق مع الجهات المختصة من قبل الوزارة و الجهة الصحية، و هذا ما أكده الدستور في المادة (19) بكفالة المجتمع للمواطنين وسائل الوقاية و العلاج من الأمراض و الأوبئة، و بالرغم من أن المادة (29) من الدستور أكدت على حرية التنقل للأفراد إلا أن ما يحدث في حال تفشي الأوبئة من تقييد لحرية الأفراد[1] لا يعتبر عدم تطبيق لنص الدستور إنما هو استثناءً لفترة زمنية حتى انتهاء الوباء. كما تم توظيف خوارزميات الذكاء الاصطناعي في أحد التطبيقات وهو تطبيق (الحصن)[2]، لسهولة الحد من انتشار هذا الوباء.

الفرع الثالث: القيود الواردة في المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية

لقد وضع المشرع الإماراتي ضوابط مشددة لحماية البيانات الشخصية الإلكترونية و لكنه استثنى بعض الحالات التي يمكن الإطلاع فيها على البيانات الشخصية، فقد نصت المادة (4) من المرسوم بقانون الإماراتي بشأن حماية البيانات الشخصية و التي جاءت بعنوان (حالات معالجة البيانات الشخصية بدون موافقة صاحبها) على عدة حالات يجوز فيها معالجة البيانات الشخصية بدون تطلب موافقة صاحب البيانات و هي كالتالي:

- أن تكون المعالجة ضرورية لإقامة أي من المطالبة بالحقوق و الدعاوى القانونية أو الدفاع عنها أو تتعلق بالإجراءات القضائية أو الأمنية: نص المشرع الإماراتي في البند الثالث من المادة الرابعة على ذلك، ففي حال كان المعالجة ضرورية للمطالبة بالحقوق أو الدفاع عنها سواء كانت هذه المطالبة تتعلق بالدعاوى المدنية أو الجزائية، أو المعالجة التي تتعلق بالإجراءات القضائية أو الأمنية كأن يكون من الضروري معالجة البيانات لغرض منع أو كشف جريمة بناءً على قرار قضائي أو أمر من المدعي العام يهدف إلى منع أو كشف أو متابعة الجرائم المرتكبة، أو في حال كانت هذه المعالجة ضرورية للإجراءات السابقة على وقوع الجرائم للكشف السريع عنها، كقيام الجهات الأمنية في الدولة بتسجيل بصمات من يقطن على أرض الدولة من مواطنين و مقيمين[3]، مما يهدف إلى بناء مجتمع آمن من خلال الكشف السريع و الدقيق الذي يوصل إلى مرتكب الجريمة.

---

1 المادة 18 من القانون الإتحادي رقم 14 لسنة 2014 في شأن مكافحة الأمراض السارية المنشور في الجريدة الرسمية، العدد (572)، السنة (44)، الموافق 2014/11/30.

2 تطبيق "مجتمع واعي" (البحرين)، تطبيقي "توكلنا، تباعد" (السعودية)، تطبيق "شلونك" (الكويت)، تطبيق "احتراز" (قطر) تطبيق "احمي" (تونس) تطبيق (CovidSafe) (أستراليا)، تطبيق "صحة مصر" (مصر).

انظر لطفي، سعد (ديسمبر 2020). "جائحة كورونا" تطبيقات التتبع الإلكتروني قد تهدد الخصوصية. المنشور على:

/https://www.scientificamerican.com/arabic/articles/news/tracking-applications-may-threaten-privacy

Access date:14/12/2021.

3 انظر سعد، سومية. خبر صحفي بعنوان "تسجيل بصمات جميع سكان دبي قريباً" بتاريخ 2022/03/21. جريدة الخليج. منشور على الرابط:

https://www.alkhaleej.ae/2022-03-21/الدار-أخبار-من-الإمارات/أخبار/قريباً-دبي-سكان-جميع-بصمات-تسجيل Access date:24/03/2022.

- أن تكون المعالجة مرتبطة بالبيانات الشخصية التي أصبحت متاحة و معلومة للكافة بفعل صاحب البيانات: وضعت الدولة العديد من التشريعات التي تحد من المعالجة غير المشروعة للبيانات الشخصية بدون موافقة صاحب البيانات موافقة صريحة خالية من عيوب الإرادة، و ذلك لأنها تنتهك خصوصية الأفراد في المجتمع، لكن في بعض الأحيان يقوم صاحب البيانات بنشر بياناته الشخصية على الملأ، فإذا نشرت هذه البيانات و أصبحت متاحة و معلومة لكافة الأفراد بفعلٍ من صاحب البيانات، فذلك يعطي مؤشراً بإمكانية معالجتها دون الرجوع لموافقة صاحب البيانات.

- أن تكون المعالجة ضرورية لأغراض الطب المهني أو الوقائي من أجل تقييم قدرة الموظفين على العمل، أو التشخيص الطبي أو تقديم الرعاية الصحية أو الاجتماعية أو العلاج أو خدمات التأمين الصحي أو إدارة أنظمة و خدمات الرعاية الصحية أو الاجتماعية وفقاً للتشريعات السارية في الدولة.

لا يشترط موافقة صاحب البيانات على معالجة بياناته الشخصية في مسائل معينة تدخل في الطب كأغراض الطب المهني أو الوقائي، فيهدف الطب المهني[1] إلى التركيز على تأثير العمل على صحة العاملين في قطاعات الدولة المختلفة، مما ينعكس إيجاباً على قوة العمل المستقرة نفسياً و بدنياً، و يؤدي إلى إنتاجية عالية و تقليل فترات الغياب عن العمل، من جانب آخر يهدف الطب الوقائي إلى الاستباقية في الوقاية من انتشار الأوبئة الصحية مما يؤدي لرفع الصحة العامة للمجتمعات البشرية، و كذلك اتخاذ الإجراءات السريعة في حال حدوثها منعاً من انتشارها و لحصر أضرارها، فمعالجة البيانات لهدف الطب الوقائي يهدف إلى التقليل من الأمراض الوراثية المنتشرة بين الأسر للحفاظ على صحة أفراد المجتمع.

- أن تكون المعالجة ضرورية لأغراض أرشيفية أو دراسات علمية و تاريخية و إحصائية وفقاً للتشريعات السارية في الدولة. الأصل عدم جواز الإطلاع على البيانات الشخصية للأفراد، لكن أجاز المشرع الإطلاع على بيانات الأفراد الشخصية إذا كانت المعالجة ضرورية لأغراض الأرشيف، أو للدراسات التاريخية كالأحداث المتعلقة برجال السياسة أو القضاء و القانون أو الدراسات العلمية و كذلك الإحصائية.

- أن تكون المعالجة ضرورية لتنفيذ عقد يكون صاحب البيانات طرفاً فيه أو لاتخاذ إجراءات بناءً على طلب صاحب البيانات بهدف إبرام عقد أو تعديله أو إنهائه.

تقابل هذه النصوص ما أورده المشرع الأوروبي في المادة السادسة من اللائحة الأوروبية، و التي تناولت قانونية المعالجة (Lawfulness of processing).

1 أو ما يسمى "طب العمل".

https://ar.wikipedia.org/wiki/طب_العمل , Access date:24/03/2022.

الفصل الثالث: مضمون الحماية القانونية للحق في الخصوصية المعلوماتية في تطبيقات الذكاء الاصطناعي

تمهيد و تقسيم

كرست المواثيق الدولية والتشريعات الوطنية مجموعة من المبادئ التي تضمن إجراء عملية جمع ومعالجة ونقل البيانات الشخصية بطريقة صحيحة وشفافة ونزيهة، كما أنها منحت صاحب الحق بخصوصية البيانات الشخصية العديد من الحقوق وفرضت مجموعة من الالتزامات على المسؤول عن تخزين ومعالجة ونقل هذه البيانات. ومن أهم هذه الحقوق، حق المستخدم في الاعتراض على جمع بياناته الشخصية، والحق في مراقبة هذه البيانات، وحق الدخول إليها والتعديل عليها وحق سحب البيانات الخاصة به، والحق في السلامة، والحق في النسيان. كما أن من أهم التزامات الأشخاص المسؤولين عن حفظ ومعالجة البيانات الشخصية وجوب إعلام المستخدم بالغاية من الجمع والمعالجة، وجوب الحصول على إذنه، وجوب استخدام وسائل تقنية آمنة وسليمة خلال عملية الجمع والمعالجة لمنع اختراق البيانات، وإذا تم الإخلال بأي من هذه الحقوق والالتزامات تنشأ مسؤولية القائمين على الجمع والمعالجة، وهو ما ندرسه، حيث سنتطرق أولاً لنطاق حماية الحق في الخصوصية المعلوماتية في التشريع الإماراتي و المقارن، ثم سنتطرق للمسؤولية عن المساس بهذا الحق في المبحث الثاني.

المبحث الأول: نطاق حماية الحق في الخصوصية المعلوماتية في التشريع الاماراتي والمقارن

تمهيد و تقسيم

كما أشرنا سابقاً إلى عناصر و مخاطر الحق في الخصوصية في ظل تطبيقات الذكاء الاصطناعي، فكان لابد من التطرق إلى البحث في أطر الحماية التي وضعتها القوانين الدولية و الوطنية لحماية الحق في الخصوصية في ظل تطبيقات الذكاء الاصطناعي، و هذا ما سنتطرق له في هذا المبحث حيث سنقسم المبحث إلى مطلب أول نتحدث فيه عن المبادئ الضامنة لمشروعية حماية الخصوصية المعلوماتية في ظل التشريع الاماراتي والمقارن و شروطها، ثم نتحدث عن حقوق المستخدم صاحب البيانات الشخصية و الالتزامات الملقاة على مشغلي تطبيقات الذكاء الاصطناعي المطلب الثاني.

المطلب الأول: المبادئ الضامنة لحماية الخصوصية المعلوماتية وشروطها

تنبهت الدول لضرورة تنظيم حماية الحق في الخصوصية المعلوماتية والبيانات الشخصية ووضعت التشريعات اللازمة لذلك، وقد تنوعت النماذج التشريعية المتبعة لتنظيم حماية الخصوصية والبيانات الشخصية، فمنها ما وضع نصوصاً صريحة في قوانين خاصة بحماية البيانات الشخصية، كالمرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية وقانون حماية البيانات الشخصية المصري رقم (151) لسنة 2020 والقانون الأردني بشأن حماية البيانات الشخصية لسنة 2022 والقانون التونسي بمشروع قانون أساسي عدد 2018/25 يتعلق

بحماية المعطيات الشخصية[1]، ومنها ما تطرق لمسألة حماية البيانات الشخصية في قوانين أخرى تنظم المعاملات الالكترونية أو حماية المستهلك بشكل عام، كما فعل المشرع العماني في الفصل السابع من قانون المعاملات الالكترونية لسنة 2008 والكويتي في قانون المعاملات الالكترونية، ومنها ما جاء بشكل قوانين شاملة تتضمن نصوصاً تحكم جمع ومعالجة وتخزين البيانات من قبل جهات في القطاعين العام والخاص ونقلها للخارج، وأوجدت هذه القوانين هيئة أو جهة تشرف على تطبيق القانون بشكل صحيح، كما في دول الاتحاد الأوروبي وكندا وأستراليا. بينما تتبنى دول أخرى نموذجاً يعتمد على القوانين القطاعية المتخصصة، حيث لا يتم وضع تشريع عام لحماية الخصوصية في كل المجالات، بل تصدر قوانين متخصصة لكل قطاع على حده، كالقوانين الخاصة بالخصوصية في القطاع البنكي، وسرية البيانات بقطاع عمل الشرطة، وفي قطاع الاتصالات، والسرية في مجال المحاماة، وميزة هذا النموذج أن يتواكب مع التطورات الحديثة، لكنه يتطلب سن قوانين جديدة بشكل مستمر، كذلك لا يوجد جهة عامة لمراقبة تطبيق القانون. بالمقابل، تترك بعض الدول، كاليابان والولايات المتحدة وسنغافورة، موضوع حماية الخصوصية والبيانات الشخصية لنموذج التنظيم الذاتي أو التبادلي[2]، حيث تؤسس من خلاله الشركات نظاماً خاصاً لتخزين ومعالجة البيانات والمعايير المتبعة من قبلها، فلا يكون لتدخل الدولة أثراً كبيراً، بل هو من عمل المؤسسات والشركات التي تعمل في مجال يتضمن معالجة وتخزين البيانات، فتقوم هي بوضع قواعد وسياسات للخصوصية تطبقها على كل من يتعامل معها، وهو ما نجده على مواقع مثل جوجل، وفيسبوك، وتويتر وغيرها.[3]

أما التشريع الأمريكي، فكما أشرنا أنه قد وضع تشريعات قطاعية لحماية الخصوصية، كما أنه سمح باللجوء لفكرة التنظيم الذاتي والتبادلي، قد نص المشرع الأمريكي في التعديل الرابع من الدستور[4] على أنه: "لا يجوز المساس بحق الشعب في أن يكونوا آمنين في أشخاصهم ومنازلهم ومستنداتهم ومقتنياتهم من أي تفتيش أو مصادرة غير معقولة"، فهو يؤكد على الحق في احترام الخصوصية. ونشير هنا إلى عدم وجود تشريع فيدرالي عام وشامل يضمن خصوصية البيانات وحمايتها، بل تحمى البيانات ضمن سياقات خاصة بقطاع معين، بالإضافة إلى أن هذه التشريعات تكون محلية أي صادرة من ولاية معينة و يكون تطبيقها في حدود الولاية، فقد سنت ولاية نيويورك تشريعات لحماية الخصوصية عبر الإنترنت تفرض العديد من إجراءات حماية سرقة الهوية، و بالرغم من التشريعات المحلية التي تسنها الولايات إلا أن هناك وكالة لإنفاذ الخصوصية في الولايات المتحدة الأمريكية وهي لجنة التجارة الفيدرالية (FTC)[5]، فاللجنة مسؤولة عن عدة قضايا تتعلق بالخصوصية وأمن البيانات كحماية خصوصية الأطفال على الإنترنت وحماية المعلومات الشخصية للمستهلكين؛ وحمايتهم من الممارسات غير القانونية [6]، بالإضافة إلى حالات البريد العشوائي وبرامج

1 http://www.inpdp.nat.tn/Receuil_INPDP.pdf, Access date:19/05/2022.

2 عائشة كركيط، مرجع سابق، ص271.

3 انظر، خصاونه، علاء الدين و فراس، الكساسبه و درادكه، لافي محمد. (2011). الحماية القانونية للخصوصية و البيانات الشخصية في نطاق المعلوماتية. *مجلة جامعة الشارقة للعلوم الشرعية و القانونية*. (2)*8*، ص190.

4 دستور الولايات المتحدة الأمريكية الصادر في 1789 شاملاً تعديلاته لغاية 1992، والمنشور من قبل

https://www.constituteproject.org/constitution/United_States_of_America_1992.pdf?lang=ar Access date:16/01/2022.

5 Federal Trade Commission.

6 Federal Trade Commission 2020 Privacy and Data Security Update, May 2021.

https://www.ftc.gov/reports/federal-trade-commission-2020-privacy-data-security-update Access date: 16/01/2022.

التجسس وقد اقترحت اللجنة تطبيق آلية عدم التتبع في 2010 وأصدرت إرشادات وأفضل الممارسات للتنظيم الذاتي. ونشير أيضا إلى القانون الفيدرالي للحماية ضد التنصت لسنة 1968 The Federal Wiretap Statute وقانون حماية الخصوصية في مجال الاتصالات الإلكترونية لسنة 1986 Electronic Communications Privacy Act (ECPA)، وقانون الحق في الخصوصية لسنة 1994 (privacy act) وقوانين الولايات، كاليفورنيا، قانون باتريوت لسنة 2001 (قانون مكافحة الإرهاب)، وقانون الحرية الأمريكي لعام 2015، وهذا القانون يوجب التدمير الفوري لجميع سجلات تفاصيل المكالمات، ويحاول القانون أيضًا اتخاذ خطوات لزيادة شفافية الرقابة الحكومية من خلال اشتراط النشر السنوي لـعدد الطلبات المطلوبة والممنوحة وكذلك عدد الأشخاص الأمريكيون الذين تم استهدافهم. وقانون المسمى (HIPAA)[1] والخاص بحماية الخصوصية الطبية في البيئة الرقمية، وقانون حماية الخصوصية PPA، وقانون حماية خصوصية الأطفال على شبكة الإنترنت (COPPA 1998).

وبالنسبة للتشريع الأوروبي، فقد تبنى الاتحاد الأوروبي النموذج الأول كما أشرنا، وأوجب على الدول المنظمة للاتحاد أن توائم تشريعاتها مع التوجيهات والإرشادات التي تصدرها عبر مجلس أوروبا واللجنة الأوروبية والاتحاد الأوروبي. فقد وضعت التوجيهات الأوروبية التي صدرت في هذا المجال الركيزة القانونية للتعامل مع البيانات الشخصية في دول الاتحاد الأوروبي وضمان مستوى معين من الحماية لمواطني الاتحاد الأوروبي وقد سمحت بالتدفق الحر للبيانات الشخصية في إطار دول الاتحاد الأوروبي، ولكنها بالمقابل تبنت مبدأ الميناء الآمن وكرست مجموعة من المبادئ الواجب احترامها عند تعامل الشركات الأمريكية مع بيانات الأفراد الشخصية التي تنقل إليها. ومن هذه الإرشادات التوجيه الأوروبي لسنة 1995 وتوجيه 1997 وأخيراً اللائحة العامة لحماية البيانات. وبخلاف التشريع الأمريكي الذي لا يوجد فيه تشريع فيدرالي عام وشامل فإن التشريع الأوروبي يتضمن تشريعاً عاماً و شاملاً لحماية الخصوصية لأفراد الاتحاد الأوروبي داخل وخارج الاتحاد على حد السواء، فقد جاءت اللائحة العامة الأوروبية لحماية البيانات (GDPR)[2]، لتقر بضرورة حماية البيانات الشخصية لأفراد الاتحاد الأوروبي من خلال وضع ضوابط وأسس تلزم القائمين على العمل في مجال البيانات الشخصية بحمايتها من أي انتهاك يطرأ عليها سواء داخل الاتحاد الأوروبي أم خارجه. من خلال استعراض أهم التشريعات المنظمة لحماية البيانات الشخصية على المستوى الأوروبي والأمريكي والوطني نجد أن هنالك عدة مبادئ تحكم معالجة البيانات الشخصية وحفظها وتداولها. كما فرضت مجموعة من الالتزامات بخصوص التأكد من أن البيانات الشخصية الخاصة بالمواطن الأوروبي تحظى بنفس مستوى الحماية عند نقلها للخارج أو عند معالجتها خارج حدود الاتحاد الأوروبي، ويحظر نقلها لدول لا توفر هذا المستوى من الحماية، كما تفرض التزامات على جهات المقدمة لخدمة الاتصالات الالكترونية والانترنت، ونعرضها في الآتي:

الفرع الأول: المبادئ الضامنة لمشروعية حماية الخصوصية المعلوماتية في ظل التشريع الاماراتي والمقارن

أقرت اللائحة العامة لحماية البيانات مجموعة من المبادئ الأساسية لحماية البيانات الشخصية التي تضمن جمع ومعالجة البيانات الشخصية بشكل مشروع وخصصت هذه اللائحة حماية فعالة للبيانات الحساسة، كالبيانات

1 Health Insurance Portability and Accountability Act.

2 General Data Protection Regulation.

الصحية والبيومترية والبيانات الخاصة بالمعتقدات والتوجهات الفكرية، بالإضافة إلى حماية الحق في خصوصية الأطفال عند معالجة البيانات الشخصية للأطفال[1]. كما أوجدت التشريعات الوطنية وجوب وجود جهة رقابية تشرف على تنفيذ القانون، كالمفوض أو المراقب أو مسجل البيانات. وهذه المبادئ هي:

المبدأ الأول- المسؤولية: أي أن يتم تحديد وتوثيق سياسات وإجراءات الخصوصية المتعلقة بجهة التحكم واعتمادها من قبل المسؤول الأول بالجهة (أو من يفوضه)، ونشرها إلى جميع الأطراف المعنية بتطبيقها.

المبدأ الثاني- الشفافية: أن يتم إعداد إشعار عن سياسات وإجراءات الخصوصية الخاصة بجهة التحكم يحدد فيه الأغراض التي من أجلها تم معالجة البيانات الشخصية وذلك بصورة محددة وواضحة وصريحة[2].

المبدأ الثالث- الاختيار والموافقة: أن يتم تحديد جميع الخيارات الممكنة لصاحب البيانات الشخصية والحصول على موافقته (الضمنية والصريحة) فيما يتعلق بجمع بياناته واستخدامها أو الإفصاح عنها. يقوم الفرد باستخدام بياناته الشخصية في كثير من المعاملات اليومية التي يجريها بمساعدة تطبيق من تطبيقات الذكاء الاصطناعي و قد تكون هذه البيانات من البيانات الشخصية الحساسة التي لا يجوز لأي طرف الاطلاع عليها أو معالجتها غير أن يكون مخول بذلك و بموافقة صاحب البيانات، وهذا ما أكده المشرع الإماراتي في المادة (4) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية بنصه على أن: "يُحظر معالجة البيانات الشخصية دون موافقة صاحبها"[3]، و قد عرف المشرع الإماراتي الموافقة في المادة الأولى من المرسوم بقانون ذاته بأنها: "الموافقة التي يصرح فيها صاحب البيانات للغير بمعالجة بياناته الشخصية، على أن تكون هذه الموافقة بشكل محدد و واضح لا لبس فيه على قبوله بمعالجة بياناته الشخصية من خلال بيان أو إجراء إيجابي واضح". يتبين لنا من خلال النصين السابقين أن أي معالجة للبيانات الشخصية أو البيانات الحساسة للأفراد خارج إطار النص وفي غير الأحوال المنصوص عليها في القانون استثناءً أو التي لم ترد في اللائحة التنفيذية يعتبر اختراقاً و انتهاكاً للبيانات الشخصية. كما تبنى المشرع المصري الرأي ذاته في المادة (2) من القانون رقم 151 لسنة 2020 بإصدار حماية البيانات الشخصية بنصه على أنه: "لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح أو الإفشاء عنها بأية وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانوناً"[4]، وأكدت ذلك المادة السادسة من ذات القانون بخصوص مشروعية معالجة البيانات الشخصية بشرط موافقة صاحب البيانات على إجراء المعالجة ومن أجل تحقيق غرض محدد أو أكثر، وأوجبت المادة (1/12) منه ضرورة الموافقة الكتابية الصريحة على جمع ومعالجة البيانات الحساسة أو نقلها أو تخزينها أو حفظها أو إتاحتها للغير. وحسناً فعل المشرع المصري عندما شمل في حظره أي إجراء وفعل يترتب على البيانات الشخصية ويؤدي إلى المساس بالخصوصية. وهو نفس النهج الذي سار عليه المشرع الأوروبي في المادة

1 Alkhasawneh, A. (2020). The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do We Need to Comply with the GDPR? Journal of Legal, Ethical and Regulatory Issues. 23(2).1-19.

2 See article 5 / 1(B) of Regulation (EU) 2016/679, B. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3 المادة (4) من المرسوم بقانون رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية المنشور في الجريدة الرسمية في العدد 712 (ملحق 1)، السنة الواحدة و الخمسون 19 صفر 1443هـ - الموافق 26 سبتمبر 2021م.

4 المادة (2) من القانون رقم 151 لسنة 2020م بإصدار حماية البيانات الشخصية المنشور في العدد 28 من الجريدة الرسمية، 15 يوليو 2020.

(11/4) من اللائحة العامة لحماية البيانات الشخصية (GDPR) [1]، و هي بمثابة قانون ينظم آلية حماية خصوصية البيانات الشخصية لأفراد الاتحاد الأوروبي، و لا يقتصر على حماية البيانات داخل الاتحاد الأوروبي بل يتعدى إلى خارجه ، فقد نص في مادته السادسة من اللائحة بأن المعالجة لا تكون قانونية إلا بموافقة صاحب البيانات على معالجة ما يتعلق به من بيانات شخصية بالإضافة إلى وضعه ضوابط و شروط لموافقة صاحب البيانات التي سيتم معالجتها في المادة (7) من اللائحة ذاتها، فعندما تعتمد معالجة البيانات على الموافقة يجب أن يكون المتحكم بالبيانات قادراً على إثبات أن صاحب البيانات قد وافق على معالجة بياناته الشخصية، وإذا تم منح الموافقة في سياق إعلان مكتوب يتعلق أيضاً بمسائل أخرى يجب تقديم طلب الموافقة بطريقة يمكن تمييزها بوضوح عن المسائل الأخرى وبشكل صريح يسهل الوصول إليه وبلغة صريحة وواضحة، كما يحق لصاحب البيانات سحب موافقته في أي وقت وأن يكون الانسحاب متاحاً بنفس سهولة منح الموافقة. كما أفرد المادة الثامنة لشروط موافقة الطفل فيما يتعلق بجمع بياناته ومعالجتها، نرى من خلال ذلك أن رضا صاحب البيانات في معالجة بياناته الشخصية يشكل ركناً هاماً من أركان معالجة البيانات الشخصية سواء في اللائحة الأوروبية أو قانون حماية البيانات الشخصية المصري وقانون حماية البيانات الشخصية الإماراتي. ومن جانب آخر، فقد تفرد المشرع الأوروبي بالمادة (9)، فبالرغم من إعطاء الأهمية الكبيرة لرضا صاحب البيانات في معالجة بياناته إلا أن هناك أنواعاً محددة من البيانات لا يجوز معالجتها حتى مع وجود رضا صاحب البيانات وبشروط معينة على سبيل الحصر، ومن هذه البيانات تلك ذات الطبيعة الحساسة. وقد أكدت المادة (7) من القانون الفرنسي على ضرورة الموافقة الصريحة لصاحب البيانات الشخصية حتى تتم معالجة بياناته.

المبدأ الرابع- الحد من جمع البيانات: أن يقتصر جمع البيانات الشخصية على الحد الأدنى من البيانات الذي يمكن من تحقيق الأغراض المحددة في إشعار الخصوصية.[2]

المبدأ الخامس- الحد من استخدام البيانات والاحتفاظ بها والتخلص منها: أي أن يتم تقييد معالجة البيانات الشخصية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة، والاحتفاظ بها طالما كان ذلك ضروريًا لتحقيق الأغراض المحددة أو لما تقتضيه الأنظمة واللوائح والسياسات المعمول بها وإتلافها بطريقة آمنة تمنع التسريب أو الفقدان أو الاختلاس أو إساءة الاستخدام أو الوصول غير المصرح به.

المبدأ السادس- الوصول إلى البيانات: أن يتم تحديد وتوفير الوسائل التي من خلالها يمكن لصاحب البيانات الوصول إلى بياناته الشخصية لمراجعتها وتحديثها وتصحيحها.

المبدأ السابع- الحد من الإفصاح عن البيانات: أن يتم تقييد الإفصاح عن البيانات الشخصية للأطراف الخارجية بالأغراض المحددة في إشعار الخصوصية والتي من أجلها قدم صاحب البيانات موافقته الضمنية أو الصريحة.

1 General Data Protection Regulation.

2 See article 5 / 1(C) of Regulation (EU) 2016/679, C. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’).

المبدأ الثامن- أمن البيانات: أن يتم حماية البيانات الشخصية من التسرب أو التلف أو الفقدان أو الاختلاس أو إساءة الاستخدام أو التعديل أو الوصول غير المصرح به.[1]

المبدأ التاسع- جودة البيانات: أن يتم الاحتفاظ بالبيانات الشخصية بصورة دقيقة وكاملة وذات علاقة مباشرة بالأغراض المحددة في إشعار الخصوصية.[2]

المبدأ العاشر- المراقبة والامتثال: أن يتم مراقبة الامتثال لسياسات وإجراءات الخصوصية الخاصة بمراقب البيانات، وأن يتم معالجة أي استفسارات وشكاوى ونزاعات متعلقة بالخصوصية.

الفرع الثاني: الشروط القانونية لمعالجة البيانات الشخصية

أوردت التشريعات المنظمة لعملية جمع ومعالجة البيانات الشخصية وانتقالها للخارج مجموعة من الشروط القانونية التي لابد من توافرها لضمان مشروعية معالجة هذه البيانات الكترونيا، وهذه الشروط تتمثل بما يأتي:

أولا: ضرورة أن يتم جمع البيانات لأغراض مشروعة ومعلنة لصاحب البيانات، وهذا تطبيق واضح لمبدأ الشفافية[3]، وقد نصت على ذلك المادة (3) من القانون المصري الخاص بحماية البيانات الشخصية حيث جاء فيها: "يجب لجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني". وهو ما أكده قانون حماية البيانات الشخصية الفرنسي في المادة السادسة منه. نلاحظ أن هذه النصوص تستلزم إخطار الشخص المعني بعملية جمع البيانات الخاصة به بصورة محددة وبيان الغرض منها وتحديد أنواع البيانات المنوي جمعها ومعالجتها وإذا تم جمع هذه البيانات دون علم صاحب البيانات اعتبرت عملية جمعها غير مشروعة.

ثانيا: يجب أن تجمع البيانات الشخصية بشكل صحيح وآمن وسليم، وهو ما ورد في المادة الثالثة من قانون حماية البيانات الشخصية المصري التي نصت على أن: "يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية: ... 2- أن تكون صحيحة وسليمة ومؤمنة". وهو ما نصت عليه أيضا الفقرة الخامسة من المادة السادسة من القانون الفرنسي السابق الإشارة إليه.

ثالثا: يجب معالجة البيانات الشخصية بطريقة مشروعة وملائمة للغرض الذي تم جمعه من أجله، وهذا ما أكدته المادة الثالثة من القانون المصري بقولها: 3- "أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم جمعها من أجلها". والمادة السادسة من اللائحة العامة لحماية البيانات الشخصية والمادة السادسة من القانون الفرنسي. وهذا يتضمن بالإضافة إلى إعلام الشخص المعني بعملية المعالجة إعلامه أيضا بأساليب وإجراءات المعالجة والغاية منها بشكل دقيق وقبل البدء بعملية المعالجة. ويجب أن تتم معالجة البيانات الشخصية بطريقة تتلاءم مع الغرض من جمع البيانات،

---

1 انظر البند السادس من المادة الخامسة "ضوابط معالجة البيانات الشخصية" من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، و التي نصت على:"أن تكون البيانات الشخصية محفوظة بشكل آمن بما فيها حمايتها من أي انتهاك أو اختراق أو معالجة غير مشروعة ....".

2 See article 5 / 1(D) of Regulation (EU) 2016/679, D. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').

3 انظر التهامي، سامح . مرجع سابق. ص406.

ليبقى الغرض من جمع البيانات الشخصية هو الفيصل لمشروعية كل إجراء من إجراءات معالجة البيانات الشخصية، فلو طلبت منه البيانات من أجل خدمة معينة فلا يجوز استخدامها لخدمة أخرى إلا بعد إعلامه وبعد الحصول على موافقته الصريحة وإلا كانت عملية الجمع والمعالجة غير مشروعة.[1]

رابعا: عدم الاحتفاظ بالبيانات الشخصية لمدة أطول من المدة اللازمة لتحقيق الغرض من جمع هذه البيانات ومعالجتها، وهذا يعني أن يحتفظ بالبيانات الشخصية لمدة كافية لتحقيق الغرض من جمعها وألا تتجاوز ذلك، وأن تتم مراجعة البيانات الشخصية المخزنة بشكل دوري وإلغاء ما تم تحقيق الغاية من جمعه منها، وإلا كانت عملية الجمع والمعالجة غير مشروعة. وقد نصت على ذلك المادة الثالثة من القانون المصري حيث جاء فيها: "4- ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها". وهو ما أوردته المادة السادسة من القانون الفرنسي في الفقرة الخامسة منها، و كذلك المادة الخامسة من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية الإماراتي.[2]

المطلب الثاني: حقوق صاحب البيانات والتزامات المسؤول عن تخزين ومعالجة البيانات الشخصية

تحدثنا في المطلب السابق من هذا الفصل عن المبادئ الضامنة لحماية الخصوصية في التشريع الإماراتي والمقارن، وأوضحنا من خلالها أن هنالك مجموعة من الحقوق التي يملكها صاحب البيانات والتي نص عليها القانون، بالمقابل هنالك مجموعة من الالتزامات المفروضة على مشغلي تطبيقات الذكاء الاصطناعي لضمان حماية الحق في خصوصية البيانات الشخصية، ونتعرض في الفرع الأول لحقوق صاحب البيانات، ثم نتحدث عن التزامات المسؤول عن تخزينها ومعالجتها.

الفرع الأول: حقوق صاحب البيانات الشخصية

صاحب البيانات أو الشخص المعني بالبيانات هو كل شخص طبيعي تنسب إليه البيانات الشخصية المعالجة الكترونيا وتدل عليه وتمكن من تمييزه عن غيره. وقد عرفته المادة الرابعة من اللائحة العامة لحماية البيانات بأنه: "الشخص الطبيعي الذي يمكن التعرف عليه أو يمكن تحديده بشكل مباشر أو غير مباشر وخاصة الرجوع إلى رقم الهوية أو إلى عامل أو أكثر من العوامل المحددة لهويته البدنية أو الفيسيولوجية أو العقلية أو الاقتصادية أو الاجتماعية".

وقد أعطت التشريعات الدولية والوطنية عدداً من الحقوق لصاحب البيانات الشخصية[3] سواء أثناء حفظها ومعالجتها أو أثناء نقلها للخارج. و في هذا الشأن أورد المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية حقوق صاحب البيانات في المواد (13–18)[4]، وهذه الحقوق هي: الحق في الوصول إلى البيانات

1 راجع، التهامي، سامح. مرجع سابق. ص411.

2 انظر البند السابع من المادة الخامسة، نص المشرع على: "عدم الاحتفاظ بالبيانات الشخصية بعد استنفاذ الغرض من معالجتها".

3 عرف المشرع الإماراتي صاحب البيانات الشخصية في المادة الأولى من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية بأنه: "الشخص الطبيعي موضوع البيانات الشخصية".

4 تقابلها المواد (12– 23) من الفصل الثالث من اللائحة الأوروبية GDPR، و كذلك المادة الثانية من القانون المصري رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية.

وتعديلها، الحق في حذف البيانات وسحبها، الحق في الحماية من أنشطة المعالجة غير المشروعة أو نقلها للخارج، الحق في الحصول على إذن لاستخدام البيانات في بعض الظروف والأغراض، وندرس هذه الحقوق:

أولا: حق صاحب البيانات بالاطلاع على البيانات الشخصية الخاصة به والعلم بها أو الحصول عليها

وقد أطلقت عليه بعض التشريعات حق النفاذ أو الوصول أو الدخول إلى البيانات الشخصية (Right of the access to data)[1]، أو كما تسميه بعض التشريعات أيضاً حق الولوج[2]، فهذا الحق يتمثل في إمكانية الوصول لهذه البيانات دون أية قيود أو تأخير غير مبرر أو أعباء مالية لمراقبة مدى احترام قواعد معالجة البيانات الشخصية المنصوص عليها قانونا. وقد أعطت المادة (15) من اللائحة العامة لحماية البيانات الشخصية لصاحب البيانات الحق في العلم بها أو الحصول على المعلومات الآتية؛ أغراض المعالجة، أنواع البيانات الشخصية المعنية، المستلمون الذين تم الكشف عن البيانات الشخصية لهم أو من سيتم الكشف لهم عنها خصوصاً إذا كانون في بلدان ثالثة، المدة التي سيتم تخزين البيانات خلالها أو على الأقل المعايير المستخدمة لتحديد تلك المدة، وجود حق تصحيح أو محو البيانات من وحدة التحكم أو تقييد معالجة البيانات الشخصية المتعلقة بموضوع البيانات أو الاعتراض على هذه المعالجة، الحق في تقديم شكوى إلى جهة إشرافية. وقد نص المشرع الإماراتي على حق الشخص المعني بالاطلاع على البيانات دون أي مقابل في المادة (13) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية والتي جاءت تحت عنوان (حق الحصول على المعلومات)، كما نص على هذا الحق المشرع المصري في البند الأول من المادة (2) من الفصل الثاني في قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية في بيان حقوق الشخص المعني بالبيانات على أنه: "يكون للشخص المعني بالبيانات: 1– العلم بالبيانات الشخصية الخاصة به الموجودة لدى أي حائز أو متحكم أو معالج و الاطلاع عليها و الوصول إليها أو الحصول عليها". وأوردت المادة العاشرة من ذات القانون مجموعة من الإجراءات التي لا بد أن يحترمها المتحكم والمعالج وحائز البيانات الشخصية وتتمثل هذه الإجراءات ب: أن يتم ذلك بناء على طلب كتابي يقدم له من ذي صفة أو وفقا لسند قانوني، ضرورة التحقق من توافر المستندات اللازمة لتنفيذ الاحتفاظ بها، البت في الطلب ومستنداته خلال ستة أيام عمل من تاريخ تقديمه إليه، وإذا تم الرفض يجب أن يكون مسببا وإذا انقضت مدة الستة أيام دون رد كان ذلك في حكم الرفض. كما أكدت هذا الحق المادة (1/39) من قانون المعلوماتية و الحريات رقم (78) لسنة 1978 و المعدل بأحكام القانون رقم (1321) الصادر في 7 أكتوبر 2016، و بناءً على ما سبق فقد أعطى المشرع الأوروبي و المصري والإماراتي والفرنسي لصاحب البيانات حق الحصول والاطلاع على بياناته الشخصية بجميع محتوياتها كأنواع البيانات التابعة له، و أغراض المعالجة، و كذلك القرارات المتخذة بناءً على المعالجة المؤتمتة بما فيها التنميط[3]. وقد ذهب المشرع التونسي إلى إعطاء الحق لورثة صاحب البيانات الاطلاع على بيانات مورثهم الخاصة موضوع المعالجة (الفصل الرابع و

1 التشريع التونسي رقم (63) لسنة 2004 بتاريخ 27 يوليو 2004 يتعلق بحماية المعطيات الشخصية، المنشور في الجريدة الرسمية رقم 61 بتاريخ 30 يوليو 2004، المنشور على:

https://legislation-securite.tn/ar/law/40972 Access date: 14/04/2022.

2 القانون المغربي رقم (8) لسنة 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة البيانات ذات الطابع الشخصي.

3 للمزيد حول المعلومات التي يحق لصاحبها الإطلاع عليها انظر المادة (13) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

الثلاثون من القانون التونسي)، فإذا رفض المسؤول عن المعالجة ذلك ففي هذه الحالة يجوز لورثة صاحب البيانات أن يقدموا طلباً للجهة الإدارية خلال مدة محددة تبدأ من تاريخ الرفض.[1]

ثانيا: حق تعديل وتصحيح البيانات الشخصية

أعطى القانون الإماراتي في المادة (15) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية لصاحب البيانات الحق المطلق في تصحيح أو تعديل البيانات الشخصية دون تحديد مدة أو شروط لذلك، فقد ذهب في البند الأول من المادة إلى إعطاء الحق لصاحب البيانات في طلب تصحيح وتعديل بياناته الشخصية غير الدقيقة، أو استكمالها في حالة النقص لدى المتحكم دون تأخير غير مبرر لدى المتحكم. كما أعطى المشرع المصري الحق ذاته لصاحب البيانات في المادة (2) من قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية في بيان حقوق الشخص المعني بالبيانات والتي جاء من ضمنها في البند الثالث من المادة ذاتها، من حق صاحب البيانات التصحيح أو التعديل أو الإضافة أو التحديث للبيانات الشخصية، وأوجب المشرع المصري في المادة السابعة منه أن يقوم معالج البيانات أو المتحكم في حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ مركز البيانات الشخصية خلال 72 ساعة وإذا تعلق الخرق باعتبارات حماية الأمن القومي يكون الإبلاغ فورياً، وأن يبلغ الشخص صاحب البيانات خلال 3 أيام عمل من تاريخ الإبلاغ وما قام به من إجراءات. ولأهمية هذا الحق لصاحب البيانات ذهب المشرع الأوروبي على إدراجه في اللائحة العامة لحماية البيانات في المادة (16) بنصه على جواز تعديل صاحب البيانات لبياناته الشخصية دون تأخير غير مبرر من خلال تقديم بيان تكميلي لمراقب البيانات، بالإضافة إلى نص المشرع الفرنسي في المادة 40 من قانون المعلوماتية و الحريات رقم (78) لسنة 1978 و المعدل بأحكام القانون رقم (1321) الصادر في 7 أكتوبر2016 "لصاحب البيانات أن يطلب من المسؤول عن المعالجة تصحيحها أو تحديثها أو حذف أو أي بيانات شخصية تخصه متى تبين أنها غير دقيقة أو ناقصة أو مضلله أم مر عليها مدة زمنية طويلة أو تم تخزينها أو الكشف عنها بطريقة غير مشروعة"[2] ومنحه المشرع الفرنسي حق طلب تقديم دليل على أن المعالج قد قام بالفعل بتعديل البيانات أو إلغاءها والاطلاع عليها وأن يطلب نسخة من ذلك ولم يحدد المشرع الفرنسي وقتاً محدداً لقيام معالج البيانات بالرد على صاحب البيانات، لذا يجب أن تتم بمدة معقولة.

وذهبت بعض التشريعات إلى تقييد هذا الحق في تحديد المدة التي يمكن فيها لصاحب البيانات من تعديل بياناته كالتشريع المغربي الذي حدد مدة عشرة أيام لتصحيح البيانات الشخصية[3].وفي حال عدم قيام صاحب البيانات بتصحيح بياناته خلال المدة المذكور يتم رفض تصحيح البيانات، ويجب في هذه الحالة أن يقوم صاحب البيانات بإيداع طلب التصحيح لدى الجهة الإدارية المختصة، ومن ثم يتم تصحيح البيانات وفقاً للطلب المقدم.[4]

1 بدوي، عمرو طه. مرجع سابق. ص130-131.

2 بدوي، عمرو طه. مرجع سابق. ص132.

3 المادة (8) فقرة (أ) من القانون المغربي على أنه: "و يلزم المسؤول عن المعالجة بالقيام بالتصحيحات اللازمة دون عوض لفائدة الطالب داخل أجل عشرة أيام كاملة".

4 مرجع سابق.

ثالثا: حق حذف البيانات الشخصية (حق النسيان)

لا يوجد تعريف واضح ومحدد للحق في النسيان في التشريعات العربية أو الغربية[1]، وهو يعد أحد حقوق صاحب البيانات الشخصية الأخرى التي كرسها قرار المحكمة الأوروبية لحقوق الإنسان بتقرير مبدأ الحق في النسيان كأحد الحقوق التي يتمتع بها الشخص في مواجهة محركات البحث على شبكة الإنترنت[2]، وكرستها المادة (17) من اللائحة العامة لحماية البيانات (GDPR)[3] فقد منح المشرع الأوروبي في المادة 17 من اللائحة العامة لحماية البيانات الشخصية لصاحب البيانات الحق في مسح ونسيان بياناته الشخصية وفق شروطٍ معينة، كقيام المعالج بجمع ومعالجة البيانات بصورة غير قانونية، أو عند الانتهاء من الغرض الذي من أجله قام المعالج بجمع البيانات ومعالجتها. كما أعطى المشرع المصري الحق ذاته لصاحب البيانات في البند الثالث من المادة (2) من قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية على أحقية صاحب البيانات في محو بياناته الشخصية، والتي سبق وأن وافق على معالجتها. وقد نص المشرع الإماراتي على هذا الحق في البند الثاني من المادة (15) حقه في طلب محو بياناته الشخصية الخاصة لدى المتحكم في الحالات التالية دون تحديد مدة لحذف البيانات الشخصية، مما قد يؤثر على فعالية الحق في حماية البيانات الشخصية، ذلك أن من قام بمعالجة هذه البيانات لا يكون ملزماً على الفور بحذف هذه البيانات و قد يحتفظ بها لمدة طويلة:

"إذا لم تعد هذه البيانات الشخصية المتعلقة بصاحب الطلب ضرورية للأغراض التي جُمعت أو عولجت من أجلها، أو إذا قام صاحب البيانات بالعدول أو التراجع عن الموافقة التي بُنيت عليها المعالجة. أو في حال قيام صاحب البيانات بالاعتراض على المعالجة، أو في حال غياب الأسباب المشروعة لاستمرار المتحكم في معالجة البيانات. أو إذا تمت معالجة بياناته الشخصية بالمخالفة لأحكام هذا المرسوم بقانون والتشريعات السارية، أو إن كانت عملية المحو ضرورية للامتثال للضوابط والتشريعات السارية".

أما البند الثالث من ذات المادة فقد جاء استثناءً على البند الثاني، فبالرغم من إعطاء المشرع لصاحب البيانات الحق في محو بياناته الشخصية، إلا أن هناك استثناءات واردة على هذا الحق في البند الثالث إذ مع توافر حالة من الحالات المذكورة في هذا البند لا يحق لصاحب البيانات محو بياناته الشخصية وهذه الحالات كالتالي:

في حال طلب صاحب البيانات محو بياناته المتعلقة بالصحة العامة لدى المنشآت الخاصة بما يخالف المصلحة العامة، أو إذا كان طلب محو البيانات فيه تأثير على إجراءات التحقيق والمطالبة بالحقوق والدعاوى القانونية أو الدفاع عنها لدى المتحكم. أو إذا كان الطلب يتعارض مع تشريعات أخرى يخضع لها المتحكم، أو في الحالات الأخرى التي تحددها اللائحة التنفيذية لهذا المرسوم بقانون. وقد أوردت المادة (17) من اللائحة العامة لحماية البيانات ذات الاستثناءات على حق حذف البيانات الشخصية، بالإضافة إلى استثناءات خاصة تتعلق بحرية الاعلام والتعبير، حالة الامتثال لالتزام

1 العوضي،عبد الهادي فوزي. مرجع سابق. ص23.

2 Google Spain SL & Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, (2014) E.C.J. C-131/12, 13 May 2014.

3 الخطيب، محمد عرفان (2018). ضمانات الحق في العصر الرقمي، من تبدل المفهوم لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي واسقاط على الموقف التشريعي الكويتي. *مجلة كلية القانون الكويتية العالمية*. (3)*10*، ملحق خاص. ص269.

قانوني يتطلب المعالجة وفقا لقانون الاتحاد الأوروبي أو الدول الأعضاء، حالات تتعلق بالأرشفة للمصلحة العامة أو البحث العلمي أو التاريخ أو لأغراض إحصائية.

و ذهب البعض إلى أن الحق في النسيان يقتصر في البيئة الرقمية على الآثار الالكترونية أو الذكريات الرقمية، و التي يقصد بها ما يتعلق بالشخص و أنشطته من بيانات و معلومات عند استخدامه للوسائل الالكترونية المختلفة ، و كذلك آراء الشخص على الانترنت مما يساهم في صنع الهوية الرقمية للفرد.[1]

رابعا: حق الاعتراض على معالجة البيانات الشخصية

يحق لصاحب البيانات الاعتراض على معالجة بياناته الشخصية متى كانت أسبابه مبرره ومبنية على أسس مشروعة، وهذا ما أقرته بعض التشريعات، كاللائحة العامة لحماية البيانات رقم 679 الصادرة سنة 2016 في المادة (21) منها، وقانون المعلوماتية والحريات الفرنسي رقم 78 لسنة 1978 والمعدل بأحكام القانون الصادر في 6 أغسطس سنة 2004 بموجب المادة (1/38) بقولها: "لكل شخص الحق في الاعتراض على معالجة بياناته الشخصية وذلك إذا كانت هناك مبررات مشروعة لهذا الغرض".

و هذا ما أكدته محكمة النقض الفرنسية في حكم صادر لها[2]، فطالما هناك أسباب مبررة و مبنية على أسس مشروعة يجوز لصاحب البيانات أن يستخدم حقه في الاعتراض على معالجة بياناته الشخصية، بالإضافة إلى أنها أرست مبدأً و هو أن "مجرد حماية الحياة الخاصة للفرد هو مبرر مشروع للاعتراض على المعالجة"، و يترتب على هذا المبدأ وجود حالتين لا يشترط فيهما إبداء المبرر عند الاعتراض على المعالجة ، الحالة الأولى: إذا كان هدف معالجة البيانات الشخصية التسويق المباشر[3] Direct Marketing، أو الدعاية التجارية فهي مبرر مشروع في الاعتراض على المعالجة ، أما الحالة الثانية: إذا كان هدف معالجة البيانات في مجال البحث العلمي الطبي و هذا البحث فيه خطر كبير على الحياة الخاصة فهي تتناول كل ما يتعلق بالسجل المرضي لصاحب البيانات فهنا يكون الحق مشروعاً في الاعتراض على المعالجة.[4]

و قد سارت على ذات النهج التشريعات الأخرى، كالتشريع الإماراتي في المادة (17) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، و التي جاءت بعنوان (الحق في إيقاف المعالجة)، بإعطاء الحق لصاحب البيانات الشخصية بإيقاف معالجة بياناته إذا كانت هناك أسباب مبرره و سائغه على ذلك، في حال كانت المعالجة بالمخالفة لأحكام المادة (5) التي نص عليها المشرع في المرسوم بقانون ذاته، أو كانت لأغراض التسويق المباشر، أو لأغراض إجراء مسوح إحصائية[5]، و كذلك التشريع المصري في البند السادس من المادة (2) من

---

1 انظر مركز بحوث القانون و التكنولوجيا . تحت إشراف عبدالحميد (2020)، أ.د.حسن. ورشة عمل بعنوان"دراسة نقدية لقانون حماية البيانات الشخصية رقم 151 لسنة 2020"، كلية القانون. الجامعة البريطانية، مصر. ص47.

2 Cass C. (2006). Bull Crim, 69, 267-269

3 See article 21 / 2&3 of Regulation (EU) 2016/679, 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

4 منشور لدى منشور لدى بدوي، عمرو طه، مرجع سابق، ص136.

5 لا يتم إيقاف معالجة البيانات الشخصية بطلب صاحب البيانات إذا كانت المعالجة لأغراض إجراء المسوح الإحصائية، و كانت هذه المعالجة لازمة لتحقيق المصلحة العامة.

قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية في بيان حقوق الشخص المعني بالبيانات و التى نصت على أنه: "يكون للشخص المعني بالبيانات الحقوق الآتية: 6–الاعتراض على معالجة البيانات الشخصية أو نتائجها متى تعارضت مع الحقوق و الحريات الأساسية للشخص المعني بالبيانات"، حيث أن هذا البند من المادة لم يرد عليه أي استثناء أو شروط للاعتراض على معالجة البيانات كما جاء في التشريع الإماراتي كالمعالجة لأغراض التسويق المباشر، حتى أن المشرع المصري جاء في المادة (17) من الفصل الثامن من القانون ذاته و نص على إمكانية الاتصال الالكتروني بغرض التسويق المباشر بتوافر عدة شروط، فإذا لم تتوافر هذه الشروط حسب نص المادة فيحضر معها الاتصال الإلكتروني بغرض التسويق المباشر للشخص المعني بالبيات، فالاتصال الالكتروني لن يحصل إلا بناءً على معالجة سابقة للبيانات.

وحق صاحب البيانات في الاعتراض على معالجة بياناته الشخصية حق مكفول له في أي مرحلة من مراحل معالجة البيانات، فالتشريعات السابقة لم تنص على المرحلة التي يجب فيها على صاحب البيانات من الاعتراض على بياناته الشخصية، أما شكل الاعتراض على معالجة البيانات، فلم تحدد التشريعات كذلك شكلاً معيناً لاعتراض صاحب البيانات على معالجة بياناته الشخصية، فيتم الاعتراض بأي شكل من الأشكال و لا يعتبر السكوت شكلاً من أشكال الاعتراض، أما اللائحة الأوروبية فقد منحت لصاحب البيانات الحق في الاعتراض على معالجة البيانات بطريقة آلية عن طريق استخدام الوسائل التقنية الخاصة[1]. وبالرغم من ذلك فحق الاعتراض ليس حقاً مطلقاً لصاحب البيانات، ففي بعض الحالات لا يجوز لصاحب البيانات أن يعترض على معالجة بياناته الشخصية إذا تمت المعالجة لأغراض بحثية أو علمية أو تاريخية أو إحصائية أو لأغراض المصلحة العامة.[2]

خامسا: حق الرجوع في الموافقة المسبقة للاحتفاظ بالبيانات الشخصية أو معالجتها

اشترط التشريع الإماراتي موافقة صاحب البيانات على معالجة بياناته الشخصية في المادة السادسة و التي جاءت تحت عنوان (شروط الموافقة على معالجة البيانات)، و قد عرف هذه الموافقة كما فعلت اللائحة الأوروبية في المادة (4/11)[3]، لكنه وضع شروطاً لصحة الموافقة بأنها يجب "أن تكون الموافقة معدة بطريقة واضحة و بسيطة و غير مبهمة و سهلة الوصول إليها سواء كانت كتابية أو الكترونية"[4]، مما سبق نرى أن المشرع الإماراتي يعتد بالموافقة

1 See article 21/5 of Regulation (EU) 2016/679, the data subject may exercise his or her right to object by automated means using technical specifications.

2 See article 21/6 of Regulation (EU) 2016/679, Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

3 See article 4 / 11 of Regulation (EU) 2016/679, consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

4 انظر (ب / 1 /6) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

فمعالجة البيانات الحساسة أو البيومترية الشخصية قد تمس الجزء الخاص من حياة الفرد الذي لا يُسمح بأن يُطلع عليها غيره، من جانب آخر نص المشرع على وجوب أن تكون الموافقة كتابية أو الكترونية لكي يعتد بها لمعالجة البيانات في حين أنه عرف المعالجة[1] في المادة الأولى من المرسوم ذاته و نص على أنها تتم بوسيلة من الوسائل الالكترونية، يبدو لنا من هذا التعريف أن المشرع يتناول صيغة الموافقة على وجوب كونها معدة بطريقة واضحة و بسيطة و غير مبهمة ويسهل الوصول إليها، و قد حدد المشرع في هذه المادة أن هذه الموافقة قد تكون كتابية أو إلكترونية، بالرغم من أن المشرع في المادة (7)[2] بعنوان "الكتابة" من المرسوم بقانون اتحادي رقم (46) لسنة 2021 بشأن المعاملات الإلكترونية و خدمات الثقة[3] لا يميز بين الكتابة التقليدية و الكتابة الإلكترونية من ناحية الأثر و الحجية، هنا يثور تساؤل و هو لماذا نص المشرع على الموافقة الإلكترونية أو الكتابية إذا كان لا يفرق بينهما في النتيجة، فغالباً قد يكون هناك نماذج شكلية محددة لإفراغ هذه الموافقة وفق الضوابط التي حددها القانون، و بالحديث عن حق الرجوع في الموافقة المسبقة فهو حق يمنح لصاحب البيانات في العدول عن الموافقة على معالجة بياناته الشخصية في أي وقت، فالموافقة المسبقة على إجراء معين لا يمنع الشخص من الاعتراض أو سحب موافقته بعد ذلك. و قد أقرها المشرع الأوروبي في اللائحة العامة في الفقرة الثالثة من المادة السابعة [4]، لكنه لم يجعل هذا الحق مطلقاً بل اشترط لذلك أن لا يؤثر سحب الموافقة على مشروعية المعالجة، بناءً على الموافقة قبل سحبها، كما نص على ذلك المشرع الإماراتي في الفقرة الثانية من المادة (6) من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية و التي نصت على أنه: "يجوز لصاحب البيانات العدول في أي وقت عن موافقته على معالجة بياناته الشخصية، و لا يؤثر هذا العدول على قانونية و مشروعية المعالجة المبنية على الموافقة التي أعطيت قبل العدول عنها"، ونظمته المادة (16) من ذات اللائحة التي منحت صاحب البيانات حق تعديلها أو تصحيحها. كذلك فقد نظمه المشرع المصري في البند الثاني من المادة (2) من قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية في بيان حقوق الشخص المعني بالبيانات والتي نصت على أنه: "يكون للشخص المعني بالبيانات الحقوق الآتية: 2– العدول عن الموافقة المسبقة على الاحتفاظ بياناته الشخصية أو معالجتها". ويجب أن يكون حق الشخص بالعدول مستندا إلى مبررات مشروعة. ولا يشترط في العدول صيغة أو شكلاً معيناً ويكفي أن يكون صريحاً مستنداً إلى مبررات مشروعة، نرى أن التشريعات منحت الحق لصاحب البيانات بالرجوع عن الموافقة المسبقة للاحتفاظ أو بمعالجة البيانات الشخصية لكنها لم تجعل هذا الحق مطلقاً إنما قيدته بتقديم مبررات مشروعة عند اللجوء للرجوع عن الموافقة، في حين جعلت الطريق مفتوحاً أمام صاحب البيانات بعدم تقييده بصوره أو صيغ أو شكل معين تفرغ فيه الموافقة مما قد يثير عدة تساؤلات لاحقاً.

1 "المعالجة: أي عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية باستخدام أي وسيلة من الوسائل الالكترونية بما فيها وسيلة المعالجة و غيرها من الوسائل الأخرى.....".

2 "إذا اشترط أي تشريع نافذ في الدولة في أي معلومة أو بيان أو مستند أو سجل أو معاملة أو بينة أن يكون مكتوباً، أو نص على ترتيب نتائج معينة على عدم الكتابة ، فإن هذا الشرط يعد متوفراً في المستند الإلكتروني إذا كانت المعلومات التي يتضمنها محفوظة بشكل يتيح استخدامها و الرجوع إليها".

3 المنشور في الجريدة الرسمية العدد سبعمائة و اثنا عشر (ملحق)، السنة الواحدة و الخمسون الموافق 26/09/2021.

4 See article 7 / 3 of Regulation (EU) 2016/679, The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

يعد من أحد المبادئ الضامنة لحماية الخصوصية التي أقرها المشرع الإماراتي للمستخدم عدم جواز نقل المعلومات الشخصية للخارج أو معالجتها إلا بضوابط و شروط، وهو ما اطلق عليه مصطلح "المعالجة عبر الحدود"، و قد عرفها المشرع الإماراتي في المادة الأولى من المرسوم بأنها: "نشر أو استخدام أو عرض أو إرسال أو استقبال أو استرجاع أو استخدام أو مشاركة البيانات الشخصية أو معالجتها خارج النطاق الجغرافي للدولة"[1]، و فرق بين نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال وجود مستوى حماية ملائم و في حال عدم وجود مستوى ملائم من الحماية، فقد أفرد المادة (22)[2] لحالة نقل ومشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال وجود مستوى حماية ملائم و قد أجاز نقل البيانات الشخصية خارج الدولة في أحوال معينة معتمدة من قبل المكتب[3]، كأن تكون الدولة التي سيتم نقل البيانات لها لديها تشريعات خاصة بحماية البيانات الشخصية و قد وضعت ضوابط و اشتراطات خاصة للحفاظ على سرية البيانات، بالإضافة إلى فرض التدابير على المتحكم أو المعالج من خلال الجهات الرقابية و القضائية، في أحوال أخرى ليتم معالجة البيانات عبر الحدود من قبل دولة أخرى يتطلب انضمام الأخيرة إلى الاتفاقيات الثنائية أو متعددة الأطراف المتعلقة بحماية البيانات الشخصية مع الدولة مرسلة البيانات، بينما لم يضع المشرع المصري الأحوال التي يجوز فيها معالجة البيانات الشخصية في الدول التي تتوفر فيها مستوى من الحماية، وإنما اكتفى بوضع معيار (توفر مستوى من الحماية لا يقل عن تلك المنصوص عليها في هذا القانون، وبترخيص أو تصريح من المركز)، و حظر ما غير ذلك من عمليات لنقل البيانات، فيما جاءت المادة (23)[4] استثناءً على المادة السابقة والتي تحدثت عن حالات جواز نقل و مشاركة البيانات الشخصية عبر الحدود لأغراض المعالجة في حال عدم وجود مستوى ملائم من الحماية و هي حالات محددة وردت على سبيل الاستثناء تحت اشتراطات و ضوابط صارمة لاستشعار أهمية حماية خصوصية معالجة البيانات الشخصية بالإضافة إلى عدم وجود مستوى ملائم من الحماية، و من هذه الحالات:

- أن يكون نقل البيانات بموجب عقد أو اتفاقية تلتزم فيها المنشأة في تلك الدولة بتطبيق الأحكام والتدابير والضوابط والاشتراطات التي وردت في هذا المرسوم، بالإضافة إلى التدابير المناسبة على المتحكم أو المعالج تحدد من خلال العقد أو الاتفاقية.
- تطلب الموافقة الصريحة من صاحب البيانات[5] على نقل بياناته الشخصية للخارج بما لا يتعارض مع المصلحة العامة والأمنية.
- أن يكون نقل البيانات ضرورياً لحماية المصلحة العامة أو تنفيذاً لإجراء متعلق بتعاون قضائي دولي.

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

2 تقابلها المادة (14) من القانون رقم 151 لسنة 2020 بإصدار حماية البيانات الشخصية.

3 مكتب الإمارات للبيانات.

4 تقابلها المادة (15) من القانون رقم 151 لسنة 2020 بإصدار حماية البيانات الشخصية.

5 بينما ذهب نظيره المصري إلى جواز حالة الموافقة الصريحة للشخص المعني بالبيانات أو من ينوب عنه.

- أو أن يكون نقل البيانات ضرورياً لتنفيذ الالتزامات وإثبات الحقوق أمام الجهات القضائية، أو لإبرام أو تنفيذ عقد مبرم بين المتحكم وصاحب البيانات أو بين المتحكم والغير لتحقيق مصلحة صاحب البيانات.
- للحفاظ على حياة الشخص صاحب البيانات، وتوفير الرعاية الطبية أو العلاجية له.[1]
- لإجراء تحويلات نقدية إلى دولة أخرى وفقاً لتشريعاتها المحددة والسارية.[2]

بعد الانتهاء من ذكر حقوق صاحب البيانات الشخصية و التي منحها له المشرع في المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في نصوص متفرقة و نظيره المشرع الأوروبي في اللائحة العامة لحماية البيانات، و كذلك المشرع المصري في قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية في نص واحد، يثور تساؤل لم تجب عليه التشريعات، هل تم ذكر هذه الحقوق على سبيل الحصر أم على سبيل المثال و أن هناك حقوقاً أخرى تكون لصاحب البيانات ذكرت في تشريعات أخرى، و الأفضل إبقاء الباب مفتوحاً لإمكانية ظهور مستجدات و تطورات تقنية في مجال حفظ و حماية البيانات.

الفرع الثاني: الالتزامات الملقاة على مشغلي تطبيقات الذكاء الاصطناعي

وضعت التشريعات المقارنة مجموعة من الالتزامات على عاتق المسؤول عن تخزين البيانات ومعالجتها، فقد أورد المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية الالتزامات الملقاة على مشغلي تطبيقات الذكاء الاصطناعي في نصوص متفرقة كالنهج الذي سار عليه المشرع الأوروبي في اللائحة العامة، قبل الحديث عن الالتزامات الملقاة على مشغلي تطبيقات الذكاء الاصطناعي يجب الإشارة إلى أن المرسوم بقانون اتحادي استثنى بعض الجهات من نطاق تطبيق أحكام المرسوم على معالجي البيانات الشخصية في هيئات القطاع العام كالجهات الحكومية المتحكمة بالبيانات الشخصية أو تلك التي تقوم بمعالجتها، و كذلك البيانات الشخصية لدى الجهات الأمنية و القضائية، بالإضافة إلى البيانات الشخصية الصحية و المصرفية و الائتمانية[3] التي لديها تشريع ينظمها كما أشرنا سابقاً، مما قد يثير العديد من الإشكاليات هنا، فالبيانات الشخصية و الحساسة و البيومترية للأفراد غالباً ما تكون في قواعد بيانات لدى هذه الجهات التي لا تسري عليها أحكام المرسوم بقانون فيما يخص معالجة البيانات الشخصية، مما قد يضعف نطاق الحماية لصاحب البيانات الشخصية و يخلق مجالاً لخرق القانون، في الحين التي تتم فيه المعاملات الإلكترونية بشكل هائل يومياً يتخللها بيانات شخصية لعدد كبير من الأفراد، هنا لابد من مد مظلة الحماية على هذه البيانات الشخصية لحمايتها من الاختراق. نتطرق في هذا الفرع لالتزامات مشغلي تطبيقات الذكاء الاصطناعي.

1 المادة (1/15) من القانون رقم 151 لسنة 2020 بإصدار حماية البيانات الشخصية.

2 المادة (6/15) من القانون رقم 151 لسنة 2020 بإصدار حماية البيانات الشخصية.

3 انظر البند الثاني من المادة (2) من المرسوم بقانون رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.

أولاً: الالتزام بتقديم نماذج شكلية مسبقة لتكوين الملفات (طلب يتم تقديمه من مشغل تطبيقات الذكاء الاصطناعي إلى اللجنة الوطنية الفرنسية للحريات و المعلوماتية (CNIL))

أحد الالتزامات التي تقع على عاتق مشغلي تطبيقات الذكاء الاصطناعي هي الالتزام بتقديم نماذج شكلية مسبقة لتكوين الملفات و هي ما نص عليه المشرع الفرنسي في المادة (16) من القانون الفرنسي لسنة 1978 حول المعلوماتية و الحريات المعدل بأحكام القانون رقم (1321) الصادر في 7 أكتوبر 2016، بأن الزم مشغلي تطبيقات الذكاء الاصطناعي على أهمية تقديم نماذج شكلية لتكوين الملفات التي تنصب على معالجة البيانات الشخصية في مراحل جمعها و تخزينها و تعتبر من جانب آخر تصريح للمعالجة الآلية للبيانات على الموقع الالكتروني، و هذا التصريح يجب أن يشمل عدة بيانات كهوية مقدم الطلب و هوية من يقوم بتكوين الملفات و الغاية من المعالجة و في حال عدم الالتزام بذلك فتفرض عقوبات على مشغلي هذه التطبيقات و التي قد تصل لحد الحبس و الغرامات المالية، و هذا الالتزام يفرض عندما تكون هناك معالجة تؤثر في البيانات الشخصية.[1]

ثانياً : الالتزام بالإعلام و الشفافية

من المبادئ و الحقوق التي تقوم عليها عملية جمع البيانات الشخصية و معالجتها مبدأ الشفافية الذي يظهر من قِبل مشغلي تطبيقات الذكاء الاصطناعي و حق الإعلام لصاحب البيانات بأنه بياناته تجمع و سيتم معالجتها، و يجب أن تتم عملية الجمع و المعالجة بطريقة مشروعة، فقد نص القانون الفرنسي لسنة 1978 المعدل بأحكام القانون رقم (1321) الصادر في 7 أكتوبر 2016 على منع أي جمع للبيانات تتم بطريقة أو وسيلة غير مشروعة أو غير نزيهة و ادرجها تحت طائلة المسؤولية الجنائية، و يتم الالتزام بالإعلام عند مرحلة جمع البيانات إما بالطريق الاختياري أو الإجباري عن طريقة وضع علامة مميزة للمعلومات التي يجب على صاحب البيانات ملؤها، فعند اختيار أيقونة أوافق (I Agree) فإنه يوافق على إجراء عملية الجمع.[2]

ثالثاً : الغاية من عملية جمع البيانات و معالجتها

يجب على مشغلي تطبيقات الذكاء الاصطناعي التصريح بالغاية من جمع البيانات و معالجتها، و لا يتعدى هذه الغاية و كذلك إذا كان هناك أية نية لاستعمال هذه البيانات مستقبلاً، فقد يتم جمع البيانات و معالجتها لأغراض تسويقية تجارية أو من أجل تنفيذ عقد اشتراك في موقع الكتروني و هو ما يجب أن يعلم به صاحب البيانات، و لا يكتفى بذلك فقط بل يجب أن يعلم صاحب البيانات عن المدة التي سيتم الاحتفاظ بها لبياناته الشخصية، لذلك يجب أن يعلم صاحب البيانات منذ اللحظة الأولى التي يولج فيها إلى الموقع الالكتروني عن معلومات عن المسؤول عن الموقع و من يقوم بجمع البيانات.[3]

1 انظر خصاونه، علاء الدين و آخرون. مرجع سابق، ص20-21.

2 خصاونه، علاء الدين و آخرون، مرجع سابق، ص22-23.

3 خصاونه، علاء الدين و آخرون، مرجع سابق، ص22.

رابعاً : الالتزام بمعالجة البيانات الشخصية بمشروعية

أقرت بعض التشريعات كاللائحة العامة[1] والمرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية[2]، وكذلك التشريع المصري في قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية[3]، هذا الالتزام بمعالجة البيانات بمشروعية كضابط من ضوابط معالجة البيانات الشخصية والذي يقع على عاتق معالجي البيانات الشخصية والمتحكمين فيها ومنهم مشغلي تطبيقات الذكاء الاصطناعي، ومعالج البيانات الشخصية كما عرفه المشرع المصري في المادة الأولى من قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية هو الشخص الطبيعي أو الاعتباري المختص بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقا لتعليماته.

أما المتحكم بالبيانات الشخصية فهو بحسب المادة الأولى من القانون المصري رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية هو: "أي شخص طبيعي أو اعتباري يكون له بحكم طبيعة عمله الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها أو معالجتها والتحكم فيها طبقا للغرض المحدد أو نشاطه".

ويقصد بهذا الالتزام وجوب التزام معالج البيانات بجمع البيانات بطرق مشروعة تستند على أساس قانوني صحيح غير مخالفة للقانون، كالوسائل الاحتيالية أو المخالفة للنظام العام، وضرورة أن يتم طبقاً للقواعد المنظمة لذلك بموجب التشريعات المختصة وأن تكون المعالجة لأغراض مشروعة وألا يتم تجاوز الغرض المحدد للمعالجة ومدته، وضرورة محو البيانات بعد انقضاء مدة المعالجة أو تسليمها للمتحكم[4]. ولم تكتفي بعض التشريعات[5] بذلك بل ذهبت إلى وضع التزام بعدم حفظ البيانات الشخصية من قبل المعالج لمدة تزيد عن المدة الضرورية لتحقيق الغرض من

---

1 See article 6 of Regulation (EU) 2016/679 , Processing shall be lawful only if and to the extent that at least one of the following applies; (a)the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;(e)processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;(f)processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

2 انظر البند الأول من المادة (5) من المرسوم بقانون رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية و التي نصت على أنه: "يتم معالجة البيانات الشخصية وفقاً للضوابط الآتية: 1. أن تكون المعالجة بطريقة عادلة و شفافة و مشروعة".

3 انظر البند الثالث من المادة (3) من قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية و التي نصت على أنه: "يجب لجمع البيانات الشخصية و معالجتها و الاحتفاظ بها، توافر الشروط الآتية: 3. أن تعالج بطريقة مشروعة و ملائمة للأغراض التي تم تجميعها من أجلها".

4 المادة الخامسة من القانون المصري رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية.

5 راجع المادة 10 من القانون القطري رقم (13) لسنة 2016 بشأن حماية البيانات الشخصية.

الجمع. وعدم إجراء أي معالجة تتعارض مع غرض المتحكم أو نشاطه إلا إذا كان لغايات إحصائية أو تعليمية غير ربحية.

و في هذا الشأن ذهب المشرع إلى النص على عقوبة الحبس و الغرامة التي لا تقل عن (50,000) خمسين ألف درهم و لا تزيد على (500,000) خمسمائة ألف درهم أو بإحدى هاتين العقوبتين، و ذلك في حال استخدام تقنية المعلومات لجمع و معالجة البيانات و المعلومات الشخصية للأفراد بالمخالفة للتشريعات النافذة في الدولة.[1]

خامساً: عدم حفظ بيانات المستخدمين ومعالجتها بدون إذنهم

لا يجوز لمشغلي تطبيقات الذكاء الاصطناعي حفظ بيانات مستخدمي هذه التطبيقات بدون إذن، فقد نص المشرع الإماراتي في المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية في البند السابع من المادة (5)[2] على أنه يجب عدم الاحتفاظ بالبيانات الشخصية بعد استنفاذ الغرض من معالجتها، و بمفهوم المخالفة لا يجوز لمشغلي تطبيقات الذكاء الاصطناعي حفظ بيانات مستخدمي هذه التطبيقات، بالإضافة إلى أنه أكد على ضرورة محو البيانات بعد انقضاء مدة المعالجة في البند الرابع من المادة الثامنة[3] من المرسوم ذاته والتي تنص على الالتزامات العامة لمعالج البيانات الشخصية. كما ذهب المشرع الأوروبي في البند (هـ) من المادة الخامسة من اللائحة العامة إلى وضع ضوابط للاحتفاظ بالبيانات الشخصية التي تم جمعها وفق شروط معينة تحت مسمى "قيود التخزين".

كما يجب على مشغلي تطبيقات الذكاء الاصطناعي عدم إجراء معالجة للبيانات الشخصية للمستخدمين بدون رضا المستخدم، فرضاء المستخدم في معالجة بياناته الشخصية له أهمية كبيرة لدى المشرع الإماراتي في المادة الرابعة من المرسوم بقانون اتحادي الذي حظر معالجة البيانات الشخصية دون موافقة صاحبها و لم يكتفِ بذلك، إنما وضع شروطاً للموافقة على معالجة البيانات الشخصية من قبل الشخص المعني في المادة السادسة من المرسوم بقانون اتحادي ذاته كأن تكون الموافقة صريحة و واضحة غير مبهمة كما أنها يجب أن تتضمن حق العدول من قِبل صاحب البيانات في أي وقت يشاء. وقد ذهب المشرع المصري إلى ما ذهب إليه نظيره الإماراتي فقد أكد في المادة الثانية من القانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية على عدم جواز جمع البيانات الشخصية أو معالجتها إلا بالموافقة و اشترط الموافقة الصريحة في ذلك، مما يعني أن الموافقة الضمنية لا تعطي مشغلي التطبيقات الذكاء الاصطناعي الحق في معالجة البيانات الشخصية لصاحب الشأن و إلا اعتبر ذلك انتهاكاً للخصوصية. و انتفاء رضا المستخدم في معالجة البيانات الشخصية يرتب المساءلة القانونية لمشغلي تطبيقات الذكاء الاصطناعي من معالج و متحكم و غيره ممن ساهم في تشغيل هذه التطبيقات. وحسناً فعل المشرع الإماراتي والمصري في هذا الشأن، فذلك يحفظ بيانات المستخدمين الشخصية من انتهاكها من قبل مشغلي تطبيقات الذكاء الاصطناعي. كما ذهب المشرع الأوروبي إلى ترسيخ المبدأ ذاته في المادة السابعة من اللائحة العامة بوضع شروط لموافقة صاحب البيانات على معالجة بياناته الشخصية، و بمفهوم

1 المادة (13) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الالكترونية.

2 تقابلها البند الرابع من المادة الثالثة في قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية المصري.

3 يقابلها البند السابع من المادة الرابعة في قانون رقم 151 لسنة 2020 حماية البيانات الشخصية المصري.

المخالفة عدم وجود هذا الشرط ينفي إمكانية معالجة البيانات الشخصية من قبل المعالج أو المتحكم، و معه يعتبر انتهاكاً للحق في خصوصية البيانات.

سادساً : عدم إفشاء سرية البيانات التي تم حفظها وتخزينها

بالرغم من إعطاء القانون الحق لمشغلي تطبيقات الذكاء الاصطناعي في جمع البيانات الشخصية بموافقة صاحب البيانات و بشروط محددة، إلا أن المشرع الإماراتي وضع ضابطاً آخر في هذا الشأن و هو التزام مشغلي تطبيقات الذكاء الاصطناعي بعدم إفشاء سرية البيانات التي تم حفظها و تخزينها، و هذا ما نص عليه المشرع الإماراتي في البند الأول المادة السابعة [1] من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية بأن رتب التزاماً على المتحكم باتخاذ الإجراءات التقنية و التنظيمية اللازمة بما يحافظ على سرية البيانات و خصوصيتها و لمنع انتهاك هذا الحق لصاحب البيانات الشخصية.

فيجب على القائم بالمعالجة اتخاذ كافة الإجراءات بما يضمن سرية البيانات، بالإضافة إلى عدم قيام المعالج بأي فعل أو عمل قد يكون من شأنه إفشاء أو تسريب البيانات، و لأهمية هذا الالتزام فقد نصت عليه اللائحة العامة في المادة (32) في القسم الثاني و الذي جاء بعنوان (سرية البيانات الشخصية).

و هذا الالتزام لا يشمل المعالج فقد بل يمتد لغيره من الأشخاص كالشخص الذي يعمل تحت سلطة المراقب أو المعالج ، أو من لديه الحق في الوصول إلى البيانات و الاطلاع عليها، و لا يقتصر الحفاظ على السرية بالمدة التي قام بها المعالج أو من يقوم بمعالجة البيانات بل تمتد حتى بعد زوال هذه الصفة عن القائم بها.[2]

سابعاً : الالتزام باتخاذ الاحتياطات اللازمة لحماية البيانات

هذا الالتزام أقرته العديد من التشريعات كالتشريع الفرنسي في المادة 34 من قانون المعلوماتية و الحريات الفرنسي رقم (78) لسنة 1978 و المعدل بأحكام القانون الصادر في 6 أغسطس 2004م، و المواد 5 و 8 من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، و كذلك البند السادس من المادة الرابعة من قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية[3]، و مضمون هذا الالتزام قيام المعالج باتخاذ كافة الإجراءات و الاحتياطات الفنية و التقنية التي تساهم في حفظ سرية البيانات الشخصية لمنع أطراف ثالثة من الاطلاع على هذه البيانات، و تتنوع صور اتخاذ الإجراءات اللازمة فعدم تمكن أطراف غير مخول لها من قراءة السندات أو نسخها أو تعديلها، و كذلك عدم التمكن من اقحام أي معطيات في النظام بدون أذن، و عدم إمكانية استخدام نظام المعالجة دون أذن، و الالتزام هنا يمتد إلى الحفاظ على اتخاذ الاحتياطات اللازمة لحماية البيانات من أي انتهاك و اختراق لها[4]. وهذا ما أكدته محكمة النقض الفرنسية في الحكم الصادر لها بأن: "الشخص المسؤول عن معالجة البيانات الشخصية

1 يقابلها البند الرابع من المادة 5 من القانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية.

2 انظر، بدوي، عمرو طه، مرجع سابق، ص149-150.

3 " اتخاذ جميع الإجراءات التقنية و التنظيمية و تطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية و تأمينها حفاظاً على سريتها، و عدم اختراقها، أو إتلافها، أو تغييرها أو العبث بها قبل أي إجراء غير مشروع".

4 منشور لدى بدوي، عمرو طه، مرجع سابق، ص149 – 150.

مطلوب منه اتخاذ جميع الاحتياطات اللازمة، نظراً لطبيعة البيانات و المخاطر التي تقدمها المعالجة، للحفاظ على أمن البيانات، و على وجه الخصوص، لمنع أطراف ثالثة الوصول غير المصرح به".[1]

ثامناً: الالتزام بالإخطار بمعالجة البيانات الشخصية

من الالتزامات التي تقع على عاتق المعالج في مواجهة صاحب البيانات هي التزامه بإخطار صاحب البيانات بمعالجة بياناته الشخصية، و كذلك التزامه بإخطاره بالغرض من المعالجة، و هذا ما أقرته المادة 32 من قانون المعلوماتية و الحريات، و في ذلك اتجهت بعض التشريعات إلى عدم إخطار صاحب البيانات بمعالجة بياناته في حالات معينة، على سبيل المثال: إذا كان تجميع البيانات و معالجتها ضرورياً للدفاع الوطني و الأمن الداخلي و الخارجي، أو للوقاية من الجريمة أو لأغراض إحصائية أو تاريخية أو علمية.

تاسعاً: الالتزام بحذف أو محو البيانات الشخصية

أحد أهم الالتزامات الأساسية التي تقع على عاتق مشغلي تطبيقات الذكاء الاصطناعي هو الالتزام بحذف أو محو البيانات الشخصية، فيترتب هذا الالتزام في حالتين، الحالة الأولى: عند طلب صاحب البيانات حذف أو محو بياناته الشخصية، أما الحالة الثانية: عند انتهاء الغرض من معالجة البيانات الشخصية فيجب على المعالج محو هذه البيانات و حذفها فلا يجوز للقائم على المعالجة الاحتفاظ بالبيانات بصفة أبدية أو كما نصت عليه بعض التشريعات بإعدام البيانات[2]، و قد نصت على هذه الالتزام عدة تشريعات كاللائحة الأوروبية رقم (679) لسنة 2016 و المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية والقانون المصري رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية، لكن التشريعات أغفلت أمراً مهماً و هو عدم وجود ضابط أو معيار لتحديد مدة الاحتفاظ بالبيانات الشخصية للمستخدمين مما قد يفتح مجالاً لاستغلال الثغرات فيما يتعلق بمدة الاحتفاظ.

و يضمن تنفيذ هذه الالتزامات التي جاء ذكرها فيما سبق و يراقب و يشرف عليها مسؤول حماية البيانات، و قد عرفته المادة الأولى من المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية بأنه:"أي شخص طبيعي أو اعتباري يتم تعيينه من قبل المتحكم أو المعالج، يتولى مهام التأكد من مدى امتثال الجهة التي يتبعها بضوابط و اشتراطات و إجراءات و قواعد معالجة حماية البيانات الشخصية المنصوص عليها في هذا المرسوم بقانون، و التأكد من سلامة أنظمتها و إجراءاتها من أجل تحقيق الالتزام بأحكامه".

بعد استعراض أهم حقوق صاحب البيانات وأبرز التزامات المسؤول عن تخزين ومعالجة البيانات الشخصية، لا بد لنا من الحديث عن الجزاء في حال الإخلال بهذه الالتزامات أو المساس بحقوق صاحب البيانات.

1 راجع، منشور لدى بدوي، عمرو طه، مرجع سابق، ص155-156.

2 راجع الفصل 45 من القانون التونسي رقم (63) لسنة 2004 بتاريخ 27 يوليو 2004 يتعلق بحماية المعطيات الشخصية.

المبحث الثاني: المسؤولية المدنية عن المساس بالحق في الخصوصية

تمهيد و تقسيم

تنشأ المسؤولية المدنية عند انتهاك الحق في الخصوصية، كالمساس بالحق في الصورة أو خرق وانتهاك البيانات الشخصية بشكل غير مشروع، مما يعطي لصاحب الحق في الخصوصية بطلب وقف الاعتداءات وطلب التعويض عما أصابه من ضرر. سنتعرض في المطلب الأول لأساس وشروط المسؤولية المدنية عن المساس بالحق في الخصوصية وفقا للقواعد العامة للفعل الضار و قواعد المسؤولية وفقاً لأنظمة خاصة كمسؤولية حارس الأشياء عن المساس بالحق في الخصوصية ومسؤولية المنتج وإمكانية قيام مسؤولية من نوع خاص بتطبيقات الذكاء الاصطناعي، ثم نتطرق في المطلب الثاني لآثار المسؤولية المدنية عن المساس بالحق في الخصوصية.

المطلب الأول: أساس وشروط المسؤولية المدنية عن المساس بالحق في الخصوصية

لم ينظم المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية وكذلك القانون المصري حول حماية البيانات الشخصية طبيعة العلاقة بين صاحب البيانات الشخصية و المعالج أو مزود الخدمة، فكان لابد من بيان طبيعة هذه العلاقة أولاً لاستخلاص المسؤول عن الأضرار الناشئة عن تطبيقات الذكاء الاصطناعي ليتم الرجوع عليه لاحقاً لاستيفاء التعويض عند استحقاقه، و لبيان ذلك لابد من الرجوع للقواعد التقليدية التي تنظم العلاقة، ثم النظر في بعض الأنظمة الخاصة لنرى مدى ملاءمة أي منها للمسؤولية عن الضرر الناشئ عن تطبيقات الذكاء الاصطناعي:

الفرع الأول: المسؤولية عن انتهاك تطبيقات الذكاء الاصطناعي للحق في الخصوصية وفقاً للقواعد العامة

ذهب الفقه والقضاء إلى تقسيم المسؤولية المدنية إلى مسؤولية عقدية ومسؤولية تقصيرية، ويختلف كل منهما من حيث شروطه وأحكامه وآثاره في حال ترتب هذه المسؤولية، ونبحث انعكاس ذلك على مسؤولية تطبيقات الذكاء الاصطناعي.

أولا: المسؤولية وفقا للقواعد العامة العقدية عن أضرار تطبيقات الذكاء الاصطناعي

العقد هو ارتباط الإيجاب الصادر من أحد المتعاقدين بقبول الآخر على نحو يثبت أثره في المعقود عليه و يترتب التزام طرفيه مما يستوجب على كل منهما الالتزام بتنفيذ ما أوجبه عليه العقد[1]. و أنه في العقود الملزمة للجانبين إذا لم يوف أحد المتعاقدين بما أوجبه العقد جاز للمتعاقد الآخر بعد أعذاره المطالبة بتنفيذ العقد و جبر المدين على الوفاء بحقوقه العقدية و القانونية الواجبة أو المطالبة بفسخ العقد، و أن حل الرابطة العقدية جزاء إخلال أحد طرفي العقد الملزم للجانبين بأحد التزاماته الناشئة عن العقد هو من النصوص المكملة لإرادة المتعاقدين، و لهذا فإن الحق يكون

1 انظر في هذا الشأن نص المادة (125) من قانون رقم (5) لسنة 1985م بإصدار قانون المعاملات المدنية لدولة الإمارات العربية المتحدة، وفقاً لأحدث تعديلاته بالمرسوم بقانون اتحادي رقم (30) لسنة 2020.

ثابتاً لكل منهما بنص القانون و يعتبر العقد متضمناً له و لو خلا من اشتراطه، و لا يجوز حرمان المتعاقد من هذا الحق أو الحد من نطاقه إلا باتفاق صريح بين المتعاقدين.[1]

تنشأ المسؤولية العقدية عندما تتواجد ثلاثة أركان و هي الإخلال بالتزام عقدي، الضرر، وعلاقة السببية، فبعد ابرام العقد يجب أن يلتزم كلا طرفيه بما احتواه العقد من شروط، فعند خرق أحد بنود العقد يتشكل الركن الأول من أركان المسؤولية العقدية، ويمكن أن يحدث ذلك في تطبيقات الذكاء الاصطناعي عندما يتم إبرام العقد بين صاحب البيانات و الطرف الآخر، كالمتحكم بالبيانات أو المعالج لها أو مزود الخدمة أو مشغل تطبيقات الذكاء الاصطناعي، فعند قيام أي من هؤلاء بانتهاك ما جاء في العقد، كحفظ البيانات دون الرجوع لموافقة صاحب البيانات أو بيعها لجهات إعلانية أو تجاوز الغرض من الجمع والمعالجة أو عدم حذف البيانات بعد انتهاء الغرض منها، مما يمثل أفعالاً تؤدي إلى الاخلال بالالتزامات فيتحقق معها الركن الأول.

و يمثل الضرر الركن الثاني للمسؤولية العقدية، فالضرر في المسؤولية العقدية لتطبيقات الذكاء الاصطناعي تتمثل بالضرر الأدبي الذي يصيب المضرور (صاحب البيانات) جراء انتهاك الحق في خصوصية البيانات في جانب غير مادي، كالشعور أو السمعة أو الشرف أو الكرامة أو العاطفة أو أية جوانب أخرى تمس شعور المضرور، من جانب آخر لا يتصور وقوع الضرر المادي للمضرور جراء انتهاك الخصوصية في تطبيقات الذكاء الاصطناعي.

أما الركن الثالث والأخير، فهو وجود العلاقة السببية بين الركنين السابقين، فلا يمكن أن تقوم المسؤولية العقدية إلا إذا كان الضرر الذي وقع على صاحب البيانات جراء الإخلال بالتزام العقدي بحفظ البيانات من قِبل مشغلي تطبيقات الذكاء الاصطناعي.

ترى الباحثة أنه يمكن اعتبار سياسة الخصوصية بمثابة عقد بين مستخدم تطبيقات الذكاء الاصطناعي و الطرف الآخر المسؤول عن تشغيل هذا التطبيق، حيث أن هذه التطبيقات لا تعطي الصلاحية للمستخدم للانتفاع بها إلا بعد موافقته على ما يسمى بسياسة الخصوصية و التي عادة ما تكون مكتوبة بخط صغير غير واضح و لا يكون هناك تناسق بين الكلمات أو حتى الأسطر و تتضمن هذه السياسة مصطلحات وشروط كثيرة و نقاط مبهمة لا تصل للمستخدم بسهولة فيضطر إلى الموافقة عليها دون قراءة ما جاء في محتواها، مما يجعل معلوماته الشخصية أو الحساسة معرضة للانتهاك بناءً على أحد البنود التي وافق عليها في سياسة الخصوصية و التي قد تعطي الحق لمشغل هذا البرنامج من الاطلاع عليها و بيعها أو الاستفادة منها دون الرجوع إلى المستخدم المعني بهذه البيانات.

1 راجع، محكمة تمييز دبي، الدائرة التجارية، الطعن رقم (417) لسنة 2016م، الصادر في جلسة 2017/04/09، موقع محامو الإمارات، تاريخ الدخول: 05/04/2022، على الرابط:

https://www-mohamoon-uae-com.uaeu.idm.oclc.org/uaeu/default.aspx?Action=IntrDisplayJudgmentFile&PageNumber=1&Type=5&ID=25556&strSearch=20%الحياة الخاصة

نظم المشرع الإماراتي أحكام المسؤولية التقصيرية في المواد (282–317) من قانون المعاملات المدنية، و تقوم المسؤولية التقصيرية في القانون المدني على الالتزام بعدم الإضرار بالغير[1]، أي أنه لا وجود لعقد سابق بين الطرفين في المسؤولية التقصيرية، بخلاف المسؤولية العقدية التي لولا الإخلال بالالتزام في العقد لما نشأت هذه المسؤولية، و هذا ما أكده المشرع الإماراتي في المادة (282) من قانون المعاملات المدنية بأنه: "كل إضرار بالغير يلزم فاعله ولو غير مميز بضمان الضرر". أما المشرع المصري، فقد أقام المسؤولية على فكرة الخطأ في المادة (163) مدني مصري، أي الانحراف عن السلوك العادي المألوف وواجب اليقظة والحذر. ونتطرق لأركان المسؤولية التقصيرية في التشريع الإماراتي وفق الآتي:

1. الإضرار[2]

يعتبر الإضرار هو الركن الأول من أركان المسؤولية التقصيرية الذي يجب توافره لاكتمال أركان المسؤولية التقصيرية، و بالرجوع للمذكرة الإيضاحية لقانون المعاملات المدنية الإماراتي نرى أن المشرع عرف الإضرار الوارد في المادة 282 بأنه:"محاولة مجاوزة الحد الواجب الوقوف عنده أو التقصير عن الحد الواجب الوصول إليه في الفعل أو الامتناع مما يترتب عليه العمد و إلى مجرد الإهمال على حد السواء"[3]، كما ذكر أن الإضرار يستلزم الفعل أو عدم الفعل الذي ينشأ عنه الضرر، يستوضح لنا مما سبق أن المعالج أو المتحكم أو مزودي الخدمة يجب أن يقوموا بالإجراءات اللازمة لحفظ البيانات الشخصية للأفراد و عدم معالجتها دون الرجوع لصاحب البيانات، فإذا ما قام هؤلاء بذلك فيكونون عندئذ قد تجاوزا الحد الذي لا يمكنهم من استعمال البيانات الشخصية في غير الغرض المخصص لها (معالجتها لغرض محدد)، مما يحقق الركن الأول للمسؤولية التقصيرية وهو انتهاك الحق في الخصوصية. وطبقا للمادة 9 من قانون الحق في احترام الحياة الخاصة الفرنسي لسنة 1970 الذي تم تنظيمه في المادة التاسعة من التقنين المدني الفرنسي لكل شخص الحق في الحصول على تعويض عن المساس بهذا الحق كما للقضاء فرض تدابير لحماية هذا الحق كالحراسة أو الحجر لمنع أو إزالة أي مساس بالحياة الخاصة، ويجوز للمتضرر أن يطلب من قاضي الأمور المستعجلة وفقا للقانون الفرنسي وقف الاعتداء فورا واتخاذ إجراءات عاجلة للحد من الخطر المحدق بهذا الحق. وهذا النص مشابه لنص المادة (50) من القانون المدني المصري. وقد أكدت المواد (79-82) من اللائحة العامة لحماية البيانات على حق صاحب البيانات بالحصول على التعويض الفعال عما أصابه من أضرار بسبب انتهاك بياناته الشخصية.

وتتمثل صور الخطأ أو الإضرار بمخالفة شروط جمع وحفظ ومعالجة وتداول البيانات الشخصية المشار إليها سابقاً. كما لو جمعت بدون إذن ولا علم صاحب البيانات أو إذا اتيحت للغير بدون إذنه أو تجاوز الغرض من المعالجة أو خزنت لأكثر من المدة اللازمة له أو لأغراض غير مشروعة.

1 الشرقاوي، الشهابي إبراهيم (2011). مصادر الالتزام غير الإرادية في قانون المعاملات المدنية الإماراتي (ص20). الطبعة الأولى. الشارقة: الآفاق المشرقة ناشرون.

2 أو ما يعرف بالخطأ في بعض التشريعات، كالتشريع المصري و التشريع الجزائري.

3 المذكرة الإيضاحية لقانون المعاملات المدنية لدولة الإمارات العربية المتحدة.

ونشير هنا إلى أنه إذا كان المعالج للبيانات شخصاً معنوياً عاماً قامت مسؤولية المتبوع عن أفعال تابعيه وإذا كان شخصاً معنوياً خاصاً، يمكن الحديث عن المسؤولية العقدية.

1. الضرر

الركن الثاني من المسؤولية التقصيرية هو الضرر، ويمكن أن تحدث تطبيقات الذكاء الاصطناعي ضرراً أدبياً لمستخدمي هذه التطبيقات عند انتهاك خصوصيتهم التي تشكل الدرع المتين للحرية و العرض و الشرف و السمعة و المركز الاجتماعي و كذلك الاعتبار المالي و أي معلومات خاصة يتمتع الفرد بعدم إمكانيه كشفها على الملأ، و لا يمكن في هذا المجال تصور الضرر المادي لتطبيقات الذكاء الاصطناعي عند انتهاك الخصوصية.

2. علاقة السببية

نص المشرع الإماراتي في المادة (292) من قانون المعاملات المدنية على وجوب وجود علاقة سببية بين الإضرار والضرر لاكتمال أركان المسؤولية التقصيرية وثبوت وقوعها مما يوجب الضمان، وبتطبيق ذلك على انتهاك الحق في الخصوصية نرى أن فعل انتهاك حق الخصوصية هو الذي سبب الضرر الأدبي من ألم، فلولا هذا الفعل لما شعر المضرور بذلك الألم الذي استوجب معه الضمان.

بعد استعراض أركان المسؤولية التقصيرية، ترى الباحثة أنه يمكن تطبيق نظرية المسؤولية التقصيرية على تطبيقات الذكاء الاصطناعي، فيمكن معها استظهار الإضرار عندما يكون هناك إضرار بالمستهلك آو صاحب البيانات سواء كان هنالك تعمد في انتهاك خصوصية البيانات الشخصية أو بإهمال في اتخاذ الإجراءات اللازمة لحفظ هذه البيانات من الانتهاك، كما يمكن استظهار الضرر الأدبي التي قد ينتج عن انتهاك البيانات الشخصية في تطبيقات الذكاء الاصطناعي، لكن ستظهر إشكالية أخرى يجب معالجتها في عدم إمكانية من تقع عليه عاتق هذه المسؤولية من مبرمج أو فني أو مسؤولي حفظ البيانات في تطبيقات الذكاء الاصطناعي مع وجود التحديثات المستمرة لهذه التطبيقات.

الفرع الثاني: المسؤولية وفقا لأنظمة خاصة

ونتطرق هنا لفكرة تأسيس مسؤولية تطبيقات الذكاء الاصطناعي على أساس فكرة الحراسة، وعلى أساس مسؤولية المنتج عن منتجاته المعيبة، بالإضافة إلى عرض إمكانية قيام مسؤولية خاصة بتطبيقات الذكاء الاصطناعي.

أولا: المسؤولية عن حراسة الأشياء

وفقا لهذا النوع من المسؤولية، يتصور أن تنطبق المسؤولية عن الأشياء و الآلات على تطبيقات الذكاء الاصطناعي، وقد نظم المشرع الإماراتي الأحكام الخاصة بالأشياء و الأموال في الفصل الرابع من قانون المعاملات المدنية في المواد من (95 – 103)[1]، و نص المشرع الإماراتي في المادة 316[2] من قانون المعاملات المدنية على

1 يقابلها المواد من (81 – 88) من القانون المدني المصري، و المواد (516 – 536) من القانون المدني الفرنسي.

2 تقابلها المادة 178 من القانون المدني المصري.

أنه:"كل من كان تحت تصرفه أشياء تتطلب عناية خاصة للوقاية من ضررها أو آلات ميكانيكية يكون ضامناً لما تحدثه هذه الأشياء أو الآلات من ضرر إلا ما لا يمكن التحرز منه، ذلك مع عدم الإخلال بما يرد في هذا الشأن من أحكام خاصة"، و لم يحدد المشرع على وجه الخصوص الأشياء التي تتطلب عناية خاصة، فيكون ذلك وفق الظروف المحيطة [1]أو قد تختلف من وقتٍ إلى آخر فيمكن اعتبار تطبيقات الذكاء الاصطناعي من الأشياء التي تتطلب عناية خاصة لما تحتفظ به من كم هائل من البيانات الخاصة للمستخدمين التي لا يجوز الاطلاع عليها إلا للمخول لهم ذلك.

وقد عُرِف الحارس وفق القانون الفرنسي بأنه:"الشخص الذي يمارس لحظة وقوع الضرر سلطة الاستعمال و الرقابة و التوجيه على الشيء"[2]، وفقاً للتعريف السابق تثبت صفة الحراسة للشخص عندما يتمتع بالسلطات الثلاث و التي تتمثل بسلطة الاستعمال و الرقابة و التوجيه وقت حدوث الضرر للمضرور، و هنا تثبت القرينة على السيطرة الفعلية للحارس، و الأصل هو أن مالك الشيء هو حارسه، مالم تقم قرينة على انتقال السيطرة الفعلية لشخص آخر فمعه يكون الأخير مسؤول مسؤولية الحارس[3]، و هذا ما أكدته المادة (178) من القانون المدني المصري: "كل من تولى حراسة أشياء تتطلب عناية خاصة أو حراسة آلات ميكانيكية يكون مسئولاً عما تحدثه هذه الأشياء من ضرر ما لم يثبت أن وقوع الضرر كان بسبب أجنبي لا يد له فيه ...."، تشير المادة إلى أن الحراسة على الأشياء الموجبة للمسئولية على أساس الخطأ المفترض وفقاً لنص المادة لا تتحقق إلا بسيطرة الشخص الطبيعى أو المعنوى على الشئ سيطرة فعلية فى الاستعمال والتوجية والرقابة لحساب نفسه، و لا يدرؤها سوى إثبات السبب الأجنبي و الذي يكون لا يد للحارس في وقوع الشيء [4]. فالحارس في أنظمة الذكاء الاصطناعي تثبت للشخص عندما يكون التطبيق أو النظام تحت سيطرته الفعلية والذي معه يكون له سلطة الاستعمال والرقابة والتوجيه للقائمين على العمل على النظام أو التطبيق، فإذا ما حدث انتهاك للبيانات الشخصية فيرجع على من ثبتت عليه مسؤولية الحارس عند وقوع الضرر حتى ولو لم يقع منه خطأ، فهذا المبدأ استندت عليه محكمة تمييز دبي في أحد أحكامها، بأن المسؤولية تتحقق في حق الحارس ولو يقع منه خطأ إعمالاً للقاعدة الفقهية (الغرم بالغنم).[5]

ترى الباحثة أنه يمكن تطبيق هذه النظرية على تطبيقات الذكاء الاصطناعي، فيمكن اعتبار تطبيقات الذكاء الاصطناعي من الأشياء التي تحتاج عناية خاصة باعتبارها تسبب ضرراً قد يؤدي إلى انتهاك خصوصية مستخدمي هذه التطبيقات، فلا بد من وجود حارس يقوم على حراستها مع امتلاكه للسلطات الثلاث التي حددها القانون لحراسة الأشياء التي تتطلب عناية خاصة، و من ثم بالرجوع عليه في حال حدوث انتهاك للبيات الشخصية في هذا التطبيق،

---

1 الشرقاوي، الشهابي إبراهيم. مرجع سابق. ص111.

2 راجع، قاسم، أحمد نصر (سبتمبر 2018). المسؤولية المدنية لحارس الأشياء "دراسة مقارنة" (أطروحة ماجستير). جامعة النجاح الوطنية. نابلس، فلسطين. ص32.

3 انظر، السلمان، خالد عبدالله (2014). طبيعة مسئولية المنتج و حالات الإعفاء منها "دراسة مقارنة" (أطروحة ماجستير). جامعة المنوفية. المنوفية، مصر. ص102.

4 راجع، محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (6420) لسنة (64) القضائية، الصادر في جلسة 2019/06/08، موقع محكمة النقض المصرية، تاريخ الدخول: 09/04/2022، على الرابط:

https://www.cc.gov.eg/judgment_single?id=111392621&&ja=267808 last visit :06/04/2022.

5 راجع، محكمة تمييز دبي، الدائرة المدنية، الطعن رقم (247) لسنة (2019)، الصادر في جلسة 2019/07/25، موقع محامو الإمارات، تاريخ الدخول: 20/04/2022، على الرابط:

https://www-mohamoon-uae-com.uaeu.idm.oclc.org/uaeu/default.aspx?Action=IntrDisplayJudgmentFile&PageNumber=1&Type=5&ID=31210&strSearch=حراسة%20الشيء. Last visit: 20/03/2022

لكن الحماية قد لا تكون كافية هنا في حال تعدد الحراس و امتلاكهم لسلطات الحارس، و من ثم ضياع حق المستخدم عند انتهاك بياناته الشخصية.

ثانيا: المسؤولية عن المنتجات المعيبة

يمكن تصور قيام مسؤولية المنتج عن منتجاته المعيبة عن الأضرار التي تحدثها تطبيقات الذكاء الاصطناعي، فقد عرف المشرع الإماراتي الروبوت الإلكتروني في المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية بأنه: "برنامج الكتروني يتم إنشاؤه أو تعديله لغرض تشغيل المهام المؤتمتة بكفاءة وسرعة". فالمشرع الإماراتي كان سباقاً عندما وضع هذا التعريف للروبوت الإلكتروني حيث لم يسبقه أي تشريع في ذلك، ومن الآثار التي تترتب على ذلك اعتبار الكثير من البرامج الالكترونية التي تعمل في مجال البرمجة أو التجميع أو المعالجة روبوتاتٍ الكترونية فهي تؤدي إلى غرض واحد وهي تشغيل المهام المؤتمتة بكفاءة وسرعة. والمسؤولية عن المنتجات المعيبة يمكن أن تكون عقدية أو تقصيرية.

أ- المسؤولية العقدية عن المنتجات المعيبة وتطبيقها على الأضرار الناشئة عن أنظمة الذكاء الاصطناعي

تدور هذه النظرية حول العلاقة العقدية سواء كانت هذه العلاقة بيعاً أو استئجاراً، سنتناول فيما يلي عقدي البيع والاستئجار في أنظمة الذكاء الاصطناعي والمسؤولية الناشئة عن كل منهما.

أما بخصوص عقد البيع في أنظمة الذكاء الاصطناعي، فقد نظم المشرع الإماراتي العلاقة بين البائع و المشتري في قانون المعاملات المدنية في الفرع الأول من الباب الأول في المواد (489-606)، و عرف المشرع الإماراتي عقد البيع في المادة 489 من قانون المعاملات المدنية بأنه: "البيع هو مبادلة مال غير نقدي بمال نقدي"، بينما عرفه المشرع المصري في المادة 418 من القانون المدني المصري بأنه: "البيع عقد يلتزم به البائع، أن ينقل للمشتري ملكية شيء، أو حقاً مالياً آخر، في مقابل ثمن نقدي"[1]، و لا يرتب عقد البيع آثاره على الأطراف إلا إذا كان صحيحاً مشتملاً على الأركان التي حددها القانون و هي ثلاثة أركان: التراضي، و المحل، و السبب، فإذا حدث تخلف لركن من هذه الأركان، كان البيع باطلاً غير مرتب لآثاره التي نص عليها القانون. كما يشترط لصحة انعقاد عقد البيع بالإضافة إلى الأركان الواردة أعلاه أهلية المتعاقدين و خلو التراضي من عيوب الإرادة، فإذا ما احتوى التراضي على عيب من عيوب الإرادة (الإكراه، التغرير و الغبن، الغلط)[2]، أو في حال كان المتعاقد ناقص الأهلية، يكون عقد البيع هنا موقوفاً على إجازة الولي أو الوصي في الحدود التي يجوز فيها التصرف في التصرفات الدائرة بين النفع و الضرر، أو موقوفاً على إجازة ناقص الأهلية نفسه بعد بلوغه سن الرشد[3]. ويرجع الأمر في تقدير مدى توافر عيوب الإرادة لقاضي الموضوع وفق تفسيره لنصوص القانون[4].

1 انظر، عبدالدايم، حسني محمود (2019م). شرح قانون المعاملات المدنية الإماراتي العقود المسماة - عقد البيع – (ص45). دبي - الإمارات: دار النهضة العربية. القاهرة - مصر، دار النهضة العلمية.

2 انظر المواد (176– 198) من قانون المعاملات المدنية الإماراتي.

3 انظر عبدالدايم، حسني محمود. مرجع سابق. ص109.

4 للمزيد راجع بدر، أسامة أحمد (2022). أحكام قانون حماية المستهلك الإتحادي رقم (15) لسنة 2020م (ص38). الطبعة الثانية . الإمارات: جامعة الإمارات العربية المتحدة.

و بمجرد انعقاد العقد صحيحاً تنشأ علاقة البيع العقدية بين البائع (مُصنع تطبيقات الذكاء الاصطناعي) و المشتري (الشركات الكبرى) و يرتب حقوقاً و التزامات في ذمة كل من البائع و المشتري ، فقيام البائع مصنع (منتج) تطبيقات الذكاء الاصطناعي ببيع هذه التطبيقات للمشتري (الشركات كبرى)، فهنا تنتقل المسؤولية وفق عقد البيع من مصنع تطبيقات الذكاء الاصطناعي إلى الشركات التي بيعت لها هذه التطبيقات. فإذا ما حدث انتهاك للبيانات الشخصية لأحد الأفراد في تطبيقات الذكاء الاصطناعي، تتحدد المسؤولية هنا فيما إذا كان المبيع (تطبيقات الذكاء الاصطناعي) قد انتقل إلى ذمة المشتري أم أنه في ذمة البائع، فإذا حدث الانتهاك من خلال تطبيقات الذكاء الاصطناعي و التطبيق تحت يد البائع فيمكن الرجوع على البائع بالتعويض.

أما عن عقد الإيجار في أنظمة الذكاء الاصطناعي، فقد نظم المشرع الإماراتي العلاقة بين المؤجر و المستأجر في قانون المعاملات المدنية في الفصل الأول من الباب الثاني في المواد (742– 848)، و يعرف عقد الإيجار بأنه:"عقد يلتزم المؤجر بمقتضاه أن يمكن المستأجر من الإنتفاع بشيء معين مدة معينة لقاء أجر معلوم"[1]، فعقد الإيجار يرتب التزامات في ذمة طرفي العقد، كالتزام المؤجر من تمكين المستأجر بالانتفاع بالعين المؤجرة، فهو عقد يرد على المنفعة، و الإيجار من العقود التي يستغرق تنفيذها مدة زمنية معينة، لم ينظم قانون المعاملات المدنية عقد الإيجار على تطبيقات الذكاء الاصطناعي، و بالرجوع للنصوص التقليدية في القانون ذاته بما يخص عقد الإيجار في تطبيقها على أنظمة الذكاء الاصطناعي، نرى إمكانية إنشاء عقد الإيجار بين المؤجر (مالك أحد تطبيقات الذكاء الاصطناعي) و المستأجر (أحد الشركات الكبرى أو المؤسسات) بحيث عند انعقاد عقد الإيجار، ينشأ التزام في ذمة المؤجر و هو وجوب تمكين المستأجر من الانتفاع بهذا التطبيق و الذي هو محل الإيجار، أي أن ملكية محل العقد (تطبيق الذكاء الاصطناعي) هنا لا تنتقل إنما يتم الإبقاء عليها في ذمة المالك، فإذا ما حدث انتهاك للبيانات الشخصية في الفترة الزمنية التي يسري فيها عقد الإيجار، فتنشأ المسؤولية هنا وفقاً لعقد الإيجار على المستأجر (الشركة التي تم تأجير تطبيق الذكاء الاصطناعي لها و تنتفع بهذا التطبيق خلال فترة الإيجار)، لكن يمكن أن تثور إشكالية هنا في حال قيام الشركة المالكة لهذا النظام أو البرنامج بتأجير البرنامج لعدد من المستأجرين فمن يكون مسؤولاً في هذه الحالة إذا ما حدث انتهاك للبيانات الشخصية لأحد المستخدمين.

ب- المسؤولية التقصيرية عن الأضرار الناشئة عن أنظمة الذكاء الاصطناعي

يثور تساؤل في إمكانية اعتبار برامج الذكاء الاصطناعي منتجات أو سلع أو خدمات، و بالرجوع للقانون الاتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك نرى أن المشرع عرف السلعة في المادة الأولى بأنها:"كل مادة طبيعية أو منتج صناعي أو زراعي أو حيواني أو تحويلي أو فكري أو تقني بما في ذلك العناصر الأولية للمواد و المكونات التي تدخل في المنتج"، و كذلك عرف الخدمة في المادة ذاتها من القانون ذاته بأنها: "كل ما يقدم للمستهلك سواء تم ذلك بأجر أو بدون أجر"[2]، و ذهب المشرع الفرنسي في تعريف في المادة (1386) الفقرة (03) من القانون

1 راجع، منصور، محمد حسين (2010م). شرح العقود المسماة(ص405). الطبعة الأولى. بيروت ، لبنان: منشورات الحلبي.

2 راجع المادة الأولى من قانون اتحادي رقم (15) لسنة 2020م في شأن حماية المستهلك، المنشور في الجريدة الرسمية: السنة الخمسون، العدد ستمائة و تسعون، 15 نوفمبر 2020م.

المدني الفرنسي بقولها:"يعد منتجاً كل مالٍ منقول، حتى و إن ارتبط بعقار، و يسري هذا الحكم على منتجات الأرض، و تربية المواشي و الدواجن، و الصيد البحري، و تعتبر الكهرباء منتجاً"[1]، مما سبق نرى بإمكانية اعتبار تطبيقات الذكاء الاصطناعي سلعة أو خدمة، فتطبيقات الذكاء الاصطناعي عبارة عن منتج فكري و تقني لذلك ينطبق عليها تعريف السلعة، و يمكن اعتبارها خدمة فهي تقدم للمستهلك سواء كان ذلك بأجر أو بدون أجر.

لا يسأل المنتج أو المزود عن أضرار أنظمة الذكاء الاصطناعي إلا إذا توافرت شروط معينة، فيجب توافر الشروط الثلاثة لتنشأ المسؤولية و هي الخطأ و الضرر و علاقة السببية، و إثبات الخطأ الصادر من المنتج أو المبرمج لأنظمة الذكاء الاصطناعي قد يكون أمراً في غاية الصعوبة، لأن هذا المنتج قد يكون معقداً في تكوينه أو تحديثه مع عدم علم المضرور بأسرار تكوينه أو تطويره و برمجته، مما يصعب على المضرور إمكانية الحصول على التعويض. بالإضافة إلى التزاماته بالتزامات أخرى نص عليها المشرع في قانون حماية المستهلك و هما:

الالتزام الأول: الالتزام بسلامة المنتج المبيع

نص المشرع الإماراتي على الالتزام بسلامة المنتج المبيع للمستهلك في الفقرة الثانية من المادة (11) على أنه:"يلتزم المزود بضمان الخدمة التي قدمها و خلوها من العيب و الخلل فترة زمنية تتناسب مع طبيعة تلك الخدمة، و إلا أعاد المبلغ الذي دفعه المستهلك أو جزءاً منه، أو أدي الخدمة مرة أخرى على الوجه الصحيح"[2]، أي اتخاذ الإجراءات الضرورية لضمان سلامة المنتجات و الخدمات و هو التزام مستقل في حد ذاته[3]، يستوضح لنا مما سبق أن الالتزام القانوني الذي يقع على عاتق المزود أو المنتج أو المبرمج هو الالتزام بسلامة البيانات الشخصية، هو التزام بتحقيق نتيجة، فإذا لم يلتزم مشغل تطبيقات الذكاء الاصطناعي بتحقيق السلامة في حفظ البيانات الشخصية و حمايتها من الانتهاك أو الاختراق، فإذا ما تعرضت للانتهاك أو الاختراق فيكون مسؤولاً إذا ما قام بإعلام صاحب البيانات بخطورة النظام الذي يقوم باستخدامه، كإعلامه بأن هذا النظام يعمل وفقاً لبرنامج الكوكيز أو أي برامج أخرى يترتب عليها تخزين البيانات الشخصية لمستخدمي التطبيق، و قد عرف الالتزام بالإعلام بأنه "بيان أو إشارة أو تعليمات يمكن أن تقدم توضيحاً بشأن واقعة أو قضية ما"[4]، و أرى أن الالتزام بالإعلام لا يكفي لمستخدمي أنظمة الذكاء الاصطناعي لأنه الخبرة التقنية للمستخدم في هذه البرامج لا ترقى للدرجة الكافية بمعرفة أضرار هذه البرامج فكان لابد أن يكون هناك إعلام بالتحذير من أن هذه البرامج قد يترتب عليها حفظ البيانات الشخصية للمستخدمين مما قد يؤدي إلى انتهاكها أو استخدامها في أغراض تسويقية بطرق غير مشروعة في بعض الأحيان، و الالتزام بالتحذير يعني "لفت نظر المتعاقد الآخر إلى المخاطر المادية و القانونية المترتبة على التعاقد"[5]، فهو ليس التزاماً بالإعلام و ليس التزاماً بالنصح فيقع في منطقة وسطى بينهما، فهو أعلى عن الالتزام بالإعلام و أقل درجة من الالتزام بالنصح.

1 انظر، منشور لدى زعبي، عمار (2017). حماية المستهلك من الأضرار الناتجة عن المنتجات المعيبة (ص76). الطبعة الأولى. عمان، الأردن: دار الأيام.

2 راجع الفقرة الثانية من المادة (11) من قانون اتحادي رقم (15) لسنة 2020م في شأن حماية المستهلك.

3 للمزيد انظر بدر، أسامة أحمد. مرجع سابق. ص158-159.

4 انظر، عباسي، بوعبيد (2008). الإلتزام بالإعلام في العقود–دراسة في حماية المتعاقد و المستهلك (ص34). مراكش–المغرب. الطبعة الأولى.

5 انظر، عباسي، بوعبيد. مرجع سابق. ص48.

من أهم الالتزامات التي تقع على المزود (المنتج) هو الإلتزام بضمان العيوب الخفية، و العيب الخفي هو العيب الكامن في المبيع أي العيب غير الظاهر[1]، و بالرجوع للقانون الإماراتي نجد عدم وجود نصوص تعالج مسؤولية المنتج عن المنتجات المعيبة، لكن المشرع الإماراتي فرض هذا الالتزام بشكل صريح على المزود في الفقرة الثانية من المادة العاشرة من قانون حماية المستهلك[2]، بالإضافة إلى أنه عرف العيب الخفي في مجال المسؤولية العقدية في المادة (4/544) بنصه على أنه:"هو العيب الذي لا يعرف بمشاهدة ظاهر المبيع أو لا يتبينه الشخص العادي أو لا يكشفه غير خبير أو لا يظهر إلا بالتجربة"، و يشترط للعيب الخفي عدة شروط: 1- أن يكون العيب قديماً و قد نص المشرع على ذلك في المادة 2/544 من قانون المعاملات المدنية بأنه: "و يعتبر العيب قديماً، إذا كان موجوداً في المبيع قبل البيع، أو حدث بعده، و هو في يد البائع قبل التسليم"، أي أن يكون العيب موجوداً و سابقاً على تسليم المبيع للمشتري، فالعيب الطارئ على المبيع بعد تمام التسليم لا يضمنه البائع[3]، 2- أن يكون العيب خفياً فالعيب الظاهر البائن لا يضمنه البائع أي الذي كان في استطاعت المشتري تبينه أثناء شراء المبيع، 3- أن يكون العيب مؤثراً، فلا يكفي أن يكون العيب قديماً و خفياً بل يجب أيضاً أن يكون العيب مؤثراً أي "أن يكون العيب من شأنه أن ينقص من قيمة المبيع، أو يقلل من منفعته"[4]، و ذهب القانون المدني الفرنسي إلى اعتبار العيب مؤثراً إذا كان من شأنه أن يجعل المبيع غير صالح لما أعد له بطبيعته[5]، و لا يعد العيب مؤثراً إذا كان مما يتسامح فيه.

و هذا ما أكدته محكمة النقض في حكمها بأنه يجب توافر شروط العيب الخفي لكي يثبت خيار العيب للمشتري، فيكون من حق المشتري طلب فسخ العقد و رد المبيع إلى البائع و الرجوع على المشتري بما دفعه من ثمن، لكن لكي يثبت هذا الحق لابد أن يكون العيب قديماً و مؤثراً في قيمة المبيع و يشترط جهل المشتري في ذلك، و أن لا يكون البائع قد اشترط البراءة منه، و قد أشارت المحكمة إلى ضابط العيب القديم بأن يكون موجوداً في المبيع وقت التسليم، بالإضافة إلى الإشارة لحالات سقوط خيار العيب فيكون بالإسقاط أو الرضا بالعيب بعد العلم به أو بالتصرف في المعقود عليه و لو قبل به و بهلاكه.[6]

ترى الباحثة أنه بالرغم من الشروط التي وضعت من قبل المشرع الإماراتي و اتسمت بالوضوح، إلا أنه من الصعوبة تطبيقها على أنظمة الذكاء الاصطناعي، فمعيار تحديد أن يكون العيب قديماً لا يمكن تطبيقه لتركيبة النظام المعقدة و كذلك للتحديثات التي تطرأ على برامج الذكاء الاصطناعي بين الحين و الآخر، و لكي تقوم المسؤولية يجب

---

1 عبد الجليل، يسرية محمد (2007). المسئولية عن الأضرار الناشئة عن عيوب تصنيع الطائرات (ص232). الإسكندرية: منشأة المعارف.

2 للمزيد راجع بدر، أسامة أحمد. مرجع سابق. ص166.

3 انظر، عبدالصمد، حسني محمود (2018). الوجيز في شرح عقد البيع وفقاً لأحكام قانون المعاملات المدنية الإماراتي رقم 5 لسنة 1985 (ص236). الطبعة الأولى. دبي: دار النهضة العلمية.

4 انظر، عبدالصمد، حسني محمود. مرجع سابق. ص239.

5 انظر، سرحان، عدنان إبراهيم (2010). أحكام البيع في قانون المعاملات المدنية الإماراتي (ص184). الطبعة الثانية. عَمان: دار الآفاق المشرقة.

6 راجع، محكمة نقض أبوظبي، الدائرة التجارية، الطعن رقم 902 لسنة 2021م، الصادر في جلسة 2021/11/02م، موقع محامو الإمارات، تاريخ الدخول: 07/05/2022، على الرابط:

https://www-mohamoon-uae-com.uaeu.idm.oclc.org/uaeu/default.aspx?Action=IntrDisplayJudgmentFile&PageNumber=1&Type=5&ID=49121&strSearch=%2Oالعيب الخفي

بالإضافة إلى شرط العيب القديم بأن يكون العيب خفياً و مؤثراً، كأن يكون العيب غير ظاهر وفقاً لمعيار الرجل المعتاد، أما عن تأثير العيب فسيكون العيب مؤثراً عندما يكون هذا العيب سبباً في انتهاك البيانات الشخصية للأفراد و بالتالي سبباً في انتهاك الخصوصية التي يجب عدم المساس بها. و في حال انتقال البرنامج من المنتج إلى المطور أو شركة أخرى تحوز هذا البرنامج فموضوع رجوع المضرور على أي منهم سيصبح أكثر تعقيداً.

ثالثا: تأسيس نظام خاص بالمسؤولية استنادا لمنح تطبيقات الذكاء الاصطناعي الشخصية القانونية

يقصد بالشخصية القانونية: "الصلاحية لاكتساب الحقوق و تحمل الالتزامات؛ أو هي صفة تلحق من تتقرر له الحقوق لمصلحة أو تجب التكاليف في ذمته"[1]، نجد أن ثبوت الشخصية القانونية للشخص الطبيعي أو الاعتباري في القانون تمنحه حقوقاً و ترتب في ذمته التزاماتٍ يجب الوفاء بها، و بالرغم من التوصية الصادرة من قِبل البرلمان الأوروبي بشأن الروبوتات في 16 فبراير 2017 و التي تنص على منح الروبوتات الشخصية الإلكترونية، و من ثم إنشاء الوضع القانوني لها على المدى الطويل، حتى يكون لها وضع الأشخاص الإلكترونية في المساءلة عن الأضرار التي قد تحدثها أو تتسبب بها، إلا أن هذه التوصية تسبب في إحداث الجدل بين فقهاء القانون في إمكانية منح الشخصية القانونية لتطبيقات الذكاء الاصطناعي مما قد يظهر فئة ثالثة من الأشخاص تختلف عن الشخص الطبيعي و الشخص الاعتباري و هي شخصية الروبوت، فلا يمكن تصور منح تطبيقات الذكاء الاصطناعي الشخصية القانونية المتعارف عليها لدى فقهاء القانون للأسباب التالية:

أن منح أنظمة الذكاء الاصطناعي الشخصية القانونية سيرتب آثاراً قانونية، تتمثل في منح هذه الأنظمة العديد من الحقوق التي تمنح لصاحب الشخصية القانونية، كالاسم أو الموطن أو الذمة المالية أو الجنسية، و بالرغم من أنه قد تم منح الجواز في بعض الدول للروبوت كما تم في السعودية حيث منحت الجنسية للروبوت صوفيا من قبل المملكة العربية السعودية في أكتوبر من العام 2017، مما يجعلها الدولة الأولى في العالم التي تمنح الجنسية للروبوت و جعل البعض يصفها بالخطوة المرعبة لما يترتب عليها آثاراً قانونية يجب منحها لها قريبة من الأشخاص[2]، إلا أن ذلك لا يمنحها الشخصية القانونية، و في إطار منح الشخصية القانونية فقد أوصى البرلمان الأوروبي بإنشاء نظام تأمين يغطي الأضرار التي يمكن أن تنشأ من عمل الروبوتات، و مع ذلك لا يمكن منحها الشخصية القانونية و بما يخص نظام التأمين فيقاس عليه التأمين على المركبات أو العقارات، و المقصود بذلك التأمين ضد المسؤولية المدنية، فهذا ما تم تأكيد من قبل التوصية الأوروبية في المادة(57)[3]، بهدف حماية الأفراد من الأضرار التي قد تسببها الروبوتات أو أنظمة الذكاء الاصطناعي.

---

1 انظر، عبيد، أحمد كمال (2019). الأهلية القانونية للوكيل الذكي و دورها في تحديد المسؤولية الناتجة عن معاملاته الإلكترونية. *مجلة جامعة الشارقة للعلوم القانونية*. (2)*16*، ص6.

2 Sam, B (2017). Saudi Arabia takes terrifying step to the future by granting a robot citizenship .Access date : 23/01/2022 .https://web.archive.org/web/20180623032828/https://www.avclub.com/saudi-arabia-takes-terrifying-step-to-the-future-by-gra-1819888111

3 Point (57) of European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics stipulates: "Points out that a possible solution to the complexity of allocating responsibility for damage caused by increasingly autonomous robots could be an obligatory insurance scheme, as is already the case, for instance, with cars; notes, nevertheless, that unlike

كما أنه بمجرد منح أنظمة الذكاء الاصطناعي الشخصية القانونية، فلن يكون هناك مساءلة للشركة المصنعة أو المبرمجة أو المشتري أو جميع الأطراف ذات العلاقة، فالمسؤولية ستكون حينئذ على هذا النظام الذي منح الشخصية القانونية ليكون هو المدعى عليه في الدعاوى المدنية لاستيفاء التعويض منه، مما سيؤدي إلى التقليل و استبعاد الشركات المصنعة أو المبرمجة أو المطورة لأنظمة الذكاء الاصطناعي، و ما سينتج عن ذلك من نتائج خطيرة كدقة في التصنيع و زيادة في خطر هذه الأنظمة على خصوصية الأفراد.

وأخيراً، فإن التعارض الكبير في الطبيعة القانونية بين أنظمة الذكاء الاصطناعي و الأشخاص الطبيعية و الاعتبارية التي منحت الشخصية القانونية يحول دون تطبيق هذه النظرية، فالشخص الطبيعي والاعتباري الذي منح الشخصية القانونية طبيعته تختلف عن طبيعة أنظمة الذكاء الاصطناعي، فعند منح الشخصية الاعتبارية لأنظمة الذكاء الاصطناعي فإنه سيتشابه في الطبيعة القانونية للأشخاص الطبيعية و الاعتبارية، فهي تعتبر من قبيل الأشياء التي لا تتمتع بالشخصية القانونية[1]. مما سبق نرى أن أنظمة الذكاء الاصطناعي أنظمة ذو طبيعة خاصة لا يمكن منحها الشخصية القانونية فبذلك تخرج عن نطاق إمكانية منحها الشخصية القانونية. و من المبادئ الحديثة التى أرستها محكمة النقض المصرية في أحد أحكامها بأن الانترنت ليس له حدود و لا قيادة قانونية، أي ليس له شخصية قانونية معنوية قد تمثله في مواجهة مستخدمي شبكات الانترنت أو الغير، فهو عبارة عن اتحادي فيدرالي للشبكات، " إذ كان من المتعارف عليه أنه توجد مناطق من الحياة الخاصة لكل فرد تُمثل أغوارًا لا يجوز النفاذ إليها وهذه المناطق من خواص الحياة ودخائلها وينبغى دومًا ــ ولإعتبار مشروع ــ ألا يقتحمها أحد ضمانًا لسريتها وصونًا لحرمتها ودفعًا لمحاولة التلصص عليها أو اختلاس بعض جوانبها، وبوجه خاص من خلال الوسائل العلمية الحديثة التى بلغ تطورها حدًا مذهلًا وكان لتنامى قدراتها على الإختراق أثرًا بعيدًا على الناس جميعهم حتى فى أدق شئونهم وما يتصل بملامح حياتهم بل وبياناتهم الشخصية والتي غدا الاطلاع عليها والنفاذ إليها كثيرًا ما يُلحق الضرر بأصحابها، إذ أن البشرية لم تعرف في أي وقت مضى مثل هذا التزايد الحالي والسرعة في العلاقات بين الناس".[2]

و في هذا الشأن يجب الإشارة إلى مشروع قانون الذكاء الاصطناعي (Artificial intelligence act) المقترح لأنظمة الذكاء الاصطناعي و الذي تم وضعه من قِبل المفوضية الأوروبية في أبريل 2021، و يركز الإطار القانوني المقترح على الاستخدام المحدد لأنظمة الذكاء الاصطناعي و المخاطر المرتبطة به، من خلال وضع تعريف منضبط لأنظمة الذكاء الاصطناعي، و تصنيف أنظمة الذكاء الاصطناعي وفقاً للنهج القائم على المخاطر لترخيص هذه الأنظمة و توسيع قائمة أنظمة الذكاء الاصطناعي المحظورة، و تعزيز آليات الإنفاذ و التعويض.[3]

---

the insurance system for road traffic, where the insurance covers human acts and failures, an insurance system for robotics should take into account all potential responsibilities in the chain".

1 راجع، بطيخ، مها رمضان محمد (2021). المسؤولية المدنية عن أضرار أنظمة الذكاء الاصطناعي –دراسة تحليلية مقارنة–. *المجلة القانونية*، جامعة القاهرة. (5)*9*، ص1552.

2 راجع، محكمة النقض المصرية، الدائرة التجارية، الطعن رقم (9542) لسنة (91) القضائية، الصادر في جلسة 2022/03/16، موقع محكمة النقض المصرية، تاريخ الدخول: 16/05/2022، على الرابط:

https://www.cc.gov.eg/i/H/111740345.pdf

3 For more, see https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792, Access date: 10/06/2022.

المطلب الثاني: آثار المسؤولية المدنية عن المساس بالحق في الخصوصية

جميع الأفعال التى تشكل مساساً بالحق في الخصوصية جرمها القانون في عدة مواضع في مختلف القوانين و وضع لها جزاءً يطبق في حال وقع الفعل، فإذا كان الفعل يرتب جزاءً فيجب أن يتبعه تعويضاً للمضرور لما أصابه من ضرر سواء كان هذا الضرر مادياً أو معنوياً كما سيأتي معنا لاحقاً:

و بالإطلاع على المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، و المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية فلم يتطرق فيهما المشرع الإماراتي لموضوع التعويض عن الأضرار التى تلحق المضرور جراء المساس بحقه في الخصوصية، عكس اللائحة العامة التي نصت على عدد من الجزاءات الإدارية[1] و ضوابطها في حالة انتهاك البيانات الشخصية. و لعدم التطرق لموضوع التعويض في التشريع الإماراتي كان لزاماً العودة إلى القواعد التقليدية في قانون المعاملات المدنية بما يخص تعويض المضرور عن حقه في المساس بالخصوصية:

الفرع الأول: الأساس في تقدير التعويض

يهدف التعويض إلى جبر الضرر، وضع المشرع الإماراتي مبدأً عاماً في تقدير الضرر في المادة 292 من قانون المعاملات المدنية، بأن نصت على أن الضمان يقدر بما لحق المضرور من ضرر و ما فاته من كسب، و وضع شرطاً بأن يكون هذا الضرر نتيجة طبيعية للفعل الضار أي شرط وجود علاقة السببية بين الفعل و النتيجة.

كما أكد على وجوب التعويض عن الضرر الأدبي في المادة 293 مع وضع عدة ضوابط على ذلك بنصه على أنه:"1- يتناول حق الضمان الضرر الأدبي ويعتبر من الضرر الأدبي التعدي على الغير في حريته أو في عرضه أو في شرفه أو في سمعته أو في مركزه الاجتماعي أو في اعتباره المالي. 2- ويجوز أن يقضي بالضمان للأزواج وللأقربين من الأسرة عما يصيبهم من ضرر أدبي بسبب موت المصاب. 3- ولا ينتقل الضمان عن الضرر الأدبي إلى الغير إلا إذا تحددت قيمته بمقتضى اتفاق أو حكم قضائي نهائي". و بالرجوع إلى المادة السابقة نرى أن المشرع الإماراتي أعطى المضرور حق التعويض الأدبي إذا ما لحقه ضرر جراء أي فعل من الأفعال الضارة، كما أنه قضى بالضمان للأزواج و الأقربين من الأسرة عما يصيبهم من حزن و أسى على فقد المضرور، و لم يحدد المشرع درجة الأقربين في هذه المادة مما يوسع من نطاق الأقربين المستفيدين من التعويض عما لحقهم من آلام نفسية.

وقد كنا استبعدنا وقوع الأضرار المادية نتيجة انتهاك الحق في الخصوصية في تطبيقات الذكاء الاصطناعي، فقد اقتصر وقوع الضرر الأدبي دون المادي من انتهاك الخصوصية، و لوقوع الضرر الأدبي الذي يوجب التعويض لابد من توافر العناصر الموجبة للتعويض، و في هذا الصدد فالكثير من التشريعات العربية و غيرها أقرت التعويض عن الضرر المعنوي. والتعويض الأدبي في تعداد صوره قد يشمل الضرر الذي يصيب الشخص في غير ماله كشرفه

1 See article 84 of Regulation (EU) 2016/679, "General conditions for imposing administrative fines". https://gdpr-info.eu/art-83-gdpr/.

و سمعته و عرضه و اعتباراته كالقذف أو الشتم، أو قد يصيبه في عاطفته و شعوره و هو كل ما يلحق الشخص من ألم في ذاته النفسية.[1]

أما عن تقدير التعويض، فتقدير التعويض يدخل في السلطة التقديرية للقاضي دون الرقابة من محكمة النقض متى كانت أسباب الحكم سائغة مع بيان عناصر الضرر و مقداره و أحقية المضرور في التعويض، فلا وجود لنص يلزم القاضي باتباع معايير معينة.[2]

لكن يصعب تقدير التعويض عن الضرر الأدبي، إذ أنه ضرر غير ملموس و لا يصيب الجسد بل على العكس فهو يصيب كل ما هو غير مالي يتصل بحياة الإنسان كانتهاك الحق في خصوصيته من سمعته و شرف أو حتى معلوماته الشخصية أو المالية أو الصحية، و مع ذلك يتم تعويضه بالمال، و نرى أن المبدأ الذي يستخدمه القاضي هنا هو تقدير التعويض حسب الضرر الذي أصاب المضرور.

و في هذا السياق لا ننسى بأن نؤكد على وجوب التعويض متى ما وقع الفعل الضار و لا يجوز الإعفاء من المسؤولية عن الفعل متى ما وقع، و هذا ما أكدته المادة 296 من قانون المعاملات المدنية الإماراتي و التى تنص على أنه:"يقع باطلاً كل شرط يقضي بالإعفاء من المسؤولية المترتبة على الفعل الضار".

الفرع الثاني : المحكمة المختصة

في الحديث عن المحكمة المختصة برفع دعوى التعويض لانتهاك الحق في الخصوصية تكون الدعوى مرفوعة أمام المحاكم المدنية، و لكن في بعض الأحيان قد يرتب انتهاك الحق في الخصوصية فعل يجرمه القانون فتختص بذلك محاكم الدولة الجزائية و توقف الدعوى المدنية إلى حين الفصل في الدعوى الجزائية، و من ثم يستطيع المضرور رفع دعوى التعويض أمام المحاكم المدنية و التى تكون دعوى لاحقة للدعوى الجزائية و التى سبق الفصل فيها، و هذا ما أكدته محكمة تمييز دبي بأن:"التزام المحكمة المدنية بالحكم الصادر في الدعوى الجزائية يكون فيما فصل فيه الحكم الجزائي فصلاً ضرورياً في وقوع الفعل المكون للأساس المشترك بين الدعويين المدنية و الجزائية و في الوصف القانوني و نسبته إلى فاعله فإذا فصلت المحكمة الجزائية نهائياً في هذه المسائل تعين على المحكمة المدنية الالتزام بها في دعاوي الحقوق المتصلة بها و امتنع إعادة بحثها لما يترتب على غير ذلك من قضاء مخالفة الحجية التي حازها الحكم الجزائي السابق".[3]

---

1 الراعي، صبري محمود و رضا السيد، عبدالعاطي (2006). الموسوعة النموذجية في شرح قضايا التعويضات و المسؤولية المدنية (ص177). الطبعة الأولى. القاهرة، مصر: دار مصر للموسوعات القانونية.

2 أحمد، إبراهيم سيد (2007). الضرر المعنوي فقهاًو قضاء (ص162). الطبعة الأولى. الإسكندرية، مصر: المكتب الجامعي الحديث.

3 محكمة تمييز دبي، الدائرة التجارية، الطعن رقم 1046 لسنة 2020، الجلسة المنعقدة يوم 2021/01/06، منشور علي موقع محامو الإمارات، تاريخ الدخول: 27/03/2022، على الرابط:

https://www-mohamoon-uae-com.uaeu.idm.oclc.org/uaeu/default.aspx?Action=IntrDisplayJudgmentFile&PageNumber=1&Type=5&ID=46166&strSearch=البيانات%لشخصية

و على مستوى الأحكام القضائية المقارنة، فقد ذهبت محكمة النقض المصرية بأنه لا تسقط دعوى التعويض الناشئة عن العمل غير المشروع بانقضاء المدد المحددة في المادة (172)[1] من القانون المدني، إذا استتبع العمل الضار نشوء دعوى جنائية إلى جانب الدعوى المدنية، و كانت مدة التقادم للدعوى الجنائية أطول من مدة التقادم للدعوى المدنية، هنا تسري مدة التقادم للدعوى الجنائية على الدعويين.[2]

و أحد المبادئ القضائية التي أكدتها محكمة النقض المصرية في شأن الحياة الخاصة استناداً لنص المادة (57)[3] من الدستور المصري، أن الدعوى الجنائية و المدنية الناشئة عن جريمة الاعتداء على الحرية الشخصية لا تسقط بالتقادم.[4]

1 "تسقط بالتقادم دعوى التعويض الناشئة عن العمل غير المشروع بانقضاء ثلاث سنوات من اليوم الذى علم فيه المضرور بحدوث الضرر وبالشخص المسئول عنه، وتسقط هذه الدعوى في كل حال بانقضاء خمس عشرة سنة من يوم وقوع العمل غير المشروع ..... "

2 راجع، محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (16389) لسنة (76) القضائية، الصادر في جلسة 2021/03/24، موقع محكمة النقض المصرية، تاريخ الدخول: 11/04/2022، على الرابط :

https://www.cc.gov.eg/i/H/111661842.pdf

3 "كُل اعتداء على الحرية الشخصية أو حُرمة الحياة الخاصَّة للمُواطنين وغيرها من الحُقوق والحُريات العامَّة التي يكفلها الدستور والقانون جريمة لا تسقط الدعوى الجنائية ولا المدنية الناشئة عنها بالتقادم وتكفل الدولة تعويضاً عادلاً لمن وقع عليه الاعتداء".

4 راجع، محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (2484) لسنة (65) القضائية، الصادر في جلسة 2019/08/01، موقع محكمة النقض المصرية، تاريخ الدخول: 18/04/2022، على الرابط:

https://www.cc.gov.eg/judgment_single?id=111398167&&ja=272586

الفصل الرابع: الخاتمة

في ختام هذه الأطروحة، بعنوان "حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي (دراسة تحليلية مقارنة)"، ترى الباحثة أنه بالرغم من وجود التشريع المختص بحماية البيانات الشخصية للأفراد من اختراقها و انتهاكها إلا أنه تم إغفال جوانب كثيرة لم يتم التطرق لمعالجتها في التشريع فيما يخص المسؤولية الرقمية عن تطبيقات الذكاء الاصطناعي، مما قد يجعل صاحب البيانات حائراً في كيفية الحصول على حقه عند انتهاك بياناته الشخصية في تطبيقات الذكاء الاصطناعي، حيث أن المرسوم بقانون رقم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية جاء في مواجهة المتحكم و المعالج للبيانات الشخصية، و بعد الخوض في غمار دراسة الموضوع توصلت الباحثة إلى العديد من النتائج، بالإضافة إلى التوصيات التي رأتها للمشرع الإماراتي بأنها قد تساهم بقدرٍ ما في علاج بعض التحديات التي قد ظهرت من موضوع الدراسة:

أولاً: النتائج

1. لم تعرف التشريعات الحق في الخصوصية أو الحق في الحياة الخاصة، فبالرغم من ترادف المصطلحان في الكثير من التشريعات إلا أن فكرة الخصوصية فكرة مرنة متغيرة حسب الزمان و المكان و المجتمع.
2. بالرغم من انقسام الفقه في التفرقة بين الحق في الخصوصية و الحقوق الأخرى، كالحق في الصورة، و الحق في الشرف و الاعتبار، و الحق في الدخول في طي النسيان، إلا أنها تدخل في الحق في الخصوصية فهي جزء لا يتجزأ منها، و هذا ما أكدته الأحكام القضائية ذات الصلة.
3. الحق في الخصوصية حق مقدس في الكثير من الدساتير حول العالم، إلا أنه مقيد باعتبارات عدة يجوز فيها الاطلاع على البيانات الخاصة بالأفراد في أحوال محددة و إطارٍ تشريعي منظم، كالأمن القومي و الصحة العامة و الحالات التي نص عليها المرسوم بقانون بشأن حماية البيانات الشخصية.
4. تتنوع مخاطر استخدام الذكاء الاصطناعي على الحق في الخصوصية من خلال ظهور تقنيات للتعرف على الوجه أو الصوت و قد تصل في بعض الأحيان إلى خلق فيديو لأشخاص لا يوجد لهم العلم بذلك، و الخطر الأكبر يتمثل في أن هذه التطبيقات تزيد يوماً بعد يوم مما قد يشكل خطراً على الخصوصية.
5. وضع المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية أطر معالجة البيانات الشخصية، فقد أعطى لصاحب البيانات الشخصية العديد من الحقوق، و من جانب آخر رتب العديد من الالتزامات على معالجي البيانات الشخصية، مما خلق نوع من التوازن في العلاقة بين صاحب البيانات و معالج البيانات.
6. لا يمكن اعتبار أنظمة الذكاء الاصطناعي من قبيل الأشخاص الطبيعية أو الاعتبارية.
7. عدم ملاءمة القواعد التقليدية العامة لتطبيقها على أنظمة الذكاء الاصطناعي في تحديد المسؤول عن انتهاكات البيانات الشخصية للأفراد في هذه الأنظمة، فتطبيقها على أنظمة الذكاء الاصطناعي أمر في غاية التعقيد و الصعوبة.
8. عدم مواءمة التشريع القائم في مواجهة تحديات أنظمة الذكاء الاصطناعي، أنظمة الذكاء الاصطناعي أنظمة ذات طبيعة خاصة متميزة و متفردة يجب استحداث نصوص تشريعية لتنظيم عملها.

9. القواعد التقليدية غير منصفة للمضرور فهي تحاكي التزام الشخص الطبيعي و الاعتباري، فأنظمة الذكاء الاصطناعي ذو طبيعة خاصة.

ثانياً: التوصيات

1. الإسراع في إصدار اللائحة التنفيذية للمرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية.
2. استحداث نظام قانوني جديد يشمل جميع المواد القانونية التي تنظم مختلف صور الحق في الخصوصية والحياة الخاصة، بالإضافة إلى الجزاءات التي تترتب على انتهاك الخصوصية.
3. توعية الأفراد في المجتمع بضرورة العلم بالحقوق التي مُنِحت له من قبل المشرع الإماراتي كصاحب بيانات وكذلك بالالتزامات التي تقع على عاتقي مشغلي تطبيقات الذكاء الاصطناعي.
4. إعادة صياغة بعض النصوص القانونية في المرسوم بقانون اتحادي:

- كالمادة (6) البند (ب) من فقرتها الأولى إذا كان لا يفرق بين الكتابة التقليدية والكتابة الإلكترونية بشأن موافقة صاحب البيانات الشخصية.
- البند الرابع من المادة (8) نص المشرع على الالتزام بمحو البيانات بعد انقضاء مدة المعالجة، فكان من الأولى وضع مدة لمحو البيانات الشخصية بعد الانتهاء من غرض المعالجة. وذلك بما يسد الثغرات القانونية في المرسوم والتي يمكن لمشغلي تطبيقات الذكاء الاصطناعي استغلالها في مواجهة صاحب البيانات.

5. إعداد منظومة تشريعية ملاءمة لمواكبة التحديات المتلاحقة للذكاء الاصطناعي.
6. ضرورة وضع قواعد قانونية خاصة تنظم أحكام المسؤولية القانونية الجديدة لتطبيقات الذكاء الاصطناعي، ويتم إدراجها ضمن المسؤولية المدنية الخاصة.
7. استحداث محاكم مختصة بالقضايا الحديثة والمستجدة المتعلقة بالذكاء الاصطناعي، مكونه من ذوي الخبرة في المنازعات ذات الصلة بموضوعات الذكاء الاصطناعي.
8. دعوة للقائمين على وضع المناهج و المساقات في الجامعات و كليات القانون بطرح مساق يتضمن "تشريعات التكنولوجيا المتقدمة"، و الذي يعنى بتدريس جميع التشريعات الدولية و الوطنية التي تختص بموضوع التكنولوجيا المتقدمة.

المراجع

المراجع العربية

الكتب:

1. أحمد، إبراهيم سيد (2007). *الضرر المعنوي فقهاً و قضاء*. الطبعة الأولى. الإسكندرية، مصر: المكتب الجامعي الحديث.
2. الأهواني، حسام الدين (2000). *الحق في احترام الحياة الخاصة، الحق في الخصوصية*. الطبعة الثانية. القاهرة: دار النهضة العربية.
3. الراعي، صبري محمود و رضا السيد، عبدالعاطي. (2006). *الموسوعة النموذجية في شرح قضايا التعويضات و المسؤولية المدنية*. الطبعة الأولى. القاهرة، مصر: دار مصر للموسوعات القانونية.
4. الزبير، حايف سالم (2018). *الاعتداء على الحياة الخاصة عن طريق الإنترنت في التشريع العراقي و اللبناني– دراسة مقارنة–*. الطبعة الأولى. القاهرة: دار النهضة العربية للنشر و التوزيع.
5. الشرقاوي، الشهابي إبراهيم (2011). *مصادر الالتزام غير الإرادية في قانون المعاملات المدنية الإماراتي*. الطبعة الأولى. الشارقة: الآفاق المشرقة ناشرون.
6. العبهجي، عصام (2005). *حماية الحق في الحياة الخاصة في ضوء حقوق الإنسان والمسؤولية المدنية*. الإسكندرية: دار الجامعة الجديدة للنشر.
7. العوضي، عبد الهادي فوزي (2014). *الحق في الدخول في طي النسيان على شبكة الإنترنت*. الطبعة الأولى. القاهرة: دار النهضة العربية.
8. المقاطع، محمد عبدالمحسن (1992). *حماية الحياة الخاصة للأفراد و ضماناتها في مواجهة الحاسب الآلي*. الكويت: دار ذات السلاسل للطباعة و النشر.
9. النمر، وليد سليم (2017). *حماية الخصوصية في الإنترنت*. الطبعة الأولى. الإسكندرية: دار الفكر الجامعي.
10. أنيس، إبراهيم آخرون (1972) . المعجم الوسيط . الطبعة الثانية (الجزء الأول). مصر: دار المعارف.
11. بحر، ممدوح خليل (2011). حماية الحياة الخاصة في القانون الجنائي– دراسة مقارنة –. القاهرة : دار النهضة العربية.
12. بدر، أسامة أحمد (2022). أحكام قانون حماية المستهلك الإتحادي رقم (15) لسنة 2020. الطبعة الثانية. الإمارات: جامعة الإمارات العربية المتحدة.
13. بدوي، عمرو طه (2020). التنظيم القانوني لمعالجة البيانات الشخصية– دراسة تطبيقية على معالجة تسجيلات المراقبة الصوتية –.الطبعة الأولى . مصر: دار النهضة العربية، الإمارات: دار النهضة العلمية.
14. حسان، أحمد محمد (2001). نحو نظرية عامة لحماية الحق في الحياة الخاصة في العلاقة بين الدولة و الأفراد "دراسة مقارنة". القاهرة: دار النهضة العربية.
15. سيد، أشرف جابر (2013). الجوانب القانونية لمواقع التواصل الاجتماعي. القاهرة: دار النهضة العربية.

16. زعبي، عمار (2017). حماية المستهلك من الأضرار الناتجة عن المنتجات المعيبة. الطبعة الأولى. عمان، الأردن: دار الأيام.
17. سرحان، عدنان إبراهيم (2010). أحكام البيع في قانون المعاملات المدنية الإماراتي. الطبعة الثانية. عَمان: دار الآفاق المشرقة.
18. عباسي، بوعبيد (2008). الإلتزام بالإعلام في العقود–دراسة في حماية المتعاقد و المستهلك.مراكش–المغرب . الطبعة الأولى.
19. عبدالجليل، يسرية محمد (2007). المسئولية عن الأضرار الناشئة عن عيوب تصنيع الطائرات. الأسكندرية: منشأة المعارف.
20. عبدالدايم، حسني محمود (2019). شرح قانون المعاملات المدنية الإماراتي العقود المسماة –عقد البيع–. بدون رقم طبعة. دبي - الإمارات: دار النهضة العربية. القاهرة - مصر، دار النهضة العلمية.
21. عبدالصمد، حسني محمود (2018). الوجيز في شرح عقد البيع وفقاً لأحكام قانون المعاملات المدنية الإماراتي رقم 5 لسنة 1985. الطبعة الأولى. دب : دار النهضة العلمية.
22. مؤمن، طاهر شوقي (2017). النظام القانوني للطائرات بدون طيار "الدرونز Les Drones". القاهرة : دار النهضة العربية.
23. منصور، محمد حسين (2010). شرح العقود المسماة. الطبعة الأولى . بيروت، لبنان: منشورات الحلبي.

الرسائل العلمية:

1. السلمان، خالد عبدالله (2014). *طبيعة مسئولية المنتج و حالات الإعفاء منها "دراسة مقارنة" (أطروحة ماجستير)*. جامعة المنوفية. المنوفية، مصر.
2. قاسم، أحمد نصر (سبتمبر 2018). *المسؤولية المدنية لحارس الأشياء "دراسة مقارنة" (أطروحة ماجستير)*. جامعة النجاح الوطنية. نابلس، فلسطين.

الأبحاث و الدوريات:

1. التهامي، سامح (2020). *ضوابط معالجة البيانات الشخصية– دراسة مقارنة بين القانون الفرنسي والكويتي* –. بحث منشور في *مجلة كلية القانون الكويتية العالمية*. السنة8. العدد8. ص401–411.
2. الخطيب، محمد عرفان (2020). المسؤولية المدنية و الذكاء الاصطناعي ... إمكانية المساءلة؟!. *مجلة كلية القانون الكويتية العالمية*. *8* (1). ص140–141.
3. الخطيب، محمد عرفان (2018). ضمانات الحق في العصر الرقمي، من تبدل المفهوم لتبدل الحماية، قراءة في الموقف التشريعي الأوروبي والفرنسي واسقاط على الموقف التشريعي الكويتي. *مجلة كلية القانون الكويتية العالمية*. *10* (3)، ملحق خاص. ص251–324.

4. الذهبي، خدوجة (ديسمبر 2017). *حق الخصوصية في مواجهة الاعتداءات الإلكترونية – دراسة مقارنة–. مجلة الأستاذ الباحث للدراسات القانونية و السياسية. 1* (8). ص143–160.
5. العمروسي، غادة علي (2021). *موقف الفقه الإسلامي من التعدي على البيانات المالية. مجلة كلية الدراسات الإسلامية و العربية. 6* (4). ص604–600.
6. أمين، محمد و إبراهيم، سليمان. (2016). *الحماية الجنائية في حرمة الحياة الخاصة في قانون العقوبات الإماراتي . مجلة جامعة الشارقة للعلوم الشرعية و القانونية. 13* (1). ص 60–88.
7. بريك، أيمن محمد (مارس 2022) . *تطبيقات الميتافيرس و علاقتها بمستقبل صناعة الصحافة الرقمية – دراسة استشرافية خلال العقدين 2022:2042–. المجلة المصرية لبحوث الإعلام* . 2022 (78). ص45–76.
8. بطيخ، مها رمضان محمد (2021). *المسؤولية المدنية عن أضرار أنظمة الذكاء الاصطناعي – دراسة تحليلية مقارنة–. المجلة القانونية، جامعة القاهرة. 9* (5). ص1513–1616.
9. خصاونه، علاء الدين و فراس، الكساسبه و درادكه، لافي محمد. (2011). *الحماية القانونية للخصوصية و البيانات الشخصية في نطاق المعلوماتية. مجلة جامعة الشارقة للعلوم الشرعية و القانونية. 8* (2). ص175–226.
10. شويكي، شوق حسين و محمود إبراهيم، فياض (2019). المسؤولية المدنية عن حوادث التاكسي الطائر في دبي: دراسة استشرافية . *مجلة جامعة الشارقة للعلوم القانونية. 17* (2). ص297–338.
11. عبدالرحمن، محمود (2020). التطورات الحديثة لمفهوم الحق في الخصوصية المعلوماتية. *مجلة كلية القانون الكويتية العالمية. 8* (8). ص101–132.
12. عبيد، أحمد كمال (2019). الأهلية القانونية للوكيل الذكي و دورها في تحديد المسؤولية الناتجة عن معاملاته الإلكترونية. *مجلة جامعة الشارقة للعلوم القانونية. 16* (2). ص358–338.
13. فاطمة، مرنيز (2016). المراقبة الإلكترونية كإجراء استدلالي في مواجهة الحق في الخصوصية. *مجلة الحقيقة. 15* (38). ص102–115.
14. فرجون، خالد محمد (2022). تكنولوجيا "ميتافيرس" و مستقبل تطوير التعليم. *المجلة الدولية للتعليم الإلكتروني. 5* (3). ص77.
15. كريكط، عائشة (2019). حق الخصوصية لمستخدم الفضاء الرقمي: المخاطر والتحديات. *مجلة الحقيقة للعلوم الاجتماعية والإنسانية، 18* (02). ص258–260.

المؤتمرات:

1. الغافري، حسين (2-4 يونيو2008). الحماية القانونية للخصوصية المعلوماتية في مشروع قانون المعاملات الالكترونية العماني، *مؤتمر أمن المعلومات و الخصوصية في ظل قانون الانترنت*. القاهرة.

المراجع الإلكترونية:

1 . استراتيجية الإمارات للثورة الصناعية الرابعة. علي الرابط :
https://u.ae/ar-ae/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/the-uae-strategy-for-the-fourth-industrial-revolution

2 . أستراليا تقاضي جوجل بسبب انتهاك خصوصية المستخدمين.أكتوبر 2019، على الرابط:
https://cutt.us/o3YvL last visit :10/02/2022.

3 . بن صغير فؤاد، الحق في حماية الحياة الخاصة الرقمية:مسالة قانونية أم حقوقية، منشور على الموقع الالكتروني، https://www.hespress.com.411211-م-الرقمية-الخاصة-الحياة-حماية-في-الحق/html

4 . جلال، أحمد (يونيو 2020)، جوجل تواجه دعوى قضائية بقيمة 5 مليارات دولار بتهمة انتهاك خصوصية المستخدمين، منشور على:
https://cutt.us/0H2m9

5 . جمال، منة الله (فبراير 2020)، جوجل أمام النائب العام بتهمة انتهاك خصوصية الأطفال، منشور على:
https://cutt.us/Fkmhz last visit: 10/02/2022.

6 . سعد، سومية. خبر صحفي بعنوان "تسجيل بصمات جميع سكان دبي قريباً" بتاريخ 2022/03/21. جريدة الخليج . منشور على الرابط :
https://www.alkhaleej.ae/2022-03-21/-من-أخبار-قريباً-دبي-سكان-جميع-بصمات-تسجيل
الإمارات/أخبار-الدار

7 . سعد (ديسمبر 2020). "جائحة كورونا" تطبيقات التتبع الإلكتروني قد تهدد الخصوصية. المنشور على :
https://www.scientificamerican.com/arabic/articles/news/tracking-applications-may-threaten-privacy/

8 . " طب العمل".
https://ar.wikipedia.org/wiki/طب_العمل

9 . مقال هل تطبيقات مراقبة الحالة الصحية تنطوي على انتهاك للخصوصية (نوفمبر 2020)، المنشور على:
https://www.bbc.com/arabic/vert-cap-54923302

التشريعات الوطنية:

1. قانون رقم (4) لسنة 2022 بشأن تنظيم الأصول الافتراضية في إمارة دبي، المنشور في الجريدة الرسمية لحكومة دبي، السنة 56، في العدد 559، 11 مارس 2022م.

2. المرسوم بقانون رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية المنشور في الجريدة الرسمية في العدد 712 (ملحق 1)، السنة الواحدة و الخمسون 19 صفر 1443 هـ – الموافق 26 سبتمبر 2021م.
3. المرسوم بقانون اتحادي رقم (31) لسنة 2021 بإصدار قانون الجرائم و العقوبات المنشور في الجريدة الرسمية ، العدد (712)، السنة (2021)، الموافق 2021/09/26.
4. المرسوم بقانون اتحادي رقم (34) لسنة 2021 في شأن مكافحة الشائعات و الجرائم الإلكترونية المنشور في الجريدة الرسمية العدد سبعمائة و اثنا عشر (ملحق)، السنة الواحدة و الخمسون الموافق 26/09/2021.
5. قانون اتحادي رقم (15) لسنة 2020 في شأن حماية المستهلك، المنشور في الجريدة الرسمية: السنة الخمسون، العدد ستمائة و تسعون، 15 نوفمبر 2020م.
6. قرار مجلس الوزراء رقم (53) لسنة 2019م في شأن تنفيذ المراقبة الإلكترونية، المنشور في العدد 660 من الجريدة الرسمية.
7. المرسوم بقانون اتحادي رقم (17) لسنة 2018م بتعديل بعض أحكام قانون الإجراءات الجزائية الصادر بالقانون الإتحادي رقم (35) لسنة 1995م، المنشور على موقع وزارة العدل.
8. القانون الإتحادي رقم 14 لسنة 2014م في شأن مكافحة الأمراض السارية المنشور في الجريدة الرسمية، العدد (572)، السنة (44)، الموافق 2014/11/30.
9. قانون رقم 35 لسنة 1992 م بشأن إصدار قانون الإجراءات الجزائية وفقاً لآخر التعديلات.
10. القانون الإتحادي رقم (20) لسنة 1991م بإصدار قانون الطيران المدني المنشور في الجريدة الرسمية، العدد (226)، الموافق 1991/06/24.
11. قانون رقم (5) لسنة 1985م بإصدار قانون المعاملات المدنية لدولة الإمارات العربية المتحدة، وفقاً لأحدث تعديلاته بالمرسوم بقانون اتحادي رقم (30) لسنة 2020م.

التشريعات العربية:

1. الدستور المصري، الدستور اللبناني، الدستور الكويتي، الدستور التونسي، الدستور الأردني.
2. القانون العماني بمرسوم سلطاني رقم 2022/6 بإصدار قانون حماية البيانات الشخصية الجريدة الرسمية الصادرة من وزارة العدل و الشؤون القانونية. العدد (1429). السنة (51). 13 فبراير 2022.
3. نظام حماية البيانات الشخصية في التشريع السعودي 1443هـ بناءً على المرسوم الملكي رقم (م/ 19) بتاريخ 1443/2/9 هـ. المنشور على موقع هيئة الخبراء بمجلس الوزراء.
4. لائحة حماية خصوصية البيانات الكويتية أنشئت في 27/06/2021، منشورة على موقع الهيئة العامة للاتصالات و تقنية المعلومات.
5. قانون رقم 151 لسنة 2020 بإصدار قانون حماية البيانات الشخصية المصري المنشور في الجريدة الرسمية - العدد 28 مكرر (هـ) – في 15 يوليه سنة 2020.

6. قانون رقم) للمعاملات الالكترونية والبيانات ذات الطابع الشخصي في التشريع اللبناني، المنشور في الجريدة الرسمية. العدد (45). السنة (158). 18 تشرين الأول 2018.
7. القانون القطري رقم (13) لسنة 2016 بشأن حماية البيانات الشخصية ، المنشور في الجريدة الرسمية . العدد (15). 29 ديسمبر 2016.
8. القانون المغربي رقم (8) لسنة 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة البيانات ذات الطابع الشخصي، المنشور في الجريدة الرسمية عدد 5711 بتاريخ 23 فبراير 2009.
9. التشريع التونسي رقم (63) لسنة 2004 بتاريخ 27 يوليو 2004 يتعلق بحماية المعطيات الشخصية ، المنشور في الجريدة الرسمية رقم 61 بتاريخ 30 يوليو 2004.
10. القانون المصري رقم 15 لسنة 2004 بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات.
11. قانون العقوبات المصري طبقاً لأحدث التعديلات بالقانون 95 لسنة 2003 م، القانون رقم 58 لسنة 1937 بإصدار قانون العقوبات (1).
12. دستور الولايات المتحدة الأمريكية الصادر في 1789 شاملاً تعديلاته لغاية 1992 على الرابط :
https://www.constituteproject.org/constitution/United_States_of_America_1992.pdf?lang=ar

الأحكام القضائية:

1. محكمة النقض المصرية، الدائرة التجارية، الطعن رقم (9542) لسنة (91) القضائية، الصادر في جلسة 2022/03/16، موقع محكمة النقض المصرية.
2. محكمة نقض أبوظبي، الدائرة التجارية، الطعن رقم 902 لسنة 2021، الصادر في جلسة 2021/11/02 م، موقع محامو الإمارات.
3. محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (16389) لسنة (76) القضائية، الصادر في جلسة 2021/03/24، موقع محكمة النقض المصرية.
4. محكمة تمييز دبي، الدائرة التجارية، الطعن رقم 1046 لسنة 2020، الجلسة المنعقدة يوم 2021/01/06، منشور علي موقع محامو الإمارات.
5. محكمة النقض المصرية، الدائرة التجارية، الطعن رقم (17689) لسنة (89) القضائية، الصادر في جلسة 2020/03/10، موقع محكمة النقض المصرية.
6. المحكمة الإتحادية العليا، الدائرة الجزائية، الطعن رقم (950) لسنة (2019) القضائية، الصادر في جلسة 2020/02/04، موقع شبكة قوانين الشرق.
7. محكمة النقض أبوظبي، الدائرة الجزائية، الطعن رقم (22) لسنة (2020) س14 ق.أ، الصادر في جلسة 2020/02/04، موقع محامو الإمارات.

8. محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (2484) لسنة (65) القضائية، الصادر في جلسة 2019/08/01، موقع محكمة النقض المصرية .
9. محكمة تمييز دبي، الدائرة المدنية، الطعن رقم (247) لسنة (2019)، الصادر في جلسة 2019/07/25، موقع محامو الإمارات.
10. محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (6420) لسنة (64) القضائية، الصادر في جلسة 2019/06/08، موقع محكمة النقض المصرية.
11. محكمة نقض أبوظبي، الدائرة الجزائية، الطعن رقم (1106) لسنة (2018) القضائية، الصادر في جلسة 2019/01/22، موقع شبكة قوانين الشرق.
12. محكمة تمييز دبي، الدائرة التجارية، الطعن رقم (417) لسنة (2016)، الصادر في جلسة 2017/04/09، موقع محامو الإمارات.
13. محكمة نقض أبوظبي، الدائرة الجزائية، الطعن رقم (1182) لسنة (2015) القضائية، الصادر في جلسة 2016/02/22، موقع شبكة قوانين الشرق.
14. محكمة النقض أبوظبي، الدائرة الإدارية، الطعن رقم (7) لسنة (2013)، الصادر في جلسة 2013/05/20، موقع محامو الإمارات.
15. محكمة النقض المصرية، الدائرة المدنية، الطعن رقم (2257) لسنة (56) القضائية، الصادر في جلسة 1992/05/24، منشور على موقع محكمة النقض المصرية.

أخرى:

1. مركز بحوث القانون و التكنولوجيا. تحت إشراف عبدالحميد (2020)، حسن. ورشة عمل بعنوان" دراسة نقدية لقانون حماية البيانات الشخصية رقم 151 لسنة 2020"، كلية القانون. الجامعة البريطانية، مصر.
2. تطورات الذكاء الاصطناعي ومقتضيات حماية الحقوق والحريات الأساسية، تقرير عن منظمة الايسيسكو (منظمة العالم الإسلامي للتربية والعلوم والثقافة)، تحت إشراف الأستاذ محمد الهادي السهيلي، 2019/12/31.
3. عاطف، كريم. الخصوصية الرقمية بين الانتهاك والغياب التشريعي (2013). القاهرة ، مصر. مركز دعم تقنية المعلومات.
4. يونس (2002). الخصوصية وحماية البيانات في العصر الرقمي- الجزء الثاني– منشورات اتحاد المصارف العربية-.
5. الإعلان العالمي لحقوق الإنسان المعتمد من قبل الجمعية العامة في 10 ديسمبر 1948.
6. المذكرة الإيضاحية لقانون المعاملات المدنية لدولة الإمارات العربية المتحدة.

المراجع الأجنبية:

1. Bartneck, C., Lutge, C., Wager, A. & Welsh, S. (2021). *An Introduction to Ethics in Robotics and AI.* 63-64. E Book: https://link.springer.com/book/10.1007/978-3-030-51110-4. Access date: 20/06/2022.
2. Alkhasawneh, A. (2020). The Future of Biometric Data Protection in Jordan in Light of the GDPR: Do We Need to Comply with the GDPR? *Journal of Legal*, Ethical and Regulatory Issues. *23*(2).1-19.
3. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence, Retrieved November, 2021 from: https://unesdoc.unesco.org/ark:/48223/pf0000380455
4. Manheim, K. & Lyric, K. (2019). Article of Artificial Intelligence: Risks to Privacy and Democracy.*The Yale Journal of Law and Techonlogy. 21*(106). 182-184.
5. Monique, M. & Marcus, S. (2017). Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *University of New South Wales Law Journal*. *40*(1). 121-145.
6. Fuchs, D. (2018). The dangers of human-like Bias in machine-learning algorithms. *Missouri University of Science and Technology .2*(1), 1-10.
7. Howard, A., Zhang, C. & Horvitz, E. (2017). Addressing bias in machine learning algorithms: A pilot study on emotion recognition for intelligent systems," *2017 IEEE Workshop on Advanced Robotics and its Social Impacts* (ARSO). 1-7.
8. Regulation (EU) 2016/679 of the European Parlimant and of the council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, 679, 2016, https://eur-lex.europa.eu/legalcontent/EN/TXT/
9. McCarthy, J. (2022) Stanford University, Retrieved March, 2022 from http://jmc.stanford.edu/artificial-intelligence/what-is-ai/index.html.
10. Lernende Systeme (2022). *Designing AI*, https://www.plattform-lernende-systeme.de/startseite.html. Access date: 20/06/2022

11. Mintz, Levin, Cohn, Ferris, Glovsky & Popeo (2022). Facebook to Pay $ 90 Million to Settle Data Privacy Lawsuit, The National Law Review, XII (49),: https://www.natlawreview.com/article/facebook-to-pay-90-million-to-settle-data-privacy-lawsuit#:~:text=Facebook's%20parent%20company%20Meta%20has,of%20the%20social%20media%20platform , Access date:16 / 05/ 2022.
12. Chesney, B & Danielle, C (2019). Deep Fakes: A Looming Challenge for Privacy. *California Law Review*. *107*(6), 1771-1776.
13. Mystakidis, S. (2022). Metaverse. *Encyclopedia2022*, *2*(1). 1-10.
14. Kevin C., Hacker sends spam to 100,000 from FBI email address, 14 Nov 2021.
15. Shead, S (2022). Serious crime in the metaverse should be outlawed by the U.N, *UAE minister says* . CNBC.com, Retrieved May, 2022 from https://www.cnbc.com/2022/05/25/metaverse-murders-need-to-be-policed-says-uae-tech-minister.html
16. Pymnts (2022). Dubai’s Virtual Assets Regulatory Authority Opens Sandbox-Based Metaverse HQ , PYMNTS.com. Retrieved May, 2022 from https://www.pymnts.com/metaverse/2022/dubais-virtual-assets-regulatory-authority-opens-sandbox-based-metaverse-hq/
17. Federal Trade Commission (2020). Privacy and Data Security Update, Retrieved May, 2021 from https://www.ftc.gov/reports/federal-trade-commission-2020-privacy-data-security-update
18. Sam, B (2017). Saudi Arabia takes terrifying step to the future by granting a robot citizenship.https://web.archive.org/web/20180623032828/https://www.avclub.com/saudi-arabia-takes-terrifying-step-to-the-future-by-gra-1819888111
19. Loi n 2004-801 du 6 aout 2004 relative a la protection des personnes physique a la regard des traitements des donnes a caractere personel et modifiant la loi n 78-17 du 6 Janvier 1978 relative a linformatique aux fishier et aux liberties, J.o n 182 du 7 aout 2004, www.legifrance.gouv.fr .
20. Cass C. (2006). Bull Crim, 69, 267-269.

21. Kacurove, D. (2020). Pokemon Go Palyers Report of Stolen Account https://www.futuregamereleases.com/2020/12/pokemon-go-players-report-of-stolen-accounts/, Access date:16/05/2022.
https://tencentgames.helpshift.com/hc/en/3-pubgm/faq/365-account-hack---linked-social-media-account-email-address-has-been-hacked/, Access date:16/05/2022.
22. PUBG Mobile Support (2022). Retrieved from: https://tencentgames.helpshift.com/hc/en/3-pubgm/faq/365-account-hack---linked-social-media-account-email-address-has-been-hacked/ accessed on 29/03/2022

جامعة الامارات العربية المتحده اطروحة ماجستير رقم 2022: 56

مع بزوغ عصر الثورة الصناعية الرابعة (4IR)، أدى ذلك إلى ازدياد ظهور تطبيقات الذكاء الاصطناعي بشكل كبير والتي دخلت في مجالات كثيرة في حياتنا اليومية، و بالرغم من الإيجابيات الكثيرة لتطبيقات الذكاء الاصطناعي إلا أن استخدامها ما زال بلا شك محفوفاً بالمخاطر ويثير العديد من المشاكل التي تمس الحقوق الأساسية للأفراد ويترتب عليها العديد من الآثار القانونية، فمع ازدياد استخدام تطبيقات الذكاء الاصطناعي في الآونة الأخيرة زادت فرص المساس بخصوصية الأفراد وظهرت صور جديدة لانتهاك خصوصية البيانات المتعلقة بهم والمساس بحقهم في الصورة و عناصر الخصوصية الآخرى. فكان لابد من الاستفادة من هذه التطبيقات في ظل إطار قانوني منضبط يضمن فعالية هذه التطبيقات و يحمي الحقوق الأساسية للأفراد.

ريم الشامسي حاصلة على درجة الماجستير من قسم القانون الخاص بكلية القانون في جامعة الإمارات العربية المتحدة. حصلت على درجة البكالوريوس من كلية القانون، جامعة الإمارات العربية المتحدة.