الحماية القانونية للبيانات الشخصية في النظامين السعودي والعماني (دراسة مقارنة)

الدكتور/ ماهر إبراهيم عبيد إمام*[١]
مشاري محمد عمر الحربي* [٢]
الدكتور/ حسين بن سعيد بن سيف الغافري*[٣]

الملخص:

ترتكز هذه الورقة على فكرة، الحماية القانونية للبيانات الشخصية في النظامين السعودي والعُماني، دراسة مقارنة، وهي فكرة تأتي أهميتها لكونها تناقش موضوع غاية في الحساسية، يتوقف عليه حماية خصوصية الناس وأسرارهم وبياناتهم الشخصية من الاختراق والتعدي، وذلك من خلال آليات تسنها الدول وتمدها بما هو لازم للقيام بهذا الدور، وقد تبني المشرعين العُماني والسعودي قوانين من أجل ايجاد حماية فاعلة للبيانات الشخصية هما قانون حماية البيانات الشخصية العُماني لسنة ٢٠٢٢م ونظام حماية البيانات الشخصية السعودي الصادر ١٤٤٣هـ، وتناقش الورقة العلمية الحق في الخصوصية ومفهومه القانوني والدستوري وعلاقته بحماية البيانات الشخصية، علاوة على ذلك تناقش الورقة مفهوم البيانات الشخصية والحماية الدستورية والجنائية لها و آليات الحماية والجهات المنوط بها القيام بهذا الدور وتشكيلها وتنظيمها، وتهدف هذه الورقة العلمية لتسليط الضوء على مفهوم حماية البيانات الشخصية وذلك من خلال تحديد ماهية هذه البيانات وأنواعها وحقوق والتزامات صاحب البيانات الشخصية والجهات التي لها علاقة بهذه البيانات والجهات المسؤولة من الحماية كما تهدف الورقة إلى مناقشة الحماية الدستورية والجنائية للبيانات الشخصية من خلال النصوص الواردة في الدساتير والقوانين الخاصة بحماية البيانات الشخصية ،ويتمثل نطاق هذه الورقة في دراسة حماية البيانات الشخصية في النظامين العُماني والسعودي مع مقارنة هذين النظامين مع أنظمة أخرى كل ما دعت الحاجة إلى ذلك، وسوف نتبع في هذه الورقة العلمية المنهج الوصفي و التحليلي والمقارن، توصلت الورقة العلمية لعدد من النتائج والتوصيات منها، وزارة أو هيئة الاتصالات هي أهم آلية لتنفيذ قانون حماية البيانات الشخصية، وتوصي بضرورة ايجاد نص على حماية البيانات الشخصية في الدستور لبيان أهميته في أسمى قاعدة قانونية في الدولة ومن ثم ترك التفاصيل بشأنه لتنظم بواسطة التشريع العادي.

الكلمات المفتاحية: الحماية – البيانات – الشخصية – المعالج – المتحكم – الخصوصية.

---

* [١] أستاذ مساعد بقسم القانون العام – الجامعة العربية المفتوحة بسلطنة عمان – عمادة القانون.
* [٢] باحث دكتوراه في القانون بقسم القانون الجنائي – جامعة القاهرة.
* [٣] أستاذ القانون العام المساعد وعميد كلية القانون – الجامعة العربية المفتوحة بسلطنة عمان.

The Legal Protection of Personal Data In the Saudi and Omani Systems (A Comparative Study)

Dr. Maher Ibrahim Ebed Emam*1
Mashare Mohmmed Omar Alharbi*2
Dr. Hussain Said Saif Al-Ghafri*3

Abstract:

This paper is based on the idea of the legal protection of personal data in the Saudi and Omani systems, a comparative study. This is an idea whose importance comes because it discusses a very sensitive topic, on which depends the protection of people's privacy, secrets, and personal data from penetration and infringement, through mechanisms enacted by states and provided with what is It is necessary to fulfill this role. Omani and Saudi legislators have adopted laws in order to provide effective protection for personal data, namely the Omani Personal Data Protection Law of 2022 AD and the Saudi Personal Data Protection Law issued in 1443 AH. The scientific paper discusses the right to privacy, its legal and constitutional concept, and its relationship to the protection of personal data. In addition, the paper discusses the concept of personal data, its constitutional and criminal protection, protection mechanisms, and the bodies entrusted with carrying out this role, forming and organizing them. This scientific paper aims to shed light on the concept of protecting personal data. By defining the nature of this data, its types, the rights and obligations of the personal data owner, the parties related to this data, and the parties responsible for protection. The paper also aims to discuss the constitutional and criminal protection of personal data through the texts contained in the constitutions and laws related to the protection of personal data.

The scope of this paper is to study the protection of personal data in the Omani and Saudi systems while comparing these two systems with other systems whenever necessary. In this scientific paper, we will follow the descriptive, analytical, and comparative approach. The scientific paper reached a number of results and recommendations, including the Ministry of... The Communications Authority is the most important mechanism for implementing the Personal Data Protection Law. It recommends the necessity of creating a provision for personal data protection in the Constitution to demonstrate its importance in the highest legal base in the country, and then leaving the details regarding it to be regulated by ordinary legislation.

Keywords: Protection - Data - Personal - Processor - Controller - Privacy.

---

*[1] Asisstant Prof., AOU, Oman
*[2] PhD Researcher at Cairo University.
*[3] Asisstant Prof., and Dean of the College of Law, AOU, Oman.

المقدمـــة

كمدخل للحديث عن حماية البيانات الشخصية طرحت مؤسسة اكسس ناو في ورقة منشورة في العام ٢٠١٨م الأسئلة التالية، هل سبق لك أن قمت بأداء الضرائب؟ أو إجراء مكالمة هاتفية؟ هل تملك هاتف ذكي؟ هل سبق لك استخدام الانترنت؟ هل لديك حساب في وسائل التواصل الاجتماعي؟ هل قمت بارتداء جهاز تعقب اللياقة البدنية؟ إذا كان الجواب هو نعم على أي من هذه الاسئلة فهذا يعني أنك كنت تتقاسم معلومات شخصية، سواء عبر الإنترنت أو خارجها،مع جهات من القطاع الخاص أو العام، بما في ذلك بعض الجهات التي لم تسمع عنها قط، وأن تقاسم البيانات الشخصية أضحى أمر منتشر على نحو متزايد في كل مكان دون استثناء بحكم استعمال المجتمعات للإنترنت، وتحميل التطبيقات المتعددة بغرض الاستفادة من عدد من الخدمات وقد أصبح تقاسم البيانات الشخصية لا يعود بالفائدة على المستخدمين فحسب، بل أيضاً على الشركات والمؤسسات والكيانات الجامعة للبيانات الشخصية علاوة على أهميته أيضاً للقيام بالواجبات الادارية وتقديم الخدمات أو التعامل مع المجتمعات اليوم، ولكن جمع البيانات الشخصية لا يخلو من المخاطر؛ لأن المعلومات الشخصية تكشف الكثير عن أصحابها، وعن أفكارهم، وحياتهم الخاصة، ولهذا الأسباب يجب أن تكون محمية،[١] وتأكيداً لخطورة البيانات الشخصية وضرورة حمايتها نسوق المثال التالي: كانت إحدى النساء في بيروت تقود سيارتها محاولة تجاهل رجل يضايقها من سيارته، بعد بضع دقائق تلقت منه مكالمة، وقبل أن تغلق الخط أخبرها الرجل بأنه يعرف عنوان بيتها، من أين حصل على هذه المعلومات؟ استخدم الرقم المكتوب على لوحة تسجيل سيارتها. فمنذ العام ٢٠١٤م في لبنان، كان بمقدور أي شخص أن يحصل على اسمك وعنوان بيتك ورقم هاتفك وبيانات شخصية

---

[١] ورقة منشورة بعنوان دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الأوربي على موقع اكسس ناو يانير ٢٠١٨م، صفحة ٢.

أخرى، مثل فصيلة دمك، بمجرد أن يدرج رقم تسجيل سيارتك في تطبيق متوفر على الهاتف الجوال[٢].

ووفقًا لدراسة جديدة نشرها الباحثان (ميركو موسوليسي) من جامعة بنجامين بارون الإيطالية، وبولوجنا من كلية لندن الجامعة البريطانية، فإن البيانات الشخصية التي تجمعها بعض التطبيقات حساسة للغاية؛ حيث استخدام الباحثان تطبيقاً قاما بتطويره بشكل خاص من أجل هذه الدراسة، وقد قام ما يصل إلى ٦٩ مشاركاً في الدراسة بتثبت التطبيق في هواتفهم لمدة أسبوعين على الأقل، بغرض معرفة كمية بيانات الموقع، والمعلومات الشخصية التي تجمعها هذه التطبيقات، وقد كانت النتائج مخيفة للغاية، فخلال هذه الفترة الزمنية، تم تتبع أكثر من ٢٠٠,٠٠٠ موقع، وحددت ما يقرب من ٢,٥٠٠ مكان، وجمعت نحو ٥,٠٠٠ عنصر من المعلومات الشخصية المتعلقة بالتركيبة السكانية والشخصية، بينما اعتقد المشاركون بحسب الدراسة أن البيانات الأكثر حساسية التي جُمعت عبر التطبيق كانت تتعلق بصحتهم ووضعهم الاجتماعي والاقتصادي وعرقهم ودينهم، وفي هذا الصدد يقول أحد الباحثين نعتقد أنه من المهم أن نظهر للمستخدمين كمية البيانات التي يتم جمعها ونوعيتها، وخاصة التي يمكن أن تجمعها التطبيقات من خلال تتبع مواقعهم الجغرافية، وعلى القدر نفسه من الأهمية بالنسبة لنا هو فهم هل المستخدمون يعتقدون أن مشاركة المعلومات مع مطوري التطبيقات أو شركات التسويق أمرًا مقبولًا أو يعدونها انتهاكًا لخصوصيتهم[٣].

ولعل السبب الرئيس في تجريم الاعتداء على البيانات الشخصية، ليس مجرد حماية تلك البيانات فحسب، بل حماية الحقوق والحريات الأساسية للأشخاص أصحاب تلك

---

[٢] مقال بعنوان عرضة للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال إفريقيا (يناير ٢٠٢١) أكسس ناو صفحة ٢ الرابط:
https://slate.com/technology/2014/05/in-lebanon-apps-let-you-get-someone-else-s-personal-info-with-ease.html

[٣] الدراسة منشورة بموقع قناة العربية بتاريخ ٢٦ فبرير ٢٠٢١م تحت عنوان البوابة العربية للأخبار التقنية.

البيانات وما صاحب ذلك من ظهور مخاطر عديدة تهدد تلك البيانات، وتمس مصلحة أصحابها، كون تلك المخاطر تبدأ في الظهور عند الوقت الذي يبدأ فيه جمع البيانات من قبل الأشخاص أو الشركات أو المؤسسات الإدارية في الدولة، ومن ثم مرحلة التعامل فيها، بل قد يتطور الأمر إلى حد الاتجار بها، وانتقالها من جهة إلى أخرى دون موافقة أصحابها، ويزيد الأمر خطورة وتعقيد عند فقدان تلك البيانات من الجهات الجامعة لها أو سرقتها أو استخدامها بطرق غير مشروعة تضر بصاحبها[٤].

والمتأمل لعالم الثورة الصناعية الرابعة يجد أنه يتأسس وينبني على البيانات بصورة أساسية، فمن خلالها تقوم الإدارة العامة في الدول بإشباع حاجات الناس من الخدمات الأساسية، ومن خلالها تشرع القوانين المناسبة في كافة الجوانب الاقتصادية والاجتماعية والسياسية والثقافية، لذلك تولدت الحاجة الملحة لجمع البيانات، لمقابلة الاحتياجات سالفة الذكر وأضحت جميع المؤسسات المعنية بتقديم الخدمات تطلب بيانات معينة من الأشخاص الذين يطلبون خدماتها على مستوى الدولة الداخلي وعلى المستوى الخارجي، مع انتشار التجارة الإلكترونية والإعلام الرقمي والاجتماعي أصبح أيضاً تقديم بعض البيانات شرط لازم للاستفادة من الخدمة، مما جعل شركات مثل فيسبوك وتويتر وتك توك وقوقل وأمازون وعلي بابا وغيرها من الشركات تمتلك كم هائل من بيانات الاشخاص، وجعل من اللازم إيجاد أطر لحماية هذه البيانات على المستويين الوطني والدولي، فعلى المستوى الوطني تقوم الدول بإصدار تشريعات لحماية البيانات الشخصية، بتفويض هيئة أو وزارة محددة متخصصة في الاتصالات للقيام بهذه المهمة، وإلزام أي جهة جامعة للبيانات لأغراض عملها بالتزامات معينة اتجاه صاحب هذه البينات، بغرض المحافظة على البيانات من الاختراق والتعدي، ولهذه الجهات أيضاً حقوق معينة نصت عليها القوانين، أما على المستوى الدولي

---

[٤] الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً، "دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي"، ورقة علمية مقدمة من د. ميادة مصطفى محمد المحروقي للمجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) دون تحديد تاريخ أو عدد المجلة، ص١٤٨٠.

نتطلع لمعاهدة أو برتوكول ملزم لجميع الجهات والشركات العابرة للدول بإلزامها بضرورة حماية البيانات الشخصية للأفراد والهيئات.

أولاً- أسباب اختيار الورقة العلمية:

هناك عدد من الأسباب التي دعتنا للبحث والتنقيب في الحماية القانونية للبيانات الشخصية في النظامين السعودي والعُماني، دراسة مقارنة تتمثل هذه الأسباب:

١. الوقوف على المصادر التي تؤطرللحماية القانونية للبيانات الشخصية على المستوى الوطني والدولي.

٢. الوقوف على التنظيم القانوني لحماية البيانات الشخصية في التشريعين العُماني والسعودي.

٣. بيان مفهوم البيانات الشخصية وعلاقته بمفهوم الحق في الخصوصية.

٤. الإضافة الموجبة التي يمكن أن يقدمها الباحثون في موضوع هذه الورقة لإثراء المكتبة القانونية.

ثانياً- أهمية موضوع الورقة العلمية:

لهذه الورقة أهمية نظرية تتمثل في بيان النصوص التي تستند عليها حماية البيانات الشخصية في الأنظمة القانونية العمانية والسعودية والمقارنة، إضافة لأهمية عملية تتمثل في الوقوف على التطبيق العملي لحماية البيانات الشخصية.

ثالثاً- المشكلة التي تناقشها الورقة العلمية:

تكمن مشكلة الدراسة في هذه الورقة العلمية في الإجابة على الأسئلة التي يثيرها موضوع حماية البيانات الشخصية وهي: ما هي الأسس والمبادي التي ترتكز عليها حماية البيانات الشخصية؟ وماهي المصادر التي تؤطر لحماية هذه البيانات؟ وما هو مفهوم البيانات الشخصية؟ وماهي الأسباب التي تدعو لحماية البيانات الشخصية؟ وما هي المخاطر التي تواجه البيانات الشخصية؟

رابعاً- أهداف الورقة العلمية:

هناك عدد من الأهداف يبتغيها الباحثون من هذه الورقة العلمية منها:

١. الوقوف على التحديات التي تواجه تطبيق النصوص الخاصة بحماية البيانات الشخصية.

٢. إبراز الجهود التي تقوم بها الجهات المسؤولة في حماية البيانات الشخصية.

خامساً– منهج الورقة العلمية:

سوف نتبع في هذه الورقة العلمية المنهج الوصفي والتحليلي والمقارن.

سادساً– الدراسات السابقة:

الحماية القانونية للبيانات الشخصية على مواقع التواصل الاجتماعي في القانون القطري والمقارن، بحث تكميلي مقدم لنيل درجة الماجستير لكلية القانون جامعة قطر من الطالبة اكرام سليمان قجم يونيو ٢٠٢١م.

حماية البيانات الشخصية الرقمية وفقاً لأحكام القانون المصرى رقم ١٥١ لسنة ٢٠٢٠ (حماية البيانات الشخصية المعالجة إلكترونياً) بين الواقع والمأمول، ورقة علمية مقدمة لمجلة القانون والاقتصاد جامعة عين شمس ٢٠٢٣م، من الباحث سيد محمود.

الحماية الجزائية للمعطيات الشخصية في التشريع الجزائري، دراسة في ظل قانون١٨–٠٧ المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، ورقة علمية منشورة بالمجلة الأكاديمية للبحث العلمي القانوني، الجزائر مقدمة من الباحث طباش عز الدين أستاذ محاضر بكلية الحقوق والعلوم السياسية جامعة بجاية الجزائر في ديسمبر ٢٠١٨م.

الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونياً، "دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي"، ورقة علمية مقدمة من د. ميادة مصطفى محمد المحروقي المجلة القانونية جامعة القاهرة فرع الخرطوم ٢٠٢٣م (مجلة متخصصة في الدراسات والبحوث القانونية).

سابعاً– خطة البحث للورقة العلمية:

تناولت الورقة العلمية الموضوع في ثلاث مباحث: في المبحث الأول تطرقت لماهية البيانات الشخصية وفيه سلطنا الضوء على مفهوم البيانات الشخصية وأنواعها

ومفهوم الخصوصية والتزامات الأطراف ذات العلاقة بالبيانات الشخصية، وفي المبحث الثاني تناولت الورقة الحماية الدستورية للبيانات الشخصية، وفي المبحث الأخير تطرقت الورقة للحماية الجنائية للبيانات الشخصية.

المبحث الأول
ما هيه البيانات الشخصية

المطلب الأول
مفهوم البيانات الشخصية

إن حماية البيانات الشخصية أو معلومات التعريف الشخصية تعني انشاء قواعد واضحة تتبع بواسطة أي هيئة أو جهة تقوم بمعالجة البيانات، وهذا الأمر ليس مفهوماً جديداً، حيث أن قوانين حماية البيانات ظهرت في العديد من البلدان منذ أكثر من أربعين عاما ولكن هذه القوانين أصبحت ذات أهمية متزايدة في الوقت الراهن بسبب ازدياد تقاسم البيانات وجمعها بواسطة الهيئات والمؤسسات والشركات، وقد تم إقرار أول قانون لحماية البيانات الشخصية في سنة ١٩٧٠م في ولاية هيس الاتحادية بألمانيا، وبعد سنوات قليلة وضعت الولايات المتحدة الأمريكية قانون للاستعمالات النزهية للمعلومات، وقد أثرت هذه القوانين على وضع القوانين الحديثة لحماية البيانات ثم صدرت أول القوانين على مستوى الدول لحماية البيانات الشخصية في السويد وألمانيا وفرنسا، قبل أن تعتمد منظمات دولية مثل مجلس أوربا الأطر الدولية لحماية البيانات الشخصية ثم جاءت اتفاقية مجلس أوربا لحماية الأفراد من المعالجة الأتوماتكية لبياناتهم الشخصية وقد سميت الاتفاقية ١٠٨ لسنة ١٩٨٠م وفي عام ١٩٨٠م أيضاً وضعت منظمة التعاون والتنمية في المجال الاقتصادي المبادي التوجيهية للخصوصية، وقد لعبت الاتفاقية ١٠٨ دوراً محورياً في اعتماد أول قانون لحماية البيانات في أوربا سنة ١٩٩٥م، ثم بدأ انتشار القوانين التي تحمي البيانات

الشخصية في العالم، وعَرفت الفقرة الأولى من المادة الرابعة من النظام الأوروبي لحماية البيانات الشخصية بأنها عبارة عن "أي معلومات متعلقة بشخص طبيعي، سواء أكان معروفاً؛ أم يمكن التعرف عليه. والشخص الطبيعي الذي يمكن التعرف عليه هو الذي يمكن تحديده بشكل مباشر، أو غير مباشر؛ من خلال الرجوع إلى وسيلةٍ تُعرف بهويته مثل الاسم، أو رقم الهوية، أو بيانات تحديد الموقع، أو مُعرف شخصي على شبكة الإنترنت أو أحد العوامل المحددة للهوية الجسدية، أو الفسيولوجية، أو الجينية، أو العقلية، أو الاقتصادية، أو الثقافية، أو الاجتماعية لذلك الشخص الطبيعي. ويطلق على الشخص الطبيعي مسمى صاحب البيانات"[٥].

فيما نصت الفقرة الرابعة من المادة الأولى من نظام حماية البيانات الشخصية السعودي على أن البيانات الشخصية هي: "كل بيان – مهما كان مصدره أو شكله – من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعل التعرف عليه ممكناً بصفة مباشرة أو غير مباشرة، ومن ذلك: الاسم، و رقم الهوية الشخصية، والعناوين، وأرقام التواصل، و أرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، و غير ذلك من البيانات ذات الطابع الشخصي"[٦].

علاوة على ذلك عرف المنظم السعودي البيانات في نظام مكافحة جرائم المعلوماتية لسنة ١٤٢٨هـ بأنها: "المعلومات، أو الأوامر، أو الرسائل، أو الأصوات،

---

[5] Paragraph 1of Article4 of the European personal Data Protection Regulation ‘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, genetic, mental, economic, cultural or social identity of that natural person.

[٦] الفقرة الرابعة من المادة الأولى من نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩هـ.

أو الصور التي تعد، أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله، وإنشاؤه بوساطة الحاسب الآلي، كالأرقام، والحروف والرموز وغيرها[٧].

كما نص المشرع العُماني على مفهوم البيانات الشخصية في المادة الأولى من قانون حماية البيانات الشخصية العُماني لسنة ٢٠٢٢م بقوله: "البيانات التي تجعل شخصاً طبيعياً معرفاً، أو قابلاً للتعريف بطريقة مباشرة، أو غير مباشرة، وذلك بالرجوع إلى معرف أو أكثر كالاسم أو الرقم المدني أو بيانات المعرفات الإلكترونية أو البيانات المكانية، أو بالرجوع إلى عامل أو أكثر خاص بالهوية الجينية أو الجسدية أو العقلية أو النفسية أو الاجتماعية أو الثقافية أو الاقتصادية".

وتجدر الإشارة إلى أن هنالك فرق بين المعلومات والبيانات؛ فقد "أجمع الفقه في فرنسا ومصر على التفرقة بين المعلومات من جهة، وبين البيانات التي تمت معالجتها إلكترونياً من جهة أُخرى، فالمعلومات عنصرها الأساسي هو الدلالة لا الدعامة التي تجسدها، ومن ثم ليس لها طبيعة مؤكدة، ومن الصعب بالتالي القول بالاعتداء عليها، أما البيانات التي تمت معالجتها إلكترونياً، فتتجسد في كيان مادي يتمثل في نبضات إلكترونية، أو إشارات كهرومغناطيسية يمكن تخزينها على «وسائط» معينة، ونقلها، وبثها، وحجبها، واستغلالها، وإعادة إنتاجها، فضلاً عن إمكانية تقديرها كميًا من حيث المبدأ، وقياسها. فهي إذن ليست شيئًا معنويًا، كالحقوق والآراء والأفكار، بل شيئًا له في العالم الخارجي المحسوس وجود مادي يصعب إنكاره[٨].

---

[٧] المادة الأولى من قانون مكافحة جرائم المعلوماتية السعودي لسنة ١٤٢٨هـ.

[٨] د. محمد السعيد رشدي، المؤتمر العلمي الثاني: الإعلام والقانون بحث بعنوان الإنترنت والجوانب القانونية لنظم المعلومات، كلية الحقوق، جامعة حلوان، ١٩٩٩م، ص٧٠٧.

إذاً هنالك فرق بين مصطلح معلومات وبيانات، ومعنى كلمة معلومات هي: "بيانات معالجة لها معنى في سياق معين"[٩]، فيما معنى كلمة بيانات هي: "تمثيل للمعلومات بصيغة مناسبة للتخزين أو المعالجة أو النقل"[١٠].

فالمعلومات هي جملة البيانات التي بعد أن تندمج ويتم معالجتها تؤدي إلى معلومة صحيحة، والبيانات هي بيان عن الشخص على سبيل المثال لا الحصر: الاسم والصورة والصوت ورقم الهوية الوطنية، وهي عبارة عن مجموعة من البيانات إذا اجتمعت مع بعضها تؤدي إلى معلومة من خلالها يمكن أن يتم التعرف على الشخص.

المطلب الثاني
أنواع البيانات

تقسم البيانات الشخصية إلى نوعين: وتصنيف ذلك بحسب طبيعتها أو بحسب أهميتها وهي كالآتي:

أ- بيانات شخصية بحسب طبيعتها: وتنقسم إلى نوعين:

١- بيانات تتعلق بذات الشخص: وهي الاسم واللقب رقم الهوية الوطنية، الجنسية، الصورة، الصوت، بيانات الشخص المهنية مثل اسم الوظيفة ومهام الوظيفة بريد الموظف، بيانات الشخص العلمية مثل الدرجة العلمية ودرجة الشهادة العلمية، بيانات الحساب البنكي والبطاقة الائتمانية.

٢- بيانات تتعلق بممتلكات الشخص: رقم الهاتف الشخصي سواء رقم الهاتف المحمول أو المنزل، رقم لوحة السيارة.

ب-بيانات شخصية بحسب أهميتها: وتنقسم أيضاً إلى نوعين:

---

[٩] معجم البيانات والذكاء الاصطناعي، الصادر من الهيئة السعودية للبيانات والذكاء الاصطناعي، الطبعة الأولى، ٢٠٢٢م، ص٧٧.

[١٠] معجم البيانات والذكاء الاصطناعي، المرجع السابق، ص٥٦.

١- **بيانات شخصية عادية:** وهي البيانات التي تتداول بطريقة يومية مثل رقم لوحة السيارة.

٢- **بيانات شخصية حساسة:** عرفها المنظم السعودي بأنها: "كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو أصله القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية، وكذلك البيانات الجنائية والأمنية[١١]، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية[١٢]، أو البيانات الائتمانية، أو البيانات الصحية[١٣]، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهما"[١٤]. وقد يؤدي اختراق وانتهاك البيانات الشخصية والتعدي عليها لجرائم غاية في الخطورة ففي

---

[١١] عرفها نظام الإنتربول (الشرطة الدولية) للتعامل مع البيانات في المادة الأولى البيانات: "أي معلومة أيا كان مصدرها تتعلق بوقائع مكونة لجريمة جزائية يسري عليها القانون العام، أو بالتحقيقات بشأنها، أو بمنعها أو بملاحقة مرتكبها أو مرتكبيها أو بالمعاقبة عليها، أو باختفاء أشخاص أو تحديد هويات جثث". نظام معاملة البيانات – اعتمدتها الجمعية العامة للإنتربول في عام ٢٠١١م، ودخلت حيّز النفاذ في عام ٢٠١٢م.

[١٢] ومن ذلك: بصمة الفرد والحمض النووي وغيرها. قد يستخدم صاحب العمل في حال وردت إليه معلومات جينية تخص العامل القيام بفصله بحجة أن العامل لا تنطبق فيه الشروط الصحية لأداء العمل المطلوب.

[١٣] على سبيل المثال لا الحصر: السجل الصحي للفرد. إن العلاقة التي تكون بين المريض والطبيب قائمة على أساس الثقة فإذا فقد المريض الثقة وظن بأن المعلومات التي يقدمها للطبيب قد يتم إفشائها بشكل أو بأخر فبتالي لا محاله لن يُقدم المريض كامل المعلومات وسينتج عن عدم الثقة عدة أمور من ضمنها: أ-إجراء المزيد من الفحوصات الطبية مقارنة في حال تم إعطاء معلومات كافية للطبيب من الممكن إجراء فحوصات أقل بناءً على المعلومات التي تقدم بها المريض للطبيب. ب-بالإضافة إلى التكاليف المالية العالية في حالة إجراء المزيد من الفحوصات الطبية. ج- صرف علاج يتعارض مع بعض المعلومات التي أخفاها المريض عن الطبيب فبتالي يؤثر سلباً على صحة المريض.

[١٤] الفقرة الحادية عشرة من المادة الأولى من نظام حماية البيانات الشخصية السعودي، مصدر سابق.

قضية،(REMSBURG V. DOCUSEARCH INC) تتلخص وقائع هذه القضية أن شركة Docusearch هي عبارة عن شركة تقدم معلومات عن طريق الأنترنت قدمت معلومات إلى السيد Liam youens مقابل تقديمه مبلغ من المال للشركة نظير أن تفصح عن معلومات أحد عملائها وهي السيدة Amy lynnby قامت الشركة بتقديم معلومات عن عنوان العمل الخاص بالسيدة Amy والذي استخدمه Liam للوصول إلى موقع الضحية و أثناء خروجها من العمل أطلق عليها الرصاص بعد ذلك قتل نفسه[١٥].

المطلب الثالث

مفهوم الخصوصية

الخصوصية في اللغة: تأتي من "خَصهُ بالشي خُصُوصاً، و خَصُوصِيةً والفتح أفصحُ، وخِصيصَى، وقولهم إنما يفعل هذا خُصِانُ من الناس، أي خَوَاص منهم، و اختَصهُ بكذا، أي خَصهَ به، والخاصةُ: خلاف العامة "[١٦]، ويأتي معنى خصص أي حدد أي جعله محدداً بذاته وميزه عن غيره.

أما الخصوصية في الاصطلاح: فهي مفهوم يشير إلى حق الأفراد في الحفاظ على سرية معلوماتهم الشخصية، والحد من جمع واستخدام ومشاركة هذه المعلومات والتعدي عليها من قبل الآخرين، سواء كانوا أفرادًا أو مؤسسات أو حكومات، وتعد الخصوصية حقًا أساسيًا للأفراد تنظمه الدساتير والقوانين، حيث تمنح الأفراد حرية التعبير والتفاعل والتفكير دون خوف من الانتهاكات الخاصة بالخصوصية.

---

(15) Remsburg v. Docusearch, Inc., A.2d (2003 WL 346260, sup. Ct., N.H.,2003).

(١٦) الصحاح تاج اللغة وصحاح العربية، أبو نصر إسماعيل بن حماد الجوهري. الفارابي(المتوفى:٣٩٣هـ)، تحقيق: أحمد عبد الغفور عطار، دار العلم للملايين، بيروت، الطبعة: الرابعة ١٤٠٧هـ -١٩٨٧ م، باب(خص)، ١٠٣٧/٣.

وتشمل الخصوصية المعلومات الشخصية التي تتمتع بالحماية بموجب الحق في الخصوصية؛ كمعلومات مثل: الاسم والعنوان ورقم الهاتف والبريد الإلكتروني والبيانات المالية والطبية والتعليمية والجنسية والدينية، بالإضافة إلى أي معلومات أخرى يمكن استخدامها لتحديد هوية الشخص أو تحديد أنشطته، ويعد حماية الحق في الخصوصية من الحقوق المهمة في العصر الرقمي؛ حيث تتراكم المعلومات الشخصية على الإنترنت، ويتم جمعها واستخدامها بشكل متزايد من قبل الشركات والحكومات وغيرها من المؤسسات لذلك، تقوم الدول والمؤسسات الأخرى بتبني قوانين وسياسات لحماية الخصوصية، وضمان أن يتم استخدام المعلومات الشخصية بطريقة ملائمة، وفي إطار القواعد القانونية.

أولاً- الخصوصية في النظام السعودي:

عالجت العديد من الأنظمة واللوائح والقواعد والسياسات، في المملكة العربية السعودية وسلطنة عمان موضوعات الحياة الخاصة، فقد أشارت إلى ذلك المادة السابعة والثلاثون من النظام الأساسي للحكم بالمملكة العربية السعودية بقولها: "للمساكن حرمتها، ولا يجوز دخولها بغير إذن صاحبها، ولا تفتيشها، إلا في الحالات التي يبينها النظام"[١٧].

كما عالجت المادة الأربعون من النظام الأساسي للحكم في المملكة موضوع آخر من موضوعات الحياة الخاصة، وهو المراسلات والمكالمات وذلك بقولها: "المراسلات البرقية، والبريدية، والمخابرات الهاتفية، وغيرها من وسائل الاتصال، مصونة، ولا يجوز مصادرتها، أو تأخيرها، أو الاطلاع عليها، أو الاستماع إليها إلا في الحالات التي يبينها النظام"[١٨].

علاوة على ذلك؛ عمد نظام الاتصالات بالمملكة على حماية الحياة الخاصة حيث نصت المادة التاسعة منه على أن: "سرية المُكالمات الهاتفية والمعلومات التي يتم

---

[١٧] المادة السابعة والثلاثون من النظام الأساسي للحكم، مصدر سابق.

[١٨] المادة الأربعون من النظام الأساسي للحكم، المصدر السابق.

إرسالها أو استِقبالُها عن طريق شبكات الاتِصالات العامة مصونة، ولا يجوز الاطلاع عليها أو الاستِماع إليها أو تسجيلِها إلا في الحالات التي تُبينها الأنظِمة"[١٩].

وأيضاً نص نظام الإجراءات الجزائية على حماية الحياة الخاصة في المادة الحادية والأربعون بقولها: "للأشخاص ومساكنهم ومكاتبهم ومراكبهم حرمة تجب صيانتها، وحرمة الشخص تحمي جسده وملابسه وماله وما معه من أمتعة، وتشمل حرمة المسكن كل مكان مسوّر أو محاط بأي حاجز، أو مُعدٍّ لاستعماله مأوى"[٢٠].

ثانياً- الخصوصية في النظام العُماني:

نظمت المادة (٣٦) من النظام الأساسي للدولة بسلطنة عمان لعام ٢٠٢١م الحق في الحياة الخاصة وذلك بقولها: "للحياة الخاصة حرمة، وهي مصونة لا تمس وللمراسلات الإلكترونية بكافة أنواعها، والمراسلات الهاتفية، والبرقية، والبريدية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، فلا يجوز مراقبتها، أو تفتيشها، أو الاطلاع عليها، أو إفشاء سريتها، أو تأخيرها، أو مصادرتها، إلا في الأحوال التي يبينها القانون، ووفقاً للإجراءات المحددة فيه"[٢١].

كما تناول قانون الإجراءات الجزائية العماني رقم ٩٩/٩٧ حماية الحياة الخاصة في عدد من نصوصه، حيث جاء في المادة (٩٠) لا يجوز ضبط المراسلات والبرقيات أو الاطلاع عليها أو ضبط الجرائد والمطبوعات والطرود أو تسجيل الأحاديث التي تجرى في مكان خاص أو مراقبة الهاتف أو تسجيل المكالمات بغير إذن من الادعاء العام"، وحددت المادة (٩١) من القانون إجراءات الإذن الذي أشارت له المادة (٩٠) بقولها: "يصدر الإذن المنصوص عليه في المادة (٩٠) من هذا القانون إذا كانت له فائدة في ظهور الحقيقة في جناية أو جنحة معاقب عليها بالسجن مدة تزيد على ثلاثة

---

[١٩] المادة التاسعة من نظام الاتصالات السعودي الصادر بالمرسوم الملكي رقم م/١٢ بتاريخ ١٤٢٢/٣/١٢هـ.

[٢٠] المادة الحادية والأربعون من قانون الإجراءات الجزائية العماني رقم ٩٩/٩٧ المواد ٩٠،٩١.

[٢١] المادة الخامسة من قانون الاتصالات العماني رقم ٢٠٠٢/٣٠م.

أشهر، ويجب أن يكون مسبباً وألا تزيد مدته على ثلاثين يوماً قابلة للتجديد مدداً أخرى مماثلة إذا اقتضت مصلحة التحقيق ذلك".

كما نظمت المادة الخامسة من قانون الاتصالات العماني رقم ٢٠٠٢/٣٠م الحياة الخاصة بقولها: "لا تجوز مراقبة وسائل الاتصال أو تفتيشها أو إفشاء سريتها أو تأخيرها أو مصادرتها ما لم تنطو على إخلال بالنظام العام أو الآداب أو اعتداء على حقوق الآخرين، وذلك مع عدم الإخلال بقانون الإجراءات الجزائية الصادر بالمرسوم السلطاني رقم ٩٧ / ٩٩"[٢٢].

ثالثاً- الخصوصية المعلوماتية:

عرف Louis Brandeis و Samuel Warren الخصوصية المعلوماتية بأنها: "حق الفرد في أن يظل بمفرده وكذا قدرته على عزل نفسه أو معلوماته عن الآخرين"، فيما عرفها Alan Westin بأنها: "حق الأفراد أو المجموعات أو المؤسسات في اتخاذ قرارات بشأن أنفسهم ومتى وكيف يتم نقل المعلومات الخاصة بهم للآخرين"، كذلك عُرفت بأنها: "عدم عبث أي فرد أو أي جهة في معلومات الأفراد أو المؤسسات الخاصة بهم دون إذنهم، المحفوظة في أجهزة الحاسب الآلي أو في أي أجهزة الكترونية خاصة بهم متصلة بالإنترنت".

ويعرفها الباحثون بأنها: الحق الذي يخول لصاحبه التحكم بمعلوماته الشخصية، وذلك بأن لا يسمح للأفراد أو الشركات باستخدامها بطريقة غير قانونية.

من التعريفات السابقة يستخلص الباحثون أن الخصوصية المعلوماتية عبارة عن:

١- حق شخصي: أي أنها حق مرتبط بشخص صاحبها لا تنفصل عنه.

٢- حق يخول صاحبه التحكم ببياناته: على سبيل المثال لا الحصر حق العلم، أي أن من حق صاحب البيانات الشخصية معرفة الغرض من الجمع وما هو المسوغ النظامي لذلك وألا تُعالج بياناته بطريقة تتنافى مع الغرض الذي جُمعت من أجله،

---

[٢٢] ٣٦ من النظام الأساسي للدولة بسلطنة عمان لعام ٢٠٢١م.

حق الوصول أي من حق صاحب البيانات الاطلاع عليها والحصول على نسخة منها بدون أي مقابل مادي، الحق في التصحيح وهو حق يخول لصاحبه تصحيح معلوماته القديمة، حق الإتلاف يخول لصاحبه اتلاف بياناته الشخصية مما انتهت الحاجة إليه.

المطلب الرابع

التزامات الأطراف ذات العلاقة بالبيانات الشخصية

أولاً- حقوق صاحب البيانات الشخصية:

صاحب البيانات الشخصية هو الشخص الطبيعي أو الاعتباري الذي يمكن التعرف عليه، وهو الشخص الذي يمكن تحديده، بشكل مباشر أو غير مباشر، على وجه الخصوص بالرجوع إلى معرّف مثل الاسم أو رقم التعريف أو بيانات الموقع أو المعرّف عبر الإنترنت أو إلى واحد أو أكثر من العوامل المحددة للعوامل المادية، وقد ورد تعريف صاحب البيانات الشخصية في المادة الأولى من قانون حماية البيانات الشخصية العماني بأنه: "الشخص الطبيعي الذي يمكن التعرف عليه من خلال بياناته الشخصية" [٢٣]، وقد أورد المشرع العماني حقوق صاحب البيانات الشخصية في الفصل الثالث من القانون في المواد (١٠ و ١١ و ١٢)، وقد أوضحت المادة العاشرة المبادئ التي ينبغي اتباعها عند معالجة البيانات الشخصية وقد جاء نص المادة"لا يجوز معالجة البيانات الشخصية إلا في إطار الشفافية والأمانة، واحترام كرامة الإنسان، وبعد الموافقة الصريحة لصاحب البيانات الشخصية على ذلك".

"ويجب أن يكون طلب معالجة البيانات الشخصية مكتوبا وبصورة واضحة وصريحة ومفهومة، ويلتزم المتحكم بإثبات الموافقة الكتابية لصاحب البيانات الشخصية لمعالجة بياناته." وتكفلت المادة الحادية عشر ببيان حقوق صاحب البيانات الشخصية والتي تتمثل في الاتي:

---

[٢٣] المادة الأولى من قانون حماية البيانات الشخصية العماني لسنة ٢٠٢٢م.

يكون لصاحب البيانات الشخصية الحق في الآتي:

أ- إلغاء موافقته على معالجة بياناته الشخصية، وذلك مع عدم الإخلال بالمعالجات التي تمت قبل الإلغاء.

ب-طلب تعديل بياناته الشخصية أو تحديثها أو حجبها.

ج- الحصول على نسخة من بياناته الشخصية المعالجة.

د- نقل بياناته الشخصية إلى متحكم آخر.

هـ-طلب محو بياناته الشخصية ما لم تكن تلك المعالجة ضرورية لأغراض الحفظ والتوثيق الوطنية.

و- إخطاره بأي اختراق أو انتهاك لبياناته الشخصية، وما تم اتخاذه من إجراءات في هذا الشأن.

وتبين اللائحة الضوابط والإجراءات اللازمة لممارسة هذه الحقوق".

كما أعطت المادة الثانية عشر صاحب البيانات الشخصية حق التقدم بشكوى إلى الوزارة إذا رأى أو اعد أن معالجة بياناته الشخصية لا تتوافق مع أحكام هذا القانون، وذلك طبقا للضوابط والإجراءات التي تحددها اللائحة" [٢٤].

وقد أورد المنظم السعودي حقوق صاحب البيانات الشخصية في المادة الرابعة التي تنص:

" 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 ألاَّ تعالج بياناته لاحقاً بصورة تتنافى مع الغرض من جمعها أو في غير الأحوال المنصوص عليها في المادة (العاشرة) من النظام[٢٥]، ويعد هذا الحق من أهم حقوق صاحب البيانات الشخصية، وقد عمدت

---

[٢٤] المواد (١٠،١٢،١١) من قانون حماية البيانات الشخصية العماني مصدر سابق.

[٢٥] المادة الرابعة من نظام حماية البيانات الشخصية السعودي مصدر سابق.

شركة امريكية للذكاء الاصطناعي تسمي كليرفيو على انتهاك هذا الحق بجمع صور للناس من جميع دول العالم من خلال الانترنت وقد جاء في تقرير لصحيفة الوشنطن بوست عن هذه الشركة:

The facial recognition company Clearview AI is telling investors it is on track to have 100 billion facial photos in its database within a year, enough to ensure "almost everyone in the world will be identifiable," according to a financial presentation from December obtained by The Washington Post. Those images - equivalent to 14 photos for each of the 7 billion people on Earth - would help power a surveillance system that has been used for arrests and criminal investigations by thousands of law enforcement and government agencies around the world.

And the company wants to expand beyond scanning faces for the police, saying in the presentation that it could monitor "gig economy" workers and is researching a number of new technologies that could identify someone based on how they walk, detect their location from a photo or scan their fingerprints from afar.

شركة أميركية للذكاء الاصطناعي، ستحصل خلال عام على ١٠٠ مليار صورة وجه في قاعدة بياناتها، وهو ما يكفي لضمان التعرف على كل شخص في العالم تقريباً، رغم قلق المشرّعين الأميركيين من أن ذلك يشكل تهديداً خطيراً للخصوصية.

وذكر مراسل الصحيفة للذكاء الاصطناعي درو هارويل أن شركة كليرفيو للذكاء الاصطناعي (Clearview AI) كشفت في عرض مالي في ديسمبر/كانون الأول الماضي، أنها قد أوشكت على جمع صور تعادل ١٤ صورة لكل شخص في العالم (عد سكان العالم حوالي ٧ مليارات شخص)، وأن هذه الصور ساعدت في تشغيل نظام مراقبة تم استخدامه للاعتقالات والتحقيقات الجنائية من قبل الآلاف من وكالات إنفاذ القانون والوكالات الحكومية في جميع أنحاء العالم. [٢٦] وقال: "ميخايلو

[٢٦] صحيفة الواشنطن بوست ٢٠٢٢/٢/١٦م.

فيدوروف نائب رئيس الوزراء الأوكراني إن الحكومة الأوكرانية تستخدم برنامج التعرف على الوجه "كليرفيو (Clearview) "لتحديد هوية القتلى من الجنود الروس، واستخدام تلك المعلومات للاتصال بأقارب القتلى وقال فيدوروف لوكالة رويترز "تقديرا لأمهات هؤلاء الجنود، نقوم بنشر هذه المعلومات عبر وسائل التواصل الاجتماعي لإعلام العائلات على الأقل بأنهم فقدوا أبناءهم، ومن ثم تمكينهم من القدوم لأخذ جثثهم"[٢٧].

صحيفة «بيزفيلد» الإلكترونية قالت في تقرير لها في ١٠ أبريل ٢٠٢١، إن هناك ٢٠٠٠ وكالة، و٧٠٠٠ خبير يستخدمون هذه التقنية حالياً، وإن الاستخدام داخل الولايات المتحدة يراوح ما بين التعرف إلى «المجرمين» والتعرف إلى أعضاء حركة «حياة السود مهمة»، كما قالت الصحيفة في تقرير آخر لها في ١٦ أبريل ٢٠٢١م، بعنوان: «قسم الشرطة الذي تتبع له يستخدم تقنية التعرف إلى الوجوه»، إن استخدام التقنية يتعلق بموضوعات «ليست بالضرورة تخص تحقيقات قضائية [٢٨].

ونتيجة لانتهاك هذه الشركة لقانون حماية البيانات الشخصية البريطاني لسنة ٢٠١٨م أصدرت هيئة حماية البيانات الشخصية في بريطانيا حكماً يقضي بتغريم هذه الشركة مبلغ سبعة مليار وخمسمائة ألف جنيه إسترليني:

The U.K.’s data protection watchdog has confirmed a penalty for the controversial facial recognition company, Clearview AI - announcing a fine of just over £7.5 million today for a string of breaches of local privacy laws. The watchdog has also issued an enforcement notice, ordering Clearview to stop obtaining and using the personal data of U.K. residents that is publicly available

---

[٢٧] موقع التاج الاخباري:
https://altaj.news/public/technology/2214742٠٢٣ /٩/١٣

[٢٨] صحيفة الإمارات اليوم النسخة الإلكترونية بتاريخ ٢٠٢٢/٣/٢٩م.
https://www.emaratalyoum.com/politics/weekly-supplements/world-press/2022-03-29-

on the internet; and telling it to delete the information of U.K. residents from its systems.

The U.S. company has amassed a database of 20 billion + facial images by scraping data off the public internet, such as from social media services, to create an online database that it uses to power an AI-based identity-matching service which it sells to entities such as law enforcement. The problem is Clearview has never asked individuals whether it can use their selfies for that. And in many countries, it has been found in breach of privacy laws. In a statement accompanying today's enforcement, the U.K.'s information commissioner, John Edwards, said: Clearview AI Inc has collected multiple images of people all over the world, including in the U.K., from a variety of websites and social media platforms, creating a database with more than 20 billion images. The company not only enables identification of those people, but effectively monitors their behaviour and offers it as a commercial service. That is unacceptable. That is why we have acted to protect people in the U.K. by both fining the company and issuing an enforcement notice.

People expect that their personal information will be respected, regardless of where in the world their data is being used. That is why global companies need international enforcement. Working with colleagues around the world helped us take this action and protect people from such intrusive activity. This international cooperation is essential to protect people's privacy rights in 2022. That means working with regulators in other countries, as we did in this case with our Australian colleagues. And it means working with regulators in Europe, which is why I am meeting them in Brussels this week so we can collaborate to tackle global privacy harms[29].

٢-الحق في وصوله إلى بياناته الشخصية المتوفرة 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

[٢٩] موقع الهيئة البريطانية لحماية البيانات الشخصية ٢٣ مايو ٢٠٢٢م.

نظام المعلومات الائتمانية فيما يخص المقابل المالي، ودون إخلال بما تقضي به المادة (التاسعة) من النظام.

٣-الحق في طلب تصحيح بياناته الشخصية المتوفرة لدى جهة التحكم، أو إتمامها، أو تحديثها.

٤-الحق في طلب إتلاف بياناته الشخصية المتوفرة لدى جهة التحكم مما انتهت الحاجة إليه منها، وذلك دون إخلال بما تقضي به المادة (الثامنة عشرة) من النظام. وهذا ما يعرف في بعض القوانين بالحق في النسيان أو حق محو البيانات الشخصية وهو حق الفرد بمسح ما يتعلق بشخصه من بيانات ومعلومات موجودة على صفحات الانترنت وما يحيل إليها من روابط من محركات البحث الإلكتروني، وترجع إشكالية الحق في النسيان إلى حقيقة بقاء تلك البيانات وهذه المعلومات على الإنترنت إلى زمن طويل، بحيث يصبح وجودها غير مجد أو فاقد للغاية منه أو ضار بمركز صاحبها أو سمعته، ولذلك ينشأ التساؤل حول مدى جواز اتاحة المجال لصاحب هذه البيانات بتقديم طلب للمتحكم في الصفحة الإلكترونية أو محرك البحث بإزالة تلك البيانات والروابط المؤدية إليها، وقد تم تعريف الحق في النسيان بأنه "مكنة قانونية تخول الفرد ازالة بيانات إلكترونية متعلقة به بطلب يقدمه إلى المتحكم فيها لمسوغ قانوني"[٣٠].

٥-الحقوق الأخرى المنصوص عليها في النظام، التي تُبينها اللوائح.

ثانياً- التزامات المتحكم والمعالج:

جاء تعريف المتحكم في المادة الاولى من قانون حماية البيانات الشخصية العماني بأنه: "الشخص الذي يتولى تحديد أهداف ووسائل معالجة البيانات الشخصية، ويقوم بهذه المعالجة بنفسه، أو يعهد بها إلى غيره." وقد وردت التزامات المتحكم والمعالج في المواد من (١٣) إلى (٢٣) من قانون حماية البيانات الشخصية العماني ورتب

---

[٣٠] ورقة بعنون الإطار الدستوري للحق في النسيان مقدمة من الدكتور خليفة ثامر الحميدة، كلية الحقوق جامعة الكويت، مجلة الحقوق للبحوث القانونية والاقتصادية جامعة الكويت ٢٠١٨م، ص١٠٨٤.

المشرع العماني عقوبات في حالة فشل المتحكم أو المعالج في الإيفاء بالتزاماتهما التي حددها القانون.

وقد عرفه المنظم الأوروبي في الفقرة السابعة من المادة الرابعة[٣١]، وهو الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي هيئة أخرى تحدد، بمفردها أو بالاشتراك مع آخرين.

أما المعالج فقد جاء تعريفه في المادة الاولى من قانون حماية البيانات الشخصية العُماني بأنه: "الشخص الذي يقوم بمعالجة البيانات الشخصية نيابة عن المتحكم"، وقد وردت التزامات المعالج في المواد من (١٥) إلى (١٨) من قانون حماية البيانات الشخصية العماني ورتب المشرع على الاخلال بهذه الالتزامات عقوبات جزائية متنوعة.

وعرف المنظم الأوروبي المعالج في الفقرة الثامنة من المادة الرابعة[٣٢] بأنه شخصًا طبيعيًا أو اعتباريًا أو سلطة عامة أو وكالة أو هيئة أخرى تعالج البيانات، وهذا ما تطرقت له الفقرة التاسعة عشرة من المادة الأولى من نظام حماية البيانات الشخصية السعودي التي تعرف المعالج بأنه: "أي جهة عامة، وأي شخصية ذات صفة طبيعية أو اعتبارية خاصة؛ تعالج البيانات الشخصية لمصلحة جهة التحكم ونيابةً عنها"[٣٣].

---

[31] Paragraph 7 of Article 4 of the European Personal Data Protection System 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[32] Paragraph 8 of Article 4 of the European Personal Data Protection System 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

[٣٣] الفقرة التاسعة عشرة من المادة الأولى من نظام حماية البيانات الشخصية السعودي مصدر سابق.

أما المعالجة فقد عرفها قانون حماية البيانات الشخصية العماني بأنها" عملية أو مجموعة عمليات يتم إجراؤها على البيانات الشخصية، تتضمن جمعها أو تسجيلها أو تحليلها أو تنظيمها أو تخزينها أو تعديلها أو تحويرها أو استرجاعها أو مراجعتها أو تنسيقها أو ضم بعضها لبعض أو حجبها أو محوها أو إلغاءها أو الإفصاح عنها، عن طريق إرسالها أو توزيعها أو نقلها أو تحويلها أو إتاحتها بوسائل أخرى".

وقد ورد تعريفها في الفقرة الثانية من المادة الرابعة من النظام الأوروبي لحماية البيانات الشخصية بأنها "أي عملية أو مجموعة من العمليات التي يتم إجراؤها على البيانات الشخصية أو على مجموعات من البيانات الشخصية، سواء بوسائل آلية أم لا، مثل التجميع أو التسجيل أو التنظيم أو الهيكلة أو التخزين أو التكيف أو التغيير أو الاسترداد أو التشاور، أو الاستخدام أو الإفصاح عن طريق الإرسال أو النشر أو الإتاحة أو المحاذاة أو الدمج أو التقييد أو المحو أو التدمير"[٣٤] ما عدا بعض الاستثناءات التي تخص الأمور المنزلية وهذا ما ذهب معه المنظم السعودي الذي عرف المعالجة بأنها[٣٥]: "أي عملية تُجرى على البيانات الشخصية بأي وسيلة كانت يدوية أو آلية، ومن ذلك: عمليات الجمع، والتسجيل، والحفظ، والفهرسة، والترتيب، والتنسيق، والتخزين، والتعديل، والتحديث، والدمج، والاسترجاع، والاستعمال، والإفصاح، والنقل، والنشر، والمشاركة في البيانات أو الربط البيني، والحجب، والمسح، والإتلاف".

وتتضمن المعالجة عمليات عدة تبدأ بجمع البيانات الشخصية، وهي عملية يقوم مرتكب جريمة التعدي على البيانات الشخصية من خلالها على الحصول على

---

(34) The second paragraph of Article 4 of the European Personal Data Protection System profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

(٣٥) الفقرة الخامسة من المادة الأولى من نظام حماية البيانات الشخصية السعودي مصدر سابق.

البيانات الشخصية للأفراد أي كانت طريقة حصوله على تلك البيانات، سواء تم ذلك يدوياً أم إلكترونياً بطريقة غير مشروعة، ويعد من قبيل جهات المعالجة، الجهات القائمة بتجميع البريد الإلكتروني للعملاء بهدف ارسال رسائل دعائية، كذلك قيام جهة بحث علمي بتجميع بيانات عن الحالات الصحية للمرضى بهدف إجراء بحث علمي، كما تعد جهة معالجة الشركات التي تقوم بإنشاء نظام لمراقبة أجهزة الحاسوب الخاصة بموظفي الشركة داخل مكان العمل وشركات الطيران التي تحتفظ ببيانات المسافرين على خطوطها وغير ذلك من الجهات التي ينطبق عليها مفهوم المعالج، كما تتضمن المعالجة عمليات أخرى أشارت إليها القوانين مثل التحليل والتنظيم وغيرها من العمليات ولا يشترط في المعالجة أن تتم بصورة إلكترونية، فيمكن أن تتم بطريقة يدوية.

وقد ألزمت المادة الثالثة عشر من قانون حماية البيانات الشخصية العُماني المتحكم بوضع الضوابط والإجراءات الواجب الالتزام بها عند معالجة البيانات الشخصية، ويجب أن تشتمل على وجه الخصوص الآتي:

أ- تحديد المخاطر التي قد تقع على صاحب البيانات الشخصية جراء المعالجة.

ب-إجراءات وضوابط نقل وتحويل البيانات الشخصية.

ج- التدابير الفنية والإجرائية لضمان تنفيذ المعالجة وفقا لأحكام هذا القانون.

د- أي ضوابط أو إجراءات أخرى تحددها اللائحة.

كما ألزمت المادة الرابعة عشر المتحكم قبل البدء في معالجة أي بيانات شخصية أن يخطر صاحب البيانات الشخصية كتابة بما يأتي:

أ- بيانات المتحكم، والمعالج.

ب-بيانات التواصل مع مسؤول حماية البيانات الشخصية.

ج- الغرض من معالجة البيانات الشخصية، والمصدر الذي جمعت منه.

د- الوصف الشامل والدقيق للمعالجة وإجراءاتها، ودرجات الإفصاح عن البيانات الشخصية.

هـ- حقوق صاحب البيانات الشخصية بما في ذلك حق الوصول إلى البيانات، وتصحيحها، ونقلها، وتحديثها.

و- أي معلومات أخرى قد تكون ضرورية لاستيفاء شروط المعالجة.

وقررت المادة الخامسة عشر إلزام المتحكم والمعالج بالضوابط والإجراءات التي تقررها الوزارة، لضمان أن معالجة البيانات الشخصية تمت وفقا لأحكام القانون.

كما يلتزم المتحكم والمعالج وفق المادة السادسة عشر - بناء على طلب الوزارة - بتعيين مدقق خارجي للتأكد من أن إجراءات معالجة البيانات الشخصية قد تمت وفقاً لأحكام القانون، ووفقاً لإجراءات وضوابط المتحكم المنصوص عليها في المادة (١٣) من القانون، وتحدد اللائحة ضوابط وإجراءات تعيين المدقق الخارجي.

ويلتزم المتحكم والمعالج بموافاة الوزارة بنسخة من تقرير المدقق الخارجي.

كما أن هناك التزام وفق المادة السابعة عشر على المتحكم والمعالج بالاحتفاظ بمستندات عمليات المعالجة، وذلك وفقاً للمدد والإجراءات التي تحددها اللائحة.

ويعطي قانون حماية البيانات الشخصية العُماني في المادة الثامنة عشر سلطة لوزارة الاتصالات باعتبارها الجهة الفنية المسؤولة عن تنفيذ القانون بإلزام المتحكم والمعالج بالتعاون معها، وتقديم ما تطلبه من بيانات ومستندات تراها لازمة لممارسة اختصاصها طبقاً لأحكام قانون حماية البيانات الشخصية، وذلك خلال المدة التي تحددها اللائحة.

كما أن هنالك التزام بموجب المادة التاسعة عشر على المتحكم، عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة.

وأيضاً هناك التزام على المتحكم وفق المادة العشرون بتحديد مسؤول حماية البيانات الشخصية، وتحدد اللائحة ضوابط اختيار هذا المسؤول ومهامه.

كما ألزمت المادة الحادي والعشرون المتحكم بضمان سرية البيانات الشخصية، وعدم نشرها إلا بموافقة مسبقة من صاحب البيانات الشخصية، وذلك على النحو الذي تحدده اللائحة.

وتلزم المادة الثانية والعشرون المتحكم بالحصول على الموافقة الكتابية لصاحب البيانات الشخصية قبل إرسال أي مادة إعلانية أو تسويقية وذات أغراض تجارية إليه، وذلك على النحو الذي تحدده اللائحة.

وهنالك التزامات أخرى تفرضها القوانين على المتحكم والمعالج تتمثل في التدابير والإجراءات الأمنية لحفظ البيانات الشخصية، وقد أشار إليها المنظم الأوروبي والسعودي، وهي توفير أعلى المعايير التقنية للتعامل مع البيانات الشخصية، وتتمثل من خلال حفظ البيانات من الوصول غير المسموح وتشمل التشفير والتخزين الاحتياطي، وذلك بهدف عدم ضياع البيانات. ويلاحظ الباحثون أن المنظم الأوروبي قد أفرد معايير عامة في هذا الصدد، فمعايير حماية البيانات تختلف بناءً على حجم البيانات وأهميتها وحساسيتها.

وتشمل هذه التدابير أن تقوم الشركة التي تقوم بجمع البيانات بكل ما يلزم لحماية البيانات، فصاحب البيانات غير مكلف بحماية بياناته لدى شركة اتصالات وإنما شركة الاتصالات ستكون مسؤولة عن حماية البيانات في حال قامت بتسريب البيانات، فنسبة تسريب البيانات من شركات الاتصالات ليست بالقليلة مقارنة بعدد البيانات التي تجمعها من الافراد، علاوة على أن الأمان في العالم التقني لن يصل بنسبة ١٠٠% بل هي بنسب مختلفة وقد يكون في بعض الحالات الخلل من الشركة لأنها لم تتخذ كافة التدابير اللازمة لحماية البيانات الشخصية مثل حفظ البيانات بدون حماية أو بدون تشفير.

علاوة على هذه التدابير هناك إجراءات تنظيمية تتمثل بعدم السماح إلا بدخول أشخاص محددين لمركز البيانات (وهو المكان الذي تخزن فيه البيانات) والمقصود بدخول الأشخاص هو الدخول الفيزيائي للأشخاص؛ لأن من الممكن أن يدخل شخص غير مخول بالدخول لمركز البيانات والقيام باستخراج قرص يحتوي على

بيانات ومن ثم بيعه لعدة شركات، علاوة على الدخول الإلكتروني لأشخاص غير مخولين بذلك للحصول على البيانات وهو ما يسمى بالهكرز، ويتكفل بحماية البيانات الأمن السيبراني ويمنع وصول هذه الحوادث أو التقليل منها وهنالك عدة إجراءات من شأنها المحافظة على حماية البيانات الشخصية وتتمثل هذه الاجراءات في الآتي:

١- فصل أو إخفاء معالم البيانات بحيث لا يمكن تحديد صاحب البيانات، ومثال ذلك شخص أسمه أحمد ولديه رقم هاتف في شركة اتصالات في حال تم فصل البيانات الخاصة باسمه عن رقم الهاتف سيؤدي إلى عدم معرفة صاحب رقم الهاتف ألا وهو أحمد [٣٦].

٢- تشفير البيانات وهي عملية تحويل نص بسيط إلى نص مشفر بحيث يؤدي إلى عدم التعرف على بيانات الشخص [٣٧].

٣- يجب أن تكون كلمة السر في الشركة معقدة.

٤- يجب استعادة البيانات في حال فقدانها.

٥- عمل خطة دورية من الشركة بشأن الإجراءات التي تتبعها لحماية البيانات الشخصية.

وتطرقت المادة التاسعة عشرة من نظام حماية البيانات السعودي للإجراءات التنظيمية[٣٨]؛ فقررت أن على جهة التحكم أن تتخذ كافة الإجراءات الإدارية والتنظيمية والتقنية من شأنها أن تضفي حماية على البيانات الشخصية، ومن الإجراءات الإيجابية التي تطرق لها المنظم السعودي هي قصر حق الاطلاع على

---

[36] The first paragraph of Article 25, the first paragraph of Article 32 of the European Personal Data Protection Regulation.

[37] The first paragraph of Article 32 of the European Personal Data Protection Regulation.

[٣٨] المادة التاسعة عشرة من نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي رقم (م/١٩) وتاريخ ١٤٤٣/٢/٩هـ. "على جهة التحكم اتخاذ ما يلزم من إجراءات ووسائل تنظيمية وإدارية وتقنية تضمن المحافظة على البيانات الشخصية، بما في ذلك عند نقلها؛ وذلك وفقاً للأحكام والضوابط التي تحددها اللوائح".

البيانات الصحية على أقل عدد من الموظفين كذلك تقييد معالجة تلك البيانات على أقل عدد ممكن من الموظفين.

المبحث الثاني

الحماية الدستورية للبيانات الشخصية

تتعلق الحماية الدستورية للبيانات الشخصية بالضمانات الدستورية التي تتضمنها الدساتير لحماية خصوصية الأفراد وبياناتهم الشخصية، علاوة على اشتمالها على النصوص التي تحمي الحقوق الأساسية للبيانات الشخصية مثل حق العلم وحق الاطلاع وسرية البيانات والحقوق الأخرى.

وتخضع هذه الضمانات للتشريعات واللوائح والقوانين التي تحدد حماية البيانات الشخصية في بلد معين، وغالباً ما تتمتع الحكومات بسلطات خاصة للحفاظ على الأمن القومي والحفاظ على القانون والنظام العام، لكن يجب أن تحترم هذه السلطات الحقوق الدستورية والتشريعات التي تحدد ضوابط استخدام البيانات الشخصية.

وتختلف المعايير التي تحدد مدى الحماية الدستورية للبيانات الشخصية من بلد لآخر، وتعتمد على عدة عوامل بما في ذلك النظام السياسي والقانوني والتشريعات الخاصة بالخصوصية والبيانات الشخصية، وعموماً، تتضمن الحماية الدستورية للبيانات الشخصية حقوقاً أساسية لصاحب البيانات الشخصية، مثل الحق في الخصوصية، والحق في الاطلاع على البيانات، والحق في التصحيح والحذف والحق في الاعتراض على معالجة البيانات الشخصية، كما تتضمن الحماية الدستورية للبيانات الشخصية الضوابط والقيود الخاصة بجمع ومعالجة واستخدام البيانات الشخصية.

سارعت العديد من الدول[٣٩] لإدراج مادة تتعلق بحماية البيانات الشخصية في دساتيرها، باعتباره حق دستوري وأساسي للفرد، مثله مثل أي حق آخر، ومن الدول

---

[٣٩] نصت الفقرة الثانية من المادة (٣٢) من دستور تايلاند: "لا يجوز السماح بأي عمل ينتهك أو يؤثر على حق أي شخص بموجب الفقرة الأولى، باستغلال المعلومات الشخصية بأي طريقة كانت، إلا بموجب حكم في القانون يتم سنه فقط في حدود ضرورة المصلحة العامة". فيما نصت المادة (١٥) من دستور كولومبيا: "لجميع الأفراد الحق في الخصوصية الشخصية والعائلية والسمعة الطيبة، وعلى الدولة احترامهم وجعل الآخرين يحترمونهم. وبالمثل، يحق للأفراد معرفة وتحديث وتصحيح المعلومات التي يتم جمعها عنهم في بنوك البيانات وفي سجلات الكيانات العامة والخاصة. تُحترم الحرية والضمانات الأخرى التي أقرها الدستور في جمع البيانات ومعالجتها وتداولها". كذلك نصت المادة (٣٥) من دستور ألبانيا: "١- لا يجوز إلزام أي شخص بنشر البيانات المتعلقة بشخصه، إلا في الحالات التي يقتضيها القانون. ٢- يتم جمع واستخدام ونشر البيانات المتعلقة بشخص ما بموافقته، باستثناء الحالات التي ينص عليها القانون. ٣- لكل فرد الحق في التعرف على البيانات التي يتم جمعها عنه، باستثناء الحالات التي ينص عليها القانون. ٤- لكل شخص الحق في طلب تصحيح أو شطب البيانات أو البيانات غير الصحيحة أو غير الكاملة التي تم جمعها في انتهاك للقانون". كذلك نصت المادة (٤٢) من دستور صربيا: "يجب ضمان حماية البيانات الشخصية، ينظم القانون جمع البيانات الشخصية وحفظها ومعالجتها واستخدامها حظر استخدام البيانات الشخصية لأي غرض آخر تم جمعه من أجله ويعاقب عليه وفقًا للقانون، ما لم يكن ذلك ضروريًا لإجراء إجراءات جنائية أو حماية سلامة جمهورية صربيا، بالطريقة المنصوص عليها في القانون، لكل فرد الحق في اطلاعه على البيانات الشخصية التي يتم جمعها عنه، وفقًا للقانون، والحق في الحماية القضائية في حالة الإساءة إليها". بالإضافة إلى دستور سلوفاكيا؛ حيث نصت الفقرة ٣ من المادة (١٩) منه: " كل شخص الحق في الحماية من عمليات جمع البيانات الشخصية أو نشرها أو إساءة استخدامها بشكل غير مصرح به". وأيضاً نصت الفقرة ١ من المادة (٢٢) من الدستور السابق: "خصوصية الخطابات وسرية الرسائل البريدية وغيرها من الوثائق المكتوبة وحماية البيانات الشخصية مضمونة". كذلك نصت الفقرة ٣، ٤، ٥، ٦، ٧ ،٨ من دستور أذربيجان: "٣- يحظر جمع أو تخزين أو استخدام أو نشر معلومات عن الحياة الخاصة لأي شخص دون موافقته. لا يجوز متابعة أي شخص أو تصويره أو تسجيله أو إخضاعه لأية أعمال أخرى مماثلة دون علمه أو على الرغم من عدم موافقته، إلا في الحالات التي ينص عليها القانون. ٤- تضمن الدولة حق الجميع في الحفاظ على سرية مراسلاتهم ومحادثاتهم الهاتفية والمعلومات

التي سارعت ونظمت نوع من الحماية الدستورية للبيانات الشخصية في دساتيرها وقوانينها الأساسية، اسبانيا، تركيا، سويسرا، روسيا البرازيل، المكسيك، الجزائر، تونس، مصر، وسنكتفي بهذه النماذج لتغطية الحماية الدستورية للبيانات الشخصية.

نصت الفقرة الرابعة من المادة الثامنة عشر من دستور اسبانيا على أن: "يقيد القانون استخدام معالجة البيانات من أجل ضمان الشرف والخصوصية الشخصية والعائلية للمواطنين والممارسة الكاملة لحقوقهم"[٤٠].

كما نصت المادة العشرون من دستور تركيا أنه: "لكل فرد الحق في طلب حماية بياناته الشخصية، ويشمل هذا الحق إبلاغه، والوصول إلى بياناته الشخصية وطلب تصحيحها وحذفها، وإبلاغه بما إذا كانت تُستخدم بما يتماشى مع الأهداف المتوخاة، كما لا يمكن معالجة البيانات الشخصية إلا في الحالات التي ينص عليها القانون أو بموافقة صريحة من الشخص، ويجب وضع المبادئ والإجراءات المتعلقة بحماية البيانات الشخصية في القانون"[٤١].

كما نصت الفقرة الثانية من المادة الثالثة عشر من دستور سويسرا: "لكل شخص الحق في الحماية من إساءة استخدام بياناته الشخصية"[٤٢].

المرسلة بالبريد أو التلغراف أو غيرهما من وسائل الاتصال. قد يتم تقييد هذا الحق، على النحو المحدد في التشريع، لمنع الجريمة أو لاكتشاف الحقائق الحقيقية عند التحقيق في قضية جنائية. ٥- قد يصبح كل شخص على دراية بالمواد التي تم جمعها فيما يتعلق به أو بها إلا في الحالات التي ينص عليها القانون. لكل شخص الحق في المطالبة بتصحيح أو حذف المعلومات التي تم جمعها بخصوصه، والتي لا تتوافق مع الحقيقة أو غير كاملة أو تم جمعها من خلال انتهاك أحكام القانون، وفي ذات السياق نصت المادة (١٠) من دستور فنلندا: "الحق في الخصوصية: الحياة الخاصة للجميع، وشرف وحرمة المنزل مكفولة. بنص القانون على أحكام أكثر تفصيلاً بشأن حماية البيانات الشخصية".

[٤٠] الفقرة الرابعة من المادة الثامنة عشر من دستور أسبانيا.

[٤١] المادة عشرون من دستور تركيا.

[٤٢] الفقرة الثانية من المادة الثالثة عشر من دستور سويسرا.

وأيضاً نصت الفقرة الأولى من المادة الرابعة والعشرون من دستور روسيا على: "لا يُسمح بجمع وحفظ واستخدام ونشر المعلومات المتعلقة بالحياة الخاصة لأي شخص دون موافقته"[٤٣].

كذلك نصت المادة السادسة عشر من دستور المكسيك على أن: "كل شخص الحق في التمتع بحماية بياناته الشخصية والوصول إلى هذه البيانات وتصحيحها وإلغائها. ولكل شخص الحق في الاعتراض على إفشاء بياناته، وفق القانون".

وعلى الرغم من الحماية التي تفرضها الدساتير والقوانين للبيانات الشخصية والحق في الخصوصية؛ إلا أنه يسمح في بعض الأحيان بالاطلاع على تلك البيانات متى توفرت ضرورة تستدعي ذلك، لا سيما إذا تعلقت هذه الضرورة بالمصلحة العامة والأمن القومي[٤٤]، وهذا ما نص عليه قانون حماية البيانات الشخصية العماني في المادة الثالثة منه بقوله: "لا تسري أحكام هذا القانون على معالجة البيانات الشخصية التي تتم في الأحوال الآتية:

أ- حماية الأمن الوطني، أو المصلحة العامة.

ب-تنفيذ وحدات الجهاز الإداري للدولة وغيرها من الأشخاص الاعتبارية العامة للاختصاصات المقررة لها قانوناً.

ج- تنفيذ التزام قانوني ملقى على عاتق المتحكم بموجب أي قانون أو حكم أو قرار من المحكمة.

د-حماية المصالح الاقتصادية، والمالية للدولة.

هـ-حماية مصلحة حيوية لصاحب البيانات الشخصية.

و-كشف أو منع أي جريمة جزائية بناء على طلب رسمي مكتوب من جهات التحقيق.

ز- تنفيذ عقد يكون صاحب البيانات الشخصية طرفاً فيه.

---

[٤٣] الفقرة الأولى من المادة الرابعة والعشرون من دستور روسيا.

[٤٤] المادة السادسة عشر من دستور المكسيك.

ح- إذا كانت المعالجة في إطار شخصي، أو أسري.

ط- أغراض البحوث التاريخية أو الإحصائية أو العلمية أو الأدبية أو الاقتصادية، وذلك من قبل الجهات المصرح لها القيام بهذه الأعمال، شريطة عدم استخدام أي دلالة أو إشارة تتعلق بصاحب البيانات الشخصية فيما تنشره من بحوث وإحصائيات، لضمان عدم نسب البيانات الشخصية إلى شخص طبيعي معرف، أو قابل للتعريف.

ي- إذا كانت البيانات متاحة للجمهور وبما لا يخالف أحكام هذا القانون"[٤٥].

وفي الجزائر نصت المادة السابعة والأربعين من الدستور على أن: "حماية الأفراد عند التعامل مع البيانات الشخصية حق أساسي"[٤٦].

وفي الجانب الآخر المنظم السعودي والعُماني لم يدرجا مادة تتعلق بحماية البيانات الشخصية في الدستور، وإن أوردا نصوصاً لحماية الخصوصية أشرنا إليها آنفاً.

ويرى الباحثون ضرورة إدراج مادة تتعلق بحماية البيانات الشخصية في الدستور؛ بهدف حماية الخدمات الإلكترونية القائمة على البيانات الشخصية، علاوة على أن وجود مثل هذا النص سيعطي لها حماية خاصة، ويلزم المشرع العادي بوجوب اتساق القوانين والأنظمة الأدنى بحماية البيانات الشخصية مع الدستور، بالإضافة إلى أنه سيعزز من ثقة الأفراد وذلك بالتعامل مع الخدمات الإلكترونية التي يقدمها القطاع العام والخاص، دون خوف أو تردد.

---

[٤٥] المادة الثالثة من قانون حماية البيانات الشخصية العماني، مصدر سابق.

[٤٦] المادة السابعة والأربعين من دستور الجزائر.

المبحث الثالث

الحماية الجنائية للبيانات الشخصية

تتعلق الحماية الجنائية للبيانات الشخصية بالتشريعات واللوائح التي تنص على السلوكيات التي تعد مخالفة لقانون حماية البيانات الشخصية، علاوة على العقوبات والجزاءات التي يمكن فرضها على الأفراد أو المؤسسات التي تنتهك خصوصية الأفراد، وتخترق أو تستخدم البيانات الشخصية لهم بشكل غير مشروع، وتهدف الحماية الجنائية للبيانات الشخصية إلى فرض عقوبات؛ بهدف التأكيد على أن المعلومات الشخصية تحصل على الحماية اللازمة من الاستخدام غير المشروع أو السرقة أو الاستخدام الخاطئ أو الاحتيال.

وتتضمن الحماية الجنائية للبيانات الشخصية عدة أمور من بينها:

١. الجزاءات والعقوبات القانونية التي يمكن فرضها على المخالفين والجهات التي تقوم بجمع أو معالجة أو نشر البيانات الشخصية بطرق غير قانونية.
٢. إجراءات الإبلاغ والتنبيهات المطلوبة من الجهات التي تجمع البيانات الشخصية عند وقوع أي انتهاكات للحماية الجنائية للبيانات الشخصية.
٣. التعاون بين الحكومات والشركات والمؤسسات المختلفة لتحقيق الحماية الجنائية للبيانات الشخصية والحد من حوادث الاختراق والتجسس والاحتيال.
٤. وضع إطار تشريعي مناسب يحمي الأفراد والشركات والحكومات من التعرض لأي مخاطر أو تهديدات بشأن الحفاظ على خصوصية البيانات الشخصية.

إن محل الحماية الجنائية للبيانات الشخصية يتمثل في نشاط معالجة البيانات الشخصية وهو وفق النظام السعودي لحماية البيانات الشخصية: "أي عملية مُعالجة لبيانات شخصية تتعلق بالأفراد تتم في المملكة بأي وسيلة كانت، بما في ذلك معالجة البيانات الشخصية المتعلقة بالأفراد المقيمين في المملكة بأي وسيلة كانت من أي جهة خارج المملكة. ويشمل ذلك بيانات المتوفى إذا كانت ستؤدي إلى معرفته أو معرفة أحد أفراد أُسرته على وجه التحديد، ويُستثنى من نطاق تطبيق النظام، قيام الفرد بمعالجة البيانات الشخصية لأغراض لا تتجاوز الاستخدام الشخصي أو

العائلي، ما دام أنه لم ينشرها أو يفصح عنها للغير، وتحدد اللوائح المقصود بالاستخدام الشخصي والعائلي المنصوص عليهما في هذه الفقرة"[٤٧].

وتتعدد وسائل الاعتداء على البيانات الشخصية ويمكن ردها إلى الابتزاز، القرصنة الاختراق، التهكير، انتحال الشخصية، الاحتيال الإلكتروني.

وقد عالج المنظم الأوروبي حماية البيانات الشخصية بإعطاء صلاحية لدول الاتحاد الأوروبي لسن عقوبات للأفعال والسلوكيات التي تشكل انتهاكاً على البيانات الشخصية، كما نوه على ضرورة أن تكون العقوبات فعالة ومناسبة ورادعة، وهذا ما تطرقت له المادة (٨٤)[٤٨] من النظام الأوروبي لحماية البيانات الشخصية، بينما نصت المادة (٨٣) على إيقاع غرامات إدارية على المخالفين لأحكام المواد (١٢ – ٢٢) من القانون، والتي تتعلق بحقوق أصحاب البيانات الشخصية أو نقل البيانات الشخصية إلى بلد ثالث ليس عضواً في النظام الأوروبي، وتصل الغرامة ٢٠,٠٠٠,٠٠٠ يورو أو استقطاع نسبة ٤% من إجمالي قيمة التداول السنوية في السنة المالية السابقة في حالة التعهد، أيهما أعلى[٤٩].

وقبل صدور نظام حماية البيانات الشخصية السعودي؛ ظهرت عدة انتهاكات تتمثل بالحصول على بيانات الأفراد، واستخدامها بطريقة غير نظامية، وكانت تعالج مثل هذه الحالات في إطار قوانين جرائم المعلوماتية والقوانين الجزائية، وعلى سبيل المثال لا الحصر هناك قضية تتلخص وقائعها بأن المدعي العام وجه اتهام على المدعى عليه لقيامه بابتزاز فتاة وذلك بنشر صورها حيث إن المدعى عليه يعمل في إحدى مكاتب السفريات، وبسبب طبيعة عمله وكونه مطلع على معلومات المسافرين بما في ذلك أرقام تليفونات العملاء، حيث إنه اتصل على الفتاة وعرض عليها رغبته في

---

[٤٧] المادة الثانية من نظام حماية البيانات الشخصية السعودي مصدر سابق.

[48] Art. 84 GDPRPenalties Member States shall lay down the rules on other penalties applicable to infringements of this Regulation for infringements which are not subject to administrative fines pursuant to Article 83, and shall take all measures necessary to ensure that they are implemented. 2Such penalties shall be effective, proportionate, and dissuasive.

[49] Art. 83 GDPR General conditions for imposing administrative fines.

الزواج منها، وبعد أن غرر بها بدأ في مساومتها بالخروج معه، وإلا سينشر صورها؛ فقامت بالخروج معه، فتم القبض عليه، واتضح أن المدعى عليه تحدث مع أكثر من ٨٠ فتاة، وكان فحوى الرسائل ما بين رسائل متعلقة بحجوزات السفر إلى رسائل فعل الفاحشة والابتزاز، وصدر الحكم بسجنه سنتان وأربعة أشهر وجلده مائتان جلده[٥٠].

وبعد صدور قانون حماية البيانات الشخصية، جرم المنظم السعودي أي سلوك يؤدي إلى الافصاح عن بيانات شخصية تخص أي شخص أو نشرها، والافصاح والنشر كما وردا في نظام حماية البيانات الشخصية السعودي هما: "تمكين أي شخص –عدا جهة التحكم– من الحصول على البيانات الشخصية أو استعمالها أو الاطلاع عليها بأي وسيلة ولأي غرض"، أما النشر فهو: "بث أي من البيانات الشخصية عبر وسيلة نشر مقروءة أو مسموعة أو مرئية، أو إتاحتها".

مع عدم الإخلال بأي عقوبة أشد منصوص عليها في نظام آخر، تكون عقوبة ارتكاب المخالفات الآتية، وفقاً لما دون أمامها:

وقد نصت المادة (٣٥) الفقرة (أ) من قانون حماية البيانات الشخصية على عنصرين للركن المادي هما: كل من يفصح عن بيانات حساسة أو ينشر بيانات حساسة ومفهوم البيانات الحساسة نصت عليه وعرفته المادة الأولى من نظام حماية البيانات الشخصية السعودي بقولها: "كل بيان شخصي يتضمن الإشارة إلى أصل الفرد العرقي أو أصله القبلي، أو معتقده الديني أو الفكري أو السياسي، أو يدل على عضويته في جمعيات أو مؤسسات أهلية، وكذلك البيانات الجنائية والأمنية، أو بيانات السمات الحيوية التي تحدد الهوية، أو البيانات الوراثية، أو البيانات الائتمانية، أو البيانات الصحية، وبيانات تحديد الموقع، والبيانات التي تدل على أن الفرد مجهول الأبوين أو أحدهم".

---

[٥٠] حكم المحكمة الجزائية الصادر في تاريخ ١٤٣٤/٥/٢٨هـ رقم الصك ٣٤٢٢٦٣٦٣، مجموعة الأحكام القضائية لعام ١٤٣٤هـ، المجلد الرابع والعشرون، ص١٣٩ وما بعدها.

وقد عاقب المشرع كل من يخالف المادة (٣٥) الفقرة (أ) من نظام حماية البيانات الشخصية السعودي 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، أما الركن المعنوي أو القصد الجنائي الذي تطلبه المشرع السعودي لتوقيع العقاب هو قصد الأضرار بصاحب البيانات أو مجرد تحقيق منفعة شخصية لمرتكب الجريمة، ويتضح من النص أن هذه الجريمة جريمة عمدية، لا يكفي لتوفر ركنها المعنوي مجرد الإهمال وعدم الاحتراز.

كما جرم المنظم السعودي أي سلوك يؤدي إلى التعدي على بيانات شخص خارج المملكة حسب المادة (٢٩) من النظام التي جاء نصها: "فيما عدا حالات الضرورة القصوى للمحافظة على حياة صاحب البيانات خارج المملكة أو مصالحه الحيوية أو الوقاية من عدوى مرضية أو فحصها أو معالجتها، لا يجوز لجهة التحكم نقل البيانات الشخصية 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، وذلك بعد أن تتوافر الشروط اللازمة... "، فعناصر الركن المادي وفق الفقرة (ب) من المادة (٢٩) تتمثل في نقل البيانات الشخصية خارج المملكة أو الافصاح عنها لجهة خارج المملكة مالم يكن ذلك لحالة ضرورة قصوى أو تنفيذ لاتفاقية المملكة طرفاً فيها أو لخدمة مصالح المملكة أو لأي غرض مشروع تنص عليه اللوائح حسبما ورد في المادة التاسعة والعشرون من النظام، وقد جاءت العقوبة لمخالفة الفقرة (ب)السجن مدة لا تزيد على (سنة) وبغرامة لا تزيد على (مليون) ريال، أو بإحدى هاتين العقوبتين.

كما حدد المنظم الجهة التي لها حق التحقيق في هذه السلوكيات التي وردت في المادة (٣٥) بقوله: "تختص النيابة العامة بمهمة التحقيق، والادعاء أمام المحكمة المختصة عن المخالفات المنصوص عليها في هذه المادة".

علاوة على ذلك بين المنظم في ذات المادة كيفية محاكمة من يخالف المادة (٣٥) من النظام بقوله: "تتولى المحكمة المختصة النظر في الدعاوى الناشئة من تطبيق

هذه المادة وإيقاع العقوبات المقررة"، وأعطى المنظم المحكمة المختصة حق تشديد عقوبة الغرامة في حالة العود بقوله: "يجوز للمحكمة المختصة مضاعفة عقوبة الغرامة في حالة العود حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد".

وأورد المنظم السعودي نص احترازي لمعالجة وتجريم كل السلوكيات التي لم يرد في شأنها نص خاص بالتجريم في المادة (٣٥)، وذلك في المادة (٣٦) من النظام، والتي جاء نصها: "دون إخلال بأيِّ عقوبة أشد منصوص عليها في نظام آخر؛ تُعاقَب بالإنذار أو بغرامة لا تزيد على (خمسة ملايين) ريال، كلُّ شخصية ذات صفة طبيعية أو اعتبارية خاصة –مشمولة بأحكام النظام– خالفت أيًّا من أحكام النظام أو اللوائح. وتجوز مضاعفة عقوبة الغرامة في حالة تكرار المخالفة حتى لو ترتب عليها تجاوز الحد الأقصى لها على ألا تتجاوز ضعف هذا الحد".

تكوّن بقرار من رئيس الجهة المختصة، لجنة (أو أكثر) لا يقل عدد أعضائها عن (ثلاثة)، ويسمى أحدهم رئيساً، ويكون من بينهم مستشار شرعي أو نظامي؛ تتولى النظر في المخالفات، وإيقاع عقوبة الإنذار أو الغرامة المنصوص عليها في الفقرة (١) من هذه المادة، وذلك بحسب نوع المخالفة المرتكبة وجسامتها ومدى تأثيرها، على أن يعتمد قرار اللجنة رئيس الجهة المختصة أو من يفوضه بذلك، ويصدر رئيس الجهة المختصة –بقرار منه– قواعد عمل اللجنة، وتحدد فيها مكافآت أعضائها.

يحق لمن صدر ضده قرار من اللجنة المنصوص عليها في الفقرة (٢) من هذه المادة التظلم منه أمام المحكمة المختصة.

كما يعاقب المشرع العماني حسب المادة الخامسة والعشرون من قانون حماية البيانات الشخصية كل من يخالف المادة الرابعة عشر منه بغرامة لا تقل عن (٥٠٠) خمسمائة ريال عماني، ولا تزيد على (٢٠٠٠) ألفي ريال عماني، والعقوبة الواردة في هذه المادة توقع على المتحكم في حالة إخلاله بمجموعة من الواجبات التي ألقاها المشرع على عاتقه وأوردها في المادة الرابعة عشر ويعطي الإخلال بهذه الواجبات صاحب البيانات حق المطالبة بمعاقبة المتحكم وتتمثل هذه الواجبات في الآتي:

"يلتزم المتحكم قبل البدء في معالجة أي بيانات شخصية أن يخطر صاحب البيانات الشخصية كتابة بما يأتي:

أ- بيانات المتحكم، والمعالج.

ب-ببيانات التواصل مع مسؤول حماية البيانات الشخصية.

ج- الغرض من معالجة البيانات الشخصية، والمصدر الذي جمعت منه.

د- الوصف الشامل والدقيق للمعالجة وإجراءاتها، ودرجات الإفصاح عن البيانات الشخصية.

هـ-حقوق صاحب البيانات الشخصية بما في ذلك حق الوصول إلى البيانات، وتصحيحها، ونقلها، وتحديثها.

و- أي معلومات أخرى قد تكون ضرورية لاستيفاء شروط المعالجة".

ويعاقب المشرع العماني حسب المادة السادسة والعشرون المتحكم أو المعالج بغرامة لا تقل عن (١٠٠٠) ألف ريال عماني، ولا تزيد على (٥٠٠٠) خمسة آلاف ريال عماني، عند مخالفة أي منهما للمواد (١٥)، (١٦)، (١٧)، (١٨)، (٢٠)، (٢٢) من قانون حماية البيانات الشخصية، وهذه المواد ترتب بعض الالتزامات على المتحكم والمعالج، وقد تمت مناقشة هذه الالتزامات في المباحث الفائتة.

كما عاقب المشرع العماني بغرامة لا تقل عن (٥٠٠٠) خمسة آلاف ريال عماني، ولا تزيد على (١٠٠٠٠) عشرة آلاف ريال عماني، كل من يخالف أحكام المادة (١٣) بمخالفة إجراءات وضوابط المتحكم.

ويعاقب المشرع العماني حسب المادة الثامنة والعشرون، بغرامة لا تقل عن (١٥٠٠٠) خمسة عشر ألف ريال عماني، ولا تزيد على (٢٠٠٠٠) عشرين ألف ريال عماني، كل من يخالف أحكام المواد (٥)، (٦)، (١٩)، (٢١) من حماية البيانات الشخصية.

والمادة الخامسة المعاقب بمخالفتها تنص على أن: "تحظر معالجة البيانات الشخصية التي تتعلق بالبيانات الجينية أو البيانات الحيوية أو البيانات الصحية أو الأصول العرقية أو الحياة الجنسية أو الآراء السياسية أو الدينية أو المعتقدات أو الإدانة الجزائية أو المتعلقة بتدابير أمنية إلا بعد الحصول على تصريح بذلك من الوزارة، وفقاً للضوابط والإجراءات التي تحددها اللائحة" فاذا تمت المعالجة للبيانات الواردة في هذه المادة قبل الحصول على التصريح تطبق العقوبة التي نصت عليها المادة الثامنة والعشرون."

أما المادة السادسة فتحظر معالجة البيانات الشخصية للطفل إلا بموافقة ولي أمره، ما لم تكن تلك المعالجة لمصلحة الطفل الفضلى، وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة.

وفي هذا السياق فقد عاقبت هيئة حماية البيانات الشخصية في بريطانيا شركة تك توك؛ لمخالفتها قانون حماية البيانات الشخصية البريطاني في قضية تتلخص وقائعها في الآتي:

More than one million UK children under 13 are estimated by the ICO to be on TikTok in 2020, contrary to its terms of service. Personal data belonging to children under 13 was used without parental consent.

TikTok "did not do enough" to check who was using their platform and take sufficient action to remove the underage children that were.

The Information Commissioner's Office (ICO) has issued a £12,700,000 fine to TikTok Information Technologies UK Limited and TikTok Inc (TikTok) for a number of breaches of data protection law, including failing to use children's personal data lawfully.

The ICO estimates that TikTok allowed up to 1.4 million UK children under 13 to use its platform in 2020, despite its own rules not allowing children that age to create an account.

UK data protection law says that organizations that use personal data when offering information society services to children under 13 must have consent from their parents or carers.

TikTok failed to do that, even though it ought to have been aware that those under 13s were using its platform. TikTok also failed to carry out adequate checks to identify and remove underage children from its platform. The ICO investigation found that a concern was raised internally with some senior employees about children under 13 using the platform and not being removed. In the ICO's view, TikTok did not respond.

أما المادة التاسعة عشر فتتحدث عن التزام المتحكم بالإبلاغ في حالة اختراق البيانات الشخصية ونصها: "يلتزم المتحكم، عند حدوث اختراق للبيانات الشخصية، يؤدي إلى تدميرها أو تغييرها أو الإفصاح عنها أو الوصول إليها أو معالجتها بصورة غير قانونية، بإبلاغ الوزارة وصاحب البيانات الشخصية عن الاختراق؛ وذلك وفقا للضوابط والإجراءات التي تحددها اللائحة".

وتلزم المادة الحادية والعشرين المتحكم بضمان سرية البيانات الشخصية، وجاء نصها: "يلتزم المتحكم بضمان سرية البيانات الشخصية، وعدم نشرها إلا بموافقة مسبقة من صاحب البيانات الشخصية، وذلك على النحو الذي تحدده اللائحة."

كما عاقب المشرع العماني في المادة التاسعة والعشرون بغرامة لا تقل عن (١٠٠٠٠٠) مائة ألف ﷼ عماني، ولا تزيد على (٥٠٠٠٠٠) خمسمائة ألف ﷼ عماني، كل من يخالف أحكام المادة (٢٣) من قانون حماية البيانات الشخصية بنقل البيانات الشخصية المعالجة إلى الخارج والتي جاء نصها: "مع عدم الإخلال بالاختصاصات المقررة لمركز الدفاع الإلكتروني، يجوز للمتحكم نقل البيانات الشخصية، والسماح بتحويلها خارج حدود سلطنة عمان وفقاً للضوابط والإجراءات التي تحددها اللائحة، ويحظر عليه نقل البيانات الشخصية إذا تمت معالجتها بالمخالفة لأحكام هذا القانون، أو كان من شأنها إلحاق ضرر بصاحب البيانات الشخص".

وقد وسع المشرع العماني حسب المادة الثلاثون مظلة التجريم، وجعلها تطال الشخص الاعتباري إضافة للشخص الطبيعي، والتي جاء نصها: "مع عدم الإخلال بالمسؤولية الجزائية للأشخاص الطبيعيين، يعاقب الشخص الاعتباري بغرامة لا تقل عن (٥٠٠٠) خمسة آلاف ﷼ عماني، ولا تزيد على (١٠٠٠٠٠) مائة ألف ﷼ عماني، إذا كانت الجريمة قد ارتكبت باسمه، أو لحسابه من قبل رئيس، أو أحد أعضاء مجلس إدارته، أو مديره، أو أي مسؤول آخر، بموافقته، أو بتستر، أو إهمال جسيم منه".

علاوة على عقوبة الغرامة التي نص عليها المشرع العماني في عدد من مواد قانون حماية البيانات الشخصية؛ فقد أورد في المادية الحادية والثلاثين عقوبة المصادرة لأدوات ارتكاب الجريمة، وهي عقوبة جوازية للمحكمة، وتنص هذه المادة على: "يجوز للمحكمة المختصة في نطاق تطبيق أحكام هذا القانون أن تحكم، بالإضافة إلى الغرامة، بمصادرة الأدوات التي استعملت لارتكاب الجريمة"، كما توج المشرع

العماني ضماناته لحماية البيانات الشخصية بإعطاء الوزارة المختصة حق توقيع جزاءات ادارية اضافة للعقوبة الجزائية التي أوقعتها المحكمة وقد جاء النص: "مع عدم الإخلال بالعقوبات المنصوص عليها في هذا القانون، يجوز للوزارة فرض جزاءات إدارية على المخالفات التي يتم ارتكابها بالمخالفة لأحكام هذا القانون أو اللائحة أو القرارات الصادرة تنفيذا له، على ألا تزيد الغرامة الإدارية على (٢٠٠٠) ألفي ريال عماني".

الخاتمـــة

أولاً- النتائج:

١- تضمن الدستوران العماني والسعودي نصوص لحماية الحق في الخصوصية ولكنهما لم يتضمنا نصوص عن حماية البيانات الشخصية، والسبب في تقديري أن قوانين حماية البيانات الشخصية في سلطنة عمان والمملكة العربية السعودية أحدث من الدساتير.

٢- أن قوانين حماية البيانات ظهرت في العديد من البلدان منذ أكثر من أربعين عاماً، ولكن هذه القوانين أصبحت ذات أهمية متزايدة في الوقت الراهن بسبب ازدياد تقاسم البيانات، وجمعها بواسطة الهيئات والمؤسسات والشركات.

٣- أجمعت التشريعات على ضرورة الموافقة الصريحة لصاحب البيانات الشخصية قبل الجمع والمعالجة.

٤- يعطي قانون حماية البيانات الشخصية العُماني سلطات واسعة لوزارة الاتصالات بإلزام المتحكم والمعالج بالتعاون معها، وتقديم ما تطلبه من بيانات ومستندات تراها لازمة لممارسة اختصاصها.

٥- قبل صدور قوانين حماية البيانات الشخصية، كانت الدساتير تحمي بيانات الاشخاص من خلال النصوص الخاصة بحماية الحق في الخصوصية أما القوانين فكانت تحمي البيانات الشخصية من خلال قواعد القانون الجزائي العامة وقوانين جرائم المعلوماتية.

٦- عمدت قوانين حماية البيانات الشخصية في سلطنة عُمان والمملكة العربية السعودية على تشديد عقوبة الغرامة لجعلها عقوبة رادعة.

٧- أن تقاسم البيانات الشخصية أضحى أمر منتشر على نحو متزايد في كل مكان دون استثناء بحكم استعمال المجتمعات للإنترنت، وتحميل التطبيقات المتعددة بغرض الاستفادة من الخدمات.

٨- تقاسم البيانات الشخصية لا يعود بالفائدة على المستخدمين فحسب، بل أيضاً على الشركات والمؤسسات والكيانات الجامعة للبيانات الشخصية.

٩- جمع البيانات الشخصية لا يخلو من المخاطر، لأن المعلومات الشخصية تكشف الكثير عن أصحابها، وعن أفكارهم، وحياتهم الخاصة.

ثانياً- التوصيات:

١- ضرورة اضافة مادة في الدستور السعودي والعُماني لحماية البيانات الشخصية.

٢- توعية المجتمع بأهمية البيانات الشخصية وبيان حقوقه وواجباته وفق قوانين حماية البيانات الشخصية، وذلك عبر الوسائل المرئية والمسموعة والمقرؤة.

٣- ضرورة ايجاد آليات ووسائل بهدف التأكد من أن معالجة البيانات الشخصية تتم في إطار الشفافية والأمانة، واحترام كرامة الإنسان.

المراجـــع

أولاً- المعاجم:

- الصحاح تاج اللغة وصحاح العربية، أبو نصر إسماعيل بن حماد الجوهري الفارابي(المتوفى:٣٩٣هـ)، تحقيق: أحمد عبد الغفور عطار، دار العلم للملايين، بيروت، الطبعة: الرابعة ١٤٠٧هـ -١٩٨٧م.
- معجم البيانات والذكاء الاصطناعي، الصادر من الهيئة السعودية للبيانات والذكاء الاصطناعي، الطبعة الأولى، ٢٠٢٢م.

ثانياً- البحوث الأكاديمية والرسائل العلمية:

- محمد السعيد رشدي، المؤتمر العلمي الثاني: الإعلام والقانون بحث بعنوان الإنترنت والجوانب القانونية لنظم المعلومات، كلية الحقوق، جامعة حلوان، ١٩٩٩م.
- -ورقة بعنون الإطار الدستوري للحق في النسيان مقدمة من الدكتور خليفة ثامر الحميدة، كلية الحقوق جامعة الكويت، مجلة الحقوق للبحوث القانونية والاقتصادية جامعة الكويت ٢٠١٨م.
- -الحماية الجنائية لبيانات الأفراد الشخصية المعالجة إلكترونيا "دراسة في ضوء التشريعات الجنائية المقارنة واللائحة التنظيمية الصادرة عن البرلمان الأوروبي ورقة علمية مقدمة من د. ميادة مصطفى محمد المحروقي المجلة القانونية جامعة القاهرة فرع الخرطوم ٢٠٢٣م (مجلة متخصصة في الدراسات والبحوث القانونية).
- -ورقة منشورة بعنوان دروس مقتبسة من القانون العام لحماية المعطيات الشخصية للاتحاد الاوربي على موقع اكسس ناو يانير ٢٠١٨.
- مقال بعنوان عرضة للكشف والاستغلال: حماية البيانات في منطقة الشرق الأوسط وشمال إفريقيا يناير ٢٠٢١) أكسس ناو.

ثالثاً- الدساتير والقوانين:

- دستور اسبانيا. لسنة ١٩٧٨ المعدل ٢٠١١م.
- دستور سويسرا. لسنة ١٩٩٩ المعدل سنة ٢٠١٤م.
- دستور روسيا ١٩٩٣ المعدل ٢٠١٤م.
- دستور المكسيك لعام ١٩١٧ المعد سنة ٢٠١٥م.
- دستور تركيا. لسنة ١٩٨٢م المعدل ٢٠١٧م.
- دستور الجزائر. لسنة ٢٠٢٠م.
- النظام الاساسي للدولة العُماني لسنة ٢٠٢١م.
- النظام الأساسي للحكم السعودي ١٤١٢هـ.
- القانون الاوربي لحماية البيانات الشخصية ١٩٩٥م.
- قانون الإجراءات الجزائية العماني رقم ٩٩/٩٧
- قانون حماية البيانات الشخصية العُماني لسنة ٢٠٢٢م.
- نظام الاتصالات السعودي١٤٢٢هـ.
- قانون مكافحة جرائم المعلوماتية السعودي لسنة ١٤٢٨هـ.
- نظام الإجراءات الجزائية السعودي ١٤٣٥هـ.
- نظام حماية البيانات السعودي ١٤٤٣هـ.

رابعاً- الأحكام والقرارات القضائية:

- حكم المحكمة الجزائية الصادر في تاريخ ١٤٣٤/٥/٢٨هـ رقم الصك ٣٤٢٢٦٣٦٣، مجموعة الأحكام القضائية لعام ١٤٣٤هـ، المجلد الرابع والعشرون.Remsburg v. Docusearch, Inc., A.2d
- (2003 WL 346260, sup. Ct., N.H.,2003)-
- قضية هيئة البيانات الشخصية البريطانية ضد شركة كلير فيو.
- قضية هيئة حماية البيانات الشخصية في بريطانيا ضد شركة تك توك ٢٠٢٠ .

خامساً- التقارير والروابط والمواقع:

- تقرير لجنة العلوم الاجتماعية والإنسانية، المؤتمر العام لمنظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، الدورة الحادية الأربعون، ٤١ C/73، باريس ٢٠٢١م، البند٨-٢ مشروع التوصية الخاصة بأخلاقيات الذكاء الاصطناعي، مجال العمل بشأن السياسات الخاصة بالبيانات.
- موقع قناة العربية بتاريخ ٢٦ فبرير ٢٠٢١م تحت عنوان البوابة العربية للاخبار التقنية.
- موقع الهيئة البريطانية لحماية البيانات الشخصية ٢٣ مايو ٢٠٢٢.

الرابط:

https://slate.com/technology/2014/05/in-lebanon-apps-let-you-get-someone-else-s-personal-info-with-ease.html.