الذكاء الاصطناعي والحق في الخصوصية الرقمية

الأستاذ الدكتور: احمد محمد براك

أستاذ دكتور في جامعة فلسطين الاهلية – بيت لحم فلسطين

النائب العام ورئيس هيئة مكافحة الفساد السابق

الملخص :

لا خلاف على أن الذكاء الاصطناعي أضحي يشكل جزء لا يتجزأ من إيقاع الحياة اليومية، حيث تدخل في كافة مناحي الحياة، بما يستحيل معه غض الطرف عنه، على أن لتكنولوجيا الاتصال والذكاء الاصطناعي آثارها الإيجابية و السلبية على خصوصية الإنسان، وحقه في طي النسيان. ومن هنا، فقد سعي المشرع في مختلف دول العالم عن وضع القوانين التي تكفل الحماية الجنائية والمدنية للحق في الخصوصية، ومواجهة استخدام الذكاء الاصطناعي بغرض التعدي على الخصوية الرقمية، من خلال تجريم الدخول على البيانات الشخصية والبقاء بدون الحصول على إذن مسبق من صاحب الشأن. فضلاً عن ملاحقة المسئولية الجنائية والمدنية للوسطاء الإلكترونيين. بمعني مزودي الخدمات الإلكترونية، حيث خدمات الإيواء، وتقديم المعلومات ومحركات البحث إلى أخره، ولا يخفي مبلغ أهمية الحق في الخصوصية الرقمية، خاصة وأن هذا الوصف من العمومية بحيث يشمل بجانب البيانات التي تتعلق بالحياة الخاصة، الحسابات المصرفية، فضلاً عن الحق في طي النسيان الرقمي، الذي يعد جزء أصيل في الخصوصية الرقمية، فلكل إنسان الحق في ألا ينبش في ماضيه.

الكلمات المفتاحية : تقنيات الذكاء الاصطناعي – الحق في الخصوصية الرقمية – الحق في طي النسيان الرقمي– البيانات الشخصية– الحياة الخاصة.

Abstract:

There is no dispute that artificial intelligence has become an integral part of the rhythm of everyday life, entering all aspects of life, making it impossible to turn a blind eye to it, but that communication technology has negative effects on human privacy and the right to be forgotten. Thus, the legislature in various countries of the world has reeled off laws guaranteeing criminal and civil protection of the right to privacy by criminalizing access to personal data and remaining without prior permission from the person concerned. as well as prosecution of the criminal and civil liability of electronic brokers. Confronting the use of artificial intelligence for the purpose of encroaching on digital privacy. In the sense of e-service providers, where shelter services, the provision of information and search engines to others, do not hide the importance of the right to digital privacy, especially since this description is public to include along with data related to private life, bank accounts, as well as the right to digital forgetfulness, which is an inherent part of digital privacy, everyone has the right not to be explored in their past.

Keywords: artificial intelligence technologies - the right to digital privacy - the right to digital forgetfulness - personal data - private life.

مقدمة

غني عن البيان ، أن الحق في الخصوصية يعتبر حقا أصيل من حقوق الانسان ، وهو حق قانوني ودستوري مضمون لما للخصوصية من أهمية بسبب ارتباطها الوثيق بكرامة الإنسان، فهو يعني في جوهره ترك الإنسان يعيش وفقا لأفكاره وإرادته ومبادئه ومعتقداته وبالطريقة التي يراها مناسبة في هدوء تام بعيدا عن فضول الآخرين.

الا أنه ومع بروز العالم الرقمي وتقنيات الذكاء الاصطناعي ، فان الحق في الخصوصية الرقمية باعتباره جزاً لا يتجزأ من الحق في الخصوصية طرأت عليه الكثير من التغيرات سواء الإيجابية أو السلبية، فمن ناحية تلك تعتبر بمثابة نقلة نوعية للرفاه البشري والتطوير المعرفي، ووسيلة لتعزيز حقوق الإنسان والدفاع عنها ، ولاسيما الحق في حرية التعبير، الا أنه من ناحية أخري أضحت خصوصية الأفراد على تطبيقات الذكاء الاصطناعي والمنصات الرقمية أكثر عرضة لخطر الانتهاك، سواء من الافراد أو الشركات التجارية أو الحكومات أو الدول أو حتي تقنية الذكاء الاصطناعي ذاته، وذلك من خلال مراقبة الاتصالات الخاصة بالأفراد والتدخل فيها لغايات التجسس، أو جمع البيانات الشخصية وتخزينها بغية استغلالها لأغراض تجارية، وهو ما يعد انتهاك للحق في الخصوصية، مما يقتضي بذل العديد من الجهود القانونية والتقنية الوطنية والدولية والإقليمية لحماية خصوصية الأفراد الرقمية في بيئة الذكاء الاصطناعي ، كون النصوص التقليدية الوطنية والدولية المتعلقة بالحق في الخصوصية لم تعد تلبي الحاجة اليوم وتحتاج الى المزيد من التعديلات الجوهرية.

ومن نافلة القول ، أنه فيما يتعلق بتقنيات الذكاء الاصطناعي، فإن مسؤولية المستخدمين عند استخدامه يمكن أن تشمل انتهاك حقوق الخصوصية والبيانات الشخصية، وكذلك تصرفات غير قانونية أو ضارة بالنسبة للشركات والمؤسسات التي توفر التقنية الذكية، فإنها مسؤولة عن العيوب التقنية أو الأخطاء التي تؤدي إلى إيذاء المستخدمين أو الأضرار بالخصوصية الرقمية المحمية بموجب القانون.

والواقع ، ان تقنيات الذكاء الاصطناعي تنطوي على أخطار كبيرة عند الأمر بحماية البيانات الشخصية، وذلك بسبب الكم الهائل من البيانات المستخدمة لتدريبها ، والتي قد يتم الحصول عليها بطرق غير قانونية اي بدون الحصول على رضاء أصحابها . ففيما يتعلق بالبيانات الشخصية لا يقتصر الأمر على انتهاك حقوق الخصوصية وحماية البيانات، فاستخدام ChatGPT على سبيل المثال، وبمجرد التحدث وطرح الأسئلة قد تنتهك بياناتك الشخصية. فباستقراء سياسة الخصوصية الخاصة بشركة OpenAI نجد أن البيانات الشخصية محل استخدام واستغلال كبير، بما يتنافى مع أصول حماية البيانات الشخصية، حيث تنص سياسة الخصوصية صراحة على التالي: "قد نستخدم المعلومات الشخصية للأغراض التالية: لتوفير الخدمات وإدارتها وصيانتها وتحسينها و / أو تحليلها؛ لإجراء البحوث للتواصل معك لتطوير برامج وخدمات جديدة؛ لمنع الاحتيال أو النشاط الإجرامي أو إساءة استخدام خدماتنا ، ولضمان أمن أنظمة تكنولوجيا المعلومات لدينا، والهندسة المعمارية ، والشبكات ؛ وللامتثال للالتزامات القانونية والإجراءات القانونية ولحماية حقوقنا أو خصوصيتنا أو سلامتنا أو ممتلكاتنا و / أو حقوق الشركات التابعة لنا أو أنت أو أطراف أخرى"[١].

ولنضرب مثالا آخر على امكانية تعرض خصوصيات المستخدمين للخطر من تقنيات الذكاء الاصطناعي هي المركبات ذاتية القيادة التي تعمل بالذكاء الاصطناعي؛ نظراً لاعتماد تقنية المركبات ذاتية القيادة على نظام تحديد المواقع العالمي (GPS) وكذلك حاجة هذه المركبات إلى ان تكون متصلة بالأنترنت بصفة مستمرة، فان هذه الاتصالات تجعل انظمتها المعلوماتية عرضة للقرصنة، بالرغم مما تقدمه هذه المركبات من عوامل الأمان والراحة لمستخدميها يقابله من ناحية اخرى امكانية تعرض خصوصياتهم للخطر من خلال تتبع تحركاتهم وتسجيلها، خاصة اذا علمنا ان تأجير

(١) ينظر: د. مروة زين العابدين سعد ود. محمد الجندي ،المشكلات القانونية للذكاء الاصطناعي التوليدي(ChatGPT) ، مجلة القانون والتكنولوجيا ، المجلد ٣،العدد١،ابريل ٢٠٢٣، ص٣٠٥.

هذه المركبات قد يتم من خلال تطبيقات الكترونية، تتطلب لإمكان الاستفادة منها تسجيل بعض البيانات الشخصية للمستخدم [٢].

إشكالية البحث: تكمن إشكالية البحث المحورية، في كيفية تصدي لمسألة المساس بالحق في الخصوصية في المجال الرقمي المزودة بتقنيات الذكاء الاصطناعي وبخاصة في حالة عجز النصوص التقليدية عن مواكبة التغيرات التي طرأت على هذا الحق بسبب التطور التكنولوجي واستخدام تقنيات الذكاء الاصطناعي ؛ وبخاصة أن معايير الحق في الخصوصية التي تضمنتها القواعد التقليدية للقانون الدولي لا سيما المادة (١٢) من الإعلان العالمي لحقوق الإنسان ١٩٤٨، والمادة (١٧) من العهد الدولي للحقوق المدنية والسياسية ١٩٦٦، ودساتير الدول المختلفة، غير كافيه لحماية الخصوصية في عصر الذكاء الاصطناعي. هذا بالإضافة الي إشكالية المسئولية الجزائية لتقنيات الذكاء الاصطناعي ذاتها اذا قامت بانتهاك الخصوصية الرقمية من تلقاء ذاتها دون إدني مسئولية من منشئها أو مبرمجها أو مستخدمها.

وبناء على ذلك سوف نقوم بتسلط الضوء على أثر تقنيات الذكاء الاصطناعي على الحياة الخاصة، وذلك بغية الاجابة على هذا الأشكال المحوري المتمثل في: ماهية الحق في الخصوصية الرقمية، وفيما تتمثل مخاطر التقنيات الذكاء الاصطناعي على هذا الحق، وإن كانت أغلب دول العالم قد وضعت ضمانات قانونية لحماية هذا الحق فما مدى كفايتها مع تطور استخدامات الذكاء الاصطناعي وهل توجد معالجة تشريعية وطنية في هذا المجال؟

ويتفرغ عن الإشكالية المحورية تساؤلات فرعية ؛ إشكالية معامل التوازن بين حماية البيانات الشخصية باستخدام الذكاء الاصطناعي من خلال المعالجة الإلكترونية، والحق في الحصول على المعلومة؟ وكذلك إشكالية ضمان الحماية الإجرائية للبيانات، خاصة مع تداول البيانات الشخصية، خلال إجراءات الاستدلال والتحقيق، إذ لا يقف الأمر عند حدود الحصول على المعلومة، من منظور عام، ولكن البحث عن الحقيقة،

---

(٢) د. أيمن مصطفي أحمد البقلي، و د. طارق جمعة السيد راشد، نحو نظام قانوني للمسئولية المدنية الناجمة عن حوادث المركبات ذاتية القيادة (أساس المسئولية– والتأمين منها)، مجلة البحوث الفقهية والقانونية، تصدر عن كلية الشريعة والقانون بدمنهور، العدد الحادي والأربعين، ٢٠٢٣، ص٨٣٠.

وهنا يأتي الدور الذي يضطلع به المشرع من جانب، في فرض عدم مباشرة إجراءات الدخول والاعتراض لسير البيانات الرقمية إلا بناءً على أمر مسبب من جهات التحقيق، ومن جانب أخر، تقييد الدخول على البيانات وتفتيش الحاسوب، واعتراض البريد الإلكتروني بغاية البحث عن الحقيقة، ومن ثم، تسليم البيانات التي تتكشف إلي جهات التحقيق، واعدامها بمجرد الانتهاء منها. مما يثير التساؤل حول الضوابط الإجرائية التي تكفل حماية المعلومات خلال مباشرة هذه الإجراءات (الاستدلال والتحقيق) ؟

أهمية البحث : تأتي أهمية البحث بالنظر إلي التطور المطرد في تقنيات الذكاء الاصطناعي، والدور الهام، الذي يضطلع به في حماية البيانات الشخصية من جانب، من خلال المعالجة الإلكترونية للبيانات. ويوازي هذا التطور في تكنولوجيا الاتصال والذكاء الاصطناعي، تطور في اختراق البيانات، ولا سيما التي تتعلق بالحسابات المصرفية، والبيانات الشخصية، التي تتداولها جهات التحقيق، والمعروضة أمام القضاء، سواء المدني، أو الجنائي، من خلال تطبيق تقنية التقاضي عن بعد، وهذا وقد تتحد تقنيات الذكاء الاصطناعي مع البيانات الشخصية لإنشاء إصدارات افتراضية للأفراد يمكن استخدامها لمجموعة متنوعة من الأغراض ،مما يثير تساؤلات قانونية وأخلاقية حول الخصوصية وملكية البيانات الشخصية سواء للأفراد أو الشركات أو الدولة. هنا يبرز الدور، الذي يقوم به تقنيات الذكاء الاصطناعي، وتلك مسألة فنية، في المقام الأول، على اعتبار أن الأمر يتعلق بمعالجة إلكترونية، وتلك مسألة فنية تسبق، بطبيعة الحال، الدور الذي يقوم به المشرع.

منهجية البحث: لا خلاف على أهمية المنهج التحليلي الذي يعنى بتحليل النصوص القانونية ذات الصلة بالموضوع ، والمنهج المقارن في البحث، وحسبنا أن الدول الغربية، وعلى رأسها الولايات المتحدة الأمريكية هي التربة الخصبة للدور الذي يقوم به الذكاء الاصطناعي في حماية أو انتهاك البيانات الشخصية. بخلاف الحال، بالنسبة للدول العربية، باعتبارها مجرد سوق لتكنولوجيا الاتصال، الأمر الذي يستحيل معه بحث هذا الموضوع بدون الوقوف على تجارب الدول الأخرى، وقد اكتفينا بالمقارنة مع

النظـام الفرنسـي، بجانـب المقارنـة مـع بعـض الـدول العربيـة، وعلـى الأخـص، دولـة الإمارات العربية المتحدة.

خطة البحث: سوف نتناول موضوع "الذكاء الاصطناعي والحق في الخصوصية الرقمية"، في المحور السادس من مؤتمر التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي، حيث الذكاء الاصطناعي وحقوق الإنسان. من خلال مطالب ثلاثة : حيث نتناول في المطلب الأول : ماهية الذكاء الاصطناعي ونشأته وماهية الحق في الخصوصية الرقمية، وطي النسيان. أما عن المطلب الثاني: فقد جري تخصيصه لحماية الحق في الخصوصية الرقمية وآليات حمايته، تحت عنوان" الذكاء الاصطناعي والإضرار بالحق في الخصوصية الرقمية" . أما عن المطلب الثالث: فقد جري تخصيصه للحماية الإجرائية للحق في الخصوصية الرقمية، خلال مراحل إجراءات الاستدلال والتحقيق.

المطلب الأول

ماهية الذكاء الاصطناعي ونشأته وماهية الحق في الخصوصية الرقمية، وطي النسيان.

تمهيد وتقسيم: في الواقع، وعلى اعتبار أن موضع البحث ينحصر في دراسة الدور، الذي يضطلع به الذكاء الاصطناعي في الخصوصية الرقمية، ومن ثم وبمنطق الحال، يجب الوقوف قبل الدخول في الموضوع على مجموعة من العناصر الأساسية، التي تتمثل في ماهية الذكاء الاصطناعي ونشأته، ثو الوقوف على ماهية الحق في الخصوصية الرقمية وطي النسيان، على النحو التالي :

الفرع الأول : ماهية الذكاء الاصطناعي ونشأته.

الفرع الثاني : ماهية الحق في الخصوصية الرقمية.

الفرع الثالث : الحق في طي النسيان.

الفرع الأول

ماهية الذكاء الاصطناعي ونشأته

لقد جاءت الإرهاصات الأولي للذكاء الاصطناعي على لسان جون مكارثي في بحث مقدم له في مؤتمر دارت موث، حيث كانت الإشارة الأولي للذكاء الاصطناعي، حيث حمل هذا المؤتمر اسم " ميلاد الذكاء الاصطناعي "[٣]. أما عن التطبيقات العملية الأولي للذكاء الاصطناعي، فقد ظهرت في بداية عام ١٩٥٦، حيث حدث خلال تلك الفترة، نوع من التوافق بين واقع الذكاء وتطبيقه وبين البحث العلمي كما بدأ الاهتمام بهندسة اللغة، لغة البرمجة والخوارزميات، وهنا بدأ نوع من التفاؤل الإنساني بتطبيقات بناء الإنسان الآلي (Robotics)[٤].

وفي خطوة تقدمية، وخلال الفترة من عام ١٩٨٠ إلي عام ١٩٨٧، حدث ارتفاع في مستويات تأثير نظم الخبرة، وأيضا الثورة المعرفية، حيث بدأت، بالفعل، بشائر العائد المادي ومشروع الجيل الخامس، وبدأت عملية إحياء الاتصالية[٥]. بينما، وخلال الفترة من عام ١٩٨٧ حتى عام ١٩٩٣، أضحت البيئة أكثر قبولاً للذكاء الاصطناعي، خاصة مع تقدم البرمجيات، ودخول الانترنت في عمل الإدارات والمؤسسات العامة، وظهور إرهاصات الحكومة الإلكترونية[٦].

خلال الفترة من عام ١٩٩٣ وحتى عام ٢٠١١ استقرت قواعد وخصائص وسمات مجال الذكاء الاصطناعي، حيث بدأت الوكالات المتخصصة نشاطها الواسع في مجال

---

(٣) Wikipedia, History of artificial Intelligence, https://en.wikipedia.org/wiki/History_of_artificial_intellegence,accesseddata ٢٢/٧/٢٠٢٣.

(٤) Javier Andreu Perez, fan Deligianni, Daniele Ravi and Guang- Zhang Yang, Artificial intelligence and Robtics UK RAS NETWORK UKRAS. ORG, centers for Doctoral training and partner University, ٢٠١٨, p.٢٧.

(٥) OECDM Directorate for Education and skills, Education policy Committee, ٢٤٠ ct., ٢٠١٨, pp. ١- ٢١.

(٦) Handler, J, Avoiding Another AI winter research gate, April ٢٠٠٨, pp ٢-٣.

الـذكاء الاصـطناعي، حيـث اتضـحت صـورته العلميـة علـى نحـو أوضـح، خاصـة مـع الامتداد المطرد في تطبيقاته[٧].

أخيـراً، وخـلال الفتـرة مـن عـام ٢٠١١ وحتـى وقتنـا الحـالي، ظهـرت مفـاهيم مـا يعـرف بـالتعلم العميـق، الـذي يتمثـل فـي إيجـاد نظريـات وخوارزميـات تسـمح للآلـة أن تـتعلم بـذاتها عـن طريـق محاكـاة الخلايـا العصـبية فـي جسـم الإنسـان، فضـلاً عـن كـم المعلومـات الهائـل في المجال، وكذا الذكاء الاصطناعي العام[٨].

والواقـع ، أنـه هنـاك العديـد مـن التعريفـات الفقهيـة للـذكاء الاصـطناعي، منهـا مـن وصـفه بالمقـدرة علـى اكتسـاب وتطبيـق المعرفـة، مـا عـن لفـظ اصـطناعي، فإنـه يعنـي مـا اصـطنع بواسـطة الإنسـان، وهـو قسـم مـن علـوم الحاسـب يهـتم بتصـميم الأنظمـة، التـي تبـرز الـذكاء الإنسـاني، حيـث فهـم اللغـة، وتعلـم معلومـات جديـدة، والاسـتدلال وحـل المشـاكل[٩]. وهنـاك تعريـف فقهـي أخـر للـذكاء الاصـطناعي، بأنـه مجموعـة البـرامج الإلكترونيـة، التـي تصـمم علـى الأجهـزة، بحيـث تحـاكي الـذكاء البشـري لأداء مهـام وذلـك اسـتنادا إلـي المعلومـات، التـي تجمعهـا[١٠]. بينمـا عرفهـا أخـر، بأنهـا، " القـدرة علـى فهـم الظـروف أو الحـالات الجديـدة والمتغيـرة؛ أي هـو القـدرة علـى إدراك وفهـم وتعلـم الحـالات أو الظروف الجديدة. وبمعنى آخر: أن مفاتيح الذكاء هي الإدراك، الفهم، والتعلم "[١١].

أمـا كلمـة الصـناعي أو الاصـطناعي تـرتبط بالفعـل يصـنع أو يصـطنع، وبالتـالي تطلـق الكلمـة علـى كـل الأشـياء التـي تنشـأ نتيجـة النشـاط أو الفعـل الـذي يـتم مـن خـلال اصـطناع وتشـكيل الأشـياء تمييـزًا عـن الأشـياء الموجـودة بالفعـل، والمولـدة بصـورة طبيعيـة

(٧) Wikipedia, HAL ٩٠٠٠, ٢٠٠١: A space Odyssey. ٧ pp/

(٨) Ian Goodfellow, Yoshua Bengio & Aaron Courville, Deep Learning, www.deepleaningbook.org. ١٢/٧/٢٠٢٣.

(٩) د. سهام النويهي، المنطق الغانم: علم جديد لتقنية المستقبل المكتبة الأكاديمية، القاهرة ،٢٠٠١، ص١١.

(١٠) أحمد عبد العظيم علي، ثورة الذكاء الاصطناعي وأثره على مهنتي المحاسبة والمينظرة، الدار العالمية للنشر والتوزيع، مصر ٢٠٢١ ص ٤

(١١) C. Ricardo: Logique pour l'informatique et pour l'intelligence artificielle, Hermes Sciences Publication, Paris, France, ٢٠١١, p. ٢٠.

من دون تدخل الإنسان[١٢]. و هناك تعريف أخر للذكاء الاصطناعي بأنه، " القدرة على التصرف كما لو كان الإنسان هو الذي يتصرف من خلال محاولة خداع المستجوب وإظهار كما لو إن إنسانًا هو الذي يقوم بالإجابة على الأسئلة المطروحة من قبل المستجوب "[١٣].

ومن ناحية المشرع المصري، فقد وضع تعريف للذكاء الاصطناعي في إطار معالجته للبيانات الشخصية، حيث جاء تعريف المعالجة الإلكترونية بطريق الذكاء الاصطناعي بأنه، (" المعالجة: أي عملية إلكترونية أو تقنية لكتابة البيانات الشخصية، أو تجميعها، أو تسجيلها، أو حفظها، أو تخزينها، أو دمجها، أو عرضها، أو إرسالها، أو استقبالها، أو تداولها، أو نشرها، أو محوها، أو تغييرها، أو تعديلها، أو استرجاعها أو تحليلها وذلك باستخدام أي وسيط من الوسائط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيا أو كليًا.")[١٤].

وهناك العديد من التعريفات الفقهية الغربية للذكاء الاصطناعي، فهناك من يعرف الذكاء الاصطناعي بأنه، " حقل علم الحاسوب المهتم بتصميم نظم حاسوب ذكية، نظم حاسوب تعرض خصائص الذكاء في السلوك الإنساني "[١٥]. وهناك من يعرفه بأنه، " العلم الذي يمكن الآلات من تنفيذ الأشياء التي تتطلب ذكاءً إذا تم تنفيذها من قبل

(١٢) د. ياسين سعد غالب، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، ط١، دار المناهج للنشر والتوزيع، الاردن ،٢٠١١، ص ٢٣.

(١٣) د. صلاح الفضلي، آلية عمل العقل عند الإنسان، دار عصير الكتب للنشر والتوزيع، القاهرة ،٢٠١٩، ص ١٤٧.

(١٤) لمزيد من التفصيل، ينظر المادة (١) من الفصل الأول من القانون رقم (١٥١) لسنة ٢٠٢٠: الجريدة الرسمية–العدد ٢٨ مكرر (هـ)– في ١٥ يوليه ٢٠٢٠.

(١٥) Barr, A, Feigenbaum E.A: The handbook of Artificial Intelligence, Kaufmann William Inc, New York, USA, ١٩٨٠, p. ٩٥.

الإنسان "[١٦]. وهناك تعريف يري في الذكاء الاصطناعي، " دراسة لجعل أجهزة الحاسوب أن تؤدي أشياء يقوم بها الإنسان بطريقة أفضل "[١٧].

من مجموع هذه التعريفات المختلفة، يتضح لنا انها تحصر الذكاء الاصطناعي في المنظومة الإلكترونية، التي تقوم بذات العمليات الذهنية، التي يقوم بها البشر. وهو ما يعني أن الذكاء الاصطناعي لا يتمتع بالحضور المتمايز المستقل عن الذكاء البشري، بل يقوم بذات العمليات التي يقوم بها الفرد، وعلى وجه الخصوص العمليات الذهنية، حتى مع التطور الكبير في استخدام الذكاء الاصطناعي في العمليات المادية، التي تتم باستخدام الخوارزميات، على سبيل المثال، المركبات ذاتية القيادة، والربوت الطبي، وكذلك القضائي.

فضلاً عن ذلك، ومع هذا الشتات في التعريفات الموضوعة للذكاء الاصطناعي، فلا يوجد حتى وقتنا الحالي، إجماع على تعريف موحد، ينطلق من خلال مجموعة من المعايير الموحدة.

ابتكر البرلمان الأوروبي نظرية " النائب الإنساني المسؤول "، وفقاً لقواعد القانون المدني الأوروبي الخاص بالروبوتات الصادر في فبراير ٢٠١٧، وذلك حتى يفرض المسؤولية عن تشغيل الروبوت على مجموعة من الأشخاص، وفقاً لمدي خطأهم في تصنيعه أو استغلاله، ومدي سلبيتهم في تفادي التصرفات المتوقعة من الروبوت، دون افتراض، ولا اعتبار الروبوت شيء[١٨]. فتقوم المسئولية عن أفعال وتقصير الروبوت

(١٦) Minsky M: Steps toward Artificial Intelligence, Proceedings of the IRE, USA, ١٩٦١, p. ٧٤.

(١٧) E. Rich, Artificial Intelligence and the Humanities, Paradigm Press, ١٩٨٥, p. ١١٧.

(١٨) د. همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت (تأثير نظرية النائب الإنساني عن جدوي القانون في المستقبل) ، ٢٠١٨، بحث منشور في مجلة الأبحاث القانونية المعمقة، العدد ٢٥ ص ٨٠.

على نائب إنساني *Human Agent*[١٩]، وهو الشخص، الذي أطلق عليه الفقه الفرنسي مصطلح قرين الروبوت *Robot Companion*[٢٠].

على أية حال، إن نظرية النائب الإنساني المسؤول هي حالة مؤقتة خاصة تهدف إلي الانتقال من نظام حارس الأشياء أو رقيب المسؤولية من الروبوت إلي الإنسان على أساس الخطأ واجب الإثبات في إدارة التصنيع أو التشغيل، أو الامتناع عن تجنب حادث خطر متوقع من الروبوت، وذلك لأن الروبوت لم يعد شيء قابل للحراسة، أو شخص قابل للرقابة المحكمة، بل آلة ذكية مستقلة في التفكير كالإنسان الراشد، الذي لا تصح الرقابة عليه بعد ترسخ استقلال الروبوت[٢١].

الفرع الثاني

ماهية الخصوصية الرقمية

بداية، ومن منظور عام، إن الحق في الخصوصية يرجع في مصدره إلي نصوص الدساتير والقوانين الوطنية، فضلاً عن حضوره في المواثيق الدولية وإعلانات الحقوق، بل لا نغالي في القول بأن هذا الحق سابق على وجود الدولة ذاتها. ومن ثم، فإن كافة المجتمعات، خاصة الديمقراطية منها تحرص كل الحرص على كفالة هذا الحق، وتعتبره حق مستقل، وقائم بذاته، حيث لا تكتفي بمجرد سن القوانين لحمايته، بل تسهر على صيانة هذا الحق[٢٢]، خاصة وأن الدول ذات النظم الاستبدادية تتباهي بوجود

(١٩) Section A.- D., Introduction, The European Parliament, Civil Law Rules on Robotics of ٢٠١٧. The European Parliament, plenary sitting, the report of ٢٧-١-٢٠١٧, page ٧.

(٢٠) Anne BOULANGE, Carole JAGGIE, "Ethique, responsabilité et statut juridique du robot compagnon: revue et perspectives", IC٢A: ١٣. Voir: https://hal.archives-ouvertes.fr/cel- dernière visite, ١٢-٨-٢٠٢٣.

(٢١) د. همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت (تأثير نظرية النائب الإنساني عن جدوي القانون في المستقبل) ، المرجع السابق، ص ٨٤.

(٢٢) بن قارة مصطفي عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، العدد السادس، يونيه ٢٠٠٦، ص ٢٧٢.

نصوص في دساتيرها تكرس للحقوق والحريات العامة، ومنها الحق في الخصوصية، على سبيل المثال، ولكنها وفي ذات الوقت تحرص على تجميد هذه النصوص.

وتعد الحياة الخاصة الوعاء لكل وجود لا يجوز لأي شخص التدخل فيه ما لم يحصل على موافقة الشخص المعني لمثل هذا التدخل، ولقد تم إقرار حرية الحياة الخاصة لكل فرد، وله الحق في منع الغير من التدخل في حياته الخاصة[٢٣]. على هذا الحال، يتعين أن تكون حرية الحياة الخاصة مضمونة، ومن ثم يجب أن يكون لكل شخص سلطة للسيطرة على كل تصرفاته، وأفكاره، ومن ثم له الحق في منع الغير من التعرف على بياناته الشخصية، ما لم يحصلوا على ترخيص منه بالتدخل[٢٤].

والحق في الخصوصية الرقمية، جزء لا يتجزأ من الحق في الحياة الخاصة، فهو أحد المكونات الأساسية للحقوق والحريات، وهو حق قانوني ودستوري مضمون لما للحياة الخاصة من أهمية بسبب ارتباطها الوثيق بكرامة الإنسان، فهو يعني في جوهره ترك الإنسان يعيش وفقاً لأفكاره وإرادته ومبادئه ومعتقداته، وبالطريقة التي يراها مناسبة في هدوء تاما بعيداً عن فضول الآخرين[٢٥].

ومع تزايد التقنيات الحديثة وتطورها المستمر وبخاصة تقنيات الذكاء الاصطناعي زادت المخاطر على الخصوصية، لاسيما مع بداية خضوع المعطيات الشخصية لنظام تحكم مركزي للإدارة العمومية، مما أثار تخوفات شديدة على حماية البيانات، التي تتصل بالأفراد وحياتهم الخاصة[٢٦]. ومن حيث مبدأ الحق في الخصوصية، بالمعني التقليدي له يعني، حق الفرد في أن يقرر بنفسه متى وإلي أي حد يمكن أن يطلع الغير على شؤونه الخاصة، وفي إطار الاعتداءات، التي أصبحت تطال حياته الخاصة

(٢٣) J. Rivero, *Libertés publiques*, Montchrestien, ١٩٨٩, p. ٧٤.

(٢٤) J. HARIVEL ; Libertés publiques, Libertés individuelles, risqué et enjeux de la sociétés numériques, thèse Sorbonne, ٢٠١٨, p.١٥٥.

(٢٥) د. عماد الدين بركات، و د. حورية طيبي، الحماية الجنائية للحق في الخصوصية المعلوماتية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد ٧ العدد ١ السنة ٢٠٢١، ص ٤٦.

(٢٦) فريد-هـ-كيث، الخصوصية في صدر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٩٩، ص ١٢٣.

بواسطة تقنيات الذكاء الاصطناعي، أصبح من الضروري إعادة النظر في هذا المفهوم، بل وقد زاد الاهتمام بهذا الحق نظراً لما يتعرض له من مخاطر تحيط به وتهدده أبرزها التقدم التكنولوجي والمعلوماتي الذي كان له دور في اقتحام حصون هذا الحق[٢٧].

ومن مخاطر تقنيات الذكاء الاصطناعي ما يقوم – ChatGPT بمعالجة البيانات التي يوفرها المستخدم عن نفسه سواء بشكل مباشر أو غير مباشر من خلال طرح الأسئلة، ولم تنص السياسة صراحة على أية إجراءات للحفاظ على البيانات الشخصية الحساسة، أو التي تجعل الشخص قابلا للتعريف، ومن ثم يستطيع جمع ومعالجة البيانات الشخصية. أما إذا كانت البيانات التي يوفرها المستخدم لـ ChatGPT بيانات متعلقة بأسرار تجارية أو غيره مما يرتبط بأعمال، يحق له وفقًا لسياسة الاستخدام إعادة إنتاجها وتقديمها لمستخدم آخر والذي قد يكون أحد المنافسين[٢٨].

هذا وقد اعتبر تقرير الأمم المتحدة لسنة ٢٠١٨ حول الحق في الخصوصية في العصر الرقمي بأنها : "التسليم بحق الأفراد في التمتع بفسحة للتنمية الذاتية، تقوم على مبدأ التفاعل والحرية، أو حقهم في المجال الخاص، يتسع لهم فيه التفاعل أو عدم

---

(٢٧) بن قارة مصطفي عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، المرجع السابق، ص ٢٧٣.

٢٨ وفي سابقة للتصدي لهذا الانتهاك من الذكاء الاصطناعي في ٣١ مارس، أصدر منظم البيانات الإيطالي قرارًا طارئًا مؤقتًا يطالب بالتوقف عن استخدام البيانات الشخصية لملايين الإيطاليين الواردة في مجموعات البيانات التي يستخدمها للتدريب وتعلم الآلة؛ حيث لا تملك OpenAI الحق القانوني في استخدام المعلومات الشخصية للأشخاص في . رداً على ذلك، منعت شركة OpenAI الأشخاص في إيطاليا من الوصول إلى برنامج الدردشة الآلي الخاص بها، بينما تقدم ردودًا على المسؤولين، الذين يحققون بشكل أكبر. ينظر : د. مروة زين العابدين سعد ود. محمد الجندي ،المشكلات القانونية للذكاء الاصطناعي التوليدي(ChatGPT) ،المرجع السابق، ص٣٠٦.

التفاعل مع الأخرين دون الخضوع الى تدخل الدولة ولا الى تدخل تطفلي زائد يمارسه افراد اخرون بلا دعوة "[٢٩].

وهناك العديد من التعريفات الفقهية للحق في الخصوصية الرقمية، حيث تتباين هذه التعريفات باختلاف توجهات الفقهاء، حيث عرفها الفقيه الأمريكي آلان يستن بأنها، " القدرة على التحكم في مقدار ما نكشفه عن أنفسنا للآخرين "[٣٠]. فقد وضع الفقيه الأمريكي ميلر تعريف للحق في الخصوصية مفاده، " قدرة الأفراد على التحكم بدورة المعلومات، التي تتعلق بهم"[٣١].

وبعيداً عن التعريفات الفقهية، فقد جاءت الاتفاقية الأوروبية رقم (١٠٨) الصادرة عن مجلس أوروبا بتعريف للبيانات الشخصية، في المادة (٢/أ) ، التي نصت على : " أن المعطيات ذات الطابع الشخصي هي كل المعلومات المتعلقة بشخص طبيعي معرف، أو قابل للتعرف عليه ". وبنفس المعني جاء تعريف البيانات الشخصية في ذات المادة من التوجيه الأوروبي رقم(٤٦/٩٥) الصادر بتاريخ ٢٤ أكتوبر ١٩٩٥، " بأن المعطيات ذات الطابع الشخصي هي كل معلومة متعلقة بشخص طبيعي، أو قابل للتعرف عليه، يعد قابلاً للتعرف عليه الشخص المعني ".

لذا ، فهذه المعلومات يطلق عليها خاصة كونها تتعلق بالشخص ذاته وتنتمي إلى كيانه كإنسان مثل الاسم والعنوان رقم الهاتف حالته الصحية وغيرها من المعلومات، فهي معلومات تأخذ شكل بيانات تلزم الالتصاق بكل شخص طبيعي معرف أو قابل للتعريف[٣٢].

([٢٩]) ينظر: تقرير مفوض الأمم المتحدة السامي لحقوق الانسان حول الحق في الخصوصية في العصر الرقمي بتاريخ ٢٠١٨/٨/٣، الملحق رقم A/HRC/٣٩/٢٩ ص ٣.

([٣٠]) رؤي سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة) ، مجلة كلية الدراسات الإسلامية والعربية للبنات، الجزء الأول، العدد السادس، ٢٠٢١، ص ١٠٣٦.

([٣١]) يونس عرب، دور حماية الخصوصية في تشجيع الادماج بالمجتمع الرقمي، ورقة مقدمة في ندوة نادي أخلاق المعلومات العربي، ١٧-١٨ أكتوبر ٢٠٠٢، عمان، الأردن، ص ٧.

([٣٢]) بن قارة مصطفي عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، المرجع السابق، ص ٢٧٤.

وهذه النوعية من المعلومات أصبحت في وقتنا الحاضر على درجة كبيرة من الأهمية في ضل التطورات التقنية، تحديدا إنشاء بنوك المعلومات وإجراء عملية المعالجة والتحليل بواسطة الذكاء الاصطناعي، من هنا ظهر ما يعرف بالخصوصية الرقمية.

وتجدر الإشارة الي أنه يعتبر نهج الاتحاد الأوروبي لإدارة مخاطر الذكاء الاصطناعي معقدا ومتعدد الأوجه بصدد حماية الخصوصية، حيث يعتمد على التشريعات المطبقة ، ولا سيما اللائحة العامة لحماية البيانات (GDPR) ، والتي تشمل التشريعات التي تم سنها حديثًا ، وهي قانون الخدمات الرقمية وقانون الأسواق الرقمية ، فضلا عن التشريعات التي لا تزال نشطة تمت مناقشته ولا سيما قانون الذكاء الاصطناعي، من بين المساعي الأخرى ذات الصلة[٣٣].

الفرع الثالث

الحق في طي النسيان الرقمي

لا يزال الحق في طي النسيان يشغل اليوم المحور الأساسي للمناقشات ، فقد أنقسم الفقه حول إعتبار هذا الحق يدخل ضمن عناصر الحق في حرمة الحياة الخاصة من عدمه [٣٤]، وان كنا نؤيد انه كذلك بالطبع . وبالطبع تتضاعف خطورة تقنيات الذكاء الاصطناعي علي هذا الحق . ومنذ شهور خلت، تساءل مشرع الاتحاد الأوروبي عن ضرورة إقرار مثل هذا الحق في المحيط الرقمي. ومن ناحية المجلس الأوروبي فقد عبر عن اهتمامه البالغ بهذا الموضوع، خاصة مع تعالي أصوات بعض رجال السياسة الوطنيين بشأن إقرار هذا الحق. وعلى هذا الحال، فقد أصبح الرهان يتعلق في الأساس بالحق في محو المعلومات التي تتعلق بالأشخاص، عقب مرور فترة من الزمن[٣٥].

---

(٣٣) Regulation (EU) ٢٠٢٢/١٩٢٥ of the European Parliament and of the Council of ٦ April ٢٠٢٢ on contestable and fair markets in the digital sector (Digital Markets Act) | (٢٠٢٢) | OJ L ١٤٥/١ | [Accessed ٢٧ April ٢٠٢٣]

(٣٤) د. يسرى عبدالله عبد الباري عبد المطلب ، الحماية المدنية للخصوصية المعلوماتية (دراسة مقارنة)، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق- جامعة عين شمس ،٢٠١٦ ، ص١١١.

(٣٥) D. Dechenaud, Introduction, Le droit à l'oubli numérique, ٢٠١٥, P. ١٣

يذهب جانب من الفقه الفرنسي إلي تعريف الحق في طي النسيان الرقمي بأنه، الحق في إزالة الآثار غير المرغوب فيها عبر الانترنت. وعلى هذا الحال، يمكننا أن نختزل المناقشات والجدل الفقهي بشأن هذا الموضوع. على أننا، وللوهلة الأولي يمكننا القول بعدم وجود حق في طي النسيان، ولكن هناك عناصر مستمدة من القانون، والقضاء، هي التي سمحت للغير أن يطلب إزالة البيانات على الانترنت، وكذلك على محركات البحث التي تعتمد علي تقنيات الذكاء الاصطناعي، التي تحيل عليها[٣٦].

وهناك تعريف أخر للحق في طي النسيان الرقمي، حيث يري بأنه، " حق الشخص في عدم نشر البيانات الرقمية التي تعنيه، بناءً على طلبه وعقب مرور فترة من الزمن[٣٧]. وفي سبيل إعمال هذا الحق يمكن اللجوء إلي العديد من الوسائل، خاصة إلغاء البيانات، أو محو الرابط، أو إغفال الهوية. وإشكالية الحق في طي النسيان الرقمي تشتق من طريقة سير الانترنت. وكل فرد حاضر عبر شبكة الانترنت، يملك اليوم هوية رقمية، تتكون من البيانات، التي تتكشف بطريق الفرد نفسه، أو بطريق الغير، وتارة يتم جمعها بدون علمه. كما أن تجميع هذه البيانات يمكن أن يجد مصدره في العديد من الظواهر[٣٨].

فالحق في طي النسيان الرقمي، لا يخرج عن كونه حق في المحو، وكذلك حق في إزالة المرجعية، أو الإحالة على البيانات الشخصية، أو إزالة المرجعية، أو الإحالة على البيانات. وهذه الأفكار تحيل بدورها على الاعتبارات المتنوعة للتصور العام لطي النسيان. ولقد جري الحال على وضع التعريف التالي لطي النسيان، "محو، وإزالة الذكريات، وعلى وجه الخصوص، إبعاد بعض الأفكار المقلقة". وعلى هذا الحال، فإن

(٣٦) F. Chaltiel, Internet et le droit à l'oubli en devenir : dialogue entre le juge européen et le juge administratif, Petites Affiches, n°١٤٩, ٢٧ juillet ٢٠١٧, p.٣.

(٣٧) A. CASSART et J.-F. HENROTTE, « Droit à l'oubli : une réponse à l'hypermnésie numérique », *Droits de l'homme numérique*, ٥٦ème conférence de l'IUA, ١er novembre ٢٠١٢, disponible sur www.uianet.org, p. ٤.

(٣٨) D. DE VIGAN, Le droit a l'oubli numérique au sein de l'Union européenne ; conséquences actuelles, lacunes et perspectives futures, Master ULB, ٢٠١٥, p.٦.

طـي النسـيان يـرتبط جـد الارتبـاط بالـذاكرة. ومـن ثـم، محـو المعلومـة المكتسـبة بصـورة مسبقة[٣٩].

ولقد ورد الـنص علـى الحـق فـي طـي النسـيان الرقمـي فـي المـادة (١٢) مـن التوجيـه الأوروبـي الصـادر فـي ١٩٩٥، الـذي يحيـل علـى الحـق فـي محـو البيانـات، علـى النحـو الـذي يتجـاوز حـدود الحـق فـي تصـحيحها. كـذلك الحـال، المـادة (٤٠) مـن قـانون الفرنسـي ٦ ينـاير ١٩٧٨، التـي تـنص علـى جـواز مطالبـة المسـئول عـن المعالجـة بمحـو البيانـات ذات الطـابع الشخصـي[٤٠]. كمـا كرَّسـت لـه المـادة(٩) مـن التقنـين المـدني الفرنسـي، والمـادة (٧) مـن الميثـاق الأوروبـي للحقـوق الأساسـية والمـادة (٩) مـن الاتفاقيـة الأوروبيـة لحقـوق الإنسـان. ومـن حيـث تمييـز الحـق فـي احتـرام الحيـاة الخاصـة والحـق فـي طـي النسـيان، يمكـن أن نحيـل فـي ذلـك علـى المعيـار المؤقـت. فـالزمن هنـا يعتبـر جـوهر ضروري ومميز للحق في طي النسيان الرقمي[٤١].

المطلب الثاني

الذكاء الاصطناعي والإضرار بالحق في الخصوصية الرقمية.

تمهيـد وتقسـيم : علـى الـرغم مـن الفوائـد الجمـة والإيجابيـات، التـي جـاء بهـا التطـور التكنولـوجي واسـتخدام تقنيـات الـذكاء الاصـطناعي علـى حيـاة الأفـراد والجماعـات، إلا أن لهـا جوانبهـا السـلبية علـى ممارسـة الحـق فـي الخصوصـية[٤٢]، نتيجـة للانتهاكـات، التـي

(٣٩) L. Libin ; Droit a l'oubli numérique- Quel paramètre territorial ?, Master prec., p.٦.

(٤٠) L. Grybaum et autres, Droit des activités numériques, ١ème éd., Dalloz, ٢٠١٤, p.٨١٥.

(٤١) M. Boizard ; Le droit a l'oubli ; Master ٢٠١٥, p.٣

(٤٢) د. محمد الطراونة، تحديات إعمال الحق في الخصوصية، في ظل التطور التكنولوجي، ورقة عمل مقدمة إلي المؤتمر الدولي حول تعزيز الحق في الخصوصية، في سياق الذكاء الاصطناعي، المنظمة العربية لحقوق الإنسان، اللجنة العليا الدائمة لحقوق الإنسان، الأمانة العامة، ٢٠٢٢، ص ٨، متاح على الموقع الإلكتروني : https://www.almasryalyoum.com ٢٨/٧/٢٠٢٣.

يمكن أن يتعرض لها بفعل استخدام تقنيات الذكاء الاصطناعي للدخول علي البيانات الشخصية والبقاء في نظام المعالجة الإلكترونية، بدون سبب مشروع .

وبإمعان النظر للمنتهك للخصوصية الرقمية نجد أنه من الجائز ان يكون مصنع التقنية الذكية بما تحويه من خلل في التصنيع ، أو المبرمج في حالة خطائه العمدي أو غير العمدي أذا وضع برامج غير مشروعة أدت الي ارتكاب الجريمة ، أو المستخدم في حالة أذا اساء التصرف بارتكاب أحدي جرائم انتهاك الخصوصية الرقمية باستخدام تقنيات الذكاء الاصطناعي . ولكن الإشكالية تثور عندما يتصرف تقنيات الذكاء الاصطناعي باستقلالية بأتخاذ قرار غير المشروع بانتهاك الخصوصية بمعزل عن بقية الأطراف الأخرى ،فهل يجوز ملاحقة تلك التقنية ؟ الإجابة بالنفي لكونه ليس انسان وليس لدية الاهلية وفقا لمبدأ الشرعية الجنائية ، لذا ننادي مع بعض الفقه العربي والغربي بمنح تلك التقنيات الذكية الشخصية القانونية الالكترونية علي غرار الشركات الاعتبارية ، مع فرض عقوبات خاصه عليه ، لكون لديه الأدراك الاصطناعي[٤٣].

وهذا وسندنا في ذلك ما ابتكره البرلمان الأوروبي من نظرية " النائب الإنساني المسؤول "، وفقاً لقواعد القانون المدني الأوروبي الخاص بالروبوتات الصادر في فبراير ٢٠١٧، وذلك حتى يفرض المسؤولية عن تشغيل الروبوت على مجموعة من الأشخاص، وفقاً لمدي خطأهم في تصنيعه أو استغلاله، ومدي سلبيتهم في تفادي التصرفات المتوقعة من الروبوت، دون افتراض، ولا اعتبار الروبوت شيء[٤٤]. فتقوم المسئولية عن أفعال وتقصير الروبوت على نائب إنساني *Human Agent*[٤٥]، وهو

([٤٣]) د. أحمد محمد براك، إشكالية المسؤولية الجزائية لتقنيات الذكاء الاصطناعي، مركز البحوث القانونية– أربيل– العراق ، الطبعة الأولي، ٢٠٢٣، ص١٥٥.

([٤٤]) د. همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت (تأثير نظرية النائب الإنساني عن جدوي القانون في المستقبل) ، ٢٠١٨، بحث منشور في مجلة الأبحاث القانونية المعمقة، العدد ٢٥ ، ص ٨٠.

([٤٥]) Section A.- D., Introduction, The European Parliament, Civil Law Rules on Robotics of ٢٠١٧. The European Parliament, plenary sitting, the report of ٢٧-١-٢٠١٧, page ٧.

الشخص، الذي أطلق عليه الفقه الفرنسي مصطلح قرين الروبوت *Robot Companion*[٤٦].

على أية حال، إن نظرية النائب الإنساني المسؤول هي حالة مؤقتة خاصة تهدف إلي الانتقال من نظام حارس الأشياء أو رقيب المسؤولية من الروبوت إلي الإنسان على أساس الخطأ واجب الإثبات في إدارة التصنيع أو التشغيل، أو الامتناع عن تجنب حادث خطر متوقع من الروبوت، وذلك لأن الروبوت لم يعد شيء قابل للحراسة، أو شخص قابل للرقابة المحكمة، بل آلة ذكية مستقلة في التفكير كالإنسان الراشد، الذي لا تصح الرقابة عليه بعد ترسخ استقلال الروبوت[٤٧]. هو تمهيد لأعطائه الشخصية القانونية الالكترونية.

وفي ذات السياق ، فقد عني المشرع المصري بوضع حماية جنائية للبيانات الشخصية، بموجب القانون رقم (١٥١) لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية[٤٨]، حيث عني المشرع المصري في المادة الثالثة من هذا القانون، باستبعاد بعض فئات البيانات الشخصية الرقمية، التي ارتبطت معالجتها بطريق الذكاء الاصطناعي بغايات وإجراءات أخري تتجاوز حدود الخصوصية الرقمية المجردة، التي ترتبط على سبيل المثال بغايات إعلامية، أو بمحاضر الضبط القضائي والتحقيقات، والدعاوي القضائية، والتي تودع لدي جهات الأمن القومي، ولدي البنك المركزي المصري، "الي أخره،..[٤٩]. كما تناول المشرع المصري كافة الضوابط الخاصة بحماية الخصوصية الرقمية، من حيث بيان حقوق الشخص المعني بالبيانات وشروط ومعالجة

(٤٦) Anne BOULANGE, Carole JAGGIE, "Ethique, responsabilité et statut juridique du robot compagnon : revue et perspectives", IC٢A : ١٣. Voir : https://hal.archives-ouvertes.fr/cel- dernière visite, ١٢-٨-٢٠٢٣.

(٤٧) د. همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت (تأثير نظرية النائب الإنساني عن جدوي القانون في المستقبل) ، المرجع السابق، ص ٨٤.

(٤٨) لمزيد من التفصيل، ينظر: قانون رقم (١٥١) لسنة ٢٠٢٠ بإصدار قانون حماية البيانات الشخصية المصري، الجريدة الرسمية-العدد (٢٨) مكرر (هـ)- في ١٥ يوليه سنة ٢٠٢٠، محدثاً حتى عام ٢٠٢٣.

(٤٩) لمزيد من التفصيل، ينظر: المادة الثالثة من القانون رقم (١٥١-٢٠٢٢) بإصدار قانون حماية البيانات الشخصية.

البيانات[٥٠]، والتزامات المعالج للبيانات الرقمية، إلي أخره، بينما ترك المواجهة الموضوعية والإجرائية للقانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات، مما سوف نتناوله بشيء من التفصيل.

وقد تناول المشرع المصري الأحكام الموضوعية للحق في الخصوصية الرقمية في المواد من(٣٥ إلي ٤٨) ، في مواجهة مزودي خدمات المعالجة الإلكترونية للبيانات، وكذلك قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨[٥١]، حيث تناول في الباب الثالث الجرائم والعقوبات، وذلك في المواد من (١٢ إلي ٣٤) ، وسوف نتناول صور الأفعال المجرمة على النحو التالي :

الفرع الاول : جريمة الدخول أو البقاء في نظام المعالجة الإلكترونية الذكي للبيانات.

الفرع الثاني : عرقلة سير نظام المعالجة الإلكترونية الذكي للبيانات.

الفرع الثالث : الإتجار في الأجهزة والبرامج الذكية، التي تستخدم في التعدي على البيانات.

الفرع الاول

جريمة الدخول أو البقاء في نظام المعالجة الإلكترونية الذكي للبيانات

لعبت تقنيات الذكاء الاصطناعي دور أساسي في جرائم اختراق البيانات، ويقدم الأستاذ الدكتور / محمد سالم وزير الاتصالات الأسبق بمصر، العديد من الأمثلة على اختراق البيانات بطريق الذكاء الاصطناعي، فيذكر علي سبيل المثال، ما حدث لشركة ياهوو خلال شهر أغسطس ٢٠١٣، وتأتي جسامة الاعتداء بالنظر إلي حجم المتأثرين

(٥٠) ينظر: المادتان (٢ و٣) من الفصل الثاني من القانون رقم (١٥١-٢٠٢) بإصدار قانون حماية البيانات الشخصية المصري.

(٥١) ينظر لمزيد من التفصيل، قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨، متاح على الموقع الإلكتروني: https//www.cc.gov.eg .١٠/٧/٢٠٢٣

بهذا الاختراق للبيانات الشخصية، حيث تأثر به ثلاثة مليارات حساب شخصي، نتيجة العبث بالمعلومات الشخصية، ويشير إلي قائمة طويلة من جرائم الاختراق للبيانات الشخصية، وما حدث في عام ٢٠١٨ بأنظمة فنادق الماريوت، واختراق البيانات في شبكات التواصل الاجتماعي، وفضيحة خصوصية بيانات كمبريدج أناليتيكا عام ٢٠١٨[٥٢]. وكذلك اختراق كلمات سر المستخدمين عبر أنظمة الذكاء الاصطناعي .

ومما هو جدير ذكره مخاطر تقنيات الذكاء الاصطناعي بخصوص تحيزه وعنصريته، لكونه يعتمد أساسًا على مجموعات البيانات التي يقوم عليها تعلم الآلة الذكية، فيمكن أن يحدث تحيز الذكاء الاصطناعي عن طريق استخدام مجموعات بيانات غير صحيحة أو معيبة او متحيزة من قبل الافراد الذين يقومون بالتحقق من صحة خوارزميات التعلم الالي، ولذا أوصى مجلس الشيوخ البريطاني في تقريره عن الآثار الاقتصادية والاجتماعية والأخلاقية بضرورة وجود فرق متعددة المراجعة البيانات، إضافة إلى تحري الدقة عند إعداد مجموعات البيانات التي يتدرب عليها خوارزميات الذكاء الاصطناعي[٥٣] .

وبالفعل وفي تطبيق عملي على ذلك ؛ قد بدأت ساحات المحاكم بالفعل النظر في قضايا تتعلق بتحيز الذكاء الاصطناعي ففي ٢١ فبراير ٢٠٢٣، ثم رفع دعوى قضائية جماعية ضد شركة Workday أمام محكمة المقاطعة الشمالية بكاليفورنيا ، بدعوى ان الشركة متورطة في تمييز غير قانوني على أساس العرق والعمر والإعاقة فيما يتعلق بأدوات الفرز التي تستخدم خوارزميات الذكاء الاصطناعي المتحيزة لفحص طلبات التوظيف المقدمة للشركة [٥٤].

([٥٢]) د. محمد سالم، تحديات إعمال الحق في الخصوصية في ظل التطور التكنولوجي، ورقة مقدمة للمؤتمر الدولي حول "تعديد الحق في الخصوصية الرقمية في سباق الذكاء الاصطناعي"، ٢٠٢٢، ص٤.

([٥٣]) د. مروة زين العابدين سعد ود. محمد الجندي ،المشكلات القانونية للذكاء الاصطناعي التوليدي(ChatGPT) ،المرجع السابق، ص٣٠٩.

([٥٤])Mobley v. Workday, Inc., N.D. Cal., No. ٢٣-cv-٠٠٧٧٠, complaint filed ٢١ February ٢٠٢٣. On February ٢١, ٢٠٢٣, the

وأمام هذه الاختراق للبيانات الشخصية، شمر المشرع عن ساعديه في العديد من الدول لمواجهة هذا الاختراق غير المشروع للخصوصية الرقمية، فمن حيث المشرع المصري، فقد خصص الفصل الأول من قانون مكافحة جرائم تقنية المعلومات رقم(١٧٥) لسنة ٢٠١٨، لجرائم الاعتداء على سلامة شبكات وأنظمة وتقنيات المعلومات. حيث جرَّم المشرع المصري الدخول غير المشروع والبقاء بدون وجه حق على البيانات الشخصية، المعالجة بالذكاء الاصطناعي، على غرار نظيره الفرنسي، والمشرع الإماراتي والمشرع الفلسطيني[٥٥]. ومن حيث الركن المادي لهذه الجريمة، فإنه وبحسب المادة(١٤) من القانون المصري سالف الذكر في الدخول بدون وجه حق على موقع أو حساب خاص، أو نظام معلوماتي محظور الدخول عليه.

ومتى ترتب على الدخول، بموجب هذه المادة سالفة الذكر، إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو

---

named plaintiff, an African American man over the age of ٤٠ who had a disability, tiled this lawsuit in the Northern District of California, Oakland Division, individually and on behalf of a class. The plaintiff sued human and financial management software vendor Workday, Inc («Workday») under Title VII of the Civil Rights Act of ١٩٦٤, the Civil Rights Act of ١٨٦٦ (٤٢ U.S.C. § ١٩٨١), the Age Discrimination in Employment Act of ١٩٦٧, and the ADA Amendments Act of ٢٠٠٨ («ADAAA). Represented by private counsel, the plaintiff sought class certification, injunctive relief, declaratory judgment, monetary relief and damages. The plaintiff sought class certification of applicants or former applicants who are African American, over the age of ٤٠, and or have à disability. The plaintiff argued that Workday provides companies with algorithm-based applicant screening software that unlawfully determines whether or not an applicant should be accepted or rejected based on individuals protected class characteristics of race, age, and disability. The case was assigned to Magistrate Judge Thomas S. Hixson. The case is ongoing.

مشار اليه لدي مرجع د. مروة زين العابدين سعد ود. محمد الجندي ،المشكلات القانونية للذكاء الاصطناعي التوليدي(ChatGPT) ،المرجع السابق، ص٣٠٨ وما بعدها .

(٥٥) ينظر : القرار بقانون رقم (١٠) لسنه ٢٠١٨ بشأن مكافحة الجرائم الالكترونية الفلسطيني .

الحساب الخاص، أو النظام المعلوماتي، فقد شدد المشرع العقوبة المفروضة على الدخول والبقاء غير المشروع[٥٦].

كذلك الحال، في دولة فلسطين حيث صدر قانون الجرائم الالكترونية رقم (١٠) لسنه ٢٠١٨ [٥٧]، وفي دولة الإمارات العربية المتحدة، حيث صدر القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات، ثم لاحقه المشرع الإماراتي بالمرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن جرائم تقنية المعلومات، وأخيراً، جري تعديل هذا القانون في عام ٢٠١٦، لمواكبة بعض التطورات التقنية، التي ظهرت كجرائم تقنية معلومات[٥٨]. حيث شمل هذا القانون الإماراتي ضمن الجرائم والعقوبات، جريمة التوصل، بغير وجه حق إلي موقع أو نظام معلوماتي بدخول الموقع، أو النظام، أو يتجاوز مدخل مصرح به، والتعدي على البيانات الشخصية، وإلغاء بيانات أو معلومات، أو حذفها، أو تدميرها، أو إفشائها، أو إتلافها، أو تغييرها، أو إعادة نشرها[٥٩].

وفي فرنسا، جرَّم المشرع الفرنسي فعل الدخول والبقاء في نظام المعالجة الإلكترونية للبيانات. حيث قضت الدائرة الجنائية بمحكمة النقض، بالمسئولية الجنائية عن فعل الدخول والبقاء بطريق الغش في نظام المعالجة الإلكترونية للبيانات، فضلاً عن سرقة هذه البيانات[٦٠]، حيث ورد النص على هذه الجرائم الجديدة في المواد من(٣٢٣-١ إلي ٣٢٣-٧) من التقنين العقابي الفرنسي، حيث تتعلق هذه الجرائم بالدخول، أو البقاء غير المشروع في كل، أو جزء من النظام المعلوماتي، وتعويق أداء نظام المعالجة الإلكترونية للبيانات، أو فعل الغش في أداء هذه المنظمة، أو كذلك فعل

---

(٥٦) ينظر: المادة (١٤) من قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ المصري.

(٥٧) ينظر : قانون الجرائم الالكترونية الفلسطيني رقم (١٠) لسنه ٢٠١٨ وتعديلاته .متاح علي موقع الإلكتروني:٨٣/https://maqam.najah.edu/legislation ٢٠٢٣/٧/٢م.

(٥٨) ينظر: القانون الاتحادي الاماراتي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات، المعدل بالمرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ في شأن جرائم تقنية المعلومات، وأخيراً، جري تعديل هذا القانون في عام ٢٠١٦.

(٥٩) د. سعيد على بحبوح النقبي، المحكمة الإلكترونية، المفهوم والتطبيق في تشريعات دولة الإمارات العربية المتحدة، الطبعة الأولي، دار النهضة العربية، ٢٠٢٠، ص ١١٨.

(٦٠) Crim. ٢٠ mars ٢٠١٥, JCP ٢٠١٥, n°٨٨٧, note Beaussonie, D. ٢٠١٥

إدخال، أو استخلاص، أو حيازة، أو نسخ، أو نقل، أو إزالة، أو تعديل البيانات التي يحويها هذا النظام بطريق الغش[٦١].

ومن الأمثلة على ذلك، ما قضت محكمة النقض الفرنسية، في حكم حديث لها، في جريمة الدخول غير المشروع، التي ارتكبها طالب بجامعة السوربون (باريس٢)، موهوب في مجال المعلوماتية، حيث استطاع التسلل إلي المنظومة المعلوماتية للجامعة وقام بتعديل نتيجة شقيقته المسجلة الكترونياً على موقع الجامعة وكذلك تقديرات صديق له، حيث قضت الدائرة الجنائية بمحكمة النقض أنه قد ارتكب بهذا الفعل الجريمة المنصوص عليها في المادة (٣٢٣-١) من التقنين العقابي، حيث تسلل إلي نظام للمعالجة الإلكترونية للبيانات، مع علمه بعدم جواز ذلك[٦٢].

الفرع الثاني

عرقلة سير نظام المعالجة الإلكترونية للبيانات

إن استخدام تقنيات الذكاء الاصطناعي في الاعتداء على البيانات الشخصية، ومن ثم خرق الخصوصية الرقمية، لا يقف عند حدود الدخول والبقاء في نظام المعالجة الإلكترونية، بل إن الاعتداء يمكن أن يقع من خلال عرقلة سير المعالجة الإلكترونية للبيانات بغرض التحكم والرقابة على هذه البيانات، ولعل هذه هي البداية المنطقية، حيث يتم التحكم في هذا النظام من خلال فك رموزه، بغرض فتح الباب للدخول عليه، ومن ثم، الاطلاع على البيانات الشخصية، ومن ثم، فقد عني المشرع بحماية الذكاء الاصطناعي ذاته بشأن دوره في معالجة البيانات الرقمية، حيث جرم كل سلوك من شأنه المساس بسير عملية المعالجة الإلكترونية للبيانات بطريق الذكاء الاصطناعي، ففي قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨، جرَّم المشرع المصري كل فعل من شأنه إيقاف شبكة معلوماتية عن العمل، أو تعطيلها، او الحد من كفاءة عملها، أو كذلك التشويش عليه، أو كذلك إعاقتها، أو اعتراض عملها، أو كذلك

(٦١) R. Boos. La lutte contre la cybercriminalité au regard de l'action des États, thèse de Lorraine, ٢٠١٦, p. ٦٥.

(٦٢) Cass. crim., ٩ mars ٢٠١٦, n° ١٤-٨٦٧٩٥, inédit. Cf. également Cass. crim., ١٢ juill. ٢٠١٦, n° ١٦-٨٢٤٥٥, inédit : RSC ٢٠١٦, p. ٥٤٠, obs. Francillon.

أجرى بدون وجه حق معالجة إلكترونية للبيانات الخاصة به، حيث فرض عقوبة الحبس مدة لا تقل عن ستة أشهر، والغرامة، التي لا تقل عن مائة ألف جنيه ولا تتجاوز خمسمائة ألف جنيه، أو بإحدى هاتين العقوبتين[٦٣].

كذلك الحال، فقد فرض المشرع الإماراتي، في المادة (٤) من القانون الاتحادي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات، عقوبة الحبس والغرامة ضد كل فعل من شأنه إعاقة أو تعطيل الدخول إلي الأجهزة أو البرامج المعلوماتية، بمعني أخر كل من أعاق أو عطل الوصول إلي الخدمة أو الدخول إلي الأجهزة أو البرامج أو مصادر البيانات أو المعلومات بأية وسيلة كانت عن طريق الشبكة المعلوماتية، أو احدي وسائل تقنية المعلومات[٦٤].

جرَّم المشرع الفرنسي فعل عرقلة أو تزوير سير نظام المعالجة الإلكترونية للبيانات (الركن المادي). ومن الممكن أن يتجسد هذا السلوك من خلال إدخال فيروس في نظام معلوماتي[٦٥]، أو ارسال رسائل الكترونية مزعجة[٦٦]. وهذه الجريمة عمدية. ومن حيث الجزاءات، فإن هذه الجنحة تستوجب عقوبة الحبس مدة خمسة أعوام والغرامة ١٥٠,٠٠٠ يورو. وتزيد العقوبة إلي الحبس مدة سبعة أعوام، والغرامة ٣٠٠,٠٠٠ يورو ضد نظام للمعالجة الإلكترونية للبيانات الشخصية، الذي يجري تطبيقه بطريق الدولة[٦٧].

الفرع الثالث

الإتجار في الأجهزة والبرامج الذكية، التي تستخدم في التعدي على البيانات

(٦٣) ينظر: المادة (٢١) من مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ المصري متاح على الموقع الإلكتروني: https://www.c.c.gov.eg. ٢/٧/٢٠٢٣.

(٦٤) ينظر: المادة (٥) من القانون الاتحادي الاماراتي رقم (٢) لسنة ٢٠٠٦ بشأن مكافحة جرائم تقنية المعلومات، متاح على الموقع الإلكتروني: https://www.wipo.int. ٢/٧/٢٠٢٣.

(٦٥) Cass. crim., ١٢ déc. ١٩٩٦, nº ٩٥-٨٢١٩٨: Bull. crim., nº ٤٦٥; RSC ١٩٩٨, p. ١٤٤, obs. Francillon.

(٦٦) CA Paris ١٨ déc. ٢٠٠١ : D. ٢٠٠٢, IR, p. ٩٤٠.

(٦٧) C. Ambroise-Castérot ; Droit pénal spécial et droit pénal des affaires, ٧ème éd., Gualino,٢٠١٩, p.٢٦٧.

عني المشرع في العديد من الدول بالوقوف على بذور استخدام الذكاء الاصطناعي، بسوء نية، في ارتكاب جرائم الاختراق المعلوماتي، فلم يقف عند حدود تجريم الدخول والبقاء في نظام المعالجة الإلكترونية بدون إذن من صاحب الشأن، وبدون عذر شرعي مرتبط بمصلحة عامة، بل خطي خطوة هامة، من خلال الاتجار بالبيع والشراء والاستيراد والتصدير للأجهزة الذكية، وبرامج الذكاء الاصطناعي لاستخدامها في الاعتداء على البيانات.

حظر المشرع المصري كل تعامل في الأجهزة والبرامج الذكية، التي يمكن استخدامها في التعدي على البيانات الشخصية، بفعل حيازة هذه الأجهزة، و احرازها، أو جلبها، أو بيعها، أو أتاح، أو صنع، أو انتج، أو استورد، أو صدَّر، أو تداول بأية صورة من صور التداول الأجهزة، او المعدات، أو الأدوات، أو كذلك البرامج المصممة أو مطورة، أو محورة، أو حتى أكواد المرور، أو شفرات الرموز، أو البيانات المماثلة، بدون الحصول على تصريح من الجهاز، أو مسوغ من الواقع، أو القانون[٦٨].

وفي فرنسا، جاء قانون ٢١ يونيه ٢٠٠٤ بشأن الثقة في الاقتصاد الرقمي بمادة جديدة، التي تعاقب على التجارة في كل ما يمكن استخدامه في التعدي على البيانات الشخصية. حيث تعاقب المادة (٣٢٣-٣-١) من قانون العقوبات الفرنسي المعدلة بالقانون رقم (٢٠١٣-١١٦٨) الصادر في ١٨ ديسمبر ٢٠١٣، على فعل استيراد، أو حيازة، أو عرض، أو التنازل، أو تقديم منظومة، أو جهاز، أو برنامج معلوماتي، أو

(٦٨) ينظر: المادة (٢٢) من مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ المصري متاح على الموقع الإلكتروني: https://www.c.c.gov.eg. ٢/٧/٢٠٢٣.

كل بيان جري تصميمه وتكييفه، بصورة خاصة، لارتكاب واحد، أو أكثر من الجرائم المنصوص عليها في المواد من(٣٢٣-١ إلي ٣٢٣-٣) [٦٩].

ومن رأي الباحث، أن النص، سواء في التشريع المصري، وكذلك الفرنسي، يعتريه نقص كبير، لعدة أسباب، نتناولها على النحو التالي :

- عدم تناول المشرع الفرض، الذي يمكن أن تستخدم معه هذه الأجهزة الذكية لأغراض مشروعة، كما أن من غير الممكن أن يلازم كل تعامل مع البرامج والأجهزة الذكية التعدي على الخصوصية الرقمية، خاصة وأن المشرع جرَّم التعامل معها بالبيع والشراء والاستيراد والتصدير، وكان حري به أن يجرم تصنيعها وابتكارها، ولكن أن يغض الطرف عن منشئ هذه الأجهزة والبرامج، ويلاحق من يستخدمها، فهذا يكشف عن قصور واضح.
- لم يبين النص على سبيل الحصر هذه الأجهزة والبرامج الذكية، كما لم يحيل في حصرها، وبيانها على ملحق فني، ولم يبين دور الخبير المعلوماتي في شأن رصد هذه الأجهزة والبرامج، مما يزيد الأمر تعقيداً في شأن اثبات هذه الجريمة.

المطلب الثالث

الحماية الإجرائية للحق في الخصوصية الرقمية

تمهيد وتقسيم: عني المشرع في العديد من الدول بكفالة الحماية الإجرائية للبيانات الشخصية، خاصة خلال مباشرة إجراءات الاستدلال والتحري، من جانب، والتحقيق،

([٦٩]) Article ٣٢٣-٣-١ Modifié par LOI n°٢٠١٣-١١٦٨ du ١٨ décembre ٢٠١٣, " Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles ٣٢٣-١ à ٣٢٣-٣ est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.", disponible sur le site, https://www.legifrance.gouv.fr. ١٣/٨/٢٠٢٣.

من جانب أخر. وذلك لصيانة الحق في الخصوصية الرقمية، وسوف نتناول الحماية الإجرائية للبيانات الشخصية على النحو التالي :

الفرع الأول : حماية البيانات خلال إجراءات الاستدلال والتحري.

الفرع الثاني : حماية البيانات خلال مرحلة التحقيق.

الفرع الأول

حماية البيانات خلال إجراءات التحري والاستدلال.

عني المشرع المصري بكفالة الحماية الإجرائية للبيانات الشخصية خلال مباشرة إجراءات الاستدلال، فلم يرخص لمأمور الضبط القضائي الدخول على البيانات الرقمية إلا بناءً على الأمر المسبب الصادر إليه من جهة التحقيق، كما ربط هذا الإجراء بغاية البحث عن الحقيقة، وقد أفرد المشرع المصري في المادة (٦) من قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨، الإجراءات التي يباشرها الضبط القضائي، خلال إجراءات الاستدلال والتحري، والتي، بحسب هذه المادة، تتمثل في الآتي :

١- ضبط أو سحب أو جمع أو التحفظ على البيانات أو المعلومات، أو أنظمة المعلومات، أو تتبعها في أي مكان أو نظام أو برنامج أو دعامة إلكترونية أو حاسب تكون موجودة فيه. ويتم تسليم أدلتها الرقمية للجهة مصدرة الآمر، على ألا يؤثر ذلك على استمرارية النظم وتقديم الخدمة إن كان لذلك مقتض.

٢- البحث والتفتيش والدخول والنفاذ إلي برامج الحاسب وقواعد البيانات وغيرها من الأجهزة والنظم المعلوماتية تحقيقاً لغرض الضبط.

٣- أن تأمر مقدم الخدمة بتسليم ما لديه من بيانات أو معلومات تتعلق بنظام معلوماتي أو جهاز تقني موجودة تحت سيطرته أو مخزنة لديه.

والجير بالذكر أن المشرع المصري أوجب أن يكون الأمر الصادر عن جهة التحقيق مسبباً، وهو ما يعني، بطبيعة الحال، إمكان الطعن بالاستئناف ضد الأوامر أمام المحكمة الجنائية المختصة منعقدة في غرفة المشورة[٧٠].

وفي فرنسا، وخلال إجراءات الاستدلال والتحري، فلم يسمح المشرع بالدخول على البيانات ومن ثم، تفتيش الحاسوب إلا بناءً على الأمر الصادر بذلك من قاض التحقيق، حيث يستطيع مأمور الضبط القضائي، بناءً على هذا الأمر، فض المراسلات، التي تتم بالطريق الإلكتروني عبر شبكات الإنترنت، وذلك في المواد من(١٠٠ إلي ١٠٠-٧) من قانون الإجراءات الجنائية الفرنسي[٧١].

ومن حيث المبدأ، يسمح تقنين الإجراءات الجنائية باستخدام العديد من الإجراءات الجديدة في مجال الجريمة المنظمة، والتي يجري تطبيقها من خلال الوكالة الوطنية لتقنيات التحقيقات الرقمية القضائية، فضلاً عن لجنة التوجيه لتقنيات التحقيق الرقمي القضائي، بموجب المرسوم رقم (٢٠١٧-٦١٤) الصادر في ٢٤ أبريل ٢٠١٧[٧٢]، ففي المقام الأول، وسع القانون الصادر في ٣ يونيه ٢٠١٦ من إجراءات

---

(٧٠) ينظر: المادة (٦) من مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ المصري متاح على الموقع الإلكتروني: https://www.c.c.gov.eg. ٢/٧/٢٠٢٣.

(٧١) Art. ١٠٠ de code de procédure pénale modifie par Loi n° ٩١-٦٤٦ du ١٠ juillet ١٩٩١, prévoit que," En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des télécommunications. Ces opérations sont effectuées sous son autorité et son contrôle.

La décision d'interception est écrite. Elle n'a pas de caractère juridictionnel et n'est susceptible d'aucun recours. ", disponible sur le site https://www.legifrance.gouv.fr. ١٥/٨/٢٠٢٣.

(٧٢) Décret n° ٢٠١٧-٦١٤ du ٢٤ avril ٢٠١٧ portant création d'un service à compétence nationale dénommé « Agence nationale des techniques d'enquêtes numériques judiciaires » et d'un comité d'orientation des techniques d'enquêtes numériques judiciaires", disponible sur le site, https://www.legifrance.gouv.fr ١٥/٨/٢٠٢٣.

الاستدلال[٧٣]، المنصوص عليها في المواد (٧٠٦-١٠١-١) وما يليها من تقنين الإجراءات الجنائية، بما يسمح بالاستحواذ على البيانات المحمولة في النظام المعلوماتي. ومن المتعين على قاضي الحريات والحبس، فضلاً عن قاضي التحقيق أن يصدر أمر بترخيص إجراءات الاستدلال الرقمي، خلال التحقيق بطريق الضبط القضائي[٧٤].

على هذا الحال، فقد أجاز المشرع الفرنسي[٧٥]، تفتيش الحاسوب متى اقتضي كشف الحقيقة، والتدليل على الجريمة، إجراء التفتيش وضبط الأشياء، أو البيانات الرقمية، ومن ثم، فإن التفتيش لم يعد قصر على محل إقامة الشخص المعني بإجراءات الضبط والتفتيش، ولكنه يمتد إلي البيانات والمعلومات الرقمية، المعلقة بالوقائع المجرَمة. ووفقاً للقواعد العامة، يستطيع مأمور الضبط القضائي الانتقال إلي كافة الأماكن، التي يمكن العثور فيها على الأموال، بغية ضبط هذه الأشياء والأموال[٧٦].

على أن المشرع الفرنسي لم يغفل مقتضي حماية البيانات الشخصية وما يعرف بالخصوصية الرقمية، حيث أوجب تسبيب الأمر الصادر باختراق البيانات الشخصية، بدون علم الشخص، المحمولة على حساب الماسينجر المادة(٧٠٦-٩٥-١) و(٧٠٦-٩٥-٢) من تقنين الإجراءات الجنائية، المعدلة بالقانون رقم (٢٠٢١-١٧٢٩)

(٧٣) LOI n° ٢٠١٦-٧٣١ du ٣ juin ٢٠١٦ renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, disponible sur le site https://www.legifrance.gouv.fr. ١٥/٨/٢٠٢٣.

(٧٤) O. Décima ; Du piratage informatique aux perquisitions et saisies numériques ?, AJ Pénal, Jull.Août ٢٠١٧, p.٣١٥.

(٧٥) Article ٥٦ Modifié par Loi n°٢٠٠١-١١٦٨ du ١١ décembre ٢٠٠١," Si la nature du crime est telle que la preuve en puisse être acquise par la saisie des papiers, documents ou autres objets en la possession des personnes qui paraissent avoir participé au crime ou détenir des pièces ou objets relatifs aux faits incriminés, l'officier de police judiciaire se transporte sans désemparer au domicile de ces derniers pour y procéder à une perquisition dont il dresse procès-verbal(…)", disponible sur le sit, https://www.legifrance.gouv.fr ١٥/٨/٢٠٢٣.

(٧٦) É. Verny ; Procédure pénale, ٦ème éd., Dalloz, ٢٠١٩, p.١١١

الصادر في ٢٢ ديسمبر ٢٠٢١[٧٧]، بينما وفيما يتعلق بالمراسلات القادمة، لم تقتضي المادة ١٠٠ من ذات التقنين تسبيب الأمر الصادر باعتراض البيانات الشخصية، إذ يكفي، على هذا النحو، وجود قرار كتابي لبيان هوية الرابط الخاصة بالدخول على البيانات الشخصية، على أن يتضمن هذا القرار بيان بالجريمة، التي صدر على أثرها قرار الدخول على البيانات الشخصية، وفض المراسلات عبر الاتصالات الإلكترونية. ويمتد زمن هذا التدبير أربعة أشهر قابلة للتجديد، فيما خلا وجود استثناءات في هذا الشأن.

وعلى أية حال، وفيما يتعلق بفض المراسلات عبر الاتصالات الإلكترونية، ولأسباب فنية غير جلية، فلم يعد من الممكن اختراق التبادلات، متى تمت من خلال منحني التطبيقات الخاصة بمنظومة الماسينجر، وهي المنظومة التي يجري تطبيقها اليوم بصورة واسعة. وفي عالم الاتصالات الإلكترونية، نجد أن الرسائل يمكن نقلها عبر

(٧٧) Article ٧٠٦-٩٥, Modifié par LOI n°٢٠٢١-١٧٢٩ du ٢٢ décembre ٢٠٢١, prévoit que : " Si les nécessités de l'enquête de flagrance ou de l'enquête préliminaire relative à l'une des infractions entrant dans le champ d'application des articles ٧٠٦-٧٣ et ٧٠٦-٧٣-١ l'exigent, le juge des libertés et de la détention du tribunal judiciaire peut, à la requête du procureur de la République, autoriser l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques selon les modalités prévues aux deuxième et dernier alinéas de l'article ١٠٠ ainsi qu'aux articles ١٠٠-١ et ١٠٠-٣ à ١٠٠-٧, pour une durée maximum d'un mois, renouvelable une fois dans les mêmes conditions de forme et de durée. Ces opérations sont faites sous le contrôle du juge des libertés et de la détention.

Les dispositions de l'article ١٠٠-٨ sont applicables aux interceptions ordonnées en application du présent article.

Pour l'application des dispositions des articles ١٠٠-٣ à ١٠٠-٥ et ١٠٠-٨, les attributions confiées au juge d'instruction ou à l'officier de police judiciaire commis par lui sont exercées par le procureur de la République ou l'officier de police judiciaire requis par ce magistrat.

Le juge des libertés et de la détention qui a autorisé l'interception est informé sans délai par le procureur de la République des actes accomplis en application de l'alinéa précédent, notamment des procès-verbaux dressés en exécution de son autorisation, par application des articles ١٠٠-٤ et ١٠٠-٥.", disponible sur le site, https://www.legifrance.gouv.fr. ١٥/٨/٢٠٢٣.

الهواتف المحمولة، كذلك من خلال استخدام تقنية الواتساب، والفيبر، فضلاً عن التطبيقات الأخرى، حيث يتم تعيين موضع الخادوم بصورة جوهرية في الولايات المتحدة الأمريكية، وهنا يتعين على البوليس أن يلتمس تجميد البيانات لدي السلطات الأمريكية، وأن يطلب تسليم هذه البيانات، من خلال اللجوء إلي طلب المساعدة الجنائية الدولية[٧٨].

أخيراً، إن الحاسوب يأخذ وصف المسكن، ليشمل الحاسوب الشخصي، على أن التفتيش في الحاسوب عن البيانات الرقمية لا يمكن أن يأخذ الوصف القانوني للتفتيش إلا إذا صدر إذن بالدخول على الحاسوب[٧٩]. ومن ناحية محكمة النقض الفرنسية، فإنه لا تقر بوصف الدخول على الخادوم على أثر عملية التفتيش المادي في مسكن الشخص المعني، بالتفتيش. وتفسر الدائرة الجنائية بمحكمة النقض الفرنسية [٨٠] هذا الموقف بقولها، بأن الارتباط يتم بطريق المحققين من خلال المنظومة المعلوماتية الخاصة بهم. باستخدام وسيلة الكود الخاص بمناسبة إجراءات التفتيش الرقمي، الصادر به إذن من قاضي الحريات والحبس. ومن الواضح، أن الأمر يتعلق بإجراءات استدلال وليس بإجراء تفتيش إلكتروني خاص، ومشمول بالإذن المسبق من قبل قاضي الحريات والحبس[٨١].

صفوة القول، لقد عني المشرع المصري ونظيره الفرنسي، حماية البيانات الشخصية الرقمية خلال إجراءات الاستدلال والتحري من جانبين، فمن جانب، أوجب صدور أمر مسبب من جهة التحقيق بالدخول على البيانات الشخصية وتفتيشها، ومن جانب أخر، ربط هذا الإجراء بغاية البحث عن الحقيقة.

---

(٧٨) O. Violeau ; Les techniques d'investigations numériques : entre insécurité juridique et limites pratiques, AJPénal Juill. Aout ٢٠١٧, p.٣٢٦

(٧٩) ينظر في هذا المعني: د. محمد جمال رجب خميس الحاوي، الحماية الجنائية للاتصالات الشخصية في العصر الرقمي دراسة مقارنة ، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق – جامعة حلوان ، ٢٠٢١، ص ٢٨٢ وما بعدها

(٨٠) Crim. ٦ nov. ٢٠١٣, n°١٢-٨٧. ١٣٠, D. ٢٠١٣. ٢٨٢٦, note P. Hennion-Jacquet

(٨١) O. Décima, art. préc., p. ٣١٧

الفرع الثاني

حماية البيانات خلال إجراءات التحقيق

عني المشرع في بعض الدول العربية والدول الغربية، وعلى وجه الخصوص، فرنسا، خاصة فيما يتعلق بإجراءات التحقيق عن بعد عبر الوسائط الالكترونية الذكية ، إذ وخلال مباشرة هذا التحقيق، يتم بطبيعة الحال، تداول بيانات التحقيق ومعلوماته، هذا ما قد يؤثر على هذه المعلومات، وخصوصيتها، وسرية بعضها، في حالة تعرضها للاختراق، أو الإتلاف[٨٢].

ومن هنا، فإننا نشدد على ضرورة حماية البيانات والمعلومات الخاصة بالتحقيق، إذ أن اختراقها والتلاعب بعا، وإتلافها يعد أكبر مسمار في نعش هذه التقنية، لما في ذلك من ضياع للعدالة، وإهدار للحقوق، إذ ما أيسر أن يفلت الجاني من العقاب، إذا ما تم اختراق المعلومات، والبيانات الخاصة بالقضية، بما يستحيل معه الوصول إلي الحقيقة، ومن ثم، فلا يجب البدء في تطبيق إجراءات التقاضي عن بعد ما لم يكن هناك منظومة إلكترونية آمنه، بما يتحقق معها مقتضيات السرية.

ومن حيث الواقع العملي، نجد أن المشرع الفلسطيني، وفي سبيل حماية البيانات الشخصية خلال إجراءات التحقيق، حدد نطاق استخدام تقنية الاتصال عن بعد عبر الوسائط الالكترونية الذكية ، من حيث الجرائم، التي يري ملائمة ذلك بالنظر إليها. فعلي سبيل المثال، فقد أدخل الفقرتين(٥ و٦) على المادة (٢٢٩) من القانون الأصلي بشأن إدخال تقنية الاتصال الحديثة في إجراء التحقيق، بموجب المادة(١٤) من هذا القانون[٨٣]، من القرار بقانون رقم (٧) لسنة ٢٠٢٢ بشأن تعديل قانون

([٨٢]) محمد سويلم، التحقيق الجنائي عبر الوسائل الإلكترونية، دراسة مقارنة، الإسكندرية، دار المطبوعات الجامعية، ٢٠٢٠، ص ٩٩.

([٨٣]) تعدل المادة (٢٢٩) من القانون الأصلي وذلك بإضافة فقرتين جديدتين تحملان الرقم (٥ و٦) على النحو الآتي: ٥.) يكون استخدام التقنيات والوسائل التكنولوجية الحديثة في مجال الصوت والصورة وجوبياً من قبل النيابة العامة ومن قبل المحكمة حال سماع أقوال المجني عليه في الجرائم الواقعة على العرض، وكذلك في حالة سماع الشاهد الذي لم يتم الخامسة عشرة من عمره، إلا إذا تعذر ذلك لأي سبب كان، ويكون استخدامها جوازياً

الاجراءات الجزائية رقم (٣) لسنة ٢٠٠١ وتعديلاته، وان كان تم الغاء هذا القانون بعد ذلك.

كما قيد المشرع الأردني وكذلك الإماراتي، استخدام تقنيات الاتصال عن بعد عبر الوسائط الالكترونية الذكية لا يتجاوز، في الإجراءات الجنائية، حدود سماع الشهود والخبراء، وفقاً للمادة العاشرة من الاتفاقية الأوروبية الجدية للمساعدة القضائية، يقتصر استخدام هذه التقنية في مجال سماع شهادة الشهود وإفادات الخبراء، حيث يمكن للسلطات القضائية لاحدي دول الاتحاد الأوروبي، طلب سماع شخص يتواجد على إقليم دولة أخرى طرف في الاتفاقية، متى استحال مثول هذا الشخص بنفسه أمامها[٨٤]. كذلك الحال، فقد حدد المشرع الإماراتي الأشخاص، اللذين يمكن للجهات المختصة استخدام تقنية الاتصال عن بعد معهم، بعد أن يقدم طلب إلي رئيس المحكمة أو النائب العام أو رئيس الجهة المكلفة باستقصاء الجرائم وجمع الأدلة، أو من يتم تفويضه منهم، لمباشرة إجراء، أو أكثر من إجراءات المحاكمة عن بعد[٨٥].

وهذا ومن الأهمية بمكان الإشارة الي المبادئ التي تم إقرارها في الميثاق الأخلاقي الأوروبي بشأن استخدام تقنيات الذكاء الاصطناعي في الأنظمة والبيئات القضائية، وهي احترام الحقوق الأساسية لضمان عمل تقنية الذكاء الاصطناعي بما يتماشى مع الحقوق الأساسية للإنسان، ثم مبدأ المساواة وعدم التميز. وبخصوص إجراءات سير الدعاوى أو المحاكمات تم إقرار مبدأ الجودة وأمن المعلومات إضافة إلى الشفافية

في جميع الحالات الأخرى : ٦.) تخضع الأدوات المستخدمة في التقنية أو الوسيلة التكنولوجية الحديثة بما في ذلك الأشرطة والأقراص المدمجة لإجراءات الحفظ والحماية، للحفاظ على سريتها وخصوصية الشاهد أو المتهم.

(٨٤) صفوان محمد شديفات، التحقيق والمحاكمة الجزائية عن بعد عبر تقنية ال Videoconference، مجلة دراسات، علوم الشريعة والقانون، المجلد ٤٢، العدد١، ٢٠١٥، ص ١٣.

(٨٥) ينظر: المادة (٢) من القانون رقم (٥) لسنة ٢٠١٧ في شأن استخدام تقنية الاتصال عن بعد في الإجراءات الجنائية الاماراتي.

والحياد والعدالة، وأخيرًا مبدأ « تحت سيطرة المستخدم " أي يجب أن يكون المستخدم مطلعا ومتحكما في الخيارات التي يقترحها الذكاء الاصطناعي "[٨٦].

خاتمة

برغم أن الغالبية العظمي من الدول العربية عنيت بوضع منظومة إلكترونية لحماية البيانات الشخصية، بالإحالة على الدور الذي يلعبه الذكاء الاصطناعي في حماية البيانات الشخصية وتلك مسألة فنية لا يد للمشرع فيها سوي في حدود وضع النصوص، التي من شأنها حماية البيانات الشخصية ذاتها، من جانب، وحماية الذكاء الاصطناعي ذاته من مخاطره بمنع استيراده وتداوله بغرض اختراق المراسلات الشخصية الإلكترونية والدخول على البيانات والبقاء بدون وجه حق، أو مقتضي قانوني، بالقياس على القوانين الغربية، التي عنيت بالقيام بهذا الدور، بحكم ما تمتعت به من الريادة في هذا المجال، إلا أنه، وبخلاف الحال في الاتحاد الأوروبي، والدور الذي اضطلع به مجلس أوروبا، من خلال التوجيهات الأوروبية التي صدرت بشأن حماية البيانات الشخصية، ومن ثم الخصوصية الرقمية، فلا يوجد في الدول العربية حماية قانونية تتجاوز حدود الدولة العربية الواحدة.

ومن ناحية أخرى، لا توجد حماية استباقية للخصوصية الرقمية، حيث يظل المشرع في البلدان العربية مكتوف الأيدي إلي حين ظهور مسلك من شأنه المساس بالخصوصية الرقمية حتى يسارع في وضع العقوبات الجنائية. كما لا يزال التوازن مفقود بين مقتضي حماية البيانات الشخصية، من جانب، والحق في حق الحصول على المعلومة في ظل استخدام تقنيات الذكاء الاصطناعي من جانب أخر. وقد خلصت الدراسة الي مجموعة من النتائج والتوصيات ، وذلك علي النحو التالي:

أولاً: النتائج:

([٨٦])Council of Europe, European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems (adopted on ٣ December ٢٠٢٠) https://www.europarl.europa.eu/emsdata/١٩٦٢٠٥/COUNCIL%٢٠ OF EUROPE%٢٠ -%٢٠ European%٢٠ Ethical %٢٠Charter%٢٠ on%٢٠ the%٢٠ use %٢٠of A١٪٢٠ in%٢٠ judicial%٢٠٪٢٠ systems. pir accessed ٢٦ April ٢٠٢٣>

بداية، ومن حيث النتائج، التي خرجنا بها من هذا البحث، فإنها تتمثل في الآتي :

١- عني المشرع في مصر والإمارات العربية المتحدة تجريم كافة التصرفات، التي من شأنها التعدي على البيانات الشخصية، ومن ثم الخصوصية الرقمية، على غرار المشرع الفرنسي، من خلال تجرم الدخول والبقاء في البيانات بدون إذن من صاحب هذه البيانات، والبقاء فيها.

٢- التوسع في الملاحقة بالتجريم لكافة التصرفات، التي يمكن أن تمس الخصوصية الرقمية، سواء كان ذلك بصورة مباشرة، أو غير مباشرة، من خلال شراء، أو استيراد، أو كافة صور التعامل مع الأجهزة والبرمجيات الذكية التي تستخدم في المعالجة الإلكترونية للبيانات.

٣ – عدم وجود مواجهة تعاونية بين الدول العربية فعالة لتبادل المعلومات والخبرات في مواجهة جرائم التعدي على الخصوصية الرقمية، بخلاف الحال، في الاتحاد الأوروبي، حيث تسمو التوجيهات الأوروبية القوانين الداخلية لدول الاتحاد الأوروبي.

٤ – عدم تمكين منظمات المجتمع المدني من القيام بدورها في تحقيق الحماية للخصوصية الرقمية، برغم الدور الهام، الذي يمكن أن تضطلع به في هذا المجال، خاصة إذا ما تحقق التواصل بينها وبين جمعيات حماية الخصوصية الرقمية في الدول الغربية لتبادل الخبرات.

٥ – قصر الحماية الإجرائية للبيانات الشخصية على مقتضي صدور أمر مسبب من جهة التحقيق للضبط القضائي بالدخول على البيانات الشخصية وتفتيش الحاسوب، وهذا لا يكفي، خاصة مع عدم وجود إدارة مستقلة يمكن للشخص المعني اللجوء إليها بالشكوى عن وجود تعدي على خصوصيته الرقمية خلال إجراءات الاستدلال والتحقيق للقيام بدورها في بحث وتحقيق ادعائه.

٦- وفقاً للقواعد العامة ، لاتزال المسئولية الجنائية تتوزع بين مستخدم تقنيات الذكاء الاصطناعي ومنشئها ومبرمجها، مع الأخذ في الاعتبار، بعدم إقرار الشخصية القانونية للذكاء الاصطناعي، وعليه لا يجوز ملاحقة تقنيات الذكاء الاصطناعي في حال اتخذ التصرف غير مشروع بانتهاك الخصوصية منفرداً ومن تلقاء ذاته.

ثانياً: التوصيات:

هناك مجموعة من التوصيات، التي نخرج بها في هذا البحث، يمكن تناولها على النحو التالي :

١- ضرورة السعي نحو تحقيق التعاون بين الدول العربية الفعال، بعيداً عن الطريق التقليدي، الذي يتمثل في الاتفاقيات الثنائية، أو متعددة الأطراف، من خلال إنشاء منظمة عربية تضطلع بهذا الدور، بصورة موضوعية ومجردة.

٢- ضرورة السعي نحو اتفاقية عالمية ملزمة بشأن حماية البيانات والمعلومات في المجال الرقمي، وبخاصة من مخاطر تقنيات الذكاء الاصطناعي.

٣- تمكين منظمات المجتمع المدني في القيام بدورها في هذا الشأن، خاصة بحكم قربها من الواقع العملي، وقدرتها على التحرك بصورة أكثر مرونة وفعالية من الضبط القضائي، بما يمكن أن يحقق غاية الحماية الاستباقية.

٤- المزيد من الدعم للحماية الإجرائية للبيانات، بحيث عدم قصرها على مجرد صدور أمر من جهات التحقيق للضبط القضائي بالسير في الإجراءات والدخول على البيانات الشخصية والرقمية وتفتيش الحاسوب.

٥- تزويد إدارة الضبط القضائي برصد كل تصرف يمكن أن ينطوي على المساس بالبيانات الشخصية، مما يدخل في الوصف الجنائي للشروع.

٦- ينبغي على الشركات والمؤسسات العاملة في مجال الذكاء الاصطناعي والحكومات والمستخدمين الامتثال للمعايير الأخلاقية والاجتماعية والالتزام بالقوانين ومراعاة حقوق الأفراد والخصوصية.

٧- التأكد من توافر خبراء مختصين في تقنيات الذكاء الاصطناعي والقانون لتحليل الأدلة وتقديم الإفادات اللازمة.

٨- ينبغي على الحكومات العمل على تحديث التشريعات والقوانين بشكل دوري لمواكبة التطور التقني والحفاظ على المساءلة القانونية والعدالة في استخدام التكنولوجيا الذكية.

٩- يجب أن يتم معالجة التوازن بين الخصوصية الرقمية والذكاء الاصطناعي بعناية بحيث يمكن استغلال فوائد التكنولوجيا الحديثة دون المساس بحقوق وحماية الأفراد؛ وهذا يتطلب تعاونا بين القطاع العام والقطاع الخاص والمجتمع المدني لتطوير إطار قوي ومستدام يحقق التوازن المطلوب.

١٠- يتعين على المستخدمين أنفسهم أن يكونوا واعين لمخاطر الخصوصية ويتخذوا التدابير اللازمة لحماية بياناتهم الشخصية مثل استخدام كلمات مرور قوية وتفعيل الحماية الثنائية للحسابات وتجنب مشاركة المعلومات الحساسة عبر وسائل غير آمنة.

١١- نوصي الدول على التكاتف لوضع تشريع دولي ينظم المسئوليّة الجنائية والمدنية للأضرار او الجرائم الناجمة من تقنيات الذكاء الاصطناعي على غرار اتفاقية الاوربية بودابست لمكافحة الجرائم الالكترونية "المعلوماتية "، وسن قوانين داخلية تتلاءم وتتماشي مع التشريعات الدولية، مع تشكيل لجنة من ذوي الخبرة والاختصاص تتولى متابعة انسجام هذا القانون مع التطورات الحاصلة، وتقديم المقترحات بتعديله إلى الجهات المختصة.

١٢- نوصي بالاعتراف بالشخصية القانونية لتقنيات الذكاء الاصطناعي بشكل واضح وصريح، كما اعترف المشرع بالشخص المعنوي، ولكن بهيكلية تختلف عن الشخص المعنوي، مما يكسبها بعض من الحقوق ويفرض عليها بعض من الالتزامات، وذلك شريطة تمتعها بالاستقلالية والوعي في اتخاذ القرار محل المسائلة الجنائية، وان تفرض تلك المسئولية بالتدريج على حسب التطور الحاصل مع تلك تقنيات الذكاء الاصطناعي.

١٣- نوصي بوضع تصور يسمح بإمكانية تطبيق قواعد المسئوليّة الجنائية على كل أطراف مرتكبي جرائم تقنية الذكاء الاصطناعي، والمنتج أو المبرمج، والمستخدم.

١٤- نوصي بوضع عقوبات تناسب مع جرائم تقنيات الذكاء الاصطناعي، كما تم مع الجرائم المرتكبة باسم ولمصلحة الشخص المعنوي.

قائمة المراجع

أولاً.- المراجع العربية

- **مراجع عامة:**

أحمد عبد العظيم علي، ثورة الذكاء الاصطناعي وأثره على مهنتي المحاسبة والمراجعة، الدار العالمية للنشر والتوزيع، مصر، ٢٠٢١.

د. أحمد محمد براك، إشكالية المسؤولية الجزائية لتقنيات الذكاء الاصطناعي، مركز البحوث القانونية– أربيل– العراق ، الطبعة الأولي، ٢٠٢٣.

د. سعيد على بحبوح النقبي، المحكمة الإلكترونية، المفهوم والتطبيق في تشريعات دولة الإمارات العربية المتحدة، الطبعة الأولي، دار النهضة العربية، ٢٠٢٠.

د. سهام النويهي، المنطق الغانم: علم جديد لتقنية المستقبل المكتبة الأكاديمية، القاهرة ،٢٠٠١.

د. صلاح الفضلي، آلية عمل العقل عند الإنسان، دار عصير الكتب للنشر والتوزيع، القاهرة ،٢٠١٩.

فريد–ه–كيث، الخصوصية في صدر المعلومات، مركز الأهرام للترجمة والنشر، القاهرة، ١٩٩٩.

د. محمد سويلم، التحقيق الجنائي عبر الوسائل الإلكترونية، دراسة مقارنة، الإسكندرية، دار المطبوعات الجامعية، ٢٠٢٠.

د. ياسين سعد غالب، أساسيات نظم المعلومات الإدارية وتكنولوجيا المعلومات، ط١، دار المناهج للنشر والتوزيع، الاردن ،٢٠١١.

- **الرسائل العلمية وأبحاث ومقالات منشورة في الدوريات:**

د. أيمن مصطفي أحمد البقلي، و د. طارق جمعة السيد راشد، نحو نظام قانوني للمسئولية المدنية الناجمة عن حوادث المركبات ذاتية القيادة (أساس المسئولية– والتأمين منها)، مجلة البحوث الفقهية والقانونية، تصدر عن كلية الشريعة والقانون بدمنهور، العدد الحادي والأربعين، ٢٠٢٣.

بن قارة مصطفي عائشة، الحق في الخصوصية المعلوماتية بين تحديات التقنية وواقع الحماية، مجلة البحوث القانونية والسياسية، العدد السادس، يونيه ٢٠٠٦.

د. رؤي سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية (دراسة مقارنة)، مجلة كلية الدراسات الإسلامية والعربية للبنات، الجزء الأول، العدد السادس، ٢٠٢١.

د. صفوان محمد شديفات، التحقيق والمحاكمة الجزائية عن بعد عبر تقنية ال Videoconference، مجلة دراسات، علوم الشريعة والقانون، المجلد ٤٢، العدد١، ٢٠١٥.

د. عماد الدين بركات، و د. حورية طيبي، الحماية الجنائية للحق في الخصوصية المعلوماتية، مجلة البحوث في الحقوق والعلوم السياسية، المجلد ٧ العدد ١/ السنة ٢٠٢١.

د. محمد جمال رجب خميس الحاوي، الحماية الجنائية للاتصالات الشخصية في العصر الرقمي دراسة مقارنة ، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق – جامعة حلوان ، ٢٠٢١.

د. محمد الطراونة، تحديات إعمال الحق في الخصوصية، في ظل التطور التكنولوجي، ورقة عمل مقدمة إلي المؤتمر الدولي حول تعزيز الحق في الخصوصية، في سياق الذكاء الاصطناعي، المنظمة العربية لحقوق الإنسان، اللجنة العليا الدائمة لحقوق الإنسان، الأمانة العامة، ٢٠٢٢، ص ٨، متاح على الموقع الإلكتروني : https://www.almasryalyoum.com

د . محمد سالم، تحديات إعمال الحق في الخصوصية في ظل التطور التكنولوجي، ورقة مقدمة للمؤتمر الدولي حول "تعديد الحق في الخصوصية الرقمية في سباق الذكاء الاصطناعي"، ٢٠٢٢.

د. مروة زين العابدين سعد ود. محمد الجندي ،المشكلات القانونية للذكاء الاصطناعي التوليدي(ChatGPT) ، مجلة القانون والتكنولوجيا ، المجلد ٣،العدد١،ابريل ٢٠٢٣.

د. همام القوصي، إشكالية الشخص المسؤول عن تشغيل الروبوت (تأثير نظرية النائب الإنساني عن جدوي القانون في المستقبل) ، ٢٠١٨، بحث منشور في مجلة الأبحاث القانونية المعمقة، العدد ٢٥.

يونس عرب، دور حماية الخصوصية في تشجيع الادماج بالمجتمع الرقمي، ورقة مقدمة في ندوة نادي أخلاق المعلومات العربي، ١٧-١٨ أكتوبر ٢٠٠٢، عمان، الأردن.

د. يسرى عبدالله عبد الباري عبد المطلب ، الحماية المدنية للخصوصية المعلوماتية (دراسة مقارنة)، رسالة مقدمة لنيل درجة الدكتوراه في الحقوق- جامعة عين شمس ،٢٠١٦.

ثانياً.- المراجع الأجنبية

- **المراجع الفرنسية:**

Ouvrages généraux :

Ambroise-Castérot (C.) ; Droit pénal spécial et droit pénal des affaires, ٧ème éd., Gualino,٢٠١٩.

Dechenaud (D.), Introduction, Le droit à l'oubli numérique, ٢٠١٥.

Grybaum (L.) et autres, Droit des activités numériques, ١ème éd., Dalloz, ٢٠١٤.

Ricardo (C.) : Logique pour l'informatique et pour l'intelligence artificielle, Hermes Sciences Publication, Paris, France, .٢٠١١

Rivero (J.), Libertés publiques, Montchrestien, ١٩٨٩.

Verny (É.) ; Procédure pénale, ٦ème éd., Dalloz, ٢٠١٩.

Ouvrages spéciaux :

Anne BOULANGE, Carole JAGGIE, "Ethique, responsabilité et statut juridique du robot compagnon : revue et perspectives", IC٢A : ١٣. Voir : https://hal.archives-ouvertes.fr/cel.

Boizard (M.) ; Le droit a l'oubli ; Master ٢٠١٥.

Boos (R.). La lutte contre la cybercriminalité au regard de l'action des États, thèse de Lorraine, ٢٠١٦.

Chaltiel (F.), Internet et le droit à l'oubli en devenir : dialogue entre Le juge européen et le juge administratif, Petites Affiches, n°١٤٩, ٢٧ juillet ٢٠١٧.

CASSART (A.) et HENROTTE (J.-F.), Droit à l'oubli : une réponse à l'hypermnésie numérique «, *Droits de l'homme numérique*, ٥٦ème conférence de l'IUA, ١er novembre ٢٠١٢, disponible sur www.uianet.org

DE VIGAN (D.), Le droit a l'oubli numérique au sein de l'Union européenne ; conséquences actuelles, lacunes et perspectives, Master ULB, ٢٠١٥.

HARIVEL (J.) ; Libertés publiques, Libertés individuelles, risqué et Enjeux de la sociétés numériques, thèse Sorbonne, ٢٠١٨.

Libin (L.) ; Droit a l'oubli numérique- Quel paramètre territorial ? Master de droit des affaires ٢٠١٨.

Violeau (O.) ; Les techniques d'investigations numériques : entre insécurité juridique et limites pratiques, AJPénal Juill. Aout ٢٠١٧.

- **المراجع الإنجليزية:**

Javier A. Perez, Fan D., Daniele R. and Yang G.-Z., Artificial intelligence, and Robotics UK RAS NETWORK UKRAS. ORG, centers for Doctoral training and partner University, ٢٠١٨.

Barr (A.), and Feigenbaum (E.-A.): The handbook of Artificial Intelligence, Kaufmann William Inc, New York, USA, ١٩٨٠.

Handler (J.); Avoiding Another AI winter research gate, April ٢٠٠٨.

Ian Goodfellow, Yoshua Bengio & Aaron Courville, Deep Learning, www.deepleaningbook.org.

Minsky (M.): Steps toward Artificial Intelligence, Proceedings of the IRE, USA, ١٩٦١.

OECDM: Directorate for Education and skills, Education policy Committee, ٢٤٠ ct., ٢٠١٨.

Rich (E.); Artificial Intelligence and the Humanities, Paradigm Press, ١٩٨٥.