"Criminal Legislation Related to the Protection of Artificial Intelligence Data: A Comparative Study"

التشريعات الجنائية المتعلقة بحماية بيانات الذكاء الاصطناعي "دراسة مقارنة"

إعداد

د/ أسامة سيد اللبان

أستاذ القانون الجنائي المساعد

بقسم الحقوق - كلية الدراسات الإنسانية والإدارية
كليات عنيزة الأهلية – المملكة العربية السعودية

المجلد الثاني -العدد السادس – سبتمبر ٢٠٢٤
ISSN-Print: 2812-6114 ISSN-Online: 2812-6122

موقع المجلة على بنك المعرفة المصري

https://aiis.journals.ekb.eg/contacts?lang=ar

الملخص:

التطور المذهل في برامج وتطبيقات الذكاء الاصطناعي والزيادة المضطردة في استخدام أدواته وتطبيقاته التي دائما تكون مُحَمَّلة ببيانات كثيرة شخصية وغير شخصية وما يعترى ذلك الاستخدام من مخاوف تتعلق بإساءته لاسيما وأن البيانات الشخصية – علي وجه الخصوص – تتعلق بحقوق وحريات الأشخاص ومن ثم فإن استخدامها لابد وأن يكون بضوابط محددة ، وهو الأمر الذي اعتنت به غالبية التشريعات العربية والعالمية في أنظمتها المتعددة إذ قامت بتعريف تلك البيانات مع تحديد أنماطها المختلفة ، ثم تطرقت إلي ضوابط استخدامها وما يجب أن يكون بشأن شرعية ذلك الاستخدام ، إضافة إلي تجريم أي استخدام يغاير ذلك الاستخدام الشخصي .

ولأهمية ذلك الموضوع وحيويته كان الدافع الرئيس إلي الكتابة فيه في محاولة لإبراز أهم ملامح التشريعات الجنائية العربية والأجنبية المتعلقة بحماية البيانات الخاصة بتطبيقات الذكاء الاصطناعي المنتشرة والمتوقع تقدمها وانتشارها خلال الفترة المقبلة أكثر وأكثر في مختلف النواحي والمجالات -لحماية الإنسان من أي تعسف في استخدام بيانات الخاصة بتطبيقات الذكاء الاصطناعي المتعددة.

الكلمات المفتاحية: التشريعات الجنائية – البيانات الشخصية – تطبيقات الذكاء الاصطناعي – اللائحة الأوربية لحماية البيانات الشخصية ٢٠١٨.

Abstract:

The remarkable development in artificial intelligence (AI) programs and applications, combined with the increasing use of its tools and applications—which are often loaded with extensive personal and non-personal data—raises concerns about potential misuse. This is particularly critical as personal data relates to individuals' rights and freedoms, necessitating strict regulations on its use. Most Arab and international legislations have addressed this issue by defining such data, specifying its various types, and establishing

rules for its use, including the legality of that use and criminalizing any misuse beyond personal applications.

Given the importance and urgency of this topic, it serves as a primary motivation to write about it. The aim is to highlight the key features of both Arab and foreign criminal legislations concerning the protection of data related to AI applications. With the expected continued advancement and proliferation of these applications in various fields, protecting individuals from any misuse of data is crucial.

Keywords: criminal legislations – personal data – artificial intelligence applications – European General Data Protection Regulation (GDPR) 2018

مقدمة:

الذكاء الاصطناعي وليد الثورة المعلوماتية، ولديه قدرة عظيمة على تحليل البيانات وإنهاء أي بحث في شتى المجالات بسرعة قصوى من شأنها إرشاد المهتمين وتمكينهم من وضع استراتيجيات تختلف باختلاف طبيعة الموضوع الذي يبحثه الذكاء الاصطناعي، لأنها تتميّز بالدّقة والشمولية بالإضافة إلى استنتاجه تصوراً شاملاً بشكل استباقي للنتائج الأكثر احتمالا، غير أن ذلك يتوقف على ما تحتويه قاعدة البيانات من وثائق ومستندات تمّ تزويده بها.

موضوع البحث:

وبناء علي ما سبق فإن التطور المذهل في برامج وتطبيقات الذكاء الاصطناعي والزيادة المضطردة في استخدام أدواته وتطبيقاته التي تكون دائما مُحَمَّلة ببيانات كثيرة شخصية وغير شخصية وما يعترى ذلك الاستخدام من مخاوف تتعلق بإساءته لاسيما وأن البيانات الشخصية – علي وجه الخصوص – تتعلق بحقوق وحريات الأشخاص خاصة إذا علمنا السرعة الفائقة

والقدرة اللانهائية في تحليله للبيانات، وهو الأمر الذي اعتنت به غالبية التشريعات العربية والعالمية في أنظمتها المتعددة إذ قامت بتعريف تلك البيانات مع تحديد أنماطها المختلفة ، ثم تطرقت إلي ضوابط استخدامها وما يجب أن يكون بشأن شرعية ذلك الاستخدام ، إضافة إلي تجريم أي استخدام يغاير ذلك الاستخدام الشخصي.

أهمية الموضوع:

يعكس الذكاء الاصطناعي تحولًا ثوريًا في عالم التكنولوجيا، وهو يشكل تحديًا وفرصة لنا جميعًا، سواء كنا مجتمعًا أو دولة، للاستعداد والتكيف مع هذا التطور الرائع. ومن المهم أن ندرك أن الذكاء الاصطناعي ليس مجرد أداة لتقليل واستبدال الوظائف، بل هو نموذج جديد للتفكير والإبداع. ويمكن للذكاء الاصطناعي أن يؤثر بشكل كبير في مختلف المجالات التي تدخل فيها بطرق عديدة ومتنوعة، ولذا تزايد الإقبال العالمي على تقنيات الذكاء الاصطناعي لما تقدمه تلك التقنيات من خدمات ومنتجات يَسَّرَت حياة الناس، إلا أنها لا تخلو من العديد من السلبيات ومن أبرزها إمكانية انتهاك البيانات الخاصة أو الشخصية.

وهو ما أدي إلي تدخل المشرع الجنائي لتحديد الاستخدامات الخاصة بالذكاء الاصطناعي التي تعتبر من قبيل الأفعال التي تدخل في إطار السلوك الإجرامي الذي يجب الوقوف في مواجهته حتى لا يؤدى إلى الإضرار بالآخرين خاصة وأن تطبيقات الذكاء الاصطناعي تم تزويدها بملايين البيانات الشخصية وغير الشخصية لتحليلها واستنتاج الكثير من النقاط الرئيسية في المجال الذي يبحث فيه الذكاء الاصطناعي، وبالتالي فقد يكون هذا الاعتداء على تلك البيانات فيه اعتداء على حريات شخصية أو براءات لأشخاص أو غير ذلك من الجرائم المتوقعة.

أسباب اختيار الموضوع:

انتشار تطبيقات الذكاء الاصطناعي وتطور أنواعها وأنماطها بل وتطورها اللانهائي هو الدافع الرئيسي لهذا البحث في محاولة لإبراز أهم الجرائم المترتبة على اختراق البيانات الخاصة بتطبيقات الذكاء الاصطناعي وانتهاك حرمات الأشخاص الفردية أو الاستيلاء على الفكر العلمي للبعض الآخر، ذلك أن الحماية الجنائية متي توافرت غالباً تكون سببا في درء الكثير من

الاعتداءات خاصة إذا كان ذلك الاعتداء من قبل أفراد لا يتراجعوا إلا من خلال نصوص قانونية جنائية رادعة.

المشكلات التي يثيرها البحث:

يحاول البحث الإجابة على التساؤلات التالية:

- ما هو الذكاء الاصطناعي؟ وماهي أهم المجالات المتعلقة به؟
- ما هي الحقوق والحريات المتعلقة ببيانات تطبيقات الذكاء الاصطناعي والدافعة إلى ضرورة حمايتها بتشريعات جنائية حازمة وصارمة؟
- ما هي أهم الدوافع التي تؤدى إلي تدخل المشرع الجنائي لحماية المضرورين؟
- ما هي أهم التشريعات الخاصة بحماية بيانات تطبيقات الذكاء الاصطناعي العربية والأجنبية؟

خطة البحث:

قسمت هذ البحث إلى مقدمة ومبحثين وخاتمة، يتعلق الأول بالتعريفات الرئيسية بكل من الذكاء الاصطناعي والبيانات المتعلقة به، وكذا أهم الحقوق والحريات المتعلقة بتلك البيانات، وأبرزت في المبحث الثاني أهم التشريعات العربية والعالمية الخاصة في هذا الشأن ، ثم نتائج البحث وأهم التوصيات .

المبحث الأول

التعريفات الرئيسية بكل من الذكاء الاصطناعي والبيانات المتعلقة به

يُعَالج هذا المبحث في مطلبين يكون الأول منهما للتعريفات الخاصة بكل من الذكاء الاصطناعي والبيانات المتعلقة به وفي المطلب الثاني أهم الحقوق والحريات المتعلقة بتلك البيانات.

المطلب الأول

التعريفات الرئيسية بكل من الذكاء الاصطناعي والبيانات المتعلقة به

بادئ ذي بدء علينا أن نبرز مفهوم الذكاء الاصطناعي والبيانات التي يحتويها، وما هي العلاقة بين تطبيقات الذكاء الاصطناعي وتلك البيانات قبل بيان الحقوق والحريات المتعلقة بها وأدت إلى سن التشريعات المتعددة لحمايتها.

والجدير بالذكرأن ثمة محاولات متعددة لتعريف الذكاء الاصطناعي من قبل الفقه حيث لا يوجد تعريف قانوني متفق عليه(١) ومن ثم اتجه الفقه إلى محاولة سد النقص في هذا الأمر ومن هذه المحاولات ما قيل بأن:

---

(١) الدكتور/ محمد أحمد شحاته حسين: "أحكام الذكاء الاصطناعي وتطبيقاته في الفقه الإسلامي بين التأصيل والتحليل " بحث بمجلة الحقوق للبحوث القانونية والاقتصادية عدد يونيو ٢٠٢٤ صـ ٣٢٠ وما بعدها، الدكتور/ محمد نور الدين سيد:" التحديات الأمنية لاستخدام الذكاء الاصطناعي والأنظمة الرقمية في العمل الأمني وسبل المواجهة" مجلة العلوم الشرطية، أكاديمية العلوم الشرطية، القيادة العامة لشرطة الشارقة، 2021م صـ ٧، الدكتور/ يحيي إبراهيم الدهشان: "المسئولية الجنائية عن جرائم الذكاء الاصطناعي" مجلة الشريعة والقانون الصادرة عن كلية القانون بجامعة الإمارات العربية عام ٢٠١٩ صـ ١٢ ، سليمة زكريا سعيد :" المسئولية القانونية في حال وقوع أضرار جسيمة بسبب تكنولوجيا الذكاء الاصطناعي" بحث بالمجلة الأفريقية للعلوم التقنية والتطبيقية المتقدمة African Journal of Advanced Pure and Applied Sciences (AJAPAS), 302–314. العدد الثالث عام ٢٠٢٤ صـ ٣٠٤، عمار راشد علاي، محمد نور الدين عبد المجيد: "استخدام تطبيقات الذكاء الاصطناعي في مجال التنبؤ بالجريمة والوقاية منها" مجلة جامعة الشارقة للعلوم القانونية المجلد رقم ٢٠ العدد ٤ ديسمبر ٢٠٢٣ صـ ٣٧٦ وما بعدها، البراء جمعان محمد الشهري: "استخدام تقنيات الذكاء الاصطناعي في مكافحة الجريمة " مقال بالمجلة العربية للنشر العلمي الإصدار السابع، العدد ٦٨ حزيران – يونيو-٢٠٢٤ صـ ٧٨.

الذكاء الاصطناعي (Artificial Intelligence) هو "فرع من فروع علوم الحاسوب يركز على تصميم وتطوير الأنظمة والبرامج القادرة على أداء المهام التي تتطلب ذكاءً بشريًا، مثل التعلم، والفهم، والتخطيط، وحل المشكلات. يهدف الذكاء الاصطناعي إلى تقليد العمليات العقلية البشرية من خلال استخدام الخوارزميات والبيانات"(٢).

وقيل بأن "الذكاء الاصطناعي هو العلم الذي يهدف إلى تصميم أنظمة قادرة على القيام بالمهام التي تتطلب ذكاءً بشريًا، مثل التعلم، التخطيط، حل المشكلات، والفهم الطبيعي للغة"(٣).

أو هو " تِقْنِية تهدف إلى إنشاء أنظمة قادرة على القيام بمهام تتطلب عادةً الذكاء البشري، مثل التعرف على الكلام، التعلم، واتخاذ القرارات". (٤)

وفي تقديري أن الذكاء الاصطناعي ما هو إلا نوع من أنواع التكنولوجيا المتقدمة يتم من خلالها تصنيع تطبيقات في صورة أجهزة بأشكال متعددة وبمسميات مختلفة وتقوم بالأعمال التي يقوم

---

(2) David Poole and Alan Mack worth, Artificial Intelligence: "Foundations of Computational Agents (Cambridge University Press, 2017)" p. 5. Wolfgang Retell, Introduction to Artificial Intelligence (Springer, 2018), p. 10.

ويعرفه البعض بقوله "الذكاء الاصطناعي هو فرع من فروع علم الحاسوب الذي يهدف إلى تطوير أنظمة قادرة على محاكاة السلوك الذكي البشري. يتضمن ذلك القدرة على التعلم، الفهم، التفاعل مع البيئة، واتخاذ القرارات. الدكتور/ عادل الأبياري:" الذكاء الاصطناعي: الأسس والمبادئ ".دار صفاء للنشر، ٢٠١٩.صـ ٣٣.

(3) Stuart Russell and Peter Nerving، Artificial Intelligence: "A Modern Approach" 4th ed. (Pearson, 2020) , pp. 1-2

(٤) الدكتور/ حسام الدين الحسن:" الذكاء الاصطناعي وتطبيقاته في العالم العربي" مركز دراسات الشرق الأوسط، ٢٠٢١ صـ ١٥.

بها البشر على اختلاف أنماطها كالأعمال اليدوية والأعمال التي تحتاج إلى فكر متقدم كالجراحات المتعمقة أو الرسوم الهندسية المتطورة وغير ذلك.

وللذكاء الاصطناعي تطبيقات كثيرة ومتنوعة، تؤدى إلى استخدام تقنيات الذكاء الاصطناعي (AI) (٥) بطرائق متعددة للعمل على وضع حلول مختلفة بأسلوب مماثل وقدرات مشابهة لعمل العقل البشرى، وتتضمن تلك التطبيقات مجموعة كبيرة من المجالات التي تستفيد من قدرة التقنيات الخاصة بالذكاء الاصطناعي على التعلم من البيانات، واتخاذ القرارات، والتفاعل مع البيئة.

ومن الأمثلة الخاصة بتطبيقات الذكاء الاصطناعي:

١. **المساعدات الصوتية** :هي تلك التقنيات الإليكترونية التي تستخدم تقنيات الذكاء الاصطناعي لفهم الأوامر الصوتية والرد عليها.مثل **سيري (Siri)** من Apple و**أليكسا (Alexa)** من Amazon، فهذه التطبيقات تستفيد من معالجة اللغات الطبيعة في الذكاء الاصطناعي (NLP)للاستجابة بسرعة وفعالية إذ يمكن لهؤلاء المساعدين الصوتيين الرد على الطلبات والتحكم في الأجهزة الأخرى والمزيد بناءً على سجل المستخدم وتفضيلاته (٦).

---

(٥) اختصار "AI" يعني "Artificial Intelligence" والذي يُترجم إلى العربية بـ "الذكاء الاصطناعي". يشير هذا المصطلح إلى مجال من مجالات علوم الحاسوب الذي يركز على تصميم وتطوير الأنظمة والبرامج التي تمكن الحواسيب والآلات من أداء مهام تتطلب ذكاءً بشريًا، مثل التعلم، والفهم، واتخاذ القرارات، وحل المشكلات.

(٦) بشاير عبد الله:" تقنيات الذكاء الاصطناعي في تحسين خدمة العملاء" رابط المقال

https://triggers.sa/ar/blog/%D9%81%D9%88%D8%A7%D8%A6%D8%AF-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A/

٢. **القيادة الذاتية** :مثل سيارات تسلا (Tesla) التي تستخدم الذكاء الاصطناعي لمعالجة البيانات من مستشعرات السيارة لتوجيهها بدون تدخل بشري (٧).

٣. **الترجمة الآلية** :كمواقع وبرامج الترجمة الإليكترونية مثل جوجل ترانسليت (Google Translate) وغيره، التي تقوم باستخدام الذكاء الاصطناعي لترجمة النصوص بين لغات مختلفة.

٤. **التشخيص الطبي** :مثل أنظمة **IBM Watson Health**، التي تستخدم الذكاء الاصطناعي لتحليل الصور الطبية وتقديم توصيات تشخيصية.

٥. **التوصيات الشخصية** :مثل خوارزميات التوصية في **نتفليكس (Netflix)** وأمازون **(Amazon)**، التي تستخدم الذكاء الاصطناعي لتحليل سلوك المستخدمين وتقديم توصيات مخصصة (٨).

وبناء على ما سبق فإن التطبيقات الخاصة بالذكاء الاصطناعي كثيرة ومتنوعة وتعتمد على كونها تقوم بإجراء تصرفات كما لو كان المتصرف هو إنسان بشرى ومن ثم يمكن استخدامها في مختلف المجالات ومنها ما يلي:

---

(٧) وأسلوب أو ما يطلق عليه بالقيادة الذاتية، إنما هو نظام يعتمد على الذكاء الاصطناعي لتوجيه السيارة والتحكم فيها بدون أي تدخل من أي عنصر بشرى حيث يتم استخدام مجموعة من الحساسات وغيرها من الأجهزة الإليكترونية داخل السيارات كالكاميرات، والرادارات، وأجهزة الاستشعار الأخرى لجمع بيانات حول المكان المحيط بالسيارة. ومن ثم يعالج النظام هذه البيانات لتحديد ما هو التصرف الواجب القيام به كتغيير المسارات، وتفادي العقبات، والتسارع أو الكبح وهكذا.

Shadier, S., & Sweat man, P. C. *Autonomous Vehicles:" The Road to Self-Driving Cars*. Cambridge University Press" 2020, pp. 15-18.

)8(Stuart Russell and Peter Nerving، Artificial Intelligence:" A Modern Approach" pp. 20-22 & Wolfgang Retell," Introduction to Artificial Intelligence," pp. 45-47. & David Poole and Alan Mack worth" Artificial Intelligence: Foundations of Computational Agents" pp. 60-63

- التعلم الآلي Machine Learning أحد فروع الذكاء الاصطناعي يرتكز على تطوير نماذج وتقنيات تؤدى إلى حصول الأنظمة على المعرفة وتحسين أدائها من خلال البيانات (٩) وذلك بخلاف تقنيات البرمجة الصريحة. ويعمل التعلم الآلي للأنظمة من خلال البيانات التي يتم بثها فيه وتعمل على تحديث نفسها بنفسها من خلال عمليات معقدة، ويُعتبر التعلم الآلي أحد التطبيقات التي تُستخدم في الذكاء الاصطناعي لجعل الأنظمة قادرة على التعلم والتكيف مع المعلومات الجديدة بشكل تلقائي.
- **الشبكات العصبية الاصطناعية Neural Networks-**(١٠)هي نماذج عملية حسابية مستوحاة من طريقة عمل الدماغ البشري، تُستخدم هذه الشبكات في مجالات متعددة مثل التعلم الآلي، معالجة الصور، معالجة اللغة الطبيعية للبشر وفهمها، والذكاء الاصطناعي

---

(٩) ويقوم التعلم الآلي علي أسس محددة تبدأ **بجمع البيانات الكثيرة** التي تؤدى إلى إكساب القدرة على التنبؤ أو اتخاذ القرارات بناءً على البيانات التي لم يرها من قبل، ومن بعدها **تحليل البيانات** وتحويلها إلى صورة متوافقة، يمكن من خلالها **اختيار نموذج** التعلم الآلي المناسبة من خلال البيانات والمشكلة المراد حلها. ثم نأتي إلى مرحلة **تنفيذ أو تدريب النموذج** حيث يتم استخدام البيانات المحددة والمناسبة، و**بعدها نصل إلى مرحلة تقييم النموذج** باستخدام بيانات لم يرها من قبل لضمان دقته وفعاليته، ثم يكون **التحسين والتعديل** بناءً على نتائج التقييم. راجع في تفصيلات ذلك

Ian Good fellow, Joshua Bagnio, and Aaron Carville" Deep Learning" (2016: MIT Press), pp. 1-45. Ethen Aladdin, Introduction to Machine Learning (2020: MIT Press), pp. 15-30.

(١٠) **تعتبر الشبكة العصبية الاصطناعية** هي إحدى طرائق الذكاء الاصطناعي تعمل عليها أجهزة الحاسوب تُعَالج بها البيانات بذات الطرق التي تعمل بها الدماغ البشري إذ إنها نوع من عمليات التعلم الآلي، تسمى التعلم العميق، يستخدم ذات الطرائق التي تعمل بها الدماغ البشري.، وتعمل هذه الشبكات العصبونية الاصطناعية علي حل المشكلات المعقدة، كتلخيص المستندات أو التعرّف على الوجوه، بدقة أكبر، مقال بعنوان " ما لمقصود بالشبكات العصبونية " رابط https://aws.amazon.com/ar/what-is/neural-network/

وبالتالي فهي عبارة عن تقليد للهيكل العصبي البشري، وتُستخدم في معالجة البيانات المعقدة(١١).

- **الروبوتات Robotics** (١٢) هو جهاز ميكانيكي أو إلكتروني يمكن برمجته لأداء مهام معينة بشكل أوتوماتيكي أو شبه أوتوماتيكي. يُستخدم الروبوتات في مجموعة متنوعة من التطبيقات، بدءًا من الصناعة والتصنيع وصولاً إلى الرعاية الصحية والخدمات المنزلية (١٣).

وفي تقديري فإن الذكاء الاصطناعي يتدخل في كافة المجالات المختلفة والمتعددة ومن أهمها القضاء والتحقيق الجنائي والقطاع التعليمي، والقطاع المصرفي والقطاع الاقتصادي والقطاع الصحي وغيرها من القطاعات، وما يهمنا بحكم التخصص هو القضاء والتحقيق الجنائي (١٤).

) 11(Haskin, Simon S. Neural Networks and Learning Machines. 3rd ed., Pearson, 2009, pp. 5-15.

(١٢) يعتبر الروبوت " تطبيق لبرنامج مؤتمت يقوم بأداء مهام متكررة على الشبكة، حيث يتبع الروبوت تعليمات محددة ليماثل ويحاكي السلوك البشري بسرعة ودقة كبيرتين، كما يمكن أن يؤدى الروبرت الأعمال المناطة به بشكل مستقل من غير أي تدخل بشري، إذ يمكن أن تتفاعل الروبوتات مع المواقع الإلكترونية، أو أن تُجْري دردشة مع زوار الموقع، وغير ذلك من الأعمال ولذا تستخدم الروبوتات من أجل زيادة الكفاءة التشغيلية ومن ثم تبدو أن الغالبية العظمي من الأعمال التي تقوم بها معظم الروبوتات مفيدة، إلا أن ثمة أطراف خارجية تُصمم بعض الروبوتات التي لها غرض خبيث، ولذا تقوم الهيئات والمؤسسات وغيرهما من الشركات بتأمين أنظمتها من أجهزة الروبوتات الضارة" انظر في ذلك مقال بعنوان ما المقصود بالروبرت " والرابط هو

https://aws.amazon.com/ar/what-is/bot/

(13) Sicilian, Bruno, and Lorenzo Sciatica. Robotics: Modelling, Planning and Control. Springer, 2009, pp. 1-20.

(١٤) سيكون هناك بحث خاص ومستقل متعلق بدور الذكاء الاصطناعي في القضاء الجنائي إن شاء الله تعالي.

وسبق القول إن الذكاء الاصطناعي في كافة تطبيقاته ومجالاته إنما يتم وفق البيانات المرتبطة به حيث يتم تجميع البيانات المحملة عليه وتحليلها والوصول من ورائها إلى القرارات التي تتخذ، وهو الأمر الذي قد يترتب عليه اختراق تلك البيانات وبالتالي التعدي على الحقوق الخاصة بها كما هو واضح في المطلب الثاني.

المطلب الثاني

المصلحة التي يحميها الشارع الجنائي

عند تجريمه للاعتداء على البيانات الخاصة بتطبيقات الذكاء الاصطناعي

يمكن معالجة هذا المطلب في فرعين الأول لبيان المصلحة التي يحميها الشارع الجنائي عند تجريمه للاعتداء على البيانات الخاصة بتطبيقات الذكاء الاصطناعي وفي الثاني الحقوق والحريات المتعلقة بتلك البيانات.

الفرع الأول

المصلحة التي يحميها الشارع الجنائي

عند تجريمه للاعتداء على البيانات الخاصة بتطبيقات الذكاء الاصطناعي

من المسلم به أنه لكي يتدخل المشرع الجنائي لتجريم فعل معيناً وتحديد عقاب مترتب عليه لابد أن يكون ذلك التدخل لحماية مصلحة عامة أو خاصة إضافة إلى حماية وضمان النظام الاجتماعي من الأفعال التي تؤدى إلى زعزعة أمنه واستقراره، لذا يتدخل بتجريم الأفعال التي تضر بالسلامة العامة ومن ثم يحاول المساهمة في المحافظة على أمن واستقرار المجتمع، ومن ثم فإن الشارع الجنائي يتدخل في الأحوال الآتية:

١. **أولى هذه المصالح التي يعمل الشارع الجنائي على حمايتها هي "حماية الحقوق والحريات الفردية"** ذلك أنه لابد من تدخل المشرع الجنائي لحماية حقوق الأفراد وحراتهم عند الاعتداء عليها من خلال تجريم الأفعال التي تمس هذه الحقوق، كالاعتداءات الجسدية أو السرقة أو الاحتيال.

٢. **وثاني هذه المصالح يتمثل في "ردع الأفراد عن ارتكاب الأفعال غير المشروعة وتحقيق العدالة"** لأن تدخل المشرع الجنائي للتجريم يكون وسيلة لردع الأفراد عن ارتكاب الأفعال غير القانونية، إذ إنه من المعلوم أن العقوبات المترتبة على تلك الأفعال الإجرامية تؤدى إلى تحقيق الردع بنوعيه العام والخاص، وتدفع الأفراد إلى الالتزام بالقانون، فضلاً عن تحقيق العدالة من خلال مُحاكمة مرتكبي تلك الجرائم المنصوص عليها وتنفيذ الأحكام الجنائية الصادرة ضدهم، وهو الأمر الذي يعمل علي تعزيز ثقة الأفراد في النظام القضائي ويؤدى إلي الشعور بالعدالة (١٥).

٣. **ومن المصالح التي يحميها الشارع الجنائي " المصالح الاقتصادية لكل من الدولة والأفراد"**، ولذا نجد تدخلاً كثيراً من خلال تشريعات جنائية متعددة يكون الهدف الأساسي منها هو حماية المصالح الاقتصادية لأن تجريم الأفعال التي تؤدي إلى الإضرار بالمصالح الاقتصادية كالسرقة والاحتيال والتهريب يُساعد كثيراً في الاستقرار الاقتصادي ويشجع على التنمية الاقتصادية.

٤. **ومن المصالح التي يعمل الشارع الجنائي علي حمايتها في هذا الصدد "حماية القيم والمبادئ الاجتماعي وتقليل الأضرار الاجتماعية المرتبطة بها"** لأن المشرع الجنائي يتدخل لتجريم الأفعال التي تتعارض مع القيم والمبادئ الاجتماعية السائدة، كالقيم

---

(١٥) الدكتور/ حسن عبد الله:" النظرية العامة للعقوبات في القانون الجنائي" طبعة عام ٢٠١٥ الناشر دار النهضة العربية"، ص. ٤٥-٥٠، والدكتور/ محمد البرادعي:" الجرائم الاقتصادية في القانون الجنائي " طبعة عام ٢٠١٧ الناشر دار الثقافة، ص ٨٩-٩٥، والدكتور/ سامي الزغبي:" مبادئ قانون العقوبات" طبعة عام ٢٠١٩ مطبعة جامعة القاهرة، ص. ١٢٠-١٢٥، الدكتور فوزي العمري:" أثر الجرائم الاقتصادية على التنمية الاقتصادية" طبعة عام ٢٠١٦ الناشر دار الشروق، ٢٠١٦، ص٦٢-٧٠.

الأخلاقية والدينية، إنما يهدف من وراء ذلك ضمان احترام هذه القيم والمحافظة عليها، ومن ثم يتدخل الشارع الجنائي لتجريم الأفعال التي تؤدي إلى الإضرار بالمجتمع مثل الجريمة المنظمة أو التهديدات الأمنية وبالتالي يساهم في تقليل الأضرار الاجتماعية التي قد تنجم عن هذه الأفعال (١٦).

٥. **ومن المصالح الهامة والرئيسية التي يحافظ عليها المشرع الجنائي ويتدخل لحمايتها "حماية الوظائف العامة"** وذلك عندما يتدخل المشرع بتجريم الرشوة فإنه في الأصل يحافظ على حرمة الوظيفة العامة وعدم المساس بها.

٦. **وتعتبر "حماية الثقة العامة بين أفراد المجتمع"** من المصالح الضرورية التي تؤدى إلي تدخل الشارع الجنائي لتجريم أفعال معينة كما في حالة تدخل الشارع لتجريم أفعال التزييف والتزوير فإن الهدف من هذا التدخل هو حماية الثقة المتبادلة بين أفراد المجتمع في العملات الورقية والمعدنية المزورة أو المزيفة وكذلك في الأوراق والمستندات وغيرهما من الملفات التي من الممكن أن يَطَالها التزوير أو التزييف ومن ثم يترتب عليها الاعتداء على الثقة العامة بين أفراد الدولة.

وبصفة عامة، فإن المشرع الجنائي يهدف من خلال تجريم الأفعال إلى تحقيق التوازن بين حماية مصالح الأفراد والمجتمع وضمان تطبيق العدالة والوقاية من الجرائم.

ويثار التساؤل الآن حول الدوافع التي يحميها المشرع الجنائي عند تدخله لحماية البيانات المتعلقة بتطبيقات الذكاء الاصطناعي.

)16 (Dressler, Joshua. Understanding Criminal Law. *LexisNexis,* 2022 ، P.77-80. &Hart, H.L.A. Punishment and Responsibility: Essays in the Philosophy of Law. Oxford University Press, 2008 P.155 &Robinson, Paul H. Criminal Law*:* Doctrine, Application, and Practice. Aspen Publishers2021. P.214. & Semester, A.P., and Sullivan, G.R. Criminal Law*:* Theory and Doctrine. Hart Publishing, 2018.P.8

وفي تقديري فإن الشارع الجنائي إنما يتدخل لحماية البيانات المتعلقة بتطبيقات الذكاء الاصطناعي يأتي من عدة دوافع هامة، تتعلق بالضمانات الأمنية والقانونية اللازمة للتعامل مع التكنولوجيا المتطورة وتأثيرها على الأفراد والمجتمع، ومن أهم هذه الدوافع والمصالح الهامة التي تؤدى إلى التدخل من قبل الشارع الجنائي لحمايتها عند تجريم الاعتداءات على البيانات المتعلقة بتطبيقات الذكاء الاصطناعي:

١. **يُعتقد أن "حماية الحقوق والحريات الشخصية"** المتعلقة بالبيانات المرتبطة بتطبيقات الذكاء الاصطناعي والتي غالبًا تتضمن بيانات الشخصية لا حصر لها وهو الأمر الذي يتطلب تدخل المشرع الجنائي لحماية هذه البيانات من الاعتداءات مثل السرقة أو التلاعب بأي صورة من الصور كالتعديل أو المحو أو الاستغلال السيء والمُشِين ولذا كان هناك ضرورة لتدخل الشارع الجنائي لضمان حماية حقوق الأفراد في الخصوصية والحفاظ على سرية معلوماتهم الشخصية.
٢. **كما يعتبر تعزيز وسلامة الأمن والأمان السيبراني** من أي هجمات إليكترونية خطيرة من المصالح الرئيسية التي يرمي إليها الشارع الجنائي عند تدخله في هذا الشأن ذلك أنه مع تزايد استخدام الذكاء الاصطناعي، تصبح الهجمات الإلكترونية أكثر خطورة وتعقيدًا، وبناءً على ذلك فإن تجريم الاعتداءات على البيانات المرتبطة بالذكاء الاصطناعي يساعد في تعزيز الأمن السيبراني ويعمل على حماية الأنظمة الحَسَّاسة من الهجمات التي قد تؤدي إلى خسائر مَالية أو تَضر بالسلامة العامة (١٧).
٣. **ويُعد العمل على حماية كل من النزاهة والشفافية** من المصالح التي يرمى إليها الشارع في هذا الصدد لأن تطبيقات الذكاء الاصطناعي تعتمد على البيانات لتقديم نتائج دقيقة

(١٧) الدكتور/ عبد الرحمن التميمي:" الجرائم الإلكترونية وحماية البيانات الشخصية" طبعة عان ٢٠٢٠، الناشر دار النهضة العربية، ص. ٥٥-٧٠ ، الدكتور/ محمد البرادعي:" الأمن السيبراني وتطبيقات الذكاء الاصطناعي" طبعة عام ٢٠١٩ ، الناشر دار الثقافة، ص ٨٨-١٠٢.الدكتور/ سليمان الحميدي: "حماية البيانات في ظل التقنيات الحديثة" طبعة عام ٢٠٢١ الناشر دار الشروق، ص. ١٢٠-١٣٥.

وموثوقة، ومن ثم فإن أي اعتداء على هذه البيانات قد يؤدي إلى نتائج مُضَللة أو غير دقيقة، وبالتالي يؤدى إلى الإضرار بالثقة المفترض أن تتواجد في هذه التطبيقات، وبناءً عليه فإن تجريم التلاعب بالبيانات يساعد في الحفاظ على النزاهة والموثوقية في تطبيقات الذكاء الاصطناعي.

٤. **ومن المصالح التي يحميها الشارع في هذا الشأن "العمل على حماية المصالح الاقتصادية"** خاصة بالشركات والهيئات التي تعتمد في بياناتها على الذكاء الاصطناعي كأصل اقتصادي حيوي، فالاعتداء على هذه البيانات قد يؤدي إلى اضرار اقتصادية جسيمة، ولذا كان لابد من تجريم الاعتداءات على هذه البيانات لأنها تساعد في حماية هذه المصالح الاقتصادية ومنع التلاعب أو السرقة التي قد تؤثر سلبًا على الأعمال (١٨).

وفي تقديري فإن المشرع الجنائي يهدف من تجريمه لأفعال الاعتداء على البيانات المتعلقة بتطبيقات الذكاء الاصطناعي حماية الحقوق والحريات الخاصة بالأفراد وكذلك حماية من الهجمات السيبرانية التي تتضمن اعتداءات سافرة على الأفراد، وحماية النزاهة والشفافية المرتبطة بتلك البيانات، ومن ثم حماية القيم الأخلاقية ولذا يسعى المشرع الجنائي إلى تجريم الاعتداءات على البيانات الخاصة بتطبيقات الذكاء الاصطناعي.

الفرع الثاني

(18) Solove, Daniel J.. Understanding Privacy. Harvard University Press, 2022.P122. & Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs, 2019.P85& Miller, Claire Cain. Data and Privacy: The New Challenges. Oxford University Press, 2021. P*153&* Schneider, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015.P65.

إذا كانت تطبيقات الذكاء الاصطناعي (AI) واحدة من أكثر المجالات تطورًا في العصر الرقمي، إلا أنها تتعرض لمخاطر كبيرة تتعلق بأمن البيانات وحمايتها، إذ إن اختراق البيانات في هذا السياق لا يشكل تهديدًا فقط للبيانات الشخصية، بل يمكن أن يتسبب في انتهاك حقوق وحريات الأفراد.

ومن المعلوم أن الحقوق والحريات المتعلقة ببيانات تطبيقات الذكاء الاصطناعي التي لا يجوز الاعتداء عليها كثيرة ومن أهمها ما يلي:

حق الخصوصية: يعتبر من أهم حقوق الإنسان الأساسية بل هو من الحقوق المعترف بها في معظم الدول الأوروبية والعربية، ويشمل هذا الحق حماية الفرد من نشر بياناته الشخصية والأمور الخاصة به، أو منع تعرضه لأي ابتزاز يعكر صفو حياته بسبب أموره الشخصية الخاصة، واحترام خصوصية الآخرين وعدم الاعتداء عليها (١٩).

وفي نظري فإن الحق في الخصوصية يعتبر أحد أهم الحقوق الأساسية التي تُضمن للأفراد حماية بياناتهم الشخصية ضمن تطبيقات الذكاء الاصطناعي، كأنظمة التعرف على الوجه وتحليل البيانات الكبيرة، حيث تجمع وتخزن كميات هائلة من المعلومات الشخصية، مما

(١٩) سهير القرناوى:" الحق في الخصوصية كحق من حقوق الإنسان" مقال على شبكة الانترنت بموقع موضوع الاطلاع بتاريخ ٢٠٢٤/٨/١ والرابط:

https://mawdoo3.com/%D8%A7%D9%84%D8%AD%D9%82_%D9%81%D9%8A_%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9_%D9%83%D8%AD%D9%82_%D9%85%D9%86_%D8%AD%D9%82%D9%88%D9%82_%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86#cite_note-e8eb1927_4f88_4ee8_8c34_21294958fc9d-1

يعرضها لمخاطر كبيرة من حيث الاختراق والتسريب، ومن ثم يُعتبر ضمن حق الخصوصية حق الأفراد في التحكم بمعلوماتهم الشخصية والاحتفاظ بها سرية، ويتضمن ذلك الحق في عدم الكشف عن المعلومات الشخصية دون موافقة الأفراد (٢٠).

حق الوصول إلى البيانات وتصحيحها: من المسلم به أنه يحق للأفراد الوصول إلى بياناتهم الشخصية فضلاً عن معرفة الطريقة التي تُستخدم فيها تلك البيانات، كما يحق لهم تقديم طلبات عبر تلك التطبيقات لتصحيح البيانات غير السليمة أو بالأحرى غير الدقيقة التي تحتاج إلى تصحيح لما يترتب على ذلك من تصحيح أثناء جمع البيانات وتحليلها إلى أن يصدر القرار صحيحاً ودون اختراق لأي من البيانات (٢١).

---

(20) Jay, Rosemary. Privacy and Data Protection Law. 2012. Oxford University Press 50-60. & De Hart, Paul. The Right to Privacy in the Digital Age. 2019. Routledge 120-130.

وأنظر الدكتور/ محمد علي عثمان:" حماية البيانات الشخصية في القانون العربي: دراسة مقارنة" طبعة عام ٢٠٢٠ الناشر دار النشر العربية صـ ٧٥ وما بعدها. الدكتور/ أحمد علي محمد:" قانون حماية البيانات الشخصية: دراسة تحليلية" طبعة عام ٢٠١٩ الناشر دار الثقافة للنشر والتوزيع صـ ٩٠ وما بعدها ، الدكتور/ يوسف محمود: "حقوق الأفراد في حماية البيانات الشخصية في القانون الدولي والقوانين الوطنية"طبعة عام ٢٠١٨ الناشر دار الكتاب الجامعي ١١٠ وما بعدها، الدكتور/ عادل عبد الله :"الأمن المعلوماتي وحماية البيانات الشخصية: تحديات وحلول"طبعة عام ٢٠٢١ الناشر: مركز دراسات الوحدة العربية صـ ٦٥ وما بعدها ، الدكتور/ سلوى عبد الرحمن :"حماية البيانات الشخصية في العصر الرقمي: الإطار القانوني والتحديات" طبعة عام ٢٠٢٢ الناشر دار النهضة العربية صـ ٨٠.

) 21 (David Wright:" Data Protection and Privacy: The Age of Intelligent Machines. 2017. Springer, P 150 &. Helen Nissenbaum: Data Privacy and Security. 2018. Stanford University Press. P 45.

حق الحذف (الحق في النسيان):

من أهم الحقوق (حق الحذف) إذ يحق للأفراد طلب حذف بياناتهم الشخصية في حالات معينة، كما في حالة عدم وجود ضرورة للبيانات للغرض الذي تم جمعها من أجله، أو عندما ينسحب الشخص من الموافقة وهو ما يطلق عليه بحق الحذف والمعروف أيضاً بالحق في النسيان، ويعتبر من أهم الحقوق الأساسية الخاصة بحماية البيانات الشخصية، ويُسْمَح من خلال هذا الحق للأفراد المطالبة بحذف أي بيانات شخصية تخصهم في حالات متعددة، وهذا الحق يعكس الجهود الحثيثة التي ترمي إلى حماية الخصوصية والتعامل مع البيانات الشخصية بطريقة تحترم حقوق الأفراد (٢٢).

والجدير بالذكر أنه يتم تنظيم هذا الحق بموجب تشريعات حماية البيانات الشخصية والخصوصية في الكثير من الدول ووفقاً لأسس قانونية متعددة من أهمها ما ورد باللوائح

وانظر الدكتور/ محمد علي عثمان:" حماية البيانات الشخصية في القانون العربي: دراسة مقارنة" صـ ٨١. الدكتور/ أحمد علي محمد:" قانون حماية البيانات الشخصية: دراسة تحليلية" صـ ٩٢، الدكتور/ يوسف محمود: "حقوق الأفراد في حماية البيانات الشخصية في القانون الدولي والقوانين الوطنية"صـ ١١١، الدكتور/ عادل عبد الله:" الأمن المعلوماتي وحماية البيانات الشخصية: تحديات وحلول" صـ ٦٧، الدكتور/ سلوى عبد الرحمن: "حماية البيانات الشخصية في العصر الرقمي: الإطار القانوني والتحديات" صـ ٨٤.

(٢٢) الدكتور/ محمد البرادعي "حماية البيانات الشخصية في عصر التكنولوجيا الحديثة " طبعة ٢٠١٨ الناشر دار الثقافة، ص. ٤٥-٦٠.الدكتور/ عبد الله العتيبي:" الحقوق الرقمية وحماية البيانات الشخصية" طبعة ٢٠٢٠ الناشر دار النهضة العربية، ص. ٨٠-٩٥.الدكتور/ سامي الجميل:" الحق في الخصوصية وحماية البيانات الشخصية" طبعة عام ٢٠٢١ الناشر مطبعة *جامعة* الملك سعود، ص. ١٢٠-١٣٥. الدكتور/ علي الرفاعي:" القوانين الحديثة لحماية البيانات الشخصية" طبعة ٢٠١٩ الناشر دار الشروق، ص. ٦٥-٨٠.

الأوربية أو بالأحرى **اللائحة العامة لحماية البيانات (GDPR)** التي دخلت حيز التنفيذ في الاتحاد الأوروبي في مايو ٢٠١٨ ، حيث تحدد المادة (١٧) من اللائحة الحق في حذف البيانات متضمنة الشروط المطلوبة للحق في الحذف والآليات التي يتم بها الحذف وذلك بقولها " يحق للمَعْنِى بالبيانات أن يحصل من المتحكم على محو البيانات الشخصية المتعلقة به دون تأخير غير مبرر، ويكون على المتحكم الالتزام بمحو البيانات الشخصية دون تأخير غير مبرر في الحالات الآتية:

(أ) إذا لم تعد البيانات الشخصية ضرورية بالنسبة للأغراض التي جُمعت من أجلها أو تمت معالجتها بطرق أخرى.

(ب) إذا سحب المعني بالبيانات موافقته التي تستند إليها المعالجة وفقًا للنقطة (أ) من المادة ٦(١)، أو النقطة (أ) من المادة ٩(٢)، ولا يوجد أساس قانوني آخر للمعالجة.

(ج) إذا اعترض المعني بالبيانات على المعالجة وفقًا للمادة ٢١(١) ولا توجد أسباب مشروعة overridingللمعالجة، أو إذا اعترض المعني بالبيانات على المعالجة وفقًا للمادة ٢١(٢).

(د) إذا تمت معالجة البيانات الشخصية بشكل غير قانوني.

(هـ) إذا كان يجب محو البيانات الشخصية امتثالًا لالتزام قانوني وفقًا لقانون الاتحاد الأوروبي أو قوانين الدول الأعضاء التي يخضع لها المتحكم.

(و) إذا تم جمع البيانات الشخصية في سياق تقديم خدمات معلوماتية كما هو مذكور في المادة ٨(1).

١. عندما يكون المتحكم قد جعل البيانات الشخصية علنية وملزم وفقًا للفقرة ١ بمحو البيانات الشخصية، يجب على المتحكم، مع الأخذ في الاعتبار التكنولوجيا المتاحة وتكلفة التنفيذ، اتخاذ

خطوات معقولة، بما في ذلك تدابير تقنية، لإبلاغ المتحكمين الذين يعالجون البيانات الشخصية أن المعني بالبيانات قد طلب محو الروابط، أو النسخ أو الاستنساخ لهذه البيانات الشخصية.

٢. لا تنطبق الفقرتان ١ و٢ على مدى ضرورة المعالجة في الحالات التالية:

(أ) لممارسة حق حرية التعبير والمعلومات.

(ب) للامتثال لالتزام قانوني يتطلب المعالجة وفقًا لقانون الاتحاد أو قوانين الدول الأعضاء الذي يخضع له المتحكم.

(ج) لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة وفقًا للنقاط (ح) و(ط) من المادة ٩(٢).

(د) لأغراض الأرشفة في المصلحة العامة، أو لأغراض البحث العلمي أو التاريخي أو لأغراض إحصائية وفقًا للمادة ٨٩(١).

(هـ) لإقامة أو ممارسة أو الدفاع عن الدعاوى القانونية"(٢٣).

)23 (Article 17 -Right to erasure ('right to be forgotten')

1. "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies":

   (a)" the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;"

(b)" the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing"

(c)" the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2)"

(d) "the personal data have been unlawfully processed"

(e)" the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject"

(f) "The personal data have been collected in relation to the offer of information society services referred to in Article 8(1)"

2. "Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data".
3. "Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

وبناء على النص المشار إليه فإن الشروط التي يمكن للأفراد بموجبها طلب حذف بياناتهم الشخصية هي:

- **أنه لم يعد هناك ضرورة** أو حاجة مُلحة للغرض الذي من أجله جُمعت هذه البيانات.
- **إذا سحب الشخص موافقته** التى كانت سبباً أو أساساً في معالجة البيانات.
- **الاعتراض** :عندما يعترض الشخص على معالجة البيانات التي تعتمد على المصالح المشروعة.
- **الامتثال لالتزام قانوني** عندما يتعين حذف البيانات لمراعاة الالتزامات القانونية.
- **معالجة غير قانونية** وذلك عندما تكون معالجة البيانات غير قانونية. (٢٤)

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (I) of Article 9(2);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1); or

(e) for the establishment, exercise or defense of legal claims".

)24(Kuner، Christopher. European Data Protection Law: Corporate Compliance and Regulation. Oxford University Press, 2022 .،P 155 & Cohen, Julie E. Configuring the Networked Self: Law, Code, and the Play of Everyday Practice. Yale University Press, 2012 ،P.210 & Solove, Daniel J. Understanding Privacy. Harvard University Press, 2022 P.140. & Reidenberg, Joel R. The Law of Internet Privacy. MIT Press, 2016 P.50.

فإذا توافرت الأسباب التي نص عليها المشرع وتقدم صاحب البيانات بطلب حذف لبياناته الشخصية إلى الجهة المسئولة عن مُعالجة البيانات وجب حذف هذه البيانات سواء بالكامل أو الجزئي كالإيقاف أو بالتعديل حسب كل حالة وما تريد وإلا اعتبر عدم الإجابة اعتداء علي صاحب تلك البيانات المراد حذفها غير **أن** هناك بعض الاستثناءات التي قد تمنع الحذف، كالحاجة إلى البيانات للامتثال للالتزامات القانونية أو لمصلحة عامة.

الحق في الأمان الرقمي للبيانات الشخصية:

الحق في الأمان الرقمي للبيانات الشخصية هو حق أساسي يتعلق بحماية الأفراد من التهديدات والهجمات التي قد تؤدي إلى كشف أو سوء استخدام بياناتهم الشخصية، حيث يتضمن هذا الحق ضمانات ضد الوصول غير المصرح به، والسرقة، والتلاعب، والتسريب، مما يساعد في الحفاظ على سلامة البيانات وحمايتها من الأضرار، وعليه فيجب أن تكون البيانات الشخصية محمية بأعلى مستويات الأمان حماية للأفراد من المخاطر المذكورة كالسرقة الإلكترونية والاحتيال، فالأمان الرقمي هو جزء أساسي من حماية الحقوق والحريات الشخصية، ويجب أن تتبعه التطبيقات والأنظمة الذكية (٢٥).

ومن ثم فإن الأمان الرقمي يشير إلى مجموعة التدابير والإجراءات التي تُتخذ لحماية البيانات الشخصية من المخاطر الرقمية مثل القرصنة، وتسريبات البيانات، والتلاعب، والهجمات

(25)Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2020.P.215&. Schneider, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015P 66&. Somme tad, Theodor, et al. Cybersecurity and Privacy: An Introduction. Springer, 2019 P.155&. Stallings, William. Computer Security: Principles and Practice. Pearson, 2022.P.110

الإلكترونية. يشمل ذلك تطبيق تقنيات الأمان وتطوير سياسات وإجراءات للحفاظ على سلامة البيانات وخصوصيتها.

ويكون الأمان الرقمي بآليات مختلفة تبدأ **بالتشفير** الذي يعمل علي حماية البيانات أثناء فترة التخرين حيث لا يمكن قراءتها والتعرف عليها بدون إمكانية فك ذلك التشفير ، فضلاً عن **إمكانية تحديد الوصول** لأفراد محددة إذ يمكن تقليص الإذن بالمرور أو فك التشفير لأشخاص محددين وبالتالي فلا يمكن لأحد الوصول إلي البيات غير من هم مصرح لهم وبعد أن يتم التعرف عليهم **القيام بإجراءات محددة ككلمات مرور أو بطاقات تحديد هوية ذكية** مع ضرورة تحديث وتغيير تلك الأرقام السرية أو كلمات المرور باستمرار لسد الثغرات الأمنية ومعالجة نقاط الضعف(٢٦).

ولأهمية الأمان الرقمي نصت عليه الكثير من التشريعات ومنها **اللائحة العامة لحماية البيانات (GDPR)**في الاتحاد الأوروبي، في المادة (٣٢) منها بقولها:

١. مع الأخذ بعين الاعتبار حالة التكنولوجيا الحالية، وتكاليف التنفيذ، وطبيعة ونطاق وسياق وأغراض المعالجة، فضلاً عن المخاطر ذات الاحتمالية والشدة المتباينين لحقوق وحريات الأفراد الطبيعيين، يتعين على المتحكم ومعالج البيانات تنفيذ تدابير تقنية وتنظيمية مناسبة لضمان مستوى من الأمان يتناسب مع المخاطر، بما في ذلك، على سبيل المثال لا الحصر، ما يلي:

(٢٦) الدكتور/ محمد البرادعي:" الأمن الرقمي وحماية البيانات الشخصية" دار الثقافة، ص. ٤٥-٧٠، الدكتور: سامي المحمودى:" التدابير الأمنية لحماية البيانات الشخصية في العصر الرقمي "ص. ٨٠-٩٥، الدكتور/ فوزي الزغبي:"الأمن السيبراني وحماية البيانات الشخصية" ص. ١٢٠-١٣٥. الدكتور/ عبد الله العتيبي:" أمن المعلومات وحماية البيانات في العصر الرقمي" ص ٧٠

(أ) إخفاء الهوية والتشفير للبيانات الشخصية.

(ب) القدرة على ضمان سرية وسلامة وتوافر ومرونة نظم وخدمات المعالجة بشكل مستمر.

(ج) القدرة على استعادة توفر والوصول إلى البيانات الشخصية في الوقت المناسب في حال حدوث حادث مادي أو تقني.

(د) عملية لاختبار وتقييم فعالية التدابير التقنية والتنظيمية بشكل منتظم لضمان أمان المعالجة.

٢. يجب على المتحكم ومعالج البيانات التأكد من أن أي شخص يعمل تحت سلطة المتحكم أو المعالج والذي لديه وصول إلى البيانات الشخصية لا يعالجها إلا بناءً على تعليمات المتحكم، ما لم يكن ذلك مطلوباً بموجب قانون الاتحاد أو قوانين الدول الأعضاء"(٢٧).

---

(27) **Article 32 - Security of processing**

1. "Taking into account the state of the art, the costs of implementation and the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:"

   "(a) the pseudonymization and encryption of personal data;

   (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

وثمة حقوق أخرى ترتبط بالبيانات الشخصية المتعلقة بتطبيقات الذكاء الاصطناعي ومن أهمها حق الموافقة قبل جمع البيانات ومعالجتها فضلاً عن حق الاعتراض على معالجة بياناتهم الشخصية في حالات معينة، مثل إذا كانت المعالجة تتم لأغراض تسويقية، أو نقل بياناتهم الشخصية من خدمة إلى أخرى بسهولة، مما يعزز القدرة على التحكم في المعلومات الشخصية.

وبعد التعرف علي أهم الحقوق والحريات الخاصة بالبيانات كان من الواجب التنبيه علي ضرورة التصدي من قبل الشارع لحمايتها وجب التنويه إلي أن البيانات الشخصية مَحْمية ومحظور التعرض لها والاستيلاء عليها ومعالجتها أو تخزينها أو تداولها بدون إذن من أصحابها، ومن ثم يتدخل التشريع الجنائي لحمايتها، إذ الحماية تعني عدم الاعتداء وهي إما ذاتية أو تشريعية ، والذاتية تكون من داخل النفس البشرية التي وصفها خالقها بأنها أمارة بالسوء وربطها علماء علم النفس بالرقابة الذاتية الداخلية للإنسان وإلا كانت الحماية من

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing"

2. "The controller and processor shall ensure that any person acting under the authority of the controller or processor who has access to personal data does not process them except on instructions from the controller, unless required to do so by Union or Member State law"

خلال النصوص القانونية التي تجرم الاعتداء علي تلك البيانات بشتي الصور وتضع العقوبات الرادعة في هذا الشأن.

المبحث الثاني

أهم التشريعات الجنائية العربية والعالمية

الخاصة بحماية البيانات المتعلقة بتطبيقات الذكاء الاصطناعي

يُعَالج هذا المبحث في مطلبين يكون الأول منهما للتشريعات العربية الخاصة بحماية البيانات المتعلقة بتطبيقات الذكاء الاصطناعي وفي المطلب الثاني للتشريعات الأجنبية وذلك على النحو التالي.

المطلب الأول

أهم التشريعات الجنائية العربية

الخاصة بحماية البيانات المتعلقة بتطبيقات الذكاء الاصطناعي

يُعَالج هذا المطلب في ثلاث فروع يتعلق الأول منها بالتشريعات المصرية، وفي الثاني التشريعات السعودية، وفي الثالث التشريعات الإماراتية.

الفرع الأول

التشريعات المصرية

قانون مكافحة الجرائم الإليكترونية وجرائم تكنولوجيا المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨

القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية

تم إصدار قانون مكافحة الجرائم الإلكترونية وجرائم تكنولوجيا المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، ولحقه القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، ويعتبر من الأهداف الرئيسية لهذين القانونين حماية تكنولوجيا المعلومات والبيانات الشخصية من أي اعتداءات أو جرائم المرتكبة عبر الإنترنت ومن ثم حماية المعلومات والبيانات الشخصية.

ولأهمية البيانات الشخصية تم تحديد مضمونها في كلا القانونين إذ عرفها القانون الخاص بمكافحة الجرائم الإلكترونية وجرائم تكنولوجيا المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ في المادة الأولي محددا أن البيانات والمعلومات هي كل ما يمكن إنشاؤه أو تخزينه أو معالجته أو تخليقه أو نقله أو مشاركته أو نسخه بواسطة تقنية المعلومات كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها، ثم قسمت البيانات إلي شخصية وهي البيانات المتعلقة بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى ، وبيانات حكومية متعلقة بالدولة أو إحدى سلطاتها أو أجهزتها أو هيئاتها الاعتبارية العامة وما في حكمها.

وحدد القانون الخاص بحماية البيانات رقم ١٥١ لسنة ٢٠٢٠ في المادة الأولي الخاصة بالتعريفات ماهية البيانات الشخصية ثم قام بتحديد حقوق صاحب البيانات وشروط جمعها ومعالجتها وكذا التزامات كل من المتحكم والمعالج وواضعاً العقوبات المترتبة على مخالفة أحكامه في نهايته في الفصل الرابع عشر اعتبارا من المادة ٣٥ وما بعدها.

واهتم القانون الخاص بمكافحة الجرائم الإلكترونية وجرائم تكنولوجيا المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ في نصوصه بالجرائم الإلكترونية ومنها بطبيعة الحال الأفعال المتعلقة بتجريم الاعتداء على البيانات كجريمة الاعتداء علي سلامة البيانات والمعلومات والنظم المعلوماتية كما وردت في نص المادة ١٧، والجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع كما ورد في المادة ٢٥ منه.

وفي تقديري أن أهمية البدء بتحديد ما هيه الجرائم الإليكترونية إنما يكون بسبب اعتبار الاعتداء على البيانات الشخصية المتعلقة بتطبيقات الذكاء الاصطناعي هي من الجرائم الإليكترونية، وبناءً عليه كان من أهم النقاط التي تكون في البداية هي تحديد ماهية الجرائم الإليكترونية، التي تُعرَّف بأنها الأفعال غير القانونية التي تُرتكب باستخدام أو استهداف الشبكات أو نظم المعلومات أو الأجهزة الإلكترونية، بما في ذلك اختراق الشبكات واستخدام البيانات الشخصية بطريقة غير قانونية".

وبناءً علي ما سبق فإن الجرائم الإلكترونية هي عبارة عن الأفعال غير القانونية التي تتم عبر التكنولوجيا الرقمية، سواء كانت تلك الأفعال تستهدف الشبكات المعلوماتية أو الأجهزة الإلكترونية أو تشمل استخدامها بطرق غير مشروعة ومن ثم فإن هذه الأفعال تتضمن **اختراق الشبكات أو بالأحرى كالدخول** غير المصرح به إلى الأنظمة المعلوماتية، وهو ما قد يسفر عن سرقة أو تلاعب بالبيانات، فضلاً عن **استخدام البيانات الشخصية بطريقة غير قانونية وأقرب الأمثلة في هذا الشأن** جمع أو تداول أو استخدام البيانات الشخصية بطرق تنتهك حقوق الأفراد ولا تتوافق مع القوانين واللوائح المتعلقة بحماية البيانات.

وبالنسبة للجرائم التي حددها قانون الجرائم الإلكترونية المصري الصادر في ٢٠١٨:

أولاً: جريمة الدخول غير المشروع علي الأجهزة وأنظمة الحاسب الآلي أو النظام المعلوماتي أو الموقع الإليكتروني باستخدام وسائل تؤدى إلي اختراق وسائل الحماية بشكل كلي أو جزئي لأى غرض كان بدون تفويض في ذلك أو بالتجاوز للتفويض الممنوح ، ومن الممكن أن نعتبر تلك الجريمة نوع من أنواع اختراق الشبكات المعلوماتية والدخول إليها لاستخدام ما فيها من معلومات بدون وجه حق (٢٨) وهي الجريمة **التي تم اعتمادها من خلال النصوص الخاصة في الفصل الأول تحت عنوان الاعتداء علي سلامة شبكات وأنظمة وتقنيات المعلومات حيث نصت المادة ١٣ علي من انتفع بدون وجه حق بالخدمات الإليكترونية وأبانت المادة ١٤ كل من دخل عمداً أو بخطأ دون عمدى لكنه بقي بدون وجه حق علي موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.**

(٢٨) الدكتور/ حاتم أحمد محمد بطيخ:" تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات- دراسة تحليلية مقارنة" بحث منشور بمجلة الدراسات القانونية والاقتصادية المجلد ٧ – العدد ١ – أغسطس ٢٠٢١ صـ ٣٧ وما بعدها.

وبناء على هذه المادة فإنه تم تجريم الدخول غير المصرح به إلى الأنظمة المعلوماتية، مثل اختراق الأنظمة لتعديل البيانات أو سرقتها.

تشمل تلك الجرائم، القرصنة **:**دخول غير مشروع إلى الأنظمة، التلاعب **بالبيانات :**تغيير أو حذف البيانات التي يتم الوصول إليها بصورة غير قانونية.

وبشأن الركن المادي لهذه الجريمة وعناصره المتعارف عليها وهي السلوك الإجرامي والنتيجة المترتبة عليه فضلاً عن علاقة السببية فهي من الأمور التي يمكن الوقوف عليها بسهولة ومن خلال إسقاط القواعد العامة علي هذه الجرائم وغيرها ، ومن ثم فإن الفعل الإجرامي لهذه الجرائم يتكون من عملية **الدخول غير المصرح به** ، **أي** الدخول إلى أنظمة المعلومات أو الشبكات دون الحصول على إذن مسبق ، ويشمل كذلك استخدام أدوات أو تقنيات لاختراق الأمان الرقمي للشبكات أو الأنظمة، و**التلاعب بالبيانات من خلال القيام بتعديلها أو حذفها خاصة من تلك** البيانات التي تم الوصول إليها بطريقة غير قانونية، و**الاستيلاء على البيانات مثل** سرقة البيانات الشخصية أو الحساسة أثناء الاختراق، وتسريب البيانات الشخصية أو نشرها دون إذن صاحبها.

وبناءً على هذه الأفعال فمن الممكن أن نستنتج النتيجة الإجرامية المترتبة عليه ومعرفة ما إذا الفعل قد ارتكب كاملاً وأدى إلى النتيجة الإجرامية الكاملة كما في حالة الاختراق الكامل للمعلومات أو التلاعب بها بالتعديل أو الحذف أو حتى في الاستيلاء عليها أم توقف لسبب لا إرادي وبالتالي خاب أثره ومن ثم نصبح أمام شروع في ارتكاب الفعل الإجرامي، وكذلك الأمر بالنسبة للمساهمة الجنائية وعما إذا كانت الجريمة مكونة من مجموعة من الأفراد وبالتالي يُعاقب كل فرد حسب مساهمته الحقيقية في الفعل.

ثانياً: ومن أهم الجرائم الأخرى المنصوص عليها في قانون حماية البيانات الشخصية ما ورد في نص المادة ٢ الخاصة بتجريم جمع البيانات الشخصية أو استخدامها دون إذن، حيث نصت **المادة** على أنه "لا يجوز جمع البيانات الشخصية ومعالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانوناً."

وبناءً على هذا النص فإن المشرع جَرَّمَ في هذه المادة جمع أو استخدام البيانات الشخصية دون الحصول على إذن صريح من الأفراد المعنيين، ويتضمن ذلك **جمع البيانات كالحصول على** بيانات الأفراد من مصادر مختلفة دون موافقتهم، و**استخدام البيانات :**مثل استخدام تلك البيانات لأغراض تجارية أو شخصية أو غيرها دون إذن من الأفراد المعنيين، وعليه فإن هذا النص يهدف إلى حماية الأفراد من الاستغلال غير المشروع لبياناتهم الشخصية وضمان احترام خصوصيتهم.

ومن ثم فإن الأنموذج المكون للجريمة المشار إليها بعالية إنما يتكون بداءة من الركن المادي المكون لها والذي يبدأ بطبيعة الحال بالفعل الإجرامي المتمثل في البدء في جمع البيانات الخاصة بالأفراد بكل طريقة تؤدى إليها، وكذلك من المفترض أن تكون هذه الجريمة عمدية إذ ليس من المعقول أن يقوم الجاني باقتراف الفعل الإجرامي المؤدى إلي جمع المعلومات واستخدامها دون إذن صاحبها دون أن يكون بغير قصد أو نية.

ثالثا: ومن أهم الجرائم الأخرى المنصوص عليها في قانون مكافحة الجرائم الإليكترونية ما ورد في نص المادة ٢٤ المتعلقة بالجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإليكتروني، إذ نصت على أن "يُعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز ثلاثين ألف جنيه أو بإحدى هاتين العقوبتين كل من اصطنع بريداً إليكترونيات أو موقعاً أو حساباً ونسبه زوراً إلي شخص طبيعي أو اعتباري ، فإذا استخدم الجاني البريد أو الموقع أو الحساب الخاص المصطنع في أمر يسئ إلي ما نسب إليه ، تكون العقوبة الحبس الذي لا تقل مدته عن سنة والغرامة التي لا تقل عن خمسين ألف جنيه ولا

تجاوز مائتي ألف جنيه أو بإحدى هاتين العقوبتين وإذا وقعت الجريمة علي أحد الأشخاص الاعتبارية العامة تكون العقوبة السجن والغرامة التي لا تقل عن مائة ألف جنيه ولا تزيد عن ثلاثمائة ألف جنيه".

يتضح من هذا النص أن المشرع يُعَاقب الأشخاص الذين ينشئون مواقع زائفة أو يستخدمون مواقع حقيقية بطرق احتيالية، مثل **إنشاء مواقع وهمية** مثل مواقع تقليد لمواقع رسمية أو تجارية بهدف خداع المستخدمين وسرقة معلوماتهم أو أموالهم.

وكذلك في حالة الاحتيال أي استخدام تلك المواقع للوصول إلى بيانات حساسة أو لتقديم عروض وهمية لتحقيق مكاسب غير قانونية.

وبالتالي يكون الركن المادي المكون لهذه الجريمة من خلال الأفعال المشار إليها بعالية ومن أهمها **إنشاء موقع وهمي أي العمل على** تصميم موقع إلكتروني بمعني أن يقوم الجاني بتزييف موقعًا رسميًا أو تجاريًا لجذب المستخدمين بشكل احتيالي، يشمل ذلك استخدام تصميمات وشعارات مشابهة لمواقع حقيقية، أو أن يقوم بعمل من أعمال **الاحتيال الإلكتروني مثل** استخدام الموقع الوهمي لجمع معلومات شخصية أو أموال من المستخدمين تحت ظروف زائفة، أو إنشاء موقع إلكتروني مشابه لموقع مصرفي حقيقي للاحتيال على المستخدمين وجمع بياناتهم البنكية(٢٩).

أما جريمة التشهير والابتزاز الإليكتروني: فلم يتناولها صراحة قانون الجرائم الإلكترونية المصري الصادر في ٢٠١٨، وإنما يمكن أن تُسْتَشَف تلك الجريمة صراحة من خلال انتهاك حرمة الحياة الخاصة أو إرسال معلومات مسيئة سواء كانت صحيحة أم لا والمنصوص عليها

(٢٩) الدكتور/ محمد البرادعي:" الجرائم الإلكترونية وحماية البيانات الشخصية "ص. ٤٥-٦٥.الدكتور/ ناصر الزهراني:" الأمن السيبراني وحماية البيانات في العصر الرقمي" ص. ٨٠-١٠٠.الدكتور / أحمد المحمدي:" قانون الجرائم الإلكترونية وحماية البيانات" ص. ١٢٠-١٣٥.الدكتور/ عبد الله العتيبي:" حماية البيانات الشخصية والتقنيات الحديثة" ص. ٥٥-٧٥.

في **المادة ٢٥** من قانون مكافحة جرائم تقنية المعلومات التي تنص علي أن:" يعاقب بالحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين **كل من اعتدى علي أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة** أو أرسل بكثافة العديد من الرسائل الإليكترونية لشخص معين دون موافقته أو منح بيانات شخصية إلي نظام أو موقع إليكتروني لترويج السلع والخدمات دون موافقته **أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبار أو صوراً أو ما في حكمها تنتهك خصوصية أي شخص دون رضاه سواء كانت المعلومات صحيحة أو غير صحيحة"** ومن ثم فإن هذا النص يشمل التشهير والابتزاز متى تم استخدام صور أو معلومات تم الحصول عليها بطريقة غير قانونية لنشرها أو استخدامها بطريقة ضارة، وبناء على ما سبق فإن المشرع جرم كل من **التشهير الذي هو** نشر معلومات كاذبة أو ضارة عن الأفراد عبر الإنترنت، إضافة إلى **الابتزاز الذي هو** تهديد الأفراد بنشر معلومات حساسة إذا لم يتم تلبية مطالب معينة.

وبالتالي فإن **الركن المادي للتشهير الإلكتروني أو بمعني أكثر وضوحاً الفعل الإجرامي المكون للتشهير يتمثل في** نشر معلومات كاذبة أو مُضَللة تؤدي إلى الإضرار بسمعة الفرد أو تشويه صورته، ويمكن أن يتم ذلك عبر مواقع الويب، أو من خلال وسائل التواصل الاجتماعي، أو بأي وسيلة إلكترونية أخرى.

أما الابتزاز الإلكتروني فيتمثل السلوك الإجرامي في تهديد الفرد بنشر معلومات حساسة أو خاصة إذا لم يستجب لمطالب معينة، ويمكن أن يتضمن ذلك استخدام البريد الإلكتروني، الرسائل النصية، أو وسائل التواصل الاجتماعي.

وبالنسبة للركن المعنوي أو بالأحرى القصد الجنائي فإن ذلك الفعل لا يمكن أن يُتصور أنه غير عمدي ومن ثم فإن هذه الجريمة في الأصل عمدية أي أن من يُقدم عليها لديه النية في ارتكاب الفعل بإدراك تأثيره الضار على الأفراد المستهدفين سواء بالنسبة للتشهير، فإن القصد

فيه هو الإضرار بسمعة الفرد، وبالنسبة للابتزاز، القصد هو إجبار الفرد على الاستجابة للمطالب من خلال التهديد.

وتعتمد العقوبات على نوع الجريمة وظروفها، ولكنها عادةً تشمل: **الحبس :**قد يُحكم بالسجن لفترات متفاوتة بناءً على خطورة الفعل، و**الغرامة :**قد يُحكم بدفع غرامة مالية كعقوبة إضافية.

وعامة تصل عقوبات **التشهير الإلكتروني إلى** السجن لفترة تصل إلى خمس سنوات، وغرامة مالية قد تصل إلى ٣٠٠،٠٠٠ جنيه مصري.

أما الابتزاز الإلكتروني :قد تشمل العقوبات السجن لفترات متفاوتة بناءً على شدة التهديدات والتصرفات (٣٠).

الفرع الثاني

نظام حماية البيانات الشخصية في المملكة العربية السعودية الصادر بالمرسوم الملكي رقم ١٩ بتاريخ ١٤٤٣/٢/٩

ونظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم ١٧ بتاريخ ١٤٢٨/٣/٨

أصدرت المملكة العربية السعودية أكثر من نظام مُتَعَلِّق بالتقنيات الإليكترونية الحديثة ، منها نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم ١٧ بتاريخ ١٤٢٨/٣/٨ ، ونظام حماية البيانات الشخصية في المملكة العربية السعودية الصادر بالمرسوم الملكي رقم ١٩ بتاريخ ١٤٤٣/٢/٩، ويعتبر هذا النظام الأخير هو الأول من نوعه في المملكة متعلقاً بحماية البيانات الشخصية علي غرار عدد من التشريعات المختلفة الصادرة في مختلف الدول العربية والأجنبية، ويهدف إلى حماية بيانات الأفراد وتعزيز الشفافية في التعامل معها، ويعتبر هذا

(٣٠) الدكتور/ محمد البرادعي:" الجرائم الإلكترونية وحماية البيانات الشخصية "ص. ٤٥-٦٥.الدكتور/ ناصر الزهراني:" الأمن السيبراني وحماية البيانات في العصر الرقمي" ص. ٨٠-١٠٠.الدكتور / أحمد المحمدي:" قانون الجرائم الإلكترونية وحماية البيانات" ص. ١٢٠-١٣٥.الدكتور/ عبد الله العتيبي:" حماية البيانات الشخصية والتقنيات الحديثة" ص. ٥٥-٧٥.

النظام إضافة إلي نظام مكافحة الجرائم المعلوماتية من الأنظمة التي تهتم بحماية البيانات والمتضمنة الجرائم التي تعمل علي حماية البيانات الشخصية.

بادئ ذي بدء لابد من التأكيد علي أن نظام حماية البيانات الشخصية السعودي لعام ٢٠٢١ عرف البيانات الشخصية في المادة الأولي منه بقوله (البيانات الشخصية :كل بيان -مهما كان مصدره أو شكله- من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكنًا بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، ورقم الهوية الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي.)

كما تضمن نصوصاً تهدف إبراز حقوق صاحب البيانات الشخصية كما ورد في المادة الرابعة بقولها (يكون لصاحب البيانات الشخصية -وفقاً للأحكام الواردة في النظام-الحقوق الآتية:

١. الحق في العلم، ويشمل ذلك إحاطته علماً بالمسوغ النظامي أو العملي المعتبر لجمع بياناته الشخصية، والغرض من ذلك، وألاَّ تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها أو في غير الأحوال المنصوص عليها في المادة (العاشرة) من النظام.
٢. الحق في وصوله إلى بياناته الشخصية المتوافرة لدى جهة التحكم، ويشمل ذلك الاطلاع عليها، والحصول على نسخة منها بصيغة واضحة ومطابقة لمضمون السجلات وبلا مقابل مادي -وفقاً لما تحدده اللوائح-وذلك دون إخلال بما يقضي به نظام المعلومات الائتمانية فيما يخص المقابل المالي، ودون إخلال بما تقضي به المادة (التاسعة) من النظام .
٣. الحق في طلب تصحيح بياناته الشخصية المتوافرة لدى جهة التحكم، أو إتمامها، أو تحديثها.
٤. الحق في طلب إتلاف بياناته الشخصية المتوافرة لدى جهة التحكم مما انتهت الحاجة إليه منها، وذلك دون إخلال بما تقضي به المادة (الثامنة عشرة) من النظام.
٥. الحقوق الأخرى المنصوص عليها في النظام، التي تُبينها اللوائح.

كما أفصحت المادة الخامسة على ضرورة الحصول على موافقة صاحب الشأن قبل معالجة البيانات أو تغيير الغرض منها إلا بعد موافقته وتُبين اللوائح شروط الموافقة، والأحوال التي

يجب فيها أن تكون الموافقة كتابية، والشروط والأحكام المتعلقة بالحصول على الموافقة من الولي الشرعي إذا كان صاحب البيانات الشخصية ناقص أو عديم الأهلية. في جميع الأحوال، يجوز لصاحب البيانات الشخصية الرجوع عن الموافقة المشار إليها في الفقرة (١) من هذه المادة في أي وقت، وتحدد اللوائح الضوابط اللازمة لذلك.

وتنص المادة (١٥) على أنه لا يجوز لجهة التحكم الإفصاح عن البيانات الشخصية إلاَّ في الأحوال الآتية:

١. إذا وافق صاحب البيانات الشخصية على الإفصاح وفقاً لأحكام النظام .
٢. إذا كانت البيانات الشخصية قد جرى جمعها من مصدر متاح للعموم.
٣. إذا كانت الجهة التي تطلب الإفصاح جهة عامة، وذلك لأغراض أمنية أو لتنفيذ نظام آخر أو لاستيفاء مُتطلبات قضائية وفق الأحكام التي تحددها اللوائح .
٤. إذا كان الإفصاح ضروريًّا لحماية الصحة أو السلامة العامة أو حماية حياة فرد أو أفراد معينين أو حماية صحتهم. وتبيّن اللوائح الضوابط والإجراءات المتعلقة بذلك.
٥. إذا كان الإفصاح سيقتصر على معالجتها لاحقاً بطريقة لا تؤدي إلى معرفة هوية صاحب البيانات الشخصية أو أي فرد آخر على وجه التحديد. وتبيّن اللوائح الضوابط والإجراءات المتعلقة بذلك .

وبناءً على ما سبق فإن عدم المحافظة على البيانات الشخصية أو الإفصاح عنها أو معالجتها أو اتخاذ أي إجراء من شأنه المساس بها دون موافقة صاحب الشأن يعتبر جريمة حدد لها النظام السعود العقاب في المادة الخامسة والثلاثين منه بقوله "مع عدم الإخلال بأي عقوبة أشد منصوص عليها في نظام آخر، تكون عقوبة ارتكاب المخالفات الآتية وفقاً لما دون أمامها :

أ-كل من أفصح عن بيانات حساسة أو نشرها مخالفًا أحكام النظام: يعاقب بالسجن مدة لا تزيد على (سنتين) وبغرامة لا تزيد على (ثلاثة ملايين) ريال، أو بإحدى هاتين العقوبتين؛ إذا كان ذلك بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية .ب-كل من خالف أحكام المادة (التاسعة والعشرين) من النظام، وهي الخاصة بعدم جواز نقل البيانات الشخصية -لجهة التحكم -إلى خارج المملكة أو الإفصاح عنها لجهة خارج المملكة إلاَّ إذا كان ذلك تنفيذاً لالتزام

بموجب اتفاقية تكون المملكة طرفاً فيه، أو لخدمة مصالح المملكة، أو لأغراض أخرى وفقاً لما تحدده اللوائح: يعاقب بالسجن مدة لا تزيد على (سنة) وبغرامة لا تزيد على (مليون) ريال، أو بإحدى هاتين العقوبتين" .

وفي نظام الجرائم الإليكترونية عَمَدَ المُنَظم السعودي إلى تجريم الوصول -دون مسوغ نظامي صحيح -إلى بيانات بنكية، أو ائتمانية، أو بيانات متعلقة بملكية أوراق مالية للحصول على بيانات، أو معلومات، أو أموال، أو ما تتيحه من خدمات، وحدد العقاب على ذلك الفعل بالسجن مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مليوني ريال، أو بإحدى هاتين العقوبتين.

وتعتبر جريمة تجريم الوصول دون مسوغ نظامي صحيح إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية من الجرائم شديدة الخطورة التي تضرب الخصوصية فضلاً عن تهديد الأمن المالي عامة وركنها المادي يتكون من مجموعة من الأفعال المحددة وتشكل الأساس القانوني للجريمة، ذلك أن الركن المادي للجريمة يتعلق بمادياتها ومن ثم فإن عناصره الثلاثة من سلوك ونتيجة ورابطة السببية خاصة بماديات الجريمة فضلاً عن مظاهره من شروع ومساهمة ولذا فإن الركن المادي في حالة جريمة الوصول إلى بيانات بنكية أو ائتمانية أو بيانات متعلقة بملكية أوراق مالية دون مسوغ نظامي صحيح، يتضمن الركن المادي العناصر التالية:

الدخول غير المصرح به إلي أن يتم الوصول إلي البيانات أو المعلومات المحمية مثل بيانات حسابات بنكية أو ائتمانية أو معلومات أوراق مالية، دون الحصول على إذن قانوني أو تفويض من الجهات المسؤولة، علي أن يكون ذلك الوصول قد تم باستخدام وسائل أو تقنيات غير قانونية لتجاوز الحماية أو الأمان المطبق على البيانات ، ومن خلال استخدام **التقنيات والأدوات** الإليكترونية ومنها القرصنة الإلكترونية، البرمجيات الخبيثة، أو حتى الأساليب التقليدية مثل التلاعب البشري للحصول على معلومات تسجيل الدخول، ومن المعلوم أن الهدف الرئيسي الحصول على بيانات أو معلومات أو أموال أو خدمات بشكل غير قانوني، وهذا يمكن أن يكون لغرض السرقة، الاحتيال، أو التلاعب المالي، وبناء عليه فإن الركن المعنوي هنا متوفر أعني أن الجريمة عمدية والقصد الجنائي بعنصرية العلم والإرادة متوفر إذ لا يعقل أن من يعمل علي

الدخول إلي تلك المنصات الإليكترونية للحصول علي المعلومات البنكية المطلوبة غير مدرك لما يفعل أو غير عالم بتجريم ذلك الفعل أنه فعل غير مشروع.

الفرع الثالث

المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإليكترونية

مرسوم بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١ بشأن حماية البيانات الشخصية

استهل القانون الاتحادي بشأن حماية البيانات الشخصية رقم (٤٥) لسنة ٢٠٢١ ببيان ماهية البيانات عامة مبيناً أنها مجموعة منظمة أو غير منظمة من المعطيات، أو الوقائع أو المفاهيم أو التعليمات أو المشاهدات أو القياسات تكون على شكل أرقام أو حروف وكلمات 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، وتشمل المعلومات أينما وردت في هذا المرسوم بقانون .

ثم قام بتحديد تعريف للبيانات الشخصية بقوله إنها 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 الإليكتروني الخاص به، أو موقعه الجغرافي، أو صفة أو أكثر من صفاته الشكلية أو الفسيولوجية، أو الاقتصادية، أو الثقافية، أو الاجتماعية، وتشمل البيانات الشخصية الحساسة والبيانات الحيوية البيومترية.

ثم تحدث عن أمن البيانات الشخصية موضحاً أنها مجموعة من التدابير والإجراءات والعمليات التقنية والتنظيمية المحددة وفق المرسوم بقانون التي من شأنها الحفاظ على حماية خصوصية وسرية، وسلامة، ووحدة البيانات الشخصية، وتكاملها وتوافرها.

ومن ضوابط حفظ البيانات لدى التشريعات الإماراتية أنه اشترط موافقة صاحب البيانات على المعالجة وفق ضوابط محددة مادة (٦) اسماها شروط الموافقة على معالجة البيانات إضافة إلى

إلزامه المتحكم والمعالج في معالجة البيانات بضوابط محددة لا تسمح بالاعتداء عليها فيما بعد المعالجة ولا باستخدامها في غير الأغراض المعدة من أجله مع اعطاء صاحبها الحق في تعديلها أو محوها أو غير ذلك من الإجراءات في المادتين (٧ ،٨).

ثم قام المشرع الإماراتي بالنص علي الجرائم المرتبطة بحماية البيانات والخاصة بتطبيقات الذكاء الاصطناعي من خلال قانون مكافحة الشائعات والجرائم الإليكترونية رقم (٣٤) لسنة ٢٠٢١ ومحددا العقوبات الخاصة بها من خلال الجرائم الواقعة علي تقنية المعلومات كالاختراق الإليكتروني واختراق المظلة المعلوماتية الخاصة بمؤسسات الدولة والاعتداء علي البيانات والمعلومات الشخصية والبيانات والمعلومات الحكومية وغيرها من الجرائم ، وكلها تحتاج إلي بحث مستقل خاص بحماية البيانات الشخصية والحكومية في التشريعات العربية مقارنة بتشريع الاتحاد الأوربي إن شاء الله تعالي .

المطلب الثاني

أهم التشريعات الأجنبية

اللائحة الأوربية لحماية البيانات الشخصية

المطبقة من الاتحاد الأوربي والصادرة عام ٢٠١٦ والمنفذة اعتباراً من ٢٠١٨

تعتبر "اللائحة العامة لحماية البيانات الشخصية GDPR" المطبقة من الاتحاد الأوروبي والذي صدر عام ٢٠١٦ وبدأ تنفيذه عام ٢٠١٨، من أفضل القوانين في العالم لحماية البيانات الشخصية، بل وميزان للحكم على نجاح أي قانون يتعلق بالبيانات.

ولقد قامت بتعريف البيانات بقولها " بغرض هذا اللائحة: (١) يعنى "البيانات الشخصية " أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد "المعني بالبيانات" الشخص الطبيعي القابل للتحديد هو الشخص الذي يمكن تحديده مباشرة أو غير مباشر، ولا سيما من خلال

الإشارة إلى معرف مثل الاسم، أو رقم التعريف، أو بيانات الموقع، أو معرف عبر الإنترنت، أو عوامل أخرى محددة تتعلق بالجسم أو الفسيولوجيا"(٣١).

كما أوضحت الحقوق الواجب إعطائها لصاحب البيانات وهي بنصها على أن يعطي هذا القانون صاحب البيانات الحق في عدة أمور مهمة منها:

- **الحق في أخذ موافقة صريحة منه قبل جمع بياناته واستخدامها في المادة (٦)** منها التي نصت على أن يكون معالجة البيانات قانونية فقط إذا وفقًا للظروف التالية: (أ) قدم المعني بالبيانات موافقته على معالجة بياناته الشخصية لأغراض محددة أو أكثر. (ب) تكون المعالجة ضرورية لأداء عقد يكون المعني بالبيانات طرفًا فيه أو لاتخاذ خطوات بناءً على طلب المعني بالبيانات قبل دخول مثل هذا العقد. (ج) تكون المعالجة ضرورية للامتثال لالتزام قانوني يلزم المسؤول عن المعالجة به. (د) تكون المعالجة ضرورية لحماية مصالح المعني بالبيانات أو مصالح شخص طبيعي آخر. (هـ) تكون المعالجة ضرورية لأداء مهمة تُنفذ في مصلحة عامة أو في ممارسة السلطة الرسمية المخولة للمسؤول عن المعالجة. (و) تكون المعالجة ضرورية لأغراض المصالح المشروعة التي يسعى المسؤول عن المعالجة أو طرف ثالث لتحقيقها" (٣٢).

)31("For the purposes of this Regulation: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological,

)32 (**Article 6 - Lawfulness of processing**

- "1. 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 such a contract; (c) processing is necessary for compliance with a legal obligation to

- الحق في الحصول على المعلومات التي يحتاجها من مراقب البيانات، ومنها معرفة الغرض من المعالجة، والفترة المتوقعة لتخزين البيانات وذلك كما وردت في المادة (١٥) منها يكون للمعني بالبيانات الحق في الحصول من المسؤول عن المعالجة على تأكيد ما إذا كانت البيانات الشخصية المتعلقة به تُعالج أم لا، وفي حالة التعامل معها، الحصول على البيانات الشخصية والمعلومات التالية: (أ) أغراض المعالجة. (ب) فئات البيانات الشخصية المعنية. (ج) المستلمين أو فئات المستلمين الذين تم الكشف عن البيانات الشخصية لهم أو سيتم الكشف عنهم، ولا سيما المستلمين في البلدان الثالثة أو المنظمات الدولية. (د) حيثما أمكن، المدة المتوقعة التي ستتم فيها تخزين البيانات الشخصية، أو إذا لم يكن ذلك ممكنًا، المعايير المستخدمة لتحديد تلك المدة. (هـ) وجود الحق في طلب تصحيح أو حذف البيانات الشخصية أو تقييد معالجة البيانات الشخصية المتعلقة بالمعني بالبيانات أو الاعتراض على مثل هذه المعالجة. (و) الحق في تقديم شكوى إلى السلطة الإشرافية. (ز) حيث لم يتم جمع البيانات الشخصية من المعني بالبيانات، أي معلومات متاحة عن مصدرها" (٣٣).

---

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.".

(33 (**Article 15 - Right of access by the data subject**

- "1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organizations; (d) where possible, the envisaged period

- الحق في تصحيح البيانات غير الدقيقة المتعلقة به، وإكمال البيانات الشخصية غير المكتملة وذلك كما وردت في المادة (١٦) منها يحق للموضوع البيانات أن يحصل من المسؤول عن المعالجة على تصحيح البيانات الشخصية غير الدقيقة المتعلقة به دون تأخير غير مبرر، ومع الأخذ في الاعتبار أغراض المعالجة، يحق للموضوع البيانات أن يُكمل البيانات الشخصية غير الكاملة، بما في ذلك من خلال تقديم بيان إضافي (٣٤).

- الحق في مسح بياناته الشخصية Right to be forgotten وذلك كما وردت في المادة رقم (١٧) منها يحق للموضوع البيانات أن يحصل من المسؤول عن المعالجة على محو البيانات الشخصية المتعلقة به دون تأخير غير مبرر، ويكون المسؤول عن المعالجة ملزماً بمحو البيانات الشخصية دون تأخير غير مبرر عندما ينطبق أحد الأسباب التالية أ- البيانات الشخصية لم تعد ضرورية بالنسبة للأغراض التي جُمعت أو عُولجت من أجلها؛ب- سحب الموضوع البيانات للموافقة التي تعتمد عليها المعالجة وفقًا للفقرة (أ) من المادة ٦(١)، وعدم وجود أساس قانوني آخر للمعالجة؛ (ج) الاعتراض على المعالجة وفقًا للمادة ٢١(١) وعدم وجود أسباب مشروعة تبرر المعالجة، أو الاعتراض على المعالجة وفقًا للمادة ٢١(٢)؛ (د) البيانات

---

for which the personal data will be stored, or, if not possible, the criteria used to determine that period; (e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing; (f) the right to lodge a complaint with a supervisory authority; (g) where the personal data are not collected from the data subject, any available information as to their source.".

)34 (**Article 16 - Right to rectification**

- "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

الشخصية قد تمت معالجتها بطريقة غير قانونية،(هـ) البيانات الشخصية يجب محوها للامتثال لالتزام قانوني بموجب قوانين الاتحاد أو قوانين الدولة العضو التي يخضع لها المسؤول عن المعالجة؛ (و)البيانات الشخصية جُمعت فيما يتعلق بعرض خدمات المعلومات الاجتماعية المشار إليها في المادة ٨".(٣٥).

- الحق في الاعتراض، في أي وقت على معالجة البيانات الشخصية المتعلقة به، وبناءً على تلك الأحكام لن يقوم المراقب بمعالجة البيانات الشخصية ما لم يُوضح أسبابًا مشروعة ومقنعة للمعالجة تتجاوز مصالح وحقوق وحريات صاحب البيانات وذلك كما وردت في المادة (٢١): **منها** يحق لصاحب البيانات الاعتراض، بناءً على أسباب تتعلق بوضعه الخاص، في أي وقت على معالجة البيانات الشخصية المتعلقة به والتي تعتمد على النقطة (هـ) أو (و) من المادة ٦(١)، بما في ذلك التوصيف (التحليل الشخصي) بناءً على هذه الأحكام، لا يجوز للمسؤول عن المعالجة أن يستمر في معالجة البيانات الشخصية إلا إذا أثبت المسؤول عن المعالجة وجود

)35) **Article 17 - Right to erasure (‘right to be forgotten’)**

- "1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), and where there is no other legal ground for the processing; (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); (d) the personal data have been unlawfully processed; (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; (f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)."

أسباب مشروعة قوية تبرر المعالجة وتفوق مصالح وحقوق وحريات الموضوع البيانات، أو لأغراض إثبات الحقوق القانونية أو ممارستها أو الدفاع عنها (٣٦).

- الحق في تقديم شكوى إلى سلطة إشرافية، في الدولة العضو التي يُقيم فيها إذا كان يعتبر أن معالجة البيانات الشخصية المتعلقة به تنتهك اللوائح وذلك كما وردت في المادة (77) منها بدون المساس بأي إجراء إداري أو قضائي آخر، يحق لكل معني بالبيانات تقديم شكوى إلى السلطة الإشرافية، ولا سيما في الدولة العضوية التي يقيم فيها بشكل عادي، أو في مكان عمله، أو في مكان الانتهاك المزعوم إذا اعتبر المعني بالبيانات أن معالجة البيانات الشخصية المتعلقة به ينتهك هذا اللائحة .تُبلغ السلطة الإشرافية التي تم تقديم الشكوى إليها المشتكي عن تقدم الشكوى ونتيجتها، بما في ذلك إمكانية اللجوء إلى الإجراءات القضائية وفقًا للمادة ٧٨(٣٧).

---

(36)**Article 21 - Right to object**

- "1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims."

)37(**Article 77 - Right to lodge a complaint with a supervisory authority**

- "1. Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement if the data subject considers that the processing of personal data relating to him or her infringes this Regulation."

.

وبناءً علي تلك النصوص فإن اللائحة الأوربية للبيانات الشخصية نصت علي عدد من العقوبات المترتبة علي الاعتداء علي البيانات الشخصية ومن ثم فإن المبادئ المتعلقة بالبيانات والحقوق المترتبة عليها تدخل في مجال النصوص الجنائية التى يترتب علي عدم اتباعها استحقاق العقاب المترتب عليها ومن هذه العقوبات الغرامات الإدارية المنصوص عليها في المادة ٨٣ بقولها:

١-يجب على كل سلطة رقابية أن تضمن أن فرض الغرامات الإدارية في كل حالة فردية يكون فعّالًا ومتناسبًا ومرهِّبًا. يمكن فرض الغرامات الإدارية بالإضافة إلى أو بدلاً من التدابير المشار إليها في المادة ٥٨ (٢) (أ) إلى (ه).

٢. لا يجوز أن تتجاوز الغرامات الإدارية:

(أ) ١٠ ملايين يورو، أو، في حالة الشركة، ما يصل إلى ٢٪ من إجمالي دورانها السنوي للسنة المالية السابقة، أيهما أعلى، لانتهاك الأحكام التالية: (أ) التزامات المسؤول والمعالج وفقًا للمواد ٨ و١١ و٢٥ إلى ٣٩، (ب) التزامات هيئة الشهادة وفقًا للمواد ٤٢ و٤٣، (ج) التزامات هيئة المراقبة وفقًا للمادة ٤١ (٤)، (د) التزامات وفقًا للمادة ٥٥ و٥٦.

(ب) ٢٠ مليون يورو، أو ما يصل إلى ٤٪ من إجمالي دوران السنة المالية السابقة، أيهما أعلى، لانتهاك الأحكام التالية: (أ) المبادئ الأساسية للمعالجة، بما في ذلك شروط الموافقة (المواد ٥ و٦ و٧ و٩)، (ب) حقوق الأفراد المعنيين بالبيانات (المواد ١٢ إلى ٢٢)، (ج) نقل البيانات الشخصية إلى مستلم في بلد ثالث أو منظمة دولية (المواد ٤٤ إلى ٤٩)، (د) أي التزامات وفقًا لقانون الدولة العضو المعتمد بموجب هذا اللائحة، بما في ذلك الأحكام المتعلقة بحالات المعالجة المحددة. التدابير الإضافية:

٣-بالإضافة إلى الغرامات الإدارية، يمكن للسلطة الرقابية أن تفرض تدابير تصحيحية أخرى، مثل أمر تعليق عمليات المعالجة أو فرض الامتثال لحقوق المعنيين بالبيانات". (٣٨).

)38(Article 83 - General conditions for imposing administrative fines

Administrative fines:

1. "1. Each supervisory authority shall ensure that the imposition of administrative fines is in each individual case effective, proportionate, and dissuasive. Administrative fines may be imposed in addition to, or instead of, the measures referred to in Article 58(2) (a) to (h).
2. 2. The administrative fines shall not exceed:

(a) 10 million EUR, or, in the case of an undertaking, up to 2% of its total annual turnover of the preceding financial year, whichever is higher, for infringements of the following provisions:

- (i) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39,
- (ii) the obligations of the certification body pursuant to Articles 42 and 43,
- (iii) the obligations of the monitoring body pursuant to Article 41(4),
- (iv) the obligations pursuant to Article 55 and 56.

(b) 20 million EUR, or up to 4% of the total annual turnover of the preceding financial year, whichever is higher, for infringements of the following provisions:

(i) the basic principles for processing, including conditions for consent (Articles 5, 6, 7, and 9)

(ii) the data subject's rights (Articles 12 to 22),

(iii) the transfer of personal data to a recipient in a third country or an international organisation (Articles 44 to 49),

(iv) any obligations pursuant to Member State law adopted under this Regulation, including provisions relating to specific processing situations.

Additional measures:

ثم تحدثت عن العقوبات الأخرى وأهمها العقوبات الجزائية التي يجب أن تكون مُرهِبَة على حد وصفها بقولها في المادة ٨٤ "يتعين على الدول الأعضاء وضع القواعد المتعلقة بالعقوبات الأخرى، بما في ذلك العقوبات الجنائية، التي تنطبق على انتهاكات هذه اللائحة، واتخاذ جميع التدابير اللازمة لضمان تنفيذها"(٣٩).

وبناءً علي ما سبق فإن البيانات الشخصية عامة والمتعلقة بتطبيقات الذكاء الاصطناعي خاصة من الأهم الأمور الواجب حمايتها عندما نتطرق إلي التعامل مع تطبيقات الذكاء حماية للحقوق والحريات المترتبة عليها فضلاً عن عدم جواز الاعتداء عليها باستغلالها عن طريق معالجتها أو محوها أو نقلها أو تصحيحا أو محوها أو اتخاذ أي إجراء بشأنها مالم يكن هناك موافقة صريحة أو بالأحرى إذن من صاحبها وإلا لأضحت الأمور في غير نصابها وترتب علي ذلك الاعتداء فرصة لاستغلال تطبيقات الذكاء الاصطناعي للوصول إلي البيانات الشخصية للأفراد وانتهاكها وهو الأمر المرفوض عالمياً ، وأياً ما يكن من أمر فإن هناك توجه عالمي بإصدار التشريعات التي تنص علي حماية تلك البيانات الشخصية عامة والمتعلقة بتطبيقات الذكاء الاصطناعي في مختلف مجالاته خاصة أن تلك البيانات في مختلف المجالات يتم التعامل معها يومياً من خلال تطبيقات الذكاء الاصطناعي في المجالات الصحية والهندسية والحرفية

"3. In addition to the administrative fines, the supervisory authority may impose other corrective measures, such as ordering the suspension of processing operations or enforcing compliance with data subject rights."

(39) Article 84 - Penalties

1. National enforcement measures:

- "1. Member States shall lay down the rules on other penalties, including criminal penalties that apply to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented."

.

والقانونية وغيرها في شتى فروع العلم والمعرفة التي دخلها أو بمعني أوضح غزاها الذكاء الاصطناعي .

الخاتمة:

وختاماً لهذه الدراسة نقول ها نحن قد انتهينا-بعون الله وتوفيقه -من هذا البحث المتعلق بـ " التشريعات الجنائية المتعلقة بحماية بيانات الذكاء الاصطناعي "دراسة مقارنة" والذي تم تقسيمه إلى مقدمة ومبحثين وخاتمة تم الانتهاء فيه إلى النتائج الرئيسية التالية.

نتائج البحث:

أن الذكاء الاصطناعي ما هو إلا نوع من أنواع التكنولوجيا المتقدمة يتم من خلالها تصنيع تطبيقات في صورة أجهزة بأشكال متعددة وبمسميات مختلفة وتقوم بالأعمال التي يقوم بها البشر علي اختلاف أنماطها كالأعمال اليدوية والأعمال التي تحتاج إلي فكر متقدم كالجراحات المتعمقة أو الرسوم الهندسية المتطورة وغير ذلك.

يتدخل الذكاء الاصطناعي في كافة المجالات المختلفة والمتعددة ومن أهمها القضاء والتحقيق الجنائي والقطاع التعليمي، والقطاع المصرفي والقطاع الاقتصادي والقطاع الصحي وغيرها من القطاعات.

ومن المعلوم أن الذكاء الاصطناعي في كافة تطبيقاته ومجالاته إنما يتم وفق البيانات المرتبطة به حيث يتم تجميع البيانات المحملة عليه وتحليلها للوصول من ورائها إلى القرارات التي تتخذ، وهو الأمر الذي قد يترتب عليه اختراق تلك البيانات وبالتالي التعدي على الحقوق الخاصة بها.

يتدخل المشرع الجنائي لحماية البيانات المتعلقة بتطبيقات الذكاء الاصطناعي لعدة دوافع هامة، تتعلق بالضمانات الأمنية والقانونية اللازمة للتعامل مع التكنولوجيا المتطورة وتأثيرها على الأفراد والمجتمع، ومن أهم هذه الدوافع والمصالح الهامة التي تؤدى إلى التدخل من قبل الشارع الجنائي لحمايتها من خلال تجريم الاعتداءات على البيانات المتعلقة بتطبيقات الذكاء الاصطناعي.

ويهدف المشرع الجنائي من تجريمه لأفعال الاعتداء على البيانات المتعلقة بتطبيقات الذكاء الاصطناعي حماية الحقوق والحريات الخاصة بالأفراد وكذلك حماية من الهجمات السيبرانية التى تتضمن اعتداءات سافرة على الأفراد، وحماية النزاهة والشفافية المرتبطة بتلك البيانات، ومن ثم حماية القيم الأخلاقية ولذا يسعى المشرع الجنائي إلى تجريم الاعتداءات على البيانات الخاصة بتطبيقات الذكاء الاصطناعي.

يُعَدُّ الحق في الخصوصية أحد أهم الحقوق الأساسية التي تَضمن للأفراد حماية بياناتهم الشخصية ضمن تطبيقات الذكاء الاصطناعي، كما في أنظمة التعرف على الوجه وتحليل البيانات الكبيرة، حيث يكون هناك مخزون كبير بل وكميات هائلة من المعلومات الشخصية، مما يعرضها لمخاطر كبيرة من حيث الاختراق والتسريب، ومن ثم يُعتبر ضمن حق الخصوصية حق الأفراد في التحكم بمعلوماتهم الشخصية والاحتفاظ بها سرية، ويتضمن ذلك الحق في عدم الكشف عن المعلومات الشخصية دون موافقة الأفراد وما يقال بشأن الحق في الخصوصية يُعتبر أيضاً بشأن الحق في التصويب والحق في الحصول على البيانات والحق في الحذف والاعتراض، فضلاً عن الحق في الأمان الرقمي للبيانات.

وبعد التعرف علي أهم الحقوق والحريات الخاصة بالبيانات كان من الواجب التنبيه علي ضرورة التصدي من قبل الشارع لحمايتها ، حيث وجب التنويه إلي أن البيانات الشخصية مَحْمية ومحظور التعرض لها والاستيلاء عليها ومعالجتها أو تخزينها أو تداولها بدون إذن من أصحابها، ومن ثم يتدخل التشريع الجنائي لحمايتها، إذ الحماية تعني عدم الاعتداء وهي إما ذاتية أو تشريعية ، والذاتية تكون من داخل النفس البشرية التي وصفها خالقها بأنها أمارة بالسوء وربطها علماء علم النفس بالرقابة الذاتية الداخلية للإنسان وإلا كانت الحماية من خلال النصوص القانونية التي تجرم الاعتداء علي تلك البيانات بشتي الصور وتضع العقوبات الرادعة في هذا الشأن.

أما التشريعات التي أُخِذت كمثال لدراسة اهتمامها بتجريم أي اعتداء يقع على البيانات الشخصية من خلال المشرع المصري قانون مكافحة الجرائم الإليكترونية وجرائم تكنولوجيا

المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ والقانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية

ومن التشريعات السعودية نظام حماية البيانات الشخصية في المملكة العربية السعودية الصادر بالمرسوم الملكي رقم ١٩ بتاريخ ١٤٤٣/٢/٩ ونظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم ١٧ بتاريخ ١٤٢٨/٣/٨

وفي التشريعات الإماراتية المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإليكترونية والمرسوم بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١ بشأن حماية البيانات الشخصية

ومن التشريعات الأجنبية تم الاكتفاء بقراءة "اللائحة العامة لحماية البيانات الشخصية GDPR" المطبقة من الاتحاد الأوروبي والذي صدر عام ٢٠١٦ وبدأ تنفيذه عام ٢٠١٨، باعتبارها من أفضل القوانين في العالم لحماية البيانات الشخصية، بل وميزان للحكم على نجاح أي قانون يتعلق بالبيانات.

التوصيات:

ولننتهي إلي توصية عامة تتعلق بضرورة تدخل المشرع الجنائي لحماية البيانات الشخصية علي وجه الخصوص والبيانات الحكومية أو الدولية من الاعتداء عليها أثناء استخدام أي من تطبيقات الذكاء الاصطناعي انطلاقا من ضرورة حماية البيانات وعدم جواز تركها تحت وطئت مستخدمي تطبيقات الذكاء الاصطناعي عامة ، خاصة وأن العالم مقبل علي طفرة هائلة من تطبيقات الذكاء الاصطناعي في مختلف المجالات والتي سيترتب عليها إدخال بيانات لا حصر لها للاستخدام من خلال تلك التطبيقات وهو الأمر الذى قد يؤدى إلي استغلال هذه البيانات أسوء الاستغلال فضلاً عن سهولة اختراقها والاعتداء عليها بمعالجتها أو حذفها أو تزييفها أو غير ذلك من الممارسات غير القانونية والمُمَنهجة ولا يكون الهدف منها إلا في القضاء عليها أو استغلالها لمصلحة المعالج أو المتحكم أو من له القدرة علي الوصول إليها عامة.

وبعد:

فإني أحمد الله حمداً كثيراً، وأشكره شكراً جزيلاً، بما منح من الجهد، والوقت، والفهم، والمراجع، ما أعانني به على بلوغ الهدف الذي كنت أصبوا إليه، وأمدني بالصبر على القراءة والاطلاع في موضوع (التشريعات الجنائية المتعلقة بحماية البيانات الشخصية الخاصة بتطبيقات الذكاء الاصطناعي-دراسة مقارنة) واسأله سبحانه المغفرة فيما أكون قد قصرت فيما قدمته في هذه الدراسة.

اللهم إن هذا بحثي قد ضمنته رأيي، وحسبي أني بذلت الجهد لإدراك جانباً من الحق الذي يتسم به الخير أو بعضه، فإن كنت قد وفقت، فمن توفيقك المحض، وإن كانت الأخرى فمن نفسي و الشيطان أعوذ بك ربي منه (**وَمَا أُبَرِّئُ نَفْسِي إِنَّ النَّفْسَ لَأَمَّارَةٌ بِالسُّوءِ إِلَّا مَا رَحِمَ رَبِّي إِنَّ رَبِّي غَفُورٌ رَّحِيمٌ**)، وحسبي أني بذلت الجهد، وأدمت النظر، وأمعنت التفكير، فإن لم أنل أجر المجتهد المصيب فحسبي أجر المجتهد المخطئ، ومن الله وحده العون والتوفيق والسداد، وصلى اللهم على سيدنا محمد وعلى آله وصحبه وسلم، وأخر دعوانا أن الحمد لله رب العالمين.

المراجع:

عادل الأبياري:" الذكاء الاصطناعي: الأسس والمبادئ " دار صفاء للنشر، ٢٠١٩.

حسام الدين الحسن:" الذكاء الاصطناعي وتطبيقاته في العالم العربي" مركز دراسات الشرق الأوسط، ٢٠٢١.

حسن عبد الله:" النظرية العامة للعقوبات في القانون الجنائي" طبعة عام ٢٠١٥ الناشر دار النهضة العربية.

محمد البرادعي:" الجرائم الاقتصادية في القانون الجنائي" طبعة عام ٢٠١٧ الناشر دار الثقافة.

محمد البرادعي "حماية البيانات الشخصية في عصر التكنولوجيا الحديثة " طبعة ٢٠١٨ الناشردار الثقافة.

محمد البرادعي:" الأمن السيبراني وتطبيقات الذكاء الاصطناعي" طبعة عام ٢٠١٩ الناشر دار الثقافة.

سامي الزغبي:" مبادئ قانون العقوبات" طبعة عام ٢٠١٩ مطبعة جامعة القاهرة.

فوزي العمري:" أثر الجرائم الاقتصادية على التنمية الاقتصادية" طبعة عام ٢٠١٦ الناشر دار الشروق، ٢٠١٦.

عبد الرحمن التميمي:" الجرائم الإلكترونية وحماية البيانات الشخصية" طبعة عان ٢٠٢٠، الناشردار النهضة العربية.

سليمان الحميدي:"حماية البيانات في ظل التقنيات الحديثة" طبعة عام ٢٠٢١ الناشردار الشروق.

محمد علي عثمان:" حماية البيانات الشخصية في القانون العربي: دراسة مقارنة" طبعة عام ٢٠٢٠ الناشر دار النشر العربية .

أحمد علي محمد:"قانون حماية البيانات الشخصية: دراسة تحليلية" طبعة عام ٢٠١٩ الناشر دار الثقافة للنشر والتوزيع .

يوسف محمود: "حقوق الأفراد في حماية البيانات الشخصية في القانون الدولي والقوانين الوطنية"طبعة عام ٢٠١٨ الناشر دار الكتاب الجامعي .

عادل عبد الله :"الأمن المعلوماتي وحماية البيانات الشخصية: تحديات وحلول" طبعة عام ٢٠٢١ الناشر: مركز دراسات الوحدة العربية .

سلوى عبد الرحمن :"حماية البيانات الشخصية في العصر الرقمي: الإطار القانوني والتحديات" طبعة عام ٢٠٢٢ الناشر دار النهضة العربية.

بشاير عبد الله :" تقنيات الذكاء الاصطناعي في تحسين خدمة العملاء" رابط المقال

https://triggers.sa/ar/blog/%D9%81%D9%88%D8%A7%D8%A6%D8%AF-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A/

مقال بعنوان ما المقصود بالروبرت " والرابط هو https://aws.amazon.com/ar/what-is/bot/

مقال بعنوان " مالمقصود بالشبكات العصبونية " رابط https://aws.amazon.com/ar/what-is/neural-network/

سهير القرناوى:" الحق في الخصوصية كحق من حقوق الإنسان" مقال على شبكة الانترنت بموقع موضوع الاطلاع بتاريخ ٢٠٢٤/٨/١ والرابط:

https://mawdoo3.com/%D8%A7%D9%84%D8%AD%D9%82_%D9%81%D9%8A_%D8%A7%D9%84%D8%AE%D8%B5%D9%88%D8%B5%D9%8A%D8%A9_%D9%83%D8%AD%D9%82_%D9%85%D9%86_%D8%AD%D9%82%D9%88%D9%82_%D8%A7%D9%84%D8%A5%D9%86%D8%B3%D8%A7%D9%86#cite_note-e8eb1927_4f88_4ee8_8c34_21294958fc9d-1

قانون مكافحة الجرائم الإليكترونية وجرائم تكنولوجيا المعلومات المصرى رقم ١٧٥ لسنة ٢٠١٨ .

القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية.

نظام حماية البيانات الشخصية في المملكة العربية السعودية الصادر بالمرسوم الملكي رقم ١٩ بتاريخ ١٤٤٣/٢/٩ .

نظام مكافحة الجرائم المعلوماتية الصادر بالمرسوم الملكي رقم ١٧ بتاريخ ١٤٢٨/٣/٨.

المرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإليكترونية.

المرسوم بقانون اتحادي رقم (٤٥) لسنة ٢٠٢١ بشأن حماية البيانات الشخصية.

"اللائحة العامة لحماية البيانات الشخصية GDPR" المطبقة من الإتحاد الأوروبي والذي صدر عام ٢٠١٦ وبدأ تنفيذه عام ٢٠١٨.والرابط هو

https://eur-lex.europa.eu/eli/reg/2016/679/oj

Stuart Russell and Peter Norvig، Artificial Intelligence: A Modern Approach*, 4th ed. (Pearson, 2020).*

David Poole and Alan Mack worth, Artificial Intelligence: Foundations of Computational Agents (Cambridge University Press, 2017).

Wolfgang Ertel, Introduction to Artificial Intelligence (Springer, 2018).

Shladover, S., & Sweat man, P. C. *Autonomous Vehicles: The Road to Self-Driving Cars*. Cambridge University Press, 2020.

Ian Good fellow, Joshua Bagnio, and Aaron Carville, Deep Learning (2016: MIT Press)

Ethem Alpaydin, Introduction to Machine Learning (2020: MIT Press).

Haykin, Simon S. Neural Networks and Learning Machines. 3rd ed., Pearson, 2009.

Siciliano, Bruno, and Lorenzo Sciavicco. Robotics: Modelling, Planning and Control. Springer, 2009.

Dressler, Joshua. Understanding Criminal Law. LexisNexis, 2022

Hart, H.L.A. Punishment and Responsibility: Essays in the Philosophy of Law. Oxford University Press, 2008.

Robinson, Paul H. Criminal Law: Doctrine, Application, and Practice. Aspen Publishers 2021.

Semester, A.P., and Sullivan, G.R. Criminal Law: Theory and Doctrine. Hart Publishing, 2018. P.8.

Solove, Daniel J. Understanding Privacy. Harvard University Press, 2022.

Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Public Affairs, 2019.

Miller, Claire Cain. Data and Privacy: The New Challenges. Oxford University Press, 2021.

Schneider, Bruce. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W.W. Norton & Company, 2015.

Jay, Rosemary. Privacy and Data Protection Law. *2012.* Oxford University Press.

De Hart, Paul. The Right to Privacy in the Digital Age. *2019.* Routledge.

David Wright:" Data Protection and Privacy: The Age of Intelligent Machines. 2017. Springer.

Helen Nissenbaum: Data Privacy and Security. 2018. Stanford University Press. P 45.